Quest Journals
Journal of Software Engineering and Simulation
Volume 10 ~ Issue 10 (2024) pp: 61-70
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Cyber Fraud, Causes and Its Effect on Money Deposit Banks

Dr UzohNzekwe E
Madonna University, Nigeria Department of Accountancy

Abstract
The study examined cyber fraud, causes and its effect on money deposit banks (DMB) in Nigeria: a study of Zenith Bank. The main objective is to examine electronic frauds, causes and its challenges in the banking sector. The study is hinged on two hypotheses; 49 branches; sample of 557 staff. Structured questionnaire was used to capture the response of the bank staff and it was analyzed using statistical package for social science version 27 (SPSS). Descriptive statistics and multiple regression were employed in the data analysis. Among the findings were accounting fraud by bank staff, identity theft, money laundering, phishing, pharming, computer virus, lack of oversight function,lack of standards, financial loss, absence of national central control, lack of credible infrastructure, porous internet, lack of national functional database, and inadequate awareness by bank customers were the challenges militating the effort towards curbing the cyber fraud in the banking system in Nigeria. The findings also revealed that cybercrime reduced productivity; vulnerability of banks Information and Communication Technology (ICT) systems and security audit. The study recommends adequate antivirus and antimalware software technology and the use of multi-factor authentication, use of biometrics, automatic logout are the solutions identified to curb cybercrimes in banks. The study concluded that the place of security in the cyber space of banks in Nigeria cannot be oversemphasied, therefore necessary measures should be put in place towards mitigating cybercrime in Zenith Bank. Equally, Zenith Bank should employ stringent measures to monitor staff activities especially in the confidentiality of customer information, cyber security audit should be done on regular basis, sensitization of bank customers, and Multifactor authentication, biometrics and automatic log out, and strong firewall should be adopted by Zenith Bank.

Key words*: Antimalware, Antivirus, Biometrics, Identity Theft, Porous Internet.*

R*eceived 14 Oct., 2024;* ***R****evised 27 Oct., 2024;* ***A****ccepted 29 Oct., 2024 © The author(s) 2024.*
P*ublished with open access at* ***www.questjournas.org***

I. INTRODUCTION

In the contemporary landscape of global finance, the banking industry has become increasingly reliant on digital technologies, ushering in unprecedented levels of efficiency and connectivity (Angels 2022;Almedia e tal, 2022;Adeola e tal, 2022). However, this digitalization has also given rise to a myriad of cybersecurity threats, making financial institutions prime targets for malicious actors seeking unauthorized access, financial gain, or disruption (Oluwaseun e tal 2023, George, George, and Baskar, 2023, Ekakitie-Emonena andAlagba2022).The modern banking system in Nigeria traces its origin to the establishment of the first bank; the Bank of British West Africa (now known as First Bank of Nigeria), in 1892.Financial institutions like banks allow people to save and increase their wealth. Besides, banks also lend money to companies that are willing to expand their operations. Thus, the growth of a country's economy is directly related to the banking sector.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 should take immediate action to prevent these types of incidents from happening.

Cyber security refers to myriad of activities fashioned out with a view to ensuring the protection of personal and organizational data, information and networks from all possible threats whether internally or externally induced (Dapp,Slomka and Hoffmann 2014;David-West 2016). These threats could include unauthorized access and disclosures, misuse of data/information, network hacking and organized attacks in the form of the introduction of malware and similar extraneous viruses. Recently a lot of research has been conducted on cyber security related to banking industry. Fadare, (2023) believed that cyber technology has

brought about a lot of profit to financial institutions and cyber-attack also poses intensive threat to the same institutions, the study recommends that there is need for cyber security audit, cyber security training, cyber security assessment and tightening security. In Nigeria Imran & Sana, (2023) released a risk based cyber security frame work and guidelines for commercial banks in managing cyber security risk. The document is of 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.

Studies have shown that most banks do not reveal the identities of their employees involved in fraudulent activities. They also do not acknowledge that they were complicity in the actions. Instead, they quietly discipline the employees and absolve themselves of any blame. 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. 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, is Zenith Bank, which had over 167,000 unresolved issues as at December 2021. On the other hand, the country's second-largest Bank, GTB, had recorded over 600,000 complaints.

Reports have shown that some bank employers use kid gloves to avoid creating a negative image for the company. In their studyNugraha 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, Okuneye and Taiwo 2018). It is based on the aforementioned background that the study is geared towards assessing the cyber-security policies and techniques used by Guaranty Trust Bank in combating financial fraud in Nigeria.

Internet banking was first introduced to Nigeria in 2003 (Patience, Akpan-Obong Trinh and Aderonke 2023).The term ‘internet banking tends to be used interchangeably with online banking. They refer to a range of banking services via a range of technical platforms and electronic devices, such as the internet, computers, mobile phones, and bank cards (Muhammad and Murtanto 2022; Rahman, Karim and Chowdhury 2021).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 customers. 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 and e-banking, initiatives launched by financial institutions in the country are expected to help narrow the digital divide.

Despite the various advantages of internet banking, 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.

In Nigeria today, most individuals possess mobile phones with internet access and are registered on social media platforms such as Facebook, Twitter, WhatsApp, and so on. These internet based platforms have provided an array of opportunities for individuals to communicate and network with people of diverse cultures,

and also aided local business to grow by providing regional and international markets (Eze, 2021).According to an official report released by the Economic Fraud Forum of Nigeria, the country was ranked 16th globally in cybercrimes. Information flow from Nigeria are been characterized as questionable because of the criminal elements that make it unreliable, inaccurate and untrustworthy (Ogunwale 2020; Onuora e tal 2017). This has more severe implications on the technological and socio-economic development of the country when compared to conventional crimes and as highlighted by Ogunwale(2020), the contribution of the internet to the development of Nigeria has been marred by the evolution of new waves of cybercrimes.

Cybercrime can be defined as a type of criminal activity that involves the unauthorized access and use of people's personal information, through various means (Buchanan, 2016).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, internet banking is preferred to traditional banking.

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 include 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 crimes and thus prevent them from happening in the first place.

II. Literature Review

Routine Activity Theory (RAT)

This research is predicated on RAT, which states that 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' with 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

Empirical Review

Oluwaseun, *e tal* (2023). Studied digital transformation in banking: a review of Nigerian journeyto economic prosperity. The extensive economic ramifications of Nigeria's banking sector's multifaceted digital transformation were examined in this study, emphasizing the function of online platforms, digital payments, blockchain technology, and cryptocurrencies. Additionally, it explores the forces propelling this transformation, such as customer demands for seamless experiences, increased competition from fintech startups, and governmental requirements for greater transparency. The study suggests advancing digital transformation in Nigerian banking, including bolstering cybersecurity spending, updating technology infrastructure, encouraging cooperation with fintech partners, promotion of customer education and ongoing innovation are crucial for long-term success.Victory, Promise, and Mike (2022), investigated the impact of cyber-security on fraud prevention in Nigerian commercial banks. The research collected primary data through interview (WhatsApp video call), administered to the senior employees of the respective commercial banks who are familiar with the subject matter**.** The outcome of the research demonstrated that cloud security statistically enhanced 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), furthermore, 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.Olaniyan, Ekundayo, Oluwadare, and Bamisaye (2021), in their study using primary data covering ten (10) years from

2010 to 2020, discovered that while foreign accounts do not completely enhance 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.

According to Eze(2021), in her study ofchallenges of cybercrime on online banking in Nigeria a review; she maintained that the development of Information and Communication Technology has brought about unimaginable consequences such as criminal activities, spamming, credit card frauds, ATM frauds, phishing, identity theft and other related cybercrimes. In view of this, the paper noted that widespread cybercrime has negative impact on online banking system as it results in huge financial losses, threatens profitability, and tarnishes the image of the country on a global scale, which often dissuades foreign investors from investing in the country. Based on this, the paper concludes that there is need for investors and customers to protect themselves from cyber criminals by adopting simple security tips such as having updated and original anti-virus software to avoid disclosing personal information to third parties. Also, using a very strong password and changing password at intervals, will help to prevent security breaches.

In a related study by Leukfeldt and Holt (2022), using a sample of 37 offender networks to study the problem of cybercrime, opined that different cybercriminals exhibit different types of criminal activity. In that they sometimes engage in specific types of cybercrime, nearly half of the perpetrators 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, ransom ware, and other financial crimes.

Alao (2016), studied the influence of forensic auditing on financial fraud in Nigeria 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 Pvalue 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 Nigerian 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), investigated the influence of fraud on the demise of Nigerian banks. 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 anticorruption 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.

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 discovered 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.

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 brings 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 ofimplementing cyber security in an organization's systems, with an emphasis on the banking sector. Inaddition, the goal of this research is to promote the use of cyber security in order to keep information safe and proper management of the 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 maybe 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. The study 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 Bangladesh 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 multidimensional challenges to adopt IT applications in banking with cybercrime. The paper examined how 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.

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.

Hypotheses

Table 1: There is no composite impact of the types of electronic frauds and the causes of cyber fraud on the effect of cyber fraud on Nigeria banks

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

**Sig<0.05

The result in table 1 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 significant 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 2: There is no relationship between the challenges of curbing cyber fraud and the possible solutions of curbing cyber fraud in Nigeria banks.

Challenges of curbing cyber fraud		Possible solutions of curbing cyber fraud in Nigeria banks		
Kendall's tau_b	Challenges curbing of 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 2 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.

III. 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, 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 the 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.

IV. 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. This is supported by(Eze2021; McSGuire Doling 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 fraudulently. However, in some rare cases in Nigeria, the intention of cyber-criminals is to cause damage to the reputation of the bank by denying internet services to users (Dzomira 2021; Parthiban 2014) and sabotaging data in computer network of organizations.

Othermajor causes of cyber fraud in bank include: lack of oversight function by line managers or senior managers deviations from existing electronic process/controls, 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 inline with(Alao 2016; Badejo e tal 2018; Onodi e tal 2015; Hassan 2012) findings; where 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, 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.

Equally, the study showed that banks are confronted with so many Challenges in curbing the rate of cyber fraud: Among the challenges are 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 were supported by (Dzomira 2021; Oyelakin e tal 2021; Kritzznger and Solms2012) 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.

Finally, 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 (Samuel e tal 2021; Frank and Odunayo2013) 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 study recommended the following possible solutions that could curb cybercrime in the banking industry 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. Improved security of bank customer information and fund by banks through efficient cyber protocol, will enhance customer patr

References

[1] Adeola, O., Adeleye, I., Muhammed, G., Olajubu, B. J., Oji, C., &Ibelegbu, O. (2022). Savings Groups in Nigeria. In Transforming Africa (pp. 193-216): Emerald Publishing Limited

[2] 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.

[3] 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.

[4] Al-alawi, A. I. & Al-Bassam S. (2021). Assessing the factors of cyber security awareness in the banking sector. Arab Gulf Journal of Scientific Research 37(4). 17-32.

[5] Alghazo, J., Kazim, Z., &Latif, G. (2018). Cyber security analysis of internet banking in emerging economy; user and bank perspectives. 4th IEEE international conference on emerging techniques and applied sciences, ICETAS 2017, 2018 – January. PP 1 – 6.

[6] Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI and Ethics, 2(3), 377-387

[7] 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.

[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.

[9] Angeles, I. T. (2022). The moderating effect of digital and financial literacy on the digital financial services and financial behavior of MSMEs. Review of Economics and Finance, 20(20), 505-515.

[10] 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). DOI: 10.22515/shirkah.

[11] Baur-Yazbeck, S., Frickenstein, J. &Medine, D. (2019). Cyber security in financial sector development. African Journal of Emerging Issues. https://ajoeijounals.org>sys

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

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

[14] Chika, O. V., Promise, E., &Werikum, E. V. (2022). Influence of Liquidity and Profitability on Profits Growth of Nigerian Pharmaceutical Firms. GoodwoodAkuntansidan Auditing Reviu, 1(1), 1-13.

[15] 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.

[16] Dapp, T., Slomka, L., AG, D. B., & Hoffmann, R. (2014). Fintech–The digital (r) evolution in the financial sector. Deutsche Bank Research, 11, 1-39.

[17] David-West, O. (2016). The path to digital financial inclusion in Nigeria: Experiences of Firstmonie. Journal of Payments Strategy & Systems, 9(4), 256-273.

[18] 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.

[19] 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).

[20] Ekakitie-Emonena, S., &Alagba, O. S. (2022). Customer relationship marketing & enterprise performance: Empirical evidence from leading banks in South-South Nigeria. Linguistics and Culture Review, 6(S1), 106-120.

[21] Eze Patience A. U, (2021). Challenges of cyber crime on online banking in Nigeria a review. IDOSR Journal of Arts and Management, 6(1), 63-69

[22] 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).

[23] Fatoki J. O (2023). The influence of cyber security on finanacial fraud in the Nigerian banking industry. International Journal of Science and Research Archive 9(2), 503-51.

[24] 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.

[25] George, A. S., George, A. H., &Baskar, T. (2023). Digitally immune systems: building robust defences in the age of cyber threats. Partners Universal International Innovation Journal, 1(4), 155-172.

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

[27] 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.

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

[29] 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

[30] Mcguire, M. and Doling, S. (2013). Cybercrime: a review of the evidence. Home office science publication 10 page 11

[31] Muhammad A., Murtanto T.A, (2022). Bank role in preventing money laundering and cyber security. Technicum Social Sciences Journal, 37, 287-299.

[32] 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.

[33] Ogunwale, H. (2020). The Impact of Cybercrime on Nigeria"s Commercial Banking System. Research Gate. https://www.researchgate.net/pub lication/347388290 20.

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

[35] Onuora, A. C., Uche, D. C., Ogbunude, F. O. and Uwazuruike, F. O. (2017). The Challenges of Cybercrime in Nigeria: An Overview. AIPFU Journal of School of Sciences, 1(2): 6-11

[36] 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

[37] 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.

[38] 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.

[39] 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. ActaScientiarumPolonorum. Oeconomia, 20(1), 49-59.

[40] Oluwaseun A.L, Adekunle A.A, Donald O.D, Ayoola M.A, Adesola A.J, ChibuikeDaraojimba (2023). Digital transformation in banking: a review of Nigerian journey to economic prosperity. International Journal of Advanced Economics, 5(8), 215-238.

[41] Opudu D. O, Ogiriki T. (2022). Digitalization and the challenges for accounting profession in an emerging economy. Management, Accounting and Finance Journal 7(2).

[42] Ottonne A, Melikam. W and Ige O.T (2023). Adoption of Financial technology and performance of deposit money banks in Nigeria. Futurity Economics and Law 3(2), 95-114

[43] 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).

[44] Patience, I., Akpan-Obong, Mai P., Trinh, C. K. &Aderonke, O. (2023). E-Governance as good governance? Evidence from 15 West African countries. Information Technology For Development. 29(2-3). 256-275.

[45] Rahman, A. (2014). Combating money laundering and the future of banking secrecy laws in Malaysia. Journalof Money Laundering Control, 17(2), 219–229. https://doi.org/10.1108/JMLC-09-2013-0036
[46] 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.
[47] Rufus .A, Olubunmi .O, Modupe .A, Ajimbola .A (2022). Cyber security and financial innovation of selected deposit money banks in nigeria. Universal Journal of Accounting and Finance 10(3), 643-652
[48] Samuel O.D, Adedolapo .O, Odunayo .J .A, Abimbola O. A, Sarah K.E (2023). Cyber security risk assessment in banking: methodologies and best practices. Computer Science And IT Research Journal, 4(3) 220-243.
[49] 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.
[50] 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.
[51] Sethi, N. (2021). Cyber security analysis in banking sector. International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS), 04(03), 59-64
[52] 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.
[53] Tendulkar, R. (2013). Cyber-crime, securities markets and systemic risk. CFA Digest, 43(4), 3543.
[54] Victory C.O, Promise E, Mike C.N (2022). Impact of cyber security in fraud prevention in Nigerian commercial banks. JurnalAkuntansi, Keuangan danManajemen, 4(1), 15-27.