International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Research Article)

The influence of cyber security on financial fraud in the Nigerian banking industry

JACOB OBAFEMI FATOKI *

Department of Accounting and Finance Lead-City University Ibadan Nigeria.

International Journal of Science and Research Archive, 2023, 09(02), 503–515

Publication history: Received on 21 June 2023; revised on 28 July 2023; accepted on 30 July 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.9.2.0609

Abstract

The study looked at Financial Institution in Nigeria for how cyber security affects financial fraud in Nigerian banks. The study focused on the following topics: the types of electronic frauds committed in the banking industry, the reasons why cyber fraud occurs in banks, the difficulties in preventing cyber fraud in banks, the impact of cyber fraud on Nigerian banks, and potential solutions for preventing cyber fraud in banks. The two hypotheses that the study is based on. Six Nigeria Banks made up the study's population, which used a survey research design. 557 bank employees were sampled using multistage sampling techniques. The bank staff's responses were gathered using a structured questionnaire, which was then, analyzed using the SPSS statistical package for social science version 27. Descriptive analysis was used to analyze the objectives, and multiple regression and Kendal Tau B were used to test the hypotheses. The study's findings indicated that computer viruses, hacking/cracking, phishing, pharming, and accounting fraud by bank employees were the main types of cyber fraud in the banking system. The causes of cybercrime in banks included a lack of line manager or senior manager oversight on deviations from existing electronic processes or controls, current business pressure to meet set targets, collusion between employees and outside parties, insufficient data encryption, the use of third-party services, and parodying. Similarly, the study's findings showed that the challenges impeding the effort to stop cyber fraud in Nigeria's banking system included a lack of standards and national central control, a lack of infrastructure, the internet's vulnerability, a lack of national functional databases, and inadequate awareness by bank customers. A security audit, antivirus and antimalware software, the use of multi-factor authentication, the use of biometrics, and automatic logout were found to be solutions to cybercrime in banks. The findings also showed that financial loss, decreased productivity, and vulnerability of banks' Information and Communication Technology (ICT) systems and networks were effects of cybercrime on banks in Nigeria. According to the study's findings, banks' cyberspace security cannot be overextended in Nigeria, so necessary precautions should be taken to reduce cybercrime in Nigeria Banks. The study recommended that Nigeria Banks implement stringent measures to monitor staff activities, particularly in the confidentiality of customer information, cyber security audit be performed by financial institution regularly, sensitization of bank customers, and Multi-factor authentication, biometrics and automatic log out, and strong firewall should be adopted by Nigeria Financial Institutions.

Keywords: Nigeria financial institutions; Bank Customers. Cyber Security; Cyber Fraud

1. Introduction

Technology is evolving into one of the most effective tools and methods for fostering innovation, growth, and improving competitiveness and development S. Kamel 2015. The advancement of information and communication technology (ICT) has led to increased innovation, which has improved customer responsiveness and convenience in the banking sector M. Loonam, & D. O' Loughlin, D 2008. Financial institutions have started implementing new technologies as a result of these technological advancements, such as electronic transactions, to help make the most of modern technology L.F. Amboko, & J. Wagoki 2012. The significant financial losses suffered by these businesses globally as a result of cybercrime and more specifically as a result of SWIFT (digital platform) R.N. Acharya, & A. Kagan 2004, according to

* Corresponding author: JACOB OBAFEMI FATOKI

IBM, Cyber Security on the financial sector have been particularly severe in 2019. The study also reveals that these cybercriminals frequently target and attack institutions in the banking sector. This is a result of the hackers' perception that financial institutions, including banks were the most obvious target for their type of criminal activity. Around the world, there have been countless Cyber Security on banks of all sizes. The SWIFT system has been used by numerous hackers to successfully steal money from a number of banks around the world, according to J. Okoth 2019 research. We have seen numerous bank services disrupted by distributed denial-of-service attacks due to the wide variety of sophisticated hacking tools and techniques used in the dark web K. Okiro, & J. Ndungu 2013. As a result of technological advancements and a growing reliance on digital platforms, the Nigerian banking industry has undergone significant change in recent years. Numerous advantages have resulted from this change, including improved financial services accessibility, efficiency, and convenience, but it has also given cybercriminals new ways to take advantage of flaws and defraud people of their money. The Nigerian banking industry and its clients are seriously threatened by financial fraud. Cybercriminals access sensitive financial data without authorization, manipulate transactions, and steal money using a variety of techniques like phishing, identity theft, malware attacks, and social engineering. These fraudulent activities not only result in substantial financial losses for people and businesses, but they also undermine public trust in the banking system. In Nigeria, incidents of cybercrime—including financial fraud—have risen recently. The volume and dollar amount of fraudulent transactions in the banking industry have significantly increased, according to the Nigerian Inter-Bank Settlement System, or NIBSS. According to the Central Bank of Nigeria CBN, banks registered over 91,000 fraud cases in 2020 alone, totaling about 38 billion naira, or US105 million. The Nigerian government and regulators have acknowledged the seriousness of the issue and have taken steps to combat cyber threats in the banking sector in light of these alarming statistics, which highlight the urgent need for effective cyber security measures to combat financial fraud. To enhance the practices of cyber security in financial institutions, the CBN has released guidelines and regulations. Additionally, to investigate and prosecute cybercriminals engaged in financial fraud, the Economic and Financial Crimes Commission EFCC and the Nigeria Deposit Insurance Corporation NDIC collaborated. Despite these efforts, cybercriminals continue to modify their strategies, making ongoing Cyber Security improvements crucial to banking security measures and strategies. For the purpose of spotting holes in the system, enhancing it, and creating strong frameworks to defend against cyber threats, it is essential to comprehend how cyber security affects financial fraud. The aim of this study is to investigate the impact of cyber security on financial fraud in the Nigerian banking industry and to add to the body of knowledge in this field. The objective is to identify the difficulties faced by financial institutions, evaluate the efficacy of current cyber security measures, and offer suggestions for enhancing the security posture of the Nigerian banking sector. The study's ultimate goal is to rebuild customer and stakeholder trust while also fostering a more secure and resilient banking environment. Since the money is no longer just kept in the bank, a bank robbery now involves more than just a physical assault. Cyberspace is a very lucrative place to be in today's world of computers and information networks. Due to an increase in bank fraud, banks must adapt to contemporary e-commerce while defending themselves from cybercrime. To avoid such occurrences, the authorities must take immediate action. According to a report by the American Customer Satisfaction Index, bank customers are having trouble getting paid adequately due to numerous message issues, employee errors, and other mistakes. The safeguarding of digital data and the systems that house it is known as cyber security. Recent years have seen a plethora of studies on cyber security in relation to banking Olubisi, 2015. Fadare, 2015 came to the conclusion that cyber security technology has many advantages for a specific financial institution and that the same institution is also at risk from cyberattacks. The research demonstrates the necessity of cyber security audit, cyber security training, and cyber security.

To assist businesses in managing their cyber security risks, Nigerian Imran Sana published guidelines and a framework in 2013. Regulators and financial institutions have increased their focus on cyber security in the nation as a result of various financial issues that have occurred in the nation in recent years. Because of a lack of resources and training to reduce these risks, banks in the nation are more susceptible to cybercrime (Onodi, Okafor, and Onyali, 2015). As there are risks to the country's financial institutions, there are also risks to the operations of those institutions, including: Doing business with foreigners (theft) dollars; non-receipt/authorization or debiting of communications from multiple account holders; ATM card cloning issues; extortion by armed and unarmed individuals. In the hope of revealing the detrimental effects of financial crime, this paper will provide a deeper understanding of the various identified threats. This will help organizations improve their cyber security strategy and prevent financial loss due to crime.

The purpose of this study is to comprehend the significance of cyber security, investigate financial fraud in the Nigerian banking industry, pinpoint the underlying causes of cyber banking fraud, and identify the factors that contribute to cyber fraud in banking solutions.

Question analysis: What kinds of business transactions are taking place in the banking sector? What are the reasons for internet fraud in the banking sector? What are the difficulties in preventing internet banking fraud? How does cyber fraud impact Nigerian banks? What are the solutions to this problem?

Tests were conducted on the following hypothesis.

- Ho1: The type of electronic fraud and the cyber fraud caused by the bank's exposure to the cyber fraud are unrelated.
- Ho2: There is no connection between issues with online fraud prevention and solutions to issues. Preventing online fraud in banks.

The study on the effect of cyber security on financial fraud in the Nigerian banking sector is important for a number of reasons. Understanding the Threat Landscape The study will give important insights into how the cyber security and financial fraud threat landscape is changing in the Nigerian banking industry. The study can help identify the precise areas that require attention and improvements in terms of security measures by looking at the methods, vulnerabilities, and patterns of cyber-attacks. Limiting Financial Losses Financial fraud in the banking industry causes significant financial losses for people, businesses, and the overall economy. The study can assist in creating efficient strategies and countermeasures to mitigate such losses by looking at how cyber security affects financial fraud. As a result, both the general stability of Nigeria's banking system and the financial interests of both individuals and businesses can be safeguarded. Increasing Customer Confidence Financial fraud reduces customer confidence in the banking system and makes them less likely to use online banking services. Financial institutions can enhance their security procedures, assure customers that online transactions are secure, and rebuild trust by understanding the impact of cyber security on financial fraud. Building customer confidence is essential to the banking industry's success and continued growth in Nigeria. Compliance and Regulatory Framework The study can help regulators, like the Central Bank of Nigeria (CBN), create and enforce effective Cyber Security rules and policies for the banking sector.

2. Literature Review

A result of new technology and an increase in internet usage, Nigerian banks have experienced significant growth and change. People can now use banks and conduct online banking with greater ease as a result. However, it has also made it simpler for criminals to steal money from banks and con people into handing over their cash. Therefore, it is crucial for banks to safeguard both themselves and their clients from these bad actors. When someone deceives people or banks into giving them money or sensitive information that they shouldn't have, that is financial fraud. This can occur in a variety of ways, such as by impersonating another person or deceiving users of social media. It's not just bad because it deprives people and banks of money; it's bad because it undermines public confidence in banks and may prevent economic expansion. In their 2014 article, Hanafizadeh, Behboudi, Koshksaray, and Tabar explained the factors that influence banks' decisions to use the internet for banking as well as the reasons behind those decisions. People's concerns about protecting their money when using the internet for banking are also discussed. People still worry about their money being safe when they use the internet for banking, despite the fact that the banking industry has improved thanks to technology. Simply put, cyber security protects Nigerian banks from internet criminals like a superhero. It employs specialized equipment and methods to safeguard the computers, networks, and data of the banks against loss or damage. Strong passwords, unique computer locks, and instruction in online safety for bank employees are some of these tools. Cyber Security also has a plan to address any problems as soon as they arise and make sure they don't recur.

To stop criminals from stealing money from banks, cyber security acts as a sort of superhero. Important financial data is safeguarded, and it prevents hackers from breaking into the bank's computer systems. It also assists in quickly detecting any suspicious activity. Banks use robust cyber security to ensure that customers' personal information is secure and that thieves cannot steal from them. But when it comes to keeping their money secure and preventing theft, Nigerian banks face some unique challenges. These issues include a lack of effective computer systems, a lack of personnel with the necessary skills to thwart criminal activity, and increasingly inventive ways that criminals are attempting to steal money. In order for everyone to abide by them and take the best precautions to protect the money, the laws and procedures that the banks are supposed to use to protect it need to be strengthened.

It's crucial to comprehend how cyber security can help to safeguard the Nigerian banking sector from individuals stealing money online. This study examines prior research on cyber security and financial fraud. This will allow us to ascertain what deters theft of money and what doesn't. Making better rules and plans to protect Nigerian banks from fraud and cyber security will be made easier with the aid of this information. Cyber-security is the equivalent of installing locks and other security measures on computers, networks, and data to prevent unauthorized individuals from accessing, altering, or destroying them. Cyber Security is crucial in Nigeria, where banks use digital systems for financial transactions. As digital payments and online banking become more common, more hackers attempt to steal money or personal data. To protect people's money and support economic growth, it's critical to keep financial information secure, prevent unauthorized access, and ensure that everything is operating as intended.

2.1. Components of Cyber Security

Comprehensive Cyber Security frameworks consist of several interconnected components that work together to provide robust protection against cyber threats. Key components include:

- Network security is like having locks and alarms on your house to protect it from intruders. It uses different technologies to keep the network safe, just like how your home security system keeps your house safe. It makes sure that only the right people can access the network and that no one can steal or spy on the information being sent.
- Data protection is like keeping your toys safe. It means taking steps to make sure that no one can see, use, or take your toys without permission. This includes putting them in a locked box, keeping them in a safe place, and making sure they are always backed up in case they get lost or broken.
- Access control is like a special lock on a bank that only lets certain people in. It uses things like passwords, fingerprints, and extra security measures to make sure only the right people can get in and use the bank's stuff. It also makes sure that people only have access to what they need and can't do anything they're not supposed to do.
- Incident response is like being a superhero for computers. When something bad happens, like a cyber-attack, we have a plan to quickly figure out what happened and stop it. We use special tools to investigate the problem, fix it, and make sure it doesn't happen again. Acting fast and doing a good job is really important to keep the computer safe and prevent more bad things from happening.

2.2. Important of Cyber Security

It is crucial for the Nigerian banking sector to have robust cyber security measures. To protect people's money and personal information, it is necessary to ensure that all banks have excellent security. It's crucial because bad actors could steal people's money or misuse their personal information if banks don't have adequate security. To protect everyone's money and personal information, it is crucial that banks have strong security. Banks have a ton of vital information about their clients, including financial and personal information. They use unique techniques to protect this information from thieves who might try to steal it. This makes it easier to ensure that nobody can pretend to be someone else or use the money without authorization. By tricking people into disclosing their personal information or stealing money, cybercriminals can be deterred from carrying out nefarious activities online. In addition to using secret codes to protect data when it is sent over the internet, banks use specialized tools to ensure that only the right people have access to their accounts. This makes it much more difficult for criminals to steal money and commit other crimes. It's crucial for banks to maintain their customers' trust. People expect banks to keep their money safe and ensure that neither their information nor their money can be stolen when they deposit their money in a bank. Banks can ensure that their customers feel safe and trust them to handle their money by implementing strong online security measures like passwords that are difficult for hackers to crack.

In order to maintain the safety and security of data, Nigerian banks must adhere to regulations. They can make sure they are adhering to these guidelines and prevent getting into trouble or developing a bad reputation by utilizing robust cyber security measures. For the economy to expand and remain stable, a sound and robust banking system is crucial. People may stop spending money if there is fraud or people deceiving others in the banking sector. Due to this, it might be challenging for businesses to succeed and for individuals to make profitable investments. The economy, however, can expand and remain robust if we have effective methods for preventing cyberattacks and maintaining the security of the banking system. Banks in Nigeria could lower the likelihood of criminals stealing money or crucial data if they concentrated on making their computer systems extremely robust and secure. This will assist them in retaining their patrons and ensuring their happiness and safety.

2.3. Cyber Fraud

The use of computers or the internet to deceive others, steal their money, or bring about other negative outcomes is known as cyber fraud. Cyber fraud refers to deceiving users online in order to steal their money or personal data. Various tactics, such as impersonating someone else or duping you into disclosing your secrets, are possible. When someone sends messages or creates websites that appear authentic, they are phishing when they pretend to be someone else, such as a friend or a company. They do this in an effort to obtain personal information from people, such as their usernames, passwords, or credit card numbers. Identity theft occurs when dishonest online users steal someone's personal data, such as their social security number, bank account information, or credit card details. They act in this manner in order to impersonate that person and con people into giving them money or other things they desire.

The use of online scams is a technique used by dishonest people to con people out of their money or personal information. In order to obtain money or personal information like your address or phone number, they may pose as someone they are not, such as a friend or a prince, and ask for payment. It's crucial to exercise caution and avoid disclosing personal information or sending money to strangers. Losing money, damaging your reputation, running afoul of the law, and losing people's trust are all serious consequences of cyber fraud. To stop it, we must have strong security measures in place, educate people on how to stay safe, keep an eye out for bad things, and have a plan in place for when they do occur. Skimming is when someone takes your credit card information without your knowledge, according to Pal, Herath, and Rao (2019). When you hand over your credit card to a staff member at a shop or restaurant, they conceal it. The person who is stealing your information uses a specialized tool to copy every piece of data from your card's magnetic strip. To obtain your information, they may occasionally even hack into a store's computer. This is a major issue because it costs businesses and banks a lot of money, but there aren't enough laws to completely stop it. Direct and indirect electronic fraud can be distinguished from one another. Employee theft, credit card fraud, debit card fraud, and the use of false identities to conceal illicit funds are all examples of direct fraud. Indirect fraud can take the form of tricking people into disclosing their personal information or breaking into computers to steal data. Theft and credit card fraud are two prevalent forms of electronic fraud that have the same meaning. It involves obtaining money or items illegally by using another person's credit or debit card without that person's consent.

In 2014, Dzomira, there are numerous ways to commit identity theft. Identity theft involves stealing credit card information during legitimate transactions, according to Pal, Herath, and Rao (2019). When a customer's credit card information is concealed during a transaction, these fraudulent transactions typically take place in those businesses. The card will be scanned by the con artists using a "wedge" or review device, an electronic gadget that captures all the data on the magnetic stripe. Criminals can trick victims into providing credit card information or steal merchant information as sophisticated ways to obtain credit card details. However, Dzomira (2014) contends that even though losses to businesses and banks resulting from credit card fraud continue to rise, there aren't enough laws in place to stop this crime. The majority of people will suffer from technology in order to gain from it. Phishers create websites that look like legitimate websites so that victims can enter sensitive data like usernames, passwords, and credit card numbers. Frequently, emails are sent to recipients asking for the disclosure of sensitive information or the opening of investigations, and when that information is revealed, criminals alter the online environment. Phishing and phishing are two variations on phishing that deceive targets through text messages and phone calls (Dzomira, 2014). Businesses and other traders may also be the targets of this scam type. Depending on the type of business, e-commerce sites are frequently targeted because, depending on the content, they may contain valuable information or payment information that can be used for fraudulent purchases (Tendülkar, 2013). Internal fraud is typically committed by corporate con artists using "pen and paper.". However, as the business world became more computerized, the same criminals started using computer scams to pull off the same con. According to Onodi, Okafor, and Onyali (2015), embezzlement entails using funds or assets that have been entrusted to employees for their own use (for instance, employees may use the company's computer payment system to transfer data or money from the company's bank account to a personal account). Furthermore, financial institutions might grant authorized staff members access to private customer data that they can use to log into online customer accounts. Employee fraud is made more convenient as a result. The salami technique is a technique that scammers sometimes use to steal small sums of money. Long-term changes to the program are gradual and difficult to notice. This type of fraud, which involves the monthly withdrawal of several dollars from the accounts of numerous customers, is an example (Tendelkur, 2013).

In order to infect computers with errors, scammers also use malicious software and malicious codes. A program known as a computer virus is one that, while running, exhibits unwanted and frequently destructive behavior. A self-modifying illness is cockroaches. A Trojan horse is a way to introduce viruses or worms into a network or computer that appears to be legitimate or harmless because the evil is concealed (Efiong, Inyang, and Joshua, 2016). Financial transactions and/or online money transfers have turned into unethical practices during the most recent global economic crisis. This is a type of fraud where money is laundered illegally through electronic transfers of funds. Online money laundering can be a viable option because it allows for the free movement of funds without stringent controls. Both new financial investment opportunities and new challenges for law enforcement and the examination of financial transactions on the Internet are brought about by new technologies and cyberspace (Okpa, Ajah, and Igbe, 2020). Another type of scam involves spamming, where criminals send unsolicited emails or spam newsletters without the recipient's consent, frequently with malicious intent and occasionally posing as a financial institution or business (Seissa, Ibrahim, & Yahaya, 2017). In light of this, Okpa, Ajah, and Igbe (2020) propose that the only effective way to combat spam is to raise the cost of sending for senders. Victims may occasionally be diverted from a trustworthy website to a fake or fake website that mimics the real website; however, any personal information (such as passwords and credit card numbers) entered in the form may be sent to cybercriminals (Tendelkur, 2013).). Hacking or cracking is a very bad thing that people do on computers. It indicates that they access websites or programs without authorization and discover passwords or workarounds for passwords. It can be challenging to catch these cunning individuals because they are very cunning and employ unique techniques to conceal their origins. Hackers can obtain a lot of confidential information to harm businesses, cause them to lose money, or give them a bad reputation. According to (Akinbowale, Klingelhöfer, & Zerihun, 2020). Bad people occasionally use emails as a ruse to get others to transfer a large sum of money to a different party. They promise that if they use their own bank account, they will give a portion of the funds to the person they are helping. In order to get a really good deal, the bad people try to persuade the other person to give them a small sum of money first. (Bhasin) 2016, It primarily consists of significant commercial and consumer fraud, such as prepaid, 419, inheritance, and property damage fraud.

2.4. Reasons for Bank Cybercrime

The causes of cybercrime in commercial banks were identified by Niran janamurthy and Chahar (2013) as follows.

- Information that isn't encrypted: This is a basic but crucial component of top-notch cyber security. Every piece of information stored online and by your bank should be encrypted. If your data is encrypted, even if hackers steal it, they won't be able to use it right away; however, if it is not encrypted, hackers will be able to use it right away, seriously harming your financial institution.
- Viruses: Every time they connect to your network, malware-infected end user devices, including PCs and smartphones, pose a risk to the cyber security of your bank. This involves sending sensitive data. If the end user device has malware installed on it and the connection is not properly secured, the malware could attack your bank's networks.
- Unsecure services provided by third parties: Many banks and financial institutions rely on third-party services from other suppliers to provide better services to their customers. However, if those third-party providers do not have sufficient cyber security measures in place, your bank might be the one who suffers the most harm. Before implementing their solutions, it is essential to plan how you will protect yourself from third-party security risks.
- Data that has been altered: Hackers occasionally enter with the intention of modifying data rather than stealing it. Financial institutions could lose millions, if not billions of naira as a result of this type of assault, which is unfortunately difficult to spot right away. If your bank has been hacked, it might be challenging to determine what has changed and what hasn't because altered data doesn't always seem to be different from unmodified data on the surface.

Hackers imitate the URL of a banking website by creating a website that looks and functions exactly like the real thing. This is a more recent type of cyber security issue called spoofing. Hackers steal user login information and store it for later use when users submit it. Even more concerning is the fact that contemporary spoofing strategies do not depend on viewers who have already visited the correct URL to be targeted with a slightly different but similar URL. It is crucial for you, as a bank or financial institution, to come up with plans to reduce cyber security risks while still giving your customers simple, cutting-edge solutions.

2.5. Way-Out to Cyber fraud in Bank Settings

The following recommendations were made by Sikdar and Makkad (2015) in response to Cyber-Security on commercial banks. Before putting any new cyber security software into use, a thorough audit is necessary. The analysis highlights the benefits and shortcomings of the current configuration. In addition, it offers suggestions that can help you make the best investments while also saving money.

- Firewalls: Not only do they contain programs, but they also serve as a cyber-security banking setting. It also requires the right hardware to thwart attacks. With an updated firewall, banks can stop harmful activity before it spreads to other areas of the network.
- While updating a firewall increases security, attacks cannot be stopped without also updating anti-virus and anti-malware software. It's possible that outdated software lacks the most recent virus signatures and regulations. As a result, it might fail to detect a system attack that could be disastrous.
- For customers who use mobile or web apps to conduct their banking, this security feature, also known as MFA, is essential. Many users don't frequently change their passwords. Otherwise, they only make slight modifications. MFA adds another layer of security, preventing attackers from accessing the network. For instance, a customer's cell phone could receive a six-digit code.

- Biometrics: Compared to a texted code, this MFA type is more secure. Retinal scans, thumbprints, or facial recognition are used in this type of authentication to confirm a user's identity. Despite the fact that this method of authentication has been breached in the past, it is now more challenging.
- Automatic Logout: If a website or application permits it, a user may remain logged in at all times. As a result, they can access their data whenever they want without having to enter their login information.
- Credentials: But as a result of this, attackers will have an easy time obtaining customers records. Automatic logout lessens this by blocking access to a user after a short period of inactivity.

All of the aforementioned tactics can aid in enhancing cyber security in the banking sector. If customers continue to access their data from insecure locations or save their login information incorrectly, they won't be able to assist. Get a good education because of this. Customers may alter their behavior when banks inform them of the effects of these vulnerabilities because they fear losing their money. A large portion of a bank's or financial institution's business is carried out using technology, particularly the Internet. If you don't have robust cyber security protocols in place, the sensitive data from your bank may be in danger. The following list contains the five greatest threats to a bank's cyber security.

2.6. Cyber Security and Financial Fraud

It is very important to protect the Nigerian banking industry from people who try to steal money using computers. Cyber Security helps to keep the bad guys away and make sure the banks are safe. This is especially important because more and more people are using computers and the bad guys are getting smarter. Cyber Security helps to stop them and keep our money safe.

To keep bad people from getting into important banking information, banks use special tools like walls of protection, secret codes, and hidden techniques to make sure only the right people can get in. By doing this, they make it harder for someone to steal money or pretend to be someone else. Detecting and giving a warning about Cyber Security's: Special systems and techniques can help banks find out if something strange or bad is happening on the internet. When they find something suspicious, they can quickly stop it by blocking money transfers, stopping people from using their bank accounts, or looking into the problem. This helps them stop bad things from happening and keeps people's money safe. When bad guys try to steal or mess with important computer stuff, it's important to have a plan to stop them and fix any damage they might cause. This plan is called an incident response plan. By responding quickly and following the plan, we can make sure the bad guys don't do too much harm, fix any problems they caused, and get things back to normal. When banks have strong security measures to protect people's money and personal information, customers feel safe and are more likely to use online banking and stay with the bank for a long time. This trust is really important for the bank to keep growing and being successful. Nigerian banks have to follow certain rules and guidelines to make sure they protect themselves from hackers and stop people from stealing money. By doing this, they avoid getting into trouble and damaging their reputation. Following these rules also helps make sure all banks take security seriously. Working together and sharing information is really important in keeping banks safe from bad people who want to steal money. Banks, people who make rules for banks, and others who are involved in the banking industry need to work together. They share information about the different ways bad people try to steal money, the best ways to protect against them, and what they have learned from past experiences. By doing this, they can make sure they have strong defenses against cyber-attacks and can stop bad people from taking money from the banks.

2.7. Internet Banking and Electronic Banking

The Internet is one of the fastest growing areas of technological development. In today's business environment, applications such as cloud computing, social computing, and next-generation mobile devices are changing the way organizations use information technology to share information and do business online. Internet or electronic banking is a private banking method that allows bank customers to carry out various financial transactions electronically over the Internet. Online banking offers customers almost all services normally offered by local branches, including deposits, wire transfers and online payments. There are 21 banks operating in Nigeria: Access Bank, Citibank Nig Limited, Ecobank, Fidelity Bank, First Bank, Globus Bank, Guaranty Trust Bank, Heritage Bank, keystone Bank, Polaris Bank, Providus, Stanbic etc, Standard Chartered, Sterling Bank, Sun Trust, Titan Trust Bank, Union Bank of Nigeria, Unity Bank, Wema Bank plc and Nigeria banks. Ebiasuode, Onuoha, and Nwede (2017) argue that the first bank in Nigeria to start doing business on the Internet in 2000, created and improved customer trust, paving the way for business results and ensuring the success of future innovations. Today, more than 80% of business transactions are done online, placing a high demand on the security and privacy of personal information and transactions. The scope of cyber security covers not only information security in an organization, but also cyberspace and critical systems. Internet security depends on the care and judgment people use when setting up, managing and using computers and the Internet. Cyber Security covers the physical (hardware and software) protection of personal data and programs against unauthorized use.

Wapmuk (2017) developed a statistical model to explain why some banks accept the Internet while others offer more Internet products and services. The results show that there are some important differences between banks that offer internet banking services and those that do not. The COVID-19 pandemic in 2020 has further highlighted the need for people to integrate technology into many areas of society such as commerce, finance, health, energy, entertainment, communications and defence. The findings also show that public concern over privacy and personal information has increased since 2006, and investment in Cyber Security infrastructure will play an important role in protecting and safeguarding important information for the health of Nigerian citizens, businesses, governments and businesses. Plays an important role in the country.

In the process of examining the theory with the study, Game theory was proposed by Neumann and Morgenstern in 1944. To ensure stability, the theory specifies rules that allow decision pressure from individual devices to account for all other processes must be included in the network. Game theory helps develop models to analyze the interaction between attackers and defenders insecurity situations affecting the banking industry (Amadi et al., 2017). Defenders can step up their game when it comes to strategies such as network security, endpoint security, network security, and physical security. They can play the same "unfair" game as the opponent. Game theory can be used in the security field to monitor cyber situations where cyber defenders, attackers and users interact with each other and produce results. Routine Activity Theory (RAT) This theory was used in this study as child abuse is one of the most serious crimes in the world. Culatta, Clay-Warner, Boyle, and Oshri (2020) reconsidered this theory. This view focuses on "crimes" in the environment. When a potential crime occurs, the action takes place where and when the perpetrator's motivation conflicts with the victim's goal. These crimes will end where there is no necessary supervisor to deal with the target identified as a vulnerable person or a vulnerable property. Therefore, the absence of any of these three conditions may affect the crime (Valan & Srinivasan, 2021). Article: Article In the absence of suitable guardians who can prevent offenders from committing crimes, the theory predicts that crimes will occur when people have violent contact with victims. The theory argues that the evolution of crime can be explained by the presence of appropriate targets and competent observers, and the consequences as far as we can see. The crime theory is agnostic (Valan & Srinivasan, 2021).

2.8. Empirical review

Dzomira (2014) reviews the literature on electronic fraud in banking and the difficulties in managing risks. This investigation into the phenomenon of online fraud is based on a descriptive study that used content analysis. To gather information, we conducted surveys and interviews with informants chosen from 22 banks. Methods that are easy to use and reliable are employed. It has been found that the banking industry is where the majority of the aforementioned electronic fraud types are committed. Issues like a lack of resources (technology and tools for investigations), insufficient cybercrime laws, and a lack of knowledge and awareness. To safeguard business operations against cyber-security, it is advised that all partners cooperate to find solutions to Cyber Security problems. In 2022, Win, Promise, and Mike investigate how cyber security affects preventing fraud in Nigerian businesses. Through interviews (WhatsApp video calls) with senior employees of different companies who are knowledgeable about the topic, this study gathered crucial data. Findings demonstrate that cloud security analytics improves Nigerian fraud prevention; in addition, the security app does the same. This study shows that in order to detect fraud and stop it from harming customers or other departments financially or reputational, the Nigerian financial sector needs specialized knowledge to educate the public on fraud, to avoid loss of money or other services or theft of their devices, they should always use strong passwords. More significantly, Olaniyan, Ekundayo, Oluwadare, and Bamisaye (2021) looked into the use of forensic accounting in Nigeria as a tool for fraud detection and prevention, they discovered, using original data spanning ten (10) years, from 2010 to 2020, that financial analysis is useful and advantageous in preventing fraud, despite the fact that foreign currencies cannot control fraud. The study also demonstrated that money that had been fraudulently taken had not been successfully recovered. According to Leukfeldt and Holt (2022), they used 37 examples of crimes that were related to cybercrime to analyze the issue. They concluded that various cybercriminals engage in a variety of offenses. About half of the criminals in this example were computer professionals, while the other half were involved in numerous crimes both online and offline. This is because they occasionally engaged in some type of cybercrime. The correlation between intelligence and activity, particularly in online and offline activities, suggests that assigning liars to a group of criminals may not be very useful. Whether professional or medical, cybercriminal actors, fraud, ransom ware, etc. It is a component of a larger online crime network that aids in locating and profiting from opportunities for financial crime. Analysis of the effect of forensic investigation on financial fraud in Nigeria (DMB) by Alao (2016). Cross-sectional methodology was used for the selection. Employees of banks and auditing firms in Abeokuta, Ogun Province, participated in this study. The study demonstrates that forensic audit has a significant impact on the management of financial fraud (DMB) in Nigeria. The P value of the forensic evidence being collected is useful for the Nigerian court's decision on financial fraud with a P value of less than 0.05. Data from forensic investigations, significantly enhance the ability of Nigerian courts to detect financial fraud. The results show that forensic analysis (DMB) is only just beginning to be used to stop financial fraud among Nigerians. In a similar study titled "The Impact of Research on the Performance of Nigerian Financial Markets," Onodi, Okafor, and Onyali (2015) examined the efficacy of research studies in a Nigerian nation. This study employs a survey methodology based on information from primary sources including administrative surveys, interviews, and financial fraud in addition to other sources like complaints. Studies reveal a strong connection between job fraud and research studies. Evidence demonstrates that while forensic investigators' expertise is frequently required when prosecuting fraud, it is not always necessary. The effect of fraud on the demise of Nigerian banks is examined by Adeniyi (2016). In the study, ex post facto research methods and a cross-sectional survey were both used. With a P-value of 0.972, which is higher than 0.05, the study's findings showed that the occurrence of fraud has no discernible influence on the total anticipated loss suffered by Nigerian banks. Research indicates that a reliable indicator of bank failure in Nigeria is the amount of money involved in bank fraud cases. Similar to this, Samuel, Pelumi, and Fasilat (2021) looked into how internal control systems affected the prevention of fraud among deposit money institutions. All of the financial institutions in the state of Kwara were included in the target audience. The sample size for this study, which concentrated on all 17 Nigerian banks in Kwara State, was decided using purposeful random sampling. The study discovered a significant link between fraud prevention and internal control at Nigerian deposit banks. "Badjo et al.". In the Nigerian banking industry, a number of issues relating to fraud detection and prevention were evaluated in 2018. The main form of fraud in Nigeria, according to the study's findings, involves bank managers and managers stealing money rather than providing adequate incentives. The government should also strengthen its financial control over the anti-corruption organizations that are already in place. Managers and executives who stole from the company should face legal consequences in order to deter crooks in the future. A thorough investigation should be done to evaluate a candidate's moral and ethical character before hiring them as a bank employee. Cyber-security in the financial sector is examined by Sethi (2021). For developing nations, particularly in emerging economies like India, banks are crucial. Since the early 1990s, when globalization and privatization began, computerization and technology have permeated Indian banks. The term "bank" previously denoted a physical establishment, a building where branch managers and other staff members kept stacks of books behind the counter and customers lined up or waited at toll booths for greenbacks and other items. Consider this: When today's youth is referred to as a "bank," it does not mean a home or a person. Instead, he considers his computer, ATM, or phone. More technology delivery channels than any other industry in the world are connected to banking today, including ATMs, mobile phones, physical stores, and online transactions. It should come as no surprise that neither today's client nor today's banker are familiar with all of their customers. Long-standing threats have existed to the bank. The first is the actual money that was stolen. There is also the issue of computer fraud. Along with identity theft, it is now common practice to hack servers in order to steal customers' personally identifiable information (PII). Because most people and businesses conduct business online and because the risk of data breaches is growing daily, cyber security is crucial in the banking sector. So it's critical to examine how cyber security fits into the money-making process. The effect of securities policy on the profitability of deposit banks in Lagos State, Nigeria, is examined by Oyelakin, Onu, and Akinlabi in 2021. The banking sector is one of many that have grown up using the Internet and information technologies to offer customers online banking services, which has many advantages for both banks and customers. Customer data is seriously at risk because it has been accessed, used, disclosed, tampered with, altered, or destroyed, resulting in fraud and damaging many banks' reputations and operations worldwide. Security is one of the most important issues currently affecting the financial sector. As a result, this study investigates how securities policies affect deposit banks' profitability in Lagos State, Nigeria. 433 employees of the selected deposit banks' IT departments are the study's participants. The selected bank's 433 employees in total were assessed. Utilize a valid and appropriate questionnaire to gather data. The reliability test yielded a Cronbach's alpha model that ranged from 0.947 to 0.990. Analysis of data using actual data. According to the study's findings, deposit banks' profitability in Lagos State, Nigeria are significantly impacted by the security quality dimension.

3. Methodology

In this part, the paper show the things that was used in this study. We used a special plan to help us talk to a lot of people. The goal of our study is to find out how cybercrime and cyber security are connected and how they affect people. We collected information from 49 Nigeria banks in Nigeria to learn about a big group of people. Now we will follow the normal steps to analyze this information.

The concept of research design is the process used to form the basis of research. Strategy involves collecting data and developing strategies for analyzing and discussing data. In this study, the research design required by the research was used. Adegoke (2012) scientific research is when scientists watch and understand how students act. They study a lot of people to learn about cybercrime at Nigeria banks they want to know why it happens, what problems it causes, and how to stop it.

Table 1 Population of the Study

S/NO	BANKS	NO of Banks Branches
1	ACCESS	49
2	Wema	9
3	GTB	8
4	Union	4
5	UBA	3
6	F.C.MB	2

The information represented in table 1 above was sourced from the website of Nigeria banks the population of the study is the staff in Nigeria Bank. However, although, the total number Nigeria Banks in Nigeria. Multi-stage sampling technique was used. The study selected the Nigeria banks to represent some particular in Nigerians given a total of 6 banks. Thereafter, census sampling was used to capture the staff of selected Banks. The sample size of staff is 557. The study adopted structured questionnaire to capture the responses of the population. The instruments was designed under two headings section A requested for demographic information and section B captured the research questions. The hypotheses were analyzed using the Kendal Tau B and multiple regression. The result of findings was presented using table. Statistic Package for Social Science version 27 was used for the analysis.

3. Analysis of the hypothesis

3.1. H_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 banks

Table 2 Impact of the types of electronic frauds and the causes of cyber fraud on the effect of cyber fraud on banks

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

**Sig<0.05

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

3.2. H_2: Second Hypo; there is no relationship between the challenges of curbing cyber fraud and the possible solutions of curbing cyber fraud in banks.

Table 3 Challenges of curbing cyber fraud and the possible solutions of curbing cyber fraud in banks.

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

The Table showed the relationship between the challenges of curbing cyber fraud and the possiblesolutions 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.

The study found that people who use banks have experienced different types of electronic fraud, like when bank employees cheat with money, when someone pretends to be someone else to steal information, when criminals move money illegally, when hackers break into computer systems, when people trick others into giving them personal information, when fake websites try to get people's information, and when computer viruses cause problems. The study also found that cybercriminals do these things to try to take money from people's bank accounts without permission, and sometimes they do it to harm the reputation of the bank. The study also found that the main reasons why cyber fraud happens in banks are because the people in charge don't pay enough attention to the rules, there is pressure to meet goals, some employees work with outside people to cheat, the data isn't protected well enough, the bank uses services from other companies, and people pretend to be someone else. Another reason is that many people in Nigeria don't have jobs, which can lead them to commit cybercrimes. This means that because of certain reasons like technology and pressure to do well in business, people are doing more illegal things to survive. Some of these reasons include working together with others and not protecting information well. This can happen in banks too.

4. Summary of the findings

The study found that banks have a lot of problems trying to stop cyber fraud. Some of these problems include not having rules and control from a central authority, not having the right technology and systems in place, the internet being easy for hackers to get into, not having enough information about people who use the banks, and customers not knowing enough about how to protect themselves from fraud. Another study also said that people in Africa don't have the latest security measures on their computers and don't always update their software, which makes it easier for cyber fraud to happen. The study found that cyber fraud is really bad for banks. It can make them lose money, make them work less effectively, and make their computer systems easier to attack. Another study by Frank and Odunayo also said that cybercrime is a big problem for banks. The author of the study also said that cybercrime can make banks look bad, make them work less effectively, and make them lose money. The study found ways to stop cybercrime in Nigerian banks. These include checking for security problems, using special software to protect against viruses and malware, using more than one way to prove who you are, using things like fingerprints or eye scans for extra security, automatically logging out when you're done, and teaching people about how to stay safe online. Another person named Sethi also wrote about ways to stop cyber fraud in banks, like using special protection on the bank's computer systems, getting experts to regularly check for problems, and using things like fingerprints or eye scans for extra security. When banks keep their customers' information and money safe from cybercrime, more people will trust and use the bank.

5. Conclusion and Recommendations

Cybercrime is a really bad thing that we need to stop or make it happen a lot less in our country. People have done research and found out different ways that cyber criminals try to trick people and steal their money. It's a big problem for banks in Nigeria, but there are things they can do to make it happen less. Using technology and security measures can help stop the bad guys from stealing from people's bank accounts. The study showed that using cloud security can really help prevent fraud at Nigeria banks.

Compliance with ethical standards

Acknowledgement

I am grateful for the permission and support from my colleagues, both in my department and others departments, also to everyone that contribute to the success of this paper.

Disclosure of conflict of interest

I, fatoki Jacob Obafemi, I claim that I am free from any financial, personal or grant relationship that might have unnecessarily impacted the report on this research findings

Statement of informed consent

All of the study's participants gave their informed consent, which was obtained from them on a voluntary basis.

References

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

[2] 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, 945-958.

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

[4] 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.

[5] Buchanan, B. (2016). The Cyber Security dilemma: Hacking, trust, and fear between nations

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

[7] 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.

[8] 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.

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

[10] 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).

[11] 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).

[12] 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.

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

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

[15] Ibrahim, U. (2019). The Impact of Cybercrime on the Nigerian Economy and banking system.

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

[17] J. Okoth. "Fraudsters take home billion s from banks" .Nairobi: East Africa Standard 17th November 2019. Journal of Multidisciplinary Research and Growth Evaluation, 2(1), 264–271.

[18] K. Okiro, & J. Ndungu. The Impact of Mobile and Internet Banking on Performance of Financial Institutions in Kenya. Journal of Business and Management 16(9) pp. 146-161, 2013.

[19] L.F. Amboko, & J. Wagoki, Determinants of Adoption and Usage of Banking Innovations by Consumers for Competitive Advantage: A Case of Banks in Nakuru County. International Journal of Science and Research (IJSR) 3(10) pp. 1597-1601, 2012.

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

[21] 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

[22] Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style

[23] M. Loonam, & D. O'Loughlin, D. An observation analysis of e-service quality in online banking. Journal of Financial Services Marketing, 13(2), pp. 164-178, 2008.

[24] NDIC Quarterly, 34(12), 1-20.

[25] R.N. Acharya, & A. Kagan, Commercial B2B Web Site Attributes within the Perishable Sector. Journal of Internet Commerce, 3(4) pp. 79-91, 2004

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

[27] Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., & Dwivedi, Y. K. (2021). Developing a modified total interpretive structural model (M-TISM) for organizational strategic Cyber Security management. Technological Forecasting and Social Change, 170, 1208

[28] S. Kamel. The Use of Information Technology to Transform the Banking Sector in Developing Nations. Information Technology for Development vol. 11 (4) pp. 305–312, 2015.

[29] 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.

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

[31] 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.

[32] Tendulkar, R. (2013). Cyber-crime, securities markets and systemic risk. CFA Digest, 43(4), 35- 43.UK: Oxford University Press.

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

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

[35] Zheng, Y., Pal, A., Abuadbba, S., Pokhrel, S. R., Nepal, S., & Janicke, H. (2020). Toward Security Automation and Orchestration. Paper presented at the 2020