HP JARAR2024
Hummingbird Publications
Journal of African Resilience & Adv. Research
www.hummingbirdjournals.com
©August, 2024
Vol. 5 No. 2

The Effect of Cyber-Crimes on Depositors Funds in Deposit Money Banks in Nigeria

***Olalekan Olukemi Oluyemisi; *Rakiya Abba; & **Johnson Ayanwuyi**

*Department of Banking and Finance, Federal Polytechnic, Bauchi. **Department of Accounting, Federal Polytechnic, Bauchi.
Corresponding Author: *kemiyemio1@gmail.com*

Keywords: Cybercrimes, Depositors, Deposits, Deposit Money Banks

Abstract

This study investigated the effect of Cyber Crimes on Depositors Funds in Deposit Money Banks in Nigeria. A sample size of 103 depositors was used, mean and standard deviation was employed in the analysis. The result of the study indicated that there is an insignificant relationship between cyber-crimes and the level of depositor's trust. This implies that, the adverse occurrence of cyber-crimes may affect the confidence but will not affect the level of depositor's trust, i.e. the more cyber-crimes are carried-out or perpetrated will not affect the level of depositor's trust with their deposits in the bank. Depositors' fund safety is significantly influenced by the level of cyber-crimes that is carried-out, as it is felt that as more and more cyber-crimes are perpetrated by fraudsters the level of fund safety on the side of the depositors becomes low. Cyber-crime laws also have a positive influence and has a significant effect in curbing or mitigating the continuous occurrence of cyber-crimes in Nigeria.

Introduction

Background of the Study

In recent times, our society is increasingly relying on the internet and other information technology tools to engage in personal communication and conduct business activities

among other several benefits. Whilst these developments allow for enormous gain in productivity, efficiency and communication they also create a loophole which may totally destroy an organization as well as individuals in the community. The term cybercrime can be used to describe any criminal activity which involves the use of computer or the internet network (Okeshola, 2013). This term is used for crimes such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used. Cyber-crime is believed to have started in the 1960's in the form of hacking. This was followed by privacy violations, telephone tapping, trespassing and distribution of illegal materials in the 1970s.

In (Maitanmi, 2013) cybercrime was defined as a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing, duping depositors and the likes. Cyber-crime evolves from the wrong application or abuse of internet services. The concept of cybercrime is historical. It was discovered that the first published report of cybercrime occurred on the mainframe computer in the 1960s (Maitanmi, 2013). Since these computers were not connected to the internet or with other computers, the crime was committed by the employers (insider) in the company, hence it was referred to as computer crime rather than cybercrime.

Cybercrime is a new trend that is gradually growing as the internet continues to penetrate every sector of our society and no one can predict its future. The crime usually requires a hectic task to trace. Generally, cybercrime may be divided into one of two types of categories; Crimes that affects computer networks and devices directly. Examples are malicious code, computing viruses and malware etc. or Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer networks or device. Examples include Cyber Stalking, Fraud and identity theft, phishing scams and information warfare.

There are few innovations that have changed the dynamics of banking as much as the e-banking revolution. Throughout the world, banks are reorganizing their business strategies to take advantage of new business opportunities offered by e-banking. Electronic banking is believed to have started in the early 1980s It has since then been growing in an unprecedented dimension in line with the growth in ICT development. E-banking has enabled banks to overcome borders, adopt strategic outlook, and bring in new possibilities. According to (Nitsure), information communication technology has reduced the cost of processing and facilitating the transmission of information leading to drastic changes in the banking business. The E-banking system has also made it very easy for depositors to carry out numerous transactions across the internet and provides easy access and movement of funds to make payment, settle debt or in performing other services.

This research work examines what cyber-crime is, the different types of cyber-crimes that exist and their impact on bank depositors, impact and aspects of modern life and business.

Statement of the Research Problem

Advancements in Information and Communication Technology (ICT) have redefined the ways banks carry out their businesses and turned the whole world into a global village. However, it has brought about numerous problems accompanying such great benefits. Nefarious software continues to be developed on a daily basis and circulated, fraudsters are now common everywhere around the world. Vast amount of database is subsequently destroyed and lost to these vile. More so, computer hackers and crackers hack into restricted database and commit fraudulent activities using their computer skills. Large amount of bank deposits is stolen/lost making some depositors lose faith and do away with banking system. Thus, making banking operations very difficult and stressful.

The larger society expects greater accountability, fairness, transparency and effective intermediation from banks, ensuring that they carry out their responsibilities with sincerity of purpose and unquestionable integrity with respect to their operations as a means towards earning public trust and goodwill. The banking business has become more complex with the development in the field of Information and Communication Technology (ICT) which has changed the nature of bank fraud and fraudulent practices. Berney (2008) observed that customers rely heavily on the web for their banking business which leads to an increase in the number of online transactions. Gates, Jacob and Malphrus (2009) asserts that the internet provides fraudsters with more opportunities to attack customers who are not physically present on the web to authenticate transactions.

In Nigeria, in spite of the banking regulation and bank examination by the Central Bank of Nigeria (CBN), the supervisory role of the Nigeria Deposit Insurance Corporation (NDIC), and The Chartered Institute of Bankers of Nigeria (CIBN), there is still a growing concern about cyber-crime fraud and other unethical practices which concerns the banking industry. Okpara (2009) found that one of the factors that impacted the most on the performance of the banking system in Nigeria was fraudulent practices.

This informs the decision to undertake this study so as to identify, explain and understand. The problem of cyber-crimes on depositors account in listed deposit money bank in Nigeria in order to see how this problem can be address.

Objectives of the Study

The main objective of this research work is to examine the effects of cyber-crime on depositor's accounts in listed Deposit Money Banks in Nigeria.

The specific objectives are to:

1. To identify and distinguish different types of cyber-crimes.
2. To examine the impact of cyber-crimes on depositors' funds.
3. To examine the impact of cyber-crime on the level of depositor's fund safety
4. To examine the impact of cyber-crime laws in preventing cyber-crimes on depositor's account.

Research Questions

1. What impact does different types of Cyber-crimes have on depositors and on Nigerian banking industry?
2. To what extent does cyber-crime impact on the level of trust the depositors have on their deposits with the bank?
3. What impact does Cyber-crime have on the level of safety of depositor's fund with the bank?
4. What effect does government laws and regulations have in curbing or mitigating cyber-crime cases in Nigeria?

Scope of the Study

The scope of this study is to examine the effect of cyber-crimes on depositors account in listed Deposit Money Banks in Nigeria, and the study is limited to small bank depositors in some selected Deposit Money Banks in Bauchi State.

Significance of the Study

The effect of cyber-crime and fraud on the deposits of banks as well as on the operations of banks in Nigeria and indeed the economy at large is of interest to researchers and industry practitioners. Studies concerning cyber-crimes and frauds in Nigeria have highlighted the contribution of frauds to bank distress (Udegbunam, 1998). The study also seeks to improve on the methodology and findings of past researchers by conducting some statistical tests of significance. Furthermore, the study will be of value and very useful to all categories of depositors by making them more aware of different types of cyber-crimes they might be exposed to and the ways they are to protect themselves from being scammed by fraudsters when using the internet banking facility, it will also be useful to bank managers in making them more exposed to different cyber-crime activities and the ways fraud can be carried out, so that different cyber-safety measures can be implemented. The study will also be very significant to the financial information users such as existing and potential shareholders to be informed of different types and methods of cyber-crimes in order to make effective decisions on the control measures to take, in order to ensure smooth operations of the institution and also to enhance confidence and depositors trust. The study will be of value to the relevant government agencies in order to formulate more regulatory policies and

strong cyber-crime laws, which will discourage perpetrators in committing more crimes. Besides, researchers and students in the relevant field

Literature Review

Concept of Cyber-Crime

There is no universally accepted legal definition of cybercrime or computer crime. Generally, 'cybercrime' or 'computer crime' are often used interchangeably to refer to instances where digital technologies are either the target of a malicious or unlawful activity or the instrument for facilitating a crime or malicious activity. Thus, 'cybercrime' (or computer crime) is used as an umbrella term to refer to all forms of crime perpetrated with the help of computer resources, regardless of whether the final target is a computer resource itself or not. Cybercrime has also been defined as "computer-mediated activities which are either *illegal or considered illicit* by certain parties and which can be conducted *through global electronic networks*".

Cybercrime is also defined as a crime in which a computer is the object of the crime or is used as a tool to commit an offense. Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime.

Cyber-crime may also be referred to as any form of misconduct in cyber space. It is simply defined as the criminal use of the Internet. Cyber-crime is believed to have started in the 1960's in the form of hacking. This was followed by privacy violations, telephone tapping, trespassing and distribution of illegal materials in the 1970s. The 1980s witnessed the introduction of viruses. The fast pace of development of ICT from the 1990s till today has added to the list of criminal exploits in cyber space. Today, the Internet is used for espionage and as a medium to commit terrorism and transnational crimes. With e-banking gaining ground in Nigeria, customers and online buyers are facing great risk of unknowingly passing on their information to fraudsters. "Hackers" get information of those who have made purchases through websites and then make fake cards, which they use with less detection.

Types of Cyber-Crimes

This study presents the types of cyber-crimes that have economic impact either directly or indirectly depositor's account or having cross border ripple effects. Longe&Chiemeke (2008) simplified the list of unintended consequences of ICT to include acts such as Phishing, cyber terrorism, electronic spam mails, cyber-stalking, and fake copy-cat websites. While some types of cyber-crimes are specific to Nigeria, other types, such as identity theft and false statements, cut across all countries.

Phishing

According to Roger E.S (2008), phishing is simply a high-tech identity theft that does not only steal personal information and identity from unsuspecting consumers, but also an act of fraud against the legitimate businesses and financial institutions that are victimized by phishing. Phishing is usually a social engineering crime pervasive in attacking institutions or individuals(depositors) information systems in order to gather private information to be used against the institutions or depositors, to extract some benefit for the perpetrator through the anonymity of identity theft or identity deception acts (Rodger, 2008). Phishing attempts to pose significant dangers for unsuspecting victims. It has become one of the fastest-growing worldwide threats on the Internet. In phishing e-mail messages, the senders must gain the trust of the recipients to convince them to divulge their personal information. To gain this trust, fraudsters deceive or imitate, a reputable financial institution. To further convince the recipient that the e-mail originates from the reputable financial institution, the scammers use a "from" e-mail address that appears to be from the company by using the company's domain name. Phishing e-mails also try to assure the recipient that the transaction is secure in hopes of gaining the recipient's trust.

Cyber Terrorism

According to Wilson (2008), cyber terrorism is said to have taken place when the effects of a widespread computer network attack is unpredictable and might cause enough economic disruption. Cyber terrorism is the use of cyber infrastructure to launder money for financing physical terrorism. Cyber terrorism may also be seen as any premeditated or politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups

Electronic Spam Mails

These are unsolicited bulk e-mail to multiple recipients. They can be commercial, political, or religious. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media such as; instant messaging spam, web search engines, and blogs.

This type of attack is more difficult to control due to multiple source addresses and the bots which are programmed to send different messages to defeat spam filters. "Spamming" is a variant of email bombing. Here unsolicited bulk messages are sent to a large number of users, indiscriminately. Opening links given in spam mails may lead you to phishing web sites hosting malware. Spam mail may also have infected files as attachments. Email spamming worsens when the recipient replies to the email causing all the original addressees to receive the reply. Spammers collect email addresses from customer lists, newsgroups, chat-rooms, web sites and viruses which harvest users'

address books, and sell them to other spammers as well. A large amount of spam is sent to invalid email addresses.

Bank Verification Number (BVN) Scams

The BVN is a biometric identification system which consists of an 11-digit number that acts as a universal ID across all the banks in Nigeria. BVN was implemented in 2015 by the Central Bank of Nigeria. It was introduced to link various accounts to the owner thereby ensuring that fraudulent activities are minimized. For fraudsters, opportunities to extort money and to carry out other fraudulent activities arose from the implementation of the BVN. It was detected that fake and unauthorized text messages and phone calls were sent to various users demanding for personal information such as their ac-count details. In addition, phishing sites were created to acquire such information for unpleasant activities on the bank account.

Cyber-theft / Banking Fraud

Hackers target the vulnerabilities in the security of various bank systems and transfer money from innumerable accounts to theirs. Most cyber-criminals transfer bantam amounts like five (5) naira which are sometimes overlooked by the user without questions raised by the users who assumes this was deducted for either SMS or ATM withdrawal charges. Doing this for over a million accounts enriches most fraudsters. This type of cyber-crime is also known as **"Salami slicing attack".**

Cyber Stalking

Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn't physically follow his victim; he does it virtually by following his online activity to harvest information about the stalkee and harass him or her and make threats using verbal intimidation. It's an invasion of one's online privacy.

Cyber stalkers harass their victims via email, web sites, discussion forums and open publishing web sites (e.g. blogs). The availability of free email/web site space and the anonymity provided by forums has contributed to the increase of cyber stalking incidents. Everyone has an online presence nowadays, and it's really easy to do a Google search and get one's name, alias, contact number and address, contributing to the menace, that is cyber stalking. As the internet is increasingly becoming an integral part of our personal and professional lives, stalkers can take advantage of the ease of communications and the availability of personal information only a few mouse clicks away. In addition, the anonymous and non-confrontational nature of internet communications further tosses away any disincentives in the way of cyber stalking.

Fake Copy-Cat Web Sites

One recent trend in on-line fraud is the emergence of fake copy-cat web sites that take advantage of consumers who are unfamiliar with the Internet, or who do not know the

exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unknowingly entering details into a fraudster's personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud.

Identity Theft and Credit Card Fraud

Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name. The imposter may also use your identity to commit other crimes. "Credit card fraud" is a wide ranging term for crimes involving identity theft where the criminal uses your credit card to fund his transactions. Credit card fraud is identity theft in its simplest form. The most common case of credit card fraud is your pre-approved card falling into someone else's hands. He can use it to buy anything until you report to the authorities and get your card blocked. The only security measure on credit card purchases is the signature on the receipt but that can very easily be forged.

Web Jacking

Web jacking derives its name from "hijacking". Here, the hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish interests.The web jacking method attack may be used to create a clone of the web site, and present the victim with the new link saying that the site has moved. The name on the address bar will be slightly different from the original website that can trick the user into thinking it's a legitimate site. Web jacking can also be done by sending a counterfeit message to the registrar controlling the domain name registration, under a false identity asking him to connect a domain name to the web-jacker's IP address, thus sending unsuspecting consumers who enter that particular domain name to a website controlled by the web-jacker. The purpose of this attack is to try to harvest the credentials, usernames, passwords and account numbers of users by using a fake web page with a valid link which opens when the user is redirected to it after opening the legitimate site.

Duty of Banks and Financial Institutions Measures to Prevent Cyber-crimes

Banks and financial institutions occupy the most strategic position in the electronic banking and payment services system. This is because banks and financial institutions supply electronic banking and payment services to depositors which require them to acquire and hold sensitive confidential information that relate to the depositors on

their computer systems, such as bank account details and transaction records. More importantly however, the contractual relationship between banking and financial institutions and the depositors, of their services includes an implied fiduciary duty of secrecy and confidentiality. This means that a bank or financial institution is under an implied obligation to protect the confidentiality of a depositor's account details and transactions made thereon. Therefore, banks and financial institutions, given their stronger position in relationship with consumers, generally have a duty to adequately protect the confidential information of depositors that use their services from unauthorized access by third parties. Accordingly, Section 19(3) of the Cyber-Crimes Act provides that;

"Financial institutions must as a duty to their customers/depositors put in place effective counter fraud measures to safeguard their sensitive information, where a security breach occurs the proof of negligence lies on the customer/depositor to prove the financial institution in question could have done more to safeguard its information integrity".

The above provision requires banks and financial institutions to establish effective fraud prevention measures to protect the 'sensitive information' of customers/ depositors held in their computer systems from being unlawfully accessed by unauthorized third parties. The Act does not define the meaning of 'sensitive information' and such definition does not exist under relevant banking laws in Nigeria. However, the CBN Consumer Protection Framework of 2016, which Nigerian banks and financial institutions are required to comply with, appears to provide an industry working classification of what can be regarded as 'sensitive information'. In this regard, the CBN Consumer Protection Framework, provides that "the following information are considered to be confidential and shall be protected at all times; contact details, account number and balance, statement of accounts and any other information known to the financial institution.

Cyber Crime Policy in Nigeria

There is presently no law that is specific to cyber-crime in Nigeria. However, this is not to say that cyber criminals are free to operate in the country. There are general laws that are not specifically related to cyber-crime but are being enforced to deal with the crime. Some of these laws are; the Nigeria criminal code, Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2004, and the Advance Fee Fraud and other Related Offences Act 2006.

The Nigeria Criminal Code Act 1990

The Criminal Code Act of 1990 (Laws of the Federation of Nigeria, 1990) criminalizes any type of stealing of funds in whatever form, an offence punishable under the Act. Although cyber-crime is not mentioned in the Act, it is a type of stealing punishable

under the criminal code. The most renowned provision of the Act is Chapter 38, which deals with "obtaining Property by Cheating." The specific provisions relating to cyber-crime is in section 419, while section 418 gave a definition of what constitutes an offence under the Act. According to Section 418, offence is "Any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretense. "While cyber related crime in section 419 states that; "Any person who by any false pretense, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.

The Economic and Financial Crime Commission Act, 2004

The Economic and Financial Crime Commission Act (Laws of the Federation of Nigeria, 2004, as amended) provide the legal framework for the establishment of the Commission. Some of the major responsibilities of the Commission, according to part 2 of the Act, include:

- the investigation of all financial crimes, including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam, etc.;
- the coordination and enforcement of all laws against economic and financial crimes laws and enforcement functions conferred on any other person or authority;
- the examination and investigation of al1 reported cases of economic and financial crimes with a view to identifying individuals, corporate bodies, or groups involved;
- undertaking research and similar works with a view to determining the manifestation, extent, magnitude, and effects of economic and financial crimes and advising government on appropriate intervention measures for combating same;
- Taking charge of, supervising, controlling, coordinating all the responsibilities, functions, and activities relating to the current investigation and prosecution of all offences connected with or relating to economic and financial crimes, in consultation with the Attorney- General of the Federation;
- The coordination of all investigating units for existing economic and financial crimes, in Nigeria;
- The Commission is further charged with the responsibility of enforcing the provisions of the Money Laundering Act 1995; the Advance Fee Fraud and Other Fraud Related Offences Act 1995.

Concept of Deposit Account

Money and banking are part of everyday life. Banks offer all sorts of financial products to help manage depositors' money on a day-to-day basis. The bank is such a place where once we deposit money, it remains safe and also earns interest over some time. This is

known as the deposit and to each deposit, the bank assigns a unique identity which is known as the account. Each deposit corresponds to a unique account and vice versa. Sometimes we use numbers to uniquely identify an account. This is what we call the account number. It may also be a combination of alphanumeric letters. Bank deposits serve different purposes for different people. Some people cannot save regularly. They deposit money in the bank only when they have extra income. The purpose of deposit then is to keep money safe for future needs. Some may want to deposit money in a bank for as long as possible to earn interest or to accumulate savings with interest so as to meet future unforeseen contingencies.

A deposit account is a savings account, current account or any other type of bank account that allows money to be deposited and withdrawn by the account holder. These transactions are recorded on the bank's books, and the resulting balance is recorded as a liability for the bank and represents the amount owed by the bank to the customer. Some banks may charge a fee for this service, while others may pay the cu**3.**

Empirical Literature Review

There have been an extensive studies conducted in many countries on cyber-crimes and its effect on banking activities, for instance; J.A. Mshana (2020) carried out a comprehensive report on " The impact of cybercrime on society". He employed the use of survey using questionnaires which was distributed to 250 people out of which 200 people responded and also took interviews. The total respondents were 80% out of the whole 250. He came to a conclusion that the impact of cybercrime has become unsustainable, considering the global economic crisis.

Review of Empirical Review

Viraja and Purandare (2021) embarked on a qualitative research on the impact and challenges of cybercrimes. They administered qualitative questionnaires to 110 respondents of different age groups and gender then applied qualitative data analysis of grounded theory. They concluded that with the increasing rate of technology, cybercrimes can render even the entire government of a country bankrupt.

The Nigerian Communications Commission (NCC) (2021) released its findings on the "effects of cybercrime on Foreign Investments and National Development". They used secondary data for the research. Data necessary for the line of that investigation was obtained and collected through desk research using the internet and data from the CBN and NBS. Trend analysis (excel) was introduced for their data analysis and it was founded that though the internet produces opportunities even for a country, cybercrime can overthrow a nation and give a bad image of the country.

Mohammad Alghandi (2020) researched the effect of cybercrimes on society, the research utilized instruments such as questionnaires, virtual interviews, and reports from radio and electronic media. Using qualitative data analysis He came to a

conclusion that cybercrimes are fast gaining grounds in both developed and developing countries and is injurious if not combated effectively.

Nkwepa et al (2019) carried out a research on the effect of cybercrime on the performance of e-business in Konga.com. they used secondary data from Konga.com and used Ex-post facto survey design approach. They used Pearson product moment correlation coefficient analysis and t-statistics to test hypothesis. This study shows that cybercrime could bring about poor performance for e-businesses.

Barfi et al (2018) researched the effect of cybercrime in Ghana. The research methodology used was descriptive survey using questionnaires. Questionnaires were distributed to 1,505 students and SPSS was used for the data analysis. They found out that young people have been well acquainted with cybercrimes and unless measures are taken to prevent them from perpetrating such they are walking damage.

Gercke (2012) in understanding cybercrimes, used secondary data for the purpose of his research. He got data from already made reports, journals and papers. He used qualitative method of data analysis. He posed that the rise of cybercrimes is at an alarming rate and could dash any economy without effective combating.

Delroy (2019) researched on the impact of cybercrime on E-banking. He used quantitative approach (survey) for the purpose of the study. 5-point likert scale questionnaires were administered to numbers of bank customers. SPSS was introduced for the analysis of the collated data. A conclusion was drawn that cybercrimes could bring about slack in the use of E-banking tools by customers.

Frank and Michael (2015) studied the effects of cybercrimes on the Ghanian economy. They applied the use of secondary data gotten from various concerned government institutions. The results of their studies indicated that cyber fraud is fast gaining grounds in Ghana and it causes direct financial losses to consumers and businesses.

Bolaji et al (2016) showed in their studies with the use of questionnaires which were distributed to 170 people which was further analysed using SPSS that the impact of cybercrime can be felt on the lives, economy and international reputation of a nation.

Siddique &Rehman (2011) did a study on the impact of electronic crime in the Indian banking sector. The aim of their study was to establish and also to come up with a conceptual framework of how the criminal activities being conducted online are affecting the banking and financial sector in India. According to their study the main goal of the Indian financial sector is to eliminate all possibilities of electronic crime. This process involves identifying the necessary costs that needs to be incurred to ensure secure transactions. Siddique &Rehman identified that several criminal activities take place through network connections this include activities such as ATM fraud, money laundering and credit card fraud. This study identified one of the fears and costs that the banks anticipate is the fact that these activities may lead to loosing of customer trusts hence losing business as some may opt to other banks.

Cybercrime according to Douglas and Loader (2000) can be defined computer mediated activities conducted through global electronic networks which are either illegal or considered illicit by certain parties. In the banking sector, the cybercrimes which are committed using online technologies to illegally remove or transfer money to different account are tagged as banking frauds (Wall, 2001).

The cybercrimes according to Wall (2001) can be categorized into four major categories i.e. cyber deceptions, cyber-pornography, cyber-violence and cyber-trespass. The banking frauds are sub-categorized in cyber-deception which can be defines as an immoral activities including stealing, credit card fraud, and intellectual property violations (Anderson et al., 2012).

There are number of frauds or cybercrimes witnessed in the banking sector, like ATM frauds, Cyber Money Laundering and Credit Card Frauds. However, in general all the cyber-crimes and frauds are executed with the ultimate goal of gaining access to user's bank account, steal funds and transfer it to some other bank account. In some cases, the cyber criminals use the banking credentials like PIN, password, certificates, etc. to access accounts and steal meager amount of money; whereas in other cases they may want to steal all the money and transfer the funds into mule accounts. Sometimes, the intention of cybercriminals is to just harm the image of the bank and therefore, they block the bank servers so that the clients are unable to access their accounts (Hutchinson& Warren, 2003).

Another study done by Hannan& Blundell (2004) on the issue relating to electronic crime and how it's not the only concept to be worried about. Their study focused mainly on two case studies, one of the study was to do an analysis of the important and crucial factors affecting the breakdown of electronic criminal activities in Australia. The other part of the study tried to address the costs that are incurred under the legal environment of the banks. The study found out that there are many consequences and costs that banks face from poor implementation of legal requirements and security measures. The study presented a number of options and solutions required in tackling policy strategies for future development.

Raghavan&Parthiban (2014) focused on the effect of cybercrime on bank finances. The main objective of their study was to discuss the problem of cybercrime in the banking sector. The study did an in-depth analysis of criminal activities and scenarios within the networks and identified the actors involved in each scenario. The study also identified and documented the various types of criminal activities that are plaguing the banking sector and the motives behind those who commit such crimes. This study identified that one of the costs emanating from such vice is the financial loss which represents a direct cost and a huge issue globally impeding the development of systems.

According to Moore, Clayton & Anderson (2009) they did a paper on the economics of online crime. According to their study, online criminal activities take place as a result of a number of idle nuisance hackers. The paper identifies that the banking institutions

face a lot of problems trying to control their exposure to operational risks arising from network connections. Their study found that there are significant techniques and improvements that are viable in dealing with online crimes. The institutions must incur security costs for this to take full effect.The study suggested that in order to tackle online crime the banks must first understand the economic perspective.

Theoretical Framework

A coherent set of hypothetical, conceptual and pragmatic principles forming the general framework of reference for a field of inquiry is referred to as a theory (Hendrickson, 1970). FASB defines an accounting theory as a coherent system of interrelated objectives and fundamentals that can lead to consistent standards. Gibbins, Richardson and Warehouse (1990) opined that such theories are heavily dependent on environmental differences giving rise to different results and therefore different conditions were drawn. Numerous theories have been proffered which tried to explain the effect of cyber-crimes on depositors' accounts in listed deposit money bank in Nigeria.

Space Transition Theory

This theory was developed by Jaishankar 2007 and published in his book on Crimes of the Internet (Jaishankar 2007). There have been inadequate theoretical explanations as to why there is a rampant increase in cyber related crimes. This theory of space transition theory tries to give an explanation for the phenomena of cybercrimes. This theory states that people who usually feel their criminal nature is repressed by the physical space have a tendency to engage in crime in cyber space which otherwise they would not commit in a physical setting due to their status and role. sThis nature of crime is associated with characteristics such as identity flexibility, which make it easy for people to commit offenses. The emergence of and advancements in the field of information and communication technologies has created a range of new criminal activities within the economic and social space. Allthese activities have had a very great impact on how the financial institutions and more specifically banks are performing. As this theory states people involved in cyber related offenses are not hardcore but rather the white collar community who are within a closed community such as a bank. Detection becomes hard and the costs increase gradually at to a point where the impact on the intrusions bottom line is evident.

Therefore, the postulations of this theory is that one of the factors contributing greatly to the increasing costs that banks are facing in relation to cyber space loopholes is the complex nature and characteristics and behavior of the offenders within the information and communication environment. The postulates of the theory are: Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical

space, due to their status and position. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime. Criminal behavior of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well. Intermittent ventures of offenders in to the cyberspace and the dynamic spatiotemporal nature of cyberspace provide the chance to escape. Strangers are likely to unite together in cyberspace to commit crime in the physical space. Associates of physical space are likely to unite to commit crime in cyberspace. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cybercrimes.

History shows that the relationship between crime and technology is not new. Although the hardware has changed across the span of time but the basic crime ideas remain same. The significant change in modern time is on increase in personal computing power in a globalized communication network. The networked technology has become more than simply a force multiplier, because not only the ideas about committing a crime are shared on a global scale, but these ideas are also put to practice across the global network at a very fast speed. Internet is a set of social practices; it is the kind of purpose to which we put the internet that creates the possibility of criminal and deviant activities. The internet provides the means to link up the many and diverse networks already in existence. Since commercialization of the internet during the mid1990s, it has grown manifold. Even though majority of worldwide total internet connections are located in developed countries, the fact is that these are growing at a very fast rate in developing countries too. An Unequal access also follows along existing lines of social exclusion within individual countries and factors such as employment, income, education, ethnic disability is reflected in the patterns of internet use.These inequalities point out the social characteristics behind the emergence of cybercrime and cybercriminals. Thomas and Loader, (2000) conceptualize cybercrime as those Computer – Mediated-Activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Cybercrime has serious impact on society in the form of psychological disorder, social disorganization and economic losses. Even though all people suffer from its ill effects, the most vulnerable group is adolescent and youth.

Technology Theory

These theory is discussed broadly under computer ethics the philosophy of computing by Johnson (1985) which asserts that the response of technology to the cybercrime problems center on the use of computer security theories to design and evolve solutions that provides authentication, verification, non-repudiation and validation. These theories and models rely on the use of cryptography, steganography, network

protocols, and the use of software engineering process/models to develop systems that offer some form of protection for users and the information infrastructure.Cybercrime thrives on the web today because the internet did not inculcate in its protocols from the onset a mechanism that allows a host to selectively refuse messages. The advancement in this field only considered what the technology could do for them and what profit margins it would create, what they failed to consider carefully was what harm the technology could cause to them in terms of losses and costs. Technology theory looks at the weaknesses in within the system that were not considered in the inception stages of every piece of technology being used in financial institutions today. Banks are incurring a lot of costs today such as reputational damage costs, or opportunity costs, security costs and other costly variables due to the technological short comings within the systems being applied in their daily operations.

Today's society is in the midst of technological revolution. With advances in computers and telecommunications most businesses and many individuals have become highly dependent on computers and networks to carry out everyday activities (Howard, 1997; Sterling, 1992). Howard (1997) indicated that as of the 1996, 13 million hosts systems were accessing the internet. It has been estimated that by the year 2003, the number has risen and will have risen to a little over 200 million. The rush to embrace the new technology and has also introduced a new category of criminal activity and behavior, commonly known as hacking. Hacking is a criminal activity that relies on the dependence of computers and network, including the internet (Hutchison 1997). Those individuals engaged in hacking activities have been termed hackers. The term hacker has had many connotations over the years. It was originally associated with the outstanding and radical programmers in the computer science fields. Today it is commonly referred to an individual engaged in a form of criminal behavior, hacking. Hacking can be formally defined as either a successful or unsuccessful attempt to gain unauthorized use or access to a computer system. Society is now trying to come to an understanding of the new emerging criminal activity that knows no boundaries and creates a confusion on the preexisting criminal jurisdictions. Behavioral science has been lacking in its research into the phenomena of hacking and as such there has been a large research gap.

Opportunity Cost Theory

Anderson et al, (2013) this theory does not focus on the events that contribute to the crime but on the opportunities that emerge as a result of preventive measures to curb the crime. Proponents of this theory argue that crimes transverse between location, time, target, direction, and method of committing the crime. Anderson et al, (2013) further assert that Opportunity to commit a crime is a root cause of crime. Also, they posit that no crime can occur without the physical opportunity and therefore opportunity plays a role in all crimes, not just those involving physical property thereby

reducing opportunity of crime. This theory plays right in the concepts of cybercrime within the financial sector. Opportunities that arise within the banking environment for example poor security measure create an opportunity for someone with an intention of committing crime and it is not limited to the internal environment but also the external environment. According to Buchanan (1991) opportunity cost stands for or can be defined as the benefit forgone as a result of taking another alternative. There are many opportunities presented by various security firms to curb the rate of cybercrime within financial institutions. The decision by managers and directors of this institutions the disregard the eminent risk that lurks out there leads to firms incurring a lot of costs that otherwise would have been averted by taking the opportunities presented to them.

Research Methodology

Research Design

A research design is a plan showing how the problem under investigation will be solved. For the purpose of this study, the survey design will be adopted to actualize the research objectives, which aim at examining the effect of cyber-crimes on depositors account in listed deposit money banks in Nigeria through the administration of questionnaire.

Population of the Study

The population of the study encompasses the depositors/customers of UBA Bank in Bauchi State, who use the internet banking facility.

Sample Size and Sampling Techniques

This is the method or technique use in selecting a set of individual items from the population in such a way that those items are statistically representative of the whole population. The sampling technique to be used by the researcher is the probability sampling (simple random sampling). This is because the method is unbiased and gives each member of the population equal chance of being chosen.

Sample size is very important because it helps in minimizing the time and cost of conducting the research. A total of 120 depositors of UBA Bank will be surveyed to address the topical issues on cyber-crimes, which will serve as the representative of the whole population.

Source of Data Collection

For the purpose of this study, the source of data collection to be used by the researcher is based mainly on primary data.

Method of data collection

Primary data was used for this research study; data was obtained from questionnaires and observation**.**

Method of Data Analysis

In order to analyse the primary data obtained from the questionnaires administered, frequencies and simple percentage, mean and standard deviation was used.

Data Presentation and Analysis

Data Presentation:

The total number of questionnaires distributed by the researchers were 139 but only 103 were retrieved and used for the analysis of this research work.

Demography of Respondents:

Table 1: Gender Distribution of Respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	73	70.9	70.9	70.9
	Female	30	29.1	29.1	100.0
	Total	103	100.0	100.0	

Source: Field Survey, 2022

From the table above showing the gender distribution of respondents, it shows that 73 respondents forming about 70.9% of the total respondents were males while 30 respondents forming about 29.1% of the total respondents were females.

Table 2: Age Distribution of Respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20-30yrs	30	29.1	29.1	29.1
	31-40yrs	38	36.9	36.9	66.0
	Above 40yrs	35	34.0	34.0	100.0
	Total	103	100.0	100.0	

Source: Field Survey, 2022

From the table above showing the age distribution of respondents, it shows that 30 respondents forming about 29.1% of the total respondents were within the age range of 20 – 30 years, 38 respondents forming about 36.9% which is the highest were within the age range of 31-40 years while the remaining 35 respondents forming about 34% of the total respondents were within the age range of 40 years and above.

Table 3: Qualification

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SSCE/GCE	1	1.0	1.0	1.0
	OND	27	26.2	26.2	27.2
	HND/BSc.	67	65.0	65.0	92.2
	Higher Qualification	8	7.8	7.8	100.0

	Total	103	100.0	100.0	

Field Survey, 2022

From the table above showing the qualifications of respondents, it shows that 1 respondent forming about 1% of the total respondents was an SSCE/GCE. 27 respondents forming about 26.2% were OND holders. 67 respondents forming about 65% which is the highest were HND/BSc holders while 8 respondents forming about 7.8% of the total respondents had a higher qualification.
In order to analyse the primary data obtained from the questionnaires administered, frequencies and simple percentage, mean and standard deviation was used.

Section B of the questionnaire:
Table 4: When you access your E-mails with your personal computer or mobile phone, sometimes you receive a message or link which looks like a message from a reputable firm/institution.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	3	2.9	2.9	2.9
	D	9	8.7	8.7	11.7
	N	12	11.7	11.7	23.3
	A	59	57.3	57.3	80.6
	SA	20	19.4	19.4	100.0
	Total	103	100.0	100.0	

Source: Field Survey, 2022

From the table above, 3 respondents forming about 2.9% of the total respondents strongly disagreed with the assertion that when you access your E-mails with your personal computer or mobile phone, sometimes you receive a message or link which looks like a message from a reputable firm/institution. 9 respondents forming about 8.7% of the total respondents disagreed with the assertion. 12 respondents forming about 11.7% were neutral about the assertion. 59 respondents forming about 57.3% of the total respondents which is the highest agreed with the assertion while 20 respondents forming about 19.4% of the total respondents strongly agreed with the assertion.

Table 5: A fake and unauthorized text messages and phone calls are sent to various users requesting their Bank Verification Number (BVN), thereby having easy access to depositor's account information who unknowingly disclose the BVN.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	1	1.0	1.0	1.0
	D	7	6.8	6.8	7.8
	N	10	9.7	9.7	17.5
	A	53	51.5	51.5	68.9
	SA	32	31.1	31.1	100.0
	Total	103	100.0	100.0	

Source: Field Survey, 2022

From the table above, 1 respondent forming about 1.0% of the total respondents strongly disagreed with the assertion that a fake and unauthorized text messages and phone calls are sent to various users requesting their Bank Verification Number (BVN), thereby having easy access to depositor's account information who unknowingly disclose the BVN. 7 respondents forming about 6.8% of the total respondents disagreed with the assertion. 10 respondents forming about 9.7% of the total respondents were neutral about the assertion. 53 respondents forming about 51.5% of the total respondents which is the highest agreed with the assertion while 32 respondents forming about 31.1% of the total respondents strongly agreed with the assertion.

Table 6: Different types of cyber-crimes are carried out in order to defraud a bank depositor. Cyber-crime in form of cyber-stalking can be perpetrated through monitoring of one's online activity.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	D	8	7.8	7.8	7.8
	N	7	6.8	6.8	14.6
	A	60	58.3	58.3	72.8
	SA	28	27.2	27.2	100.0
	Total	103	100.0	100.0	

Field Survey, 2022

From the table above, 8 respondents forming about 7.8% of the total respondents disagreed with the assertion that different types of cyber-crimes are carried out in order to defraud a bank depositor. Cyber-crime in form of cyber-stalking can be perpetrated through monitoring of one's online activity. 7 respondents forming about 6.8% of the total respondents were neutral with the assertion. 60 respondents forming about 58.3% of the total respondents which is the highest agreed with the assertion while 28 respondents forming about 27.2% of the total respondents strongly agreed with the assertion.

Table 7: The ignorance of different cyber-crimes that can be carried out by fraudsters on unauthorized websites used by a bank depositor, leads to disclosure of vital information without hesitating.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	2	1.9	1.9	1.9
	D	3	2.9	2.9	4.9
	N	14	13.6	13.6	18.4
	A	62	60.2	60.2	78.6
	SA	22	21.4	21.4	100.0
	Total	103	100.0	100.0	

Source: Field Survey, 2022

From the table above, 2 respondent forming about 1.9% of the total respondents strongly disagreed with the assertion that the ignorance of different cyber-crimes that can be carried out by fraudsters on unauthorized websites used by a bank depositor, leads to disclosure of vital information without hesitating. 3 respondents forming about 2.9% of the total respondents disagreed with the assertion. 14 respondents forming about 13.6% of the total respondents were neutral about the assertion. 62 respondents forming about 60.2% of the total respondents which is the highest agreed with the assertion while 22 respondents forming about 21.4% of the total respondents strongly agreed with the assertion.

Table 8: Cyber-crime has results in depositors losing confidence with their deposits in the bank.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	1	1.0	1.0	1.0
	D	4	3.9	3.9	4.9
	N	16	15.5	15.5	20.4
	A	50	48.5	48.5	68.9
	SA	32	31.1	31.1	100.0
	Total	103	100.0	100.0	

Source: Field Survey, 2022

From the table above, cyber-crimes results in the loss of confidence in the banks concerning the safety of their deposits. 1 respondent forming about 1.0% of the total respondents strongly disagreed with the assertion that Cyber-crime has results in depositors losing confidence with their deposits in the bank. 4 respondents forming about 3.9% of the total respondents disagreed with the assertion. 16 respondents forming about 15.5% of the total respondents were neutral about the assertion. 50 respondents forming about 48.5% of the total respondents which is the highest agreed with the assertion while 32 respondents forming about 31.1% of the total respondents strongly agreed with the assertion.

Table 9: A depositor who have lose his money as a result of cyber-crime and other forms of scams, will finds it difficult to trust the bank.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	6	5.8	5.8	5.8
	D	8	7.8	7.8	13.6
	N	23	22.3	22.3	35.9
	A	56	54.4	54.4	90.3
	SA	10	9.7	9.7	100.0
	Total	103	100.0	100.0	

Field Survey, 2022

From the table above, it shows that cyber-crimes have negative impact on the level of trust of customers. 1 respondent forming about 1.0% of the total respondents strongly disagreed with the assertion that a depositor who have lose his money as a result of cyber-crime and other forms of scams, still trust and finds it more convenient and safer to deposit his money in the bank. 8 respondents forming about 7.8% of the total respondents disagreed with the assertion. 23 respondents forming about 22.3% of the total respondents were neutral about the assertion. 56 respondents forming about 54.4% of the total respondents which is the highest agreed with the assertion while 10 respondents forming about 9.7% of the total respondents strongly agreed with the assertion.

Table 10: Quality measures and internal control in the bank enhance more confidence and trust in the side of the depositors.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	3	2.9	2.9	2.9
	D	3	2.9	2.9	5.8
	N	19	18.4	18.4	24.3
	A	46	44.7	44.7	68.9
	SA	32	31.1	31.1	100.0
	Total	103	100.0	100.0	

Source: Field Survey, 2022

From the table above, 3 respondents forming about 2.9% of the total respondents strongly disagreed with the assertion that Quality measures and internal control in the bank enhance more confidence and trust in the side of the depositors. 3 respondents forming about 2.9% of the total respondents disagreed with the assertion. 19 respondents forming about 18.4% of the total respondents were neutral about the assertion. 46 respondents forming about 44.7% of the total respondents which is the highest agreed with the assertion while 32 respondents forming about 31.1% of the total respondents strongly agreed with the assertion.

Table 11: Cyber-crimes are mostly perpetrated by non-staffs of a banking institution, but yet some depositors still do not trust the bank with their deposits.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	4	3.9	3.9	3.9
	D	4	3.9	3.9	7.8
	N	11	10.7	10.7	18.4
	A	50	48.5	48.5	67.0
	SA	34	33.0	33.0	100.0
	Total	103	100.0	100.0	

Source: Field Survey, 2022

From the table above, 4 respondents forming about 3.9% of the total respondents strongly disagreed with the assertion that Cyber-crimes are mostly perpetrated by non-staffs of a banking institution, but yet some depositors still do not trust the bank with their deposits. 4 respondents forming about 3.9% of the total respondents disagreed with the assertion. 11 respondents forming about 10.7% of the total respondents were neutral about the assertion. 50 respondents forming about 48.5% of the total respondents which is the highest agreed with the assertion while 34 respondents forming about 33.0% of the total respondents strongly agreed with the assertion.

Table 12: Banks always guarantee the safety of depositor's fund, but many depositors feels that bank is not a place for safe keeping of money due to cyber-crimes.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	6	5.8	5.8	5.8
	D	18	17.5	17.5	23.3
	N	21	20.4	20.4	43.7
	A	48	46.6	46.6	90.3
	SA	10	9.7	9.7	100.0
	Total	103	100.0	100.0	

Field Survey, 2022

From the table above, it asserts that cyber-crimes pose a threat on the safety of depositors funds with the bank. 6 respondents forming about 5.8% of the total respondents strongly disagreed with the assertion that Banks always guarantee the safety of depositor's fund, but many depositors feels that bank is not a place for safe keeping of money due to cyber-crimes. 18 respondents forming about 17.5% of the total respondents disagreed with the assertion. 21 respondents forming about 20.4% of the total respondents were neutral about the assertion. 48 respondents forming about 46.6% of the total respondents which is the highest agreed with the assertion while 10 respondents forming about 9.7% of the total respondents strongly agreed with the assertion.

Table 13: Owning a bank account without using the online (internet) facilities for day-to-day transactions is an effective way of preventing cyber related crimes. Thus, ensuring fund safety.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	6	5.8	5.8	5.8
	D	20	19.4	19.4	25.2
	N	15	14.6	14.6	39.8
	A	38	36.9	36.9	76.7
	SA	24	23.3	23.3	100.0
	Total	103	100.0	100.0	

Source: Field Survey, 2022

From the table above, 6 respondents forming about 5.8% of the total respondents strongly disagreed with the assertion that owning a bank account without using the online (internet) facilities for day-to-day transactions is an effective way of preventing cyber related crimes. Thus, ensuring fund safety. 20 respondents forming about 19.4% of the total respondents disagreed with the assertion. 15 respondents forming about 14.6% of the total respondents were neutral about the assertion. 38 respondents forming about 36.9% of the total respondents which is the highest agreed with the assertion while 24 respondents forming about 23.3% of the total respondents strongly agreed with the assertion.

Table 14: Depositors have a major role to play in protecting their deposits in the bank, by surfing only authorized and reputable websites.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	4	3.9	3.9	3.9
	D	12	11.7	11.7	15.5
	N	9	8.7	8.7	24.3
	A	56	54.4	54.4	78.6
	SA	22	21.4	21.4	100.0
	Total	103	100.0	100.0	

Source: Field Survey, 2022

From the table above, 4 respondents forming about 3.9% of the total respondents strongly disagreed with the assertion that Depositors have a major role to play in protecting their deposits in the bank, by surfing only authorized and reputable websites. 12 respondents forming about 11.7% of the total respondents disagreed with the assertion. 9 respondents forming about 8.7% of the total respondents were neutral about the assertion. 56 respondents forming about 54.4% of the total respondents which is the highest agreed with the assertion while 22 respondents forming about 21.4% of the total respondents strongly agreed with the assertion.

Table 15: The disclosure of one's bank information to an unauthorized website or person by the depositor have significantly increase the occurrence of cyber-crime thereby reducing the safety of bank deposits.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	1	1.0	1.0	1.0
	D	3	2.9	2.9	3.9
	N	13	12.6	12.6	16.5
	A	66	64.1	64.1	80.6

	SA	20	19.4	19.4	100.0
	Total	103	100.0	100.0	

Field Survey, 2022

From the table above, 1 respondent forming about 1.0% of the total respondents strongly disagreed with the assertion that the disclosure of one's bank information to an unauthorized website or person by the depositor have significantly increase the occurrence of cyber-crime thereby reducing the safety of bank deposits. 3 respondents forming about 2.9% of the total respondents disagreed with the assertion. 13 respondents forming about 12.6% of the total respondents were neutral about the assertion. 66 respondents forming about 64.1% of the total respondents which is the highest agreed with the assertion while 20 respondents forming about 19.4% of the total respondents strongly agreed with the assertion.

Table 16: The policies/regulations enforced in Nigeria, which are aimed at controlling or reducing cyber-crimes have played a vital role in eliminating cyber-crimes in Nigeria.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	4	3.9	3.9	3.9
	D	8	7.8	7.8	11.7
	N	15	14.6	14.6	26.2
	A	60	58.3	58.3	84.5
	SA	16	15.5	15.5	100.0
	Total	103	100.0	100.0	

Source: Field Survey, 2022

From the table above, it is understood that the laws and regulations put by the government has helped in mitigating cyber-crime acts in Nigeria. 4 respondents forming about 3.9% of the total respondents strongly disagreed with the assertion that the policies/regulations enforced in Nigeria, which are aimed at controlling or reducing cyber-crimes have played a vital role in eliminating cyber-crimes in Nigeria. 8 respondents forming about 7.8% of the total respondents disagreed with the assertion. 15 respondents forming about 14.6% of the total respondents were neutral about the assertion. 60 respondents forming about 58.3% of the total respondents which is the highest agreed with the assertion while 16 respondents forming about 15.5% of the total respondents strongly agreed with the assertion.

Table 17: The penalty of cyber-crime perpetrators in Nigeria is fully effective, which is a measure of mitigating cyber-crime.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	8	7.8	7.8	7.8
	D	18	17.5	17.5	25.2
	N	21	20.4	20.4	45.6

	A	44	42.7	42.7	88.3
	SA	12	11.6	11.6	100.0
	Total	103	100.0	100.0	

Source: Field Survey, 2022

From the table above, 8 respondents forming about 7.8% of the total respondents strongly disagreed with the assertion that the penalty of cyber-crime perpetrators in Nigeria is fully effective, which is a measure of mitigating cyber-crime. 18 respondents forming about 17.5% of the total respondents disagreed with the assertion. 21 respondents forming about 20.4% of the total respondents were neutral about the assertion. 44 respondents forming about 42.7% of the total respondents which is the highest agreed with the assertion while 12 respondents forming about 11.6% of the total respondents strongly agreed with the assertion.

Table 18: The compliance of cyber-crime laws has effectively reduced the possible harmful effects and occurrence of cyber-crimes in Nigeria.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	7	6.8	6.8	6.8
	D	21	20.4	20.4	27.2
	N	24	23.3	23.3	50.5
	A	34	33.0	33.0	83.5
	SA	17	16.5	16.5	100.0
	Total	103	100.0	100.0	

Field Survey, 2022

From the table above, 7 respondents forming about 6.8% of the total respondents strongly disagreed with the assertion that the compliance of cyber-crime laws has effectively reduced the possible harmful effects and occurrence of cyber-crimes in Nigeria. 21 respondents forming about 20.4% of the total respondents disagreed with the assertion. 24 respondents forming about 23.3% of the total respondents were neutral about the assertion. 34 respondents forming about 33.0% of the total respondents which is the highest agreed with the assertion while 17 respondents forming about 16.5% of the total respondents strongly agreed with the assertion.

Table 19: With the formulation of governmental policies and regulations, the possible occurrence of cyber-crimes in Nigeria are reducing over time.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	SD	4	3.9	3.9	3.9
	D	19	18.4	18.4	22.3

	N	26	25.2	25.2	47.6
	A	36	35.0	35.0	82.5
	SA	18	17.5	17.5	100.0
	Total	103	100.0	100.0	

Source: Field Survey, 2022

From the table above, 4 respondents forming about 3.9% of the total respondents strongly disagreed with the assertion that with the formulation of governmental policies and regulations, the possible occurrence of cyber-crimes in Nigeria are reducing over time. 19 respondents forming about 18.4% of the total respondents disagreed with the assertion. 26 respondents forming about 25.2% of the total respondents were neutral about the assertion. 36 respondents forming about 35.0% of the total respondents which is the highest agreed with the assertion while 18 respondents forming about 17.5% of the total respondents strongly agreed with the assertion.

Descriptive Statistics

The descriptive statistics table is shown below:

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Question 1	103	1.00	5.00	3.8155	.94711
Question 2	103	1.00	5.00	4.0485	.87871
Question 3	103	2.00	5.00	4.0485	.80900
Question 4	103	1.00	5.00	3.9612	.80345
Question 5	103	1.00	5.00	4.0485	.84457
Question 6	103	1.00	5.00	3.5437	.97796
Question 7	103	1.00	5.00	3.9806	.93913
Question 8	103	1.00	5.00	3.9709	1.00446
Question 9	103	1.00	5.00	3.3398	1.06231
Question 10	103	1.00	5.00	3.5243	1.21142
Question 11	103	1.00	5.00	3.7767	1.03783
Question 12	103	1.00	5.00	3.9806	.72735
Question 13	103	1.00	5.00	3.7379	.94932
Question 14	103	1.00	5.00	3.2718	1.12192
Question 15	103	1.00	5.00	3.2913	1.16847
Question 16	103	1.00	5.00	3.4369	1.09964
Valid N (listwise)	103				

Source: SPSS V.20 Data Output

From the table above, the min and max values are 1.00 and 5.00 respectively for questions 1 to 16. The mean deviation shows the values 3.8155, 4.0485, 4.0485, 3.9612, 4.0485, 3.5437, 3.9806, 3.9709, 3.3398, 3.5243, 3.7767, 3.9806, 3.7379, 3.2718, 3.2913 and 3.4369 for questions 1 to 16 respectively and the standard deviation shows values of .94711, .87871, .80900, .80345, .84457, .97796, .93913, 1.00446, 1.06231, 1.21142, 1.03783, .72735, .94932, 1.12192, 1.16847 and 1.09964 respectively which implies that the level of dispersion among the responses of the respondents is not wide.

Discussion of Findings:

From the table 8 above, it was discovered that there are threats to the safety of bank deposits . In Table 9. it was also established that that the level of trust in the banks and their security measures diminishes with the continuous acts of cyber-crimes. Table 19 shows that governmental laws and regulations help in combating the perpetration of cyber-crimes in Nigeria. Majority of the respondents agreed that when you access your E-mails with your personal computer or mobile phone, sometimes you receive a message or link which looks like a message from a reputable firm/institution. From the table 5 above, it was discovered that majority of the respondents agreed that that a fake and unauthorized text messages and phone calls are sent to various users requesting their Bank Verification Number (BVN), thereby having easy access to depositor's account information who unknowingly disclose the BVN. From the table 6 above, it was discovered that majority of the respondents agreed that different types of cyber-crimes are carried out in order to defraud a bank depositor. Cyber-crime in form of cyber-stalking can be perpetrated through monitoring of one's online activity. From the table 7 above, it was discovered that majority of the respondents agreed that the ignorance of different cyber-crimes that can be carried out by fraudsters on unauthorized websites used by a bank depositor, leads to disclosure of vital information without hesitating. From the table 8 above, it was discovered that majority of the respondents agreed that Cyber-crime has resulted in depositors losing confidence with their deposits in the bank. From the table 9 above, it was discovered that majority of the respondents agreed that a depositor who have lose his money as a result of cyber-crime and other forms of scams, still trust and finds it more convenient and safer to deposit his money in the bank. From the table 10 above, it was discovered that majority of the respondents agreed that that Quality measures and internal control in the bank enhance more confidence and trust in the side of the depositors. From the table 11 above, it was discovered that majority of the respondents agreed that that Cyber-crimes are mostly perpetrated by non-staffs of a banking institution, but yet some depositors still do not trust the bank with their deposits. From the table 12 above, it was discovered that majority of the respondents agreed that Banks always guarantee the safety of depositor's fund, but many depositors feels that bank is not a place for safe keeping of money due to cyber-crimes. From the table 13 above, it was discovered that majority of

the respondents agreed that that owning a bank account without using the online (internet) facilities for day-to-day transactions is an effective way of preventing cyber related crimes. Thus, ensuring fund safety. From the table 14 above, it was discovered that majority of the respondents agreed that Depositors have a major role to play in protecting their deposits in the bank, by surfing only authorized and reputable websites. From the table 15 above, it was discovered that majority of the respondents agreed that the disclosure of one's bank information to an unauthorized website or person by the depositor have significantly increased the occurrence of cyber-crime thereby reducing the safety of bank deposits. From the table 16 above, it was discovered that majority of the respondents agreed that the policies/regulations enforced in Nigeria, which are aimed at controlling or reducing cyber-crimes have played a vital role in eliminating cyber-crimes in Nigeria. From the 17 table above, it was discovered that majority of the respondents agreed that the penalty of cyber-crime perpetrators in Nigeria is fully effective, which is a measure of mitigating cyber-crime. From the table 18 above, it was discovered that majority of the respondents agreed that the compliance of cyber-crime laws has effectively reduced the possible harmful effects and occurrence of cyber-crimes in Nigeria. From the table 19 above, it was discovered that majority of the respondents agreed that with the formulation of governmental policies and regulations, the possible occurrence of cyber-crimes in Nigeria are reducing over time.

Conclusion

Summary

This research work was embarked upon to look decisively on the effect of cyber-crimes on depositor's accounts in listed deposit money banks in Nigeria. It also examined the impact which cyber-crimes has on depositor's trust, depositor's fund safety and cyber-crime laws deposit account and types of deposits.

An examination of the result reveals that:

1. Different types of cyber-crimes have an impact on depositor's accounts and on the Nigerian banking industries.
2. Cyber-crimes have negative and insignificant impact on the level of confidence and on depositor's trust.
3. The extent of cyber-crimes has an impact and are significant which can affect the level of depositor's fund safety.
4. Cyber-crime laws/policies and regulations have a positive effect on curbing and mitigating the adverse occurrence of cyber-crimes in Nigeria.

Conclusions

1. There is an insignificant relationship between cyber-crimes and the level of depositor's trust. This implies that, the adverse occurrence of cyber-crimes may

affect the confidence but will not affect the level of depositor's trust, i.e. the more cyber-crimes are carried-out or perpetrated will not affect the level of depositor's trust with their deposits in the bank.

2. Depositors' fund safety is significantly influenced by the level of cyber-crimes that is carried-out, as it is felt that as more and more cyber-crimes are perpetrated by fraudsters the level of fund safety on the side of the depositors becomes low.
3. Cyber-crime laws also have a positive influence andhas a significant effect oncurbing or mitigating the continuous occurrence of cyber-crimes in Nigeria.

Recommendation

Based on the analysis carried out and the findings made in addition to the review of relevant literature and regression analysis, the following recommendations are necessary;

The financial institutions should create an awareness program on cyber-crimes that will help their local depositors' know more about cyber-crimes, how it can be carried out and how they can be affected if measures are not taken.

1. The government and the law makers should introduce and implement new policies or laws against cyber-crime perpetrators in the country, in order to further reduce the adverse occurrence of cyber-crimes which leads to loss of depositors' funds.
2. The financial institutions should make sure that there is no any loophole in the internal control system, and make sure all activities are carried out in transparent manner, in order to enhance depositor's trust and confidence.
3. Depositor's should be able to identify authorized and reputable web sites, where they can make their day-to-day transactions, and only supply their bank information's to secured sites, if they must make transactions online, and should report to their local banks if there is any suspect of leak of information.

REFERENCES

Anderson, R, C. Barton, R. Böhme. M. J. van Eeten, M. Levi, T. Moore and S. Savage, (2013). "Measuring the Cost of cybercrime" in R. Böhme (ed.), The Economics of Information Security and Privacy (Springer), Chapter 12.

A Summary of the Legislation on Cybercrime in Nigeria, Legislative & Government Relations Unit, Public Affairs Department,Federal Bureau of Investigation (2016). ATM skimming, Retrieved June 8, 2016 available online: https://www.fbi.gov/news/stories/2011/july/atm_071411.

Berney, L. (2008). "For online merchants, fraud prevention can be a balancing act". *Cards & Payments,* 21(2), 22-7.

Biener, C., M. Eling and J. Wirfs, (2015). "Insurability of Cyber Risk: An Empirical Analysis", *The Geneva Papers*, 40.

Böhme, R., S. Laube and M. Riek, (2017). "A Fundamental Approach to Cyber Risk Analysis", *Variance Journal*, Article in Press.

Cebula, J.J. and L.R. Young, (2010). "A taxonomy of Operational Cyber Security Risks", Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.

Ewepu G, (2016).Nigeria loses N127bn annually to cyber-crime— NSA available at:http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually-cyber-crime nsa/Retrieved Jun. 9, 2016.

Gates, T. and Jacob, K. (2009). Payments Fraud: Perception versus Reality, *Economic Perspectives*, 33(1), 7-15.

Hassan, A. B. Lass F. D. and Makinde J. (2012).Cybercrime in Nigeria: Causes, Effects and the Way Out, ARPN *Journal of Science and Technology*, 2(7), 626 – 631.

Hutchison S. &Davis, W. R.(2003) Computer Crime in Canada, Toronto: Thompson Canada Limited.*Journal of science. 2.*

Idolor, E. J. (2010). Bank Fraud in Nigeria: Underlying Cause, Effects and Possible Remedies: *African Journal of Accounting, Economics, Finance and Banking Research,* 6 (6) pp 62.

Jaishankar K., (2007). Space Transition Theory of Cyber Crimes, Crimes of the Internet, Pearson, ISBN-13:978-0-13-231886-0 pp.283-299.

Lakshmi P. andIshwarya M. (2015).Cyber Crime: Prevention & Detection,"*International Journal of Advanced Research in Computer and Communication Engineering*, 4(3).

Longe, O.B &Chiemeke, S.C. (2007). Beyond Web Intermediaries: Framework for Protecting Web Contents on Clients Systems. Paper Presented at the International Conference of the International Association of Engineers (IAENG) Imperial

Longe, O.B.&Chiemeke, S.C. (2008). Cybercrime and Criminality in Nigeria What roles are internet Access Points in Playing. *European Journal of Social Sciences*, 6 (4).

Maitanmi, O. Ogunlere, S. andAyinde S. (2013).Impact of Cyber Crimes on Nigerian Economy,*The International Journal of Engineering and Science (IJES*, 2(4), 45–51.

MichaelA., Boniface., A. and Olumide, A. (2014).Mitigating Cybercrime and Online Social Networks Threats in Nigeria, *Proceedings of the World Congress on Engineering and Computer Science Adu Michael Kz*, 1 WCECS 2014, 22–24.

Moore, R. (2005). "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

Moore, Clayton & Anderson (2009).The economics of online crime.*International journal of e-banking and finance,* 55.

Nida T., (2018). Impact of cyber-attacks on financial institutions. *Journal of internet banking and commerce, June 2018.* 23(2). (http://www.icommercecentral.com).

Okeshola F.B. and Adeta A.K, (2013).The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria,*American International Journal of Contemporary Research*, 3(9), 98-114.

Ojo, J. A. (2008). "Effect of Bank Frauds on Banking Operations in Nigeria".*International Journal of Investment and Finance*, 1 (1), p 103.

Okpara, G. C. (2009). "Bank failure and persistent distress in Nigeria: a discriminant Analysis". *Nigerian Journal of Economic and Financial Research.*2(1).

Office of Financial Research, 2017, "Cybersecurity and Financial Stability: Risks and Resilience", OFR Viewpoint, February.

Olasanmi, O. O (2010). Computer Crimes and Counter Measures in the Nigerian Banking Sector. *Journal of Internet Banking & Commerce*, 15(1), 1-10 (http://www.arraydev.com/commerce/jibc/)

Parthiban L. and Raghavan A. R. (2014).The effect of cybercrime on a Bank's finances,*International journal of Current Research and Academic Review*,2(2), ISSN:2347-3215, 173–178, Retrieved Feb. 2014 from www.ijcrar.com

Roger, E.S. (2008). Rogers Communications Inc, 2008 Annual Report

Romanosky, S. (2016). "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, 2 (2).

Shandilya, A. (2011). Online Banking: Security Issues for Online Payment Services. www.buzzle.com/articles.

Siddique, M.I. and Rehman, S. (2011). Impact of Electronic Crime in Indian Banking Sector: an overview, *International Journal of Business and Information Technology*, 1(2), September, 159-164.

Soni, R.R. and Soni, N. (2013). An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks, *Research Journal of Management Sciences*, 2(7), 22 27 July.

Steven M., Robyn M., Anika H., Cameron B., Stefan K., & Eva I., (2013). Comprehensive Study on Cybercrime. *A journal on United Nations Office onDrug and Crime,* (UNODC).

Udegbunam, R. I. (1998). "Bank Failure in Nigeria since Deregulation: Underlying Causes and Implication for Policy". *Benin Journal of Social Sciences*, 6 & 8, (1 & 2).

Vakkari, S.P. (1996). Library and information science: Content and scope. In J. Olaisen, E. Munch-Petersen, & P. Wilson (Eds.), Information science: From development of the discipline to social interaction. Oslo, Norway: Scandinavian University Press.

Wall, D.(2001). Hunting Shooting, and Phishing: New Cybercrime Challenges for Cybercanadians in The 21st Century. The ECCLES Centre for American Studies. http://bl.uk/ecclescentre,2009.

Wilson, P., Kunz, M.(2004). Computer crime and computer fraud. Report to Montegmery County Criminal Justice Coordination Commission, http://www.mongomerycountymd.gov (accessed September 2007).

Willson, R. (2006). Understanding the Offender/Environment Dynamics for Computer Crimes. *Information Technology and People,* 19(2), 170-186.

Wada F. and Odulaja G. O. (2014). "Electronic Banking and Cyber Crime in Nigeria – A Theoretical Policy Perspective on Causation,"*Afr J Comp & ICT*, 4(3), no. Issue 2.