Global Journal of Finance and Business Review | ***ISSN 1694-450X***
Published by AIR JOURNALS | *https://airjournal.org/gjfbr*
16/18 Avenue des Longaniers, Quatre Bornes, Mauritius
airjournals@gmail.com; enquiry@airjournal.org

RESEARCH ARTICLE

Cybercrime and Economic Sustainability of the Financial Institutions in Southeast, Nigeria

Kekii, Thankgod Lato
Department of Business Administration, Enugu State University of Science and Technology

Citations - APA

Kekii, T. L. (2023). Cybercrime and Economic Sustainability of the Financial Institutions in Southeast, Nigeria. *Global Journal of Finance and Business Review, 6(3), 63-77. DOI: https://doi.org/10.5281/zenodo.8371201*

ABSTRACT

This research work examined cybercrime and economic sustainability of the Financial Institutions in Southeast, Nigeria, the major objectives of the research are: to examine the effect of bank verification number scam on the profitability of the financial institutions and to examine the effect of phishing on the customer base of the financial institutions in the South East. This study adopted survey research design. Frequency distribution table and simple percentages were used to analyze data for this study. Findings show that Bank Verification Number Scam negatively affects the profitability of the financial institutions in the Southeast, Nigeria (76.2%). This is because scammed customers are prone to closing their bank accounts consequent upon the loss, they incurred by means of cybercrime. Phishing negatively affects the customer base of the financial institutions in the Southeast, Nigeria. (76.2%). This is because loss to the financial institution's customer is an indirect loss to the financial institution. In view of the above, the following are recommendations: financial institutions' customers, on their part, should ensure proper security controls and make sure they install the latest security updates on their computer systems and carefully select the sites they visit while the financial institutions should make it a practice to always educate their customers of the ways to avoid cybercrime attacks. The EFCC and other law enforcement agencies need to beef up their cybercrime fighting skills and abilities by continuous engagement in learning and development practices and adoption of more modern cyberspace fighting equipment.

Keywords: *Cybercrime; Economic Sustainability; Financial Institutions*

Introduction

Nigeria has a population of over 200 million and is ranked first in the number of internet users within Africa with 91 million active users (Hassan, Lass and Makinde, 2012). The country is multi-ethnic and culturally diverse and accounts for 47 percent of West Africa's population (Lakshmi and Ishwarya, 2015). Policing crime in Nigeria has been the sole responsibility of the Nigerian police for decades (Maitanmi, Ogunlere and Ayinde, 2013), however, maintaining of public security is one of the biggest challenges facing the country due an ineffective police force that has rendered the Nigerian government handicapped to function maximally (Michael, Boniface and Olumide 2014). This problem is further compounded with the coming of the internet and smartphones which has made the internet more accessible and affordable even to criminals (Ndible, 2016).

Due to the integration of digital technology and accessibility of the internet (Okeshola and Adeta, 2013), cybercrime has become a popular crime in Nigeria due to inadequate policing, and lack of enforcement of relevant laws and policies in the country (Parthiban and Raghavan, 2014). The negative socio-economic impact of cybercrime in Nigeria, propelled the government to take drastic measures such as creating another agency, enacting cybercrime laws, and partnering with stakeholders to drastically reduce the activities of cybercriminals (Wada and Odulaja, 2014). Thus, the Economic and Financial Crimes Commission (EFCC) was established through an act of parliament called the EFCC Act (2004) and Advance Fee Fraud and other Fraud Related Offences (AFF) Act (2006) to investigate financial crimes such as cybercrime (Iroegbu, 2014). However, over the years, the adequacies of the laws and policies in fighting cybercrime have been limited (Chawki et al., 2015), therefore, the Cybercrime Prohibition, Prevention Act (2015) was signed into law to sanitize the Nigerian cyberspace (Jolaosho, 1996). Table below illustrating the population and internet user's vis a vis the internet crime rate in Nigeria and other countries.

S/N	COUNTRY*	POPULATION (2017 EST)	INTERNET USERS (DEC 2000)	INTERNET USERS (JUNE 2017)	PENETRATION	INTERNET CRIME (VICTIMS)	FACEBOOK SUBSCRIBERS 30-JUN-2017
1	**Nigeria**	191 million	200,000	91 million	47.7%	18th	16 million
2	**Canada**	36 million	-	33 million	90%	1st	23 million
3	**India**	1.3 billion	47 million	462 million	34.4%	2nd	241 million
4	**UK**	65 million	-	62 million	94.8%	3rd	44 million
5	**Australia**	24 million	6 million	21 million	88.2%	4th	15 million
6	**France**	64 million	-	56 million	86.8%	5th	33 million
7	**Brazil**	211 million	-	139 million	65.9%	6th	139 million
8	**Mexico**	130 million	-	85 million	65.3%	7th	85 million
9	**China**	1.3 billion	22 million	738 million	53.2%	8th	1.8 million
10	**Japan**	126 million	47 million	118 million	94%	9th	26 million

Source: Adapted from Internet Crime Report 2016 & Internet World Stats 2017

The Internet Crime Report (2016) ranked Nigeria 18th in the world in terms of victim's loss, which is seen as a significant improvement to the Internet Crime Report (2010) that ranked the country 3rd after the United States and the United Kingdom with the highest prevalence of cybercrime in the world.

In recent times, the financial institutions are increasingly relying on the internet and other information technology tools to engage in profitable financial services. While these developments allow for enormous gain in productivity, efficiency, and communication they also create a loophole for unscrupulous individuals to commit cybercrime and destroy the economic sustainability of financial institutions. This research shall investigate cybercrime in relation to financial institutions from the perspective of security agency (EFCC) and proffer solutions to ameliorate cybercrime (Jolaosho, 1996).

Statement of Problem

Undeniably, the policing of crime using the traditional security agencies has many limitations (Justine, 2010), and the integrity of the security agencies has been eroded by its failure to perform its constitutional responsibilities to the society (Nwachukwu, 2012). Due to that, cybercrime has had a negative impact on the sustainability of financial institutions. Lakshmi and Ishwarya (2015) argued that cybercrime transaction worth £300 million, €200 million, and $500 million were stopped between 2003 and 2007, and recently it cost Nigerian financial institutions approximately $13.5 billion dollars in 2012 (Landwher, Bull McDermott and Choi, 1994). The problem of cybercrime in Nigeria is further compounded by the increased usage of the internet for fraudulent activities (Laura 2011) and the lack of cyber user awareness, which makes internet users vulnerable to be exploited by criminals online (Lewis 2002). Even

though, the Nigerian government have developed appropriate legal and institutional frameworks in securing the Nigerian cyberspace (Maitanmi, Ogunlere and Ayinde, 2013), policing the cyberspace would require governments and legal systems to continuously adapt to new technologies and strategies in tackling cybercrime (Niza, 2012). Currently, there is a need for the Nigerian government to work together in strengthening the legal frameworks for cybersecurity and enforcing existing laws to reduce the impact of cybercrime in the society (Okafor, 2011).
This research shall investigate various cybercrimes in relation to the activities of the security agencies towards ensuring sustainability of financial institutions in the Southeast.

Objectives of the Study
The general objective of the study is to investigate cybercrime and economic sustainability of the financial institution in Southeast. The underlisted are the specific objectives of the study:

1. To examine the effect of bank verification number scam on the profitability of the financial institutions in Southeast
2. To examine the effect of phishing on the customer base of the financial institutions in the Southeast

Research Questions

1. To what extent has bank verification number (BVN) scam affected the profitability of financial institutions in Southeast?
2. To what extent has Phishing affected the customer base of the financial institutions in the Southeast?

Statement of Hypothesis
The following hypothesis will guide this research work:

i. H_0: The extent to which bank verification number (BVN) scam has affected the profitability of financial institutions in Southeast is low
ii. H_1: The extent to which bank verification number (BVN) scam has affected the profitability of financial institutions in Southeast is high

Significance of the Study

In recent years, there has been a surge in the use of mobile devices, computer systems and the Internet in the financial institutions. Likewise, the crimes committed by cybercriminals that use the Internet, mobile devices and computer systems have gained momentum. Cybercrime prevention at financial institutions requires that information should be well secured and managed to prevent breaches in the financial institutions networks and protect the customers from cybercriminals (Herzog, 2010; Whitman & Mattord, 2011). This study will be of importance because it aims to contribute to the existing literature that educates both staff and customers of financial institutions of the potential vulnerabilities and threats associated with financial institutions' IT resources, and online transactions. The study will also be of importance to people involved in the financial services information and network management portfolios because it proposes security measures on how to protect the financial institutions information and network resources against the cybercrimes.

Scope of the Study
The scope of the study is Cybercrime and Economic Sustainability of Financial Institutions in Southeast Nigeria. For effective coverage, the work shall be limited to the perspectives of Economic and Financial Crimes Commission branches in the Southeast.

Limitations of the Study
Due to lack of access to cybercriminals, the study focused only on the EFCC staff's perspective as far as the effectiveness of cyber-security measures is concerned. The researcher acknowledges that interviews with other cyber-security experts could have been conducted to get more insights on what financial institutions should do to shield themselves from cyber-attacks for enhanced economic sustainability. Furthermore, this study focuses on the Southeast. The implication is that the outcome may not be generalized to other states in Nigeria because states are peculiar in nature. What obtains in one state may not obtain in another state.

Review of Related Literature

Conceptual Review

Cybercrime is a topical issue that has been discussed by many people from various perspectives (Okeshola and Adeta, 2013). One reason for this is the huge losses that were attributed to it. It was estimated that, global losses to cybercrime are about $400bn annually (CSIS, 2014). Others have put it at a higher value of $445bn. As technology evolved, so did the definitions of cybercrime. According to Saul (2007), cybercrime is an offence, with a criminal motive, committed against an individual or group of persons intentionally to harm the reputation of the victims as well as cause irreparable damage to hardware of sensitive infrastructure, including internet and mobile phones. Symantec Corporation, the world's biggest computer security company, defined cybercrime as any crime committed using a computer, network or hardware devices (Theohary and Finklea 2015). To explain what cybercrime means, let us look at the slit meaning of the words 'cyber' and 'crime'. The word 'cyber' has its origins from 'cybernetics', which refers to the science of communication that deals with the study of automatic control systems (much like the human nervous system/ workings of the brain) as well as the mechanical-electrical communication systems. Cyber is therefore a derivative of cybernetics used to describe interactions that relate to or involve computers or networks. 'Crime' refers to the specific actions or inactions due to negligence that is injurious to public welfare or morals, and one that is legally prohibited. Cybercrime (e-crime or hi-tech crime) is a global phenomenon which takes place in the cyberspace i.e., in the world of computers and on the internet. Cybercrime involves using specialized applications in computers with the internet by technically skilled individuals to commit crime. The aftermath of such crimes may threaten a nation's security architecture and financial health (Saul, 2007). So, cybercrime can simply be explained as a crime carried out with the aid of a computer system. It refers to criminal acts that are facilitated using the internet.

Cybercrime is a form of criminal activity that involves the use of a virtual medium such as the Internet. It also involves illegal access to computer data via the Internet (Theohary and Finklea 2015). It is one of the prevalent, and perhaps the most challenging and intricate problem in cyberspace (Wada and Odulaja 2012). According to World Development Indicator WDI (2016), it can simply be described as criminal offences that can be carried out online with the aid of technological infrastructure. Also, according to Hassan, Lass, and Makinde (2012) it is "any criminal activity that uses a computer either as an instrumentality, a target or a means for perpetuating crimes". Furthermore, Maitanmi, Ogunlere and Ayinde (2013) described cybercrime as offences that are committed against individuals, property, or government, with the motive to cause physical or mental harm or even cause reputational damage, either directly or indirectly, using modern technologies that comes with the Internet and telecommunication devices. In addition, the literature also shows that cybercrime can also be referred to as a harmful act which involves acquisition and manipulation of organizational data. Such crimes can threaten a nation's security, universities' infrastructure or individual's computer systems, communication devices and even the cyberspace.

Types and Dimension of Cybercrimes

In the past, little was known about cybercrime, but as the internet grew worldwide, the unintended consequences of computerization manifested in global notoriety. It is a worldwide problem that costs countries, businesses, and individuals billions of dollars. The first reported cybercrime was committed by employees of a company in the 1960s and involved the company's mainframe computer (Maitanmi et al., 2013). In recent times however, it not only involves employees of companies or nations, but includes organized criminal gangs, terrorists, rogue governments, and individuals (in isolated cases).

Lewis (2002) identified four important elements when assessing the risks of cybercrime. First, infrastructure as a target: cyber warfare and terrorism were placed in the historical context of attacks against infrastructure. Second, routine failure versus cyberattacks, examining cyber-attacks against a backdrop of routine infrastructure failures. Third, weapons of mass annoyance: the measurement of the dependence of infrastructure on computer networks and the redundancy already present in these systems. Finally, hacking and terror: for the case of cyber-terrorism, the use of cyber weapons in the context of the political goals and motivations of terrorists, and whether cyber-weapons are likely to achieve success.

According to Ndibeh (2016), computer crime encompasses criminal activities which can aptly be categorized by its unique typology of computer-related crime, comprising conventional crimes in which computers are instrumental to the offence. This is the case of child's pornography and intellectual property theft; attacks on computer networks; and conventional criminal cases in which abound undeniable evidence in digital form. The kinds of criminality include the following and is not limited by the underlisted issues:

i. Interference with lawful use of a computer: cyber vandalism and terrorism; denial of service; insertion of viruses, worms, ransomware and other malicious code.
ii. Dissemination of offensive materials: pornography/child pornography; on-line gaming/betting; racist content; treasonous or sacrilegious content.
iii. Threatening communications: extortion; cyber-stalking.
iv. Forgery/counterfeiting: ID theft; IP offences; software, CD, DVD piracy; copyright breaches et cetera.
v. Fraud: payment card fraud and e-funds transfer fraud; theft of Internet and telephone services; auction house and catalogue fraud; consumer fraud and direct sales (e.g., virtual 'snake oils'); on-line securities fraud.
vi. Others include illegal interception of communications; commercial/corporate espionage; communications in furtherance of criminal conspiracies; electronic money laundering.

Cybercrimes in the Financial Institution

The life wire of the banking sector is the internet. Currently, banks all over the world are taking advantage and incorporating opportunities brought about by e-banking which is believed to have started in the early 1980's (Justin 2010). As the security level in this sector becomes stronger, the strength and tactics of these fraudsters increases also. Various lucrative attacks have been launched and unfortunately, many have succeeded. In general, cybercriminals execute fraudulent activities with the goal of accessing user's bank account to either steal or/and transfer funds to another bank account without rightful authorization. However, in some rare cases in Nigeria, the intention of cybercriminals is to cause damage to the reputation of the bank by denying service to users (Parthiban, 2014) and sabotaging data in computer networks of organizations.

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 account details. In addition, phishing sites were created to acquire such information for insalubrious activities on the bank account.

Phishing: Phishing is simply the theft of an identity. It involves stealing personal information from unsuspecting users and it is also an act of fraud against the authentic, authorized businesses and financial institutions that are victimized (Wada 2012). Phishing scams are ubiquitous and are exponentially increasing. It has become one of the fastest growing cybercrimes in Nigeria. In this jet age of technology, hoipolloi subscribe to a plethora of sites using their email addresses and are therefore expecting to receive mails of updates of their membership or subscription. So, it seems natural when users get regular mails from such organizations. Fraudster have devised a means to mimic authorized organizations and retrieve confidential information from clients. In Phishing email messages, the fraudsters find a way to convince and gain the trust of users. An instance of such mail is shown in the figure below showcasing a fraudster trying to build the trust of a client to convince them to give up personal banking information. In Nigeria, phishing mails are mostly carried out on bank customers.

Theft of Bank Cards: The theft of bank cards has evolved from the physical theft of the card to simply the theft of the numbers. Today, bank card hackers do not need to be in the same country to steal other people's identities. Fraudsters make use of hidden cameras to record ATM card pins and numbers in distinct places such as an eatery payment using Pos, or at the ATM. According to the Federal Bureau of Investigation (FBI), a method known as ATM

skimming can be used and it involves placing an electronic device on an ATM that scoops information from a bank card's magnetic strip whenever a customer uses the machine (FBI, 2011). Also, another cybercrime carried out via this means in Nigeria includes internet order fraud. Internet order frauds involves fraudster inputting stolen cards numbers on online commercial sites to order goods. Credit card numbers or ATM numbers can be stolen by hackers when users type the credit card number into the Internet page of the seller for online transaction. Different applications can be used to retrieve the information such as key loggers at cybercafés or cloned websites.

Cyber-theft/Banking Fraud: Hackers target the vulnerabilities in the security of various bank systems and transfer money from innumerable accounts to theirs. Most cybercriminals transfer bantam amounts like five 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.

The Impact of Cybercrime on the Economy and Nigerian Financial Institution

Advancement in ICT no doubt brought with it, unlimited opportunities (particularly internet and financial software) for banking institutions in Nigeria. It facilitated ease of transactions and reduced cost for both depositors and the banking institutions. However, it also introduced its own peculiar risks through cybercrimes which have negatively impacted the industry and the economy in no small measure. The threats are enormous to citizens of any nation. Some of the impacts of cybercrime on the Nigerian economy are discussed below:

- **i.** Cybercrime is no doubt providing a dent on Nigeria's image which remains a crucial source of national embarrassment for the country. The fear of cybercrime has made several persons to avoid the use of ICT. This has a negative impact on the welfare of the citizenry and investors. Confidence in a nation's financial system could be eroded by activities of cyber criminals. Potential investors and tourists are equally scared, and the image of citizens is tainted.
- **ii.** Citizens face reputational risk - in today's global economy, a nation cannot afford to have its reputation and that of its financial system tarnished by being associated with cybercrime. It becomes a problem for a citizen to engage in meaningful social interaction with the rest of the world when every citizen is perceived as a potential scammer.
- **iii.** The perceived loss of confidence may also affect the country's developmental progress, as foreign investments find it difficult to flow into the economy. This gives the nation an economic pariah status. The lack of confidence in the banking sector because of cybercrime can also be devastating on the economy.
- **iv.** Impact on the financial Services Industry. It is well-known that a buoyant economy thrives on an effective and efficient financial system. Cyber-attacks are usually skewed toward deriving financial gains. Banks, other financial institutions, businesses, and individuals bear the losses of such acts.

Some economic impacts of cybercrime in Nigeria include:

- **a.** Increases in the operating cost of businesses due to huge expenses incurred on purchase of security software applications to reduce the rate of cyber-attacks.
- **b.** Failure of institutions arising from huge losses from cybercrimes - this could lead to a loss in confidence in the financial institutions and a possible run on them (where banks are involved), with possible contagion effects.
- **c.** Increase in provisions - while loan loss provisions are predictable with some level of recoverability, losses arising from cybercrimes are not predictable; leading to increase in irrecoverable provisions and a consequent depletion of capital for banks and business entities. This could undermine confidence level in the nation's financial system.
- **d.** Regulators and Supervisors of licensed deposit-taking institutions may be required to use taxpayers' money to resolve problems arising from cybercrimes. This may be in the form of problematic deposit-taking institutions receiving a lifeline through Prompt Corrective Actions or where institutions (banks) eventually fail, there would be the depletion on the Deposit Insurance Fund (DIF) to pay off depositors. Some of the modes through which cybercrimes are perpetrated in Nigeria include theft/cloning of customer bank cards; fraudulent transfer or withdrawal of customer funds; hacking of banking software for the transfer of funds; cloning of bank/business websites to deceive customers and sending

of emails/text messages requesting for personal information or assistance from unsuspecting individuals. Over the years, Automated Teller Machine (ATM) cards and Web Based (Internet Banking) frauds have contributed significantly to fraud cases in the Nigerian banking system. The Table below shows the contribution of cybercrimes to total fraud loss in the Nigeria banking system between 2011 and 2016.

Year	Cybercrime losses(ATM & INTERNET) (₦ billion)	Growth rate of cybercrime losses (%) year-on- year	Total Fraud Loss (₦ billion)	Contribution Of Cyber Crimes To Total Fraud (%)
2011	0.115	-	4.071	2.82
2012	0.794	590.4	4.516	17.58
2013	2.268	185.6	5.757	39.40
2014	4.438	95.6	6.193	71.66
2015	1.361	-69.3	3.173	42.89
2016	1.058	-22.2	2.4459	43.26

Source: NDIC Annual Report (2011-2016)

The second column shows the actual losses from cybercrime over the years, while the third column depicts the year-on-year growth rate. Beginning from 2015, one can infer the gradual decline in losses from cybercrimes in Nigeria. It declined further in 2016 to 22.2%. That largely reflects the positive performance of agencies such as the EFCC in checking cybercrime. It is also suggestive of the effectiveness of the Nigerian Cybercrime Act, 2015. On the flip side, Table 2 shows that, in recent times, cybercrime losses contribute almost half of the total banking fraud losses reported. In 2011, it was only 2.8%. It increased significantly to 71.6% in 2014 and declined gradually to 43.2% in 2016. A major deduction from this is that the cyber space is a key channel through which financial fraud is being perpetrated in the Nigerian financial institutions. This therefore reiterates our earlier stance that increased efforts should be geared towards curbing this criminal activity.

Theoretical Framework

Borgatti (1999) pinpointed a theoretical framework as a collection of interrelated concepts, in which a researcher determines what to be measured, and the corresponding relationships. To understand and explain how cybercriminals perform their activities, the researcher adopted Routine Activity Theory (RAT) as a theoretical framework to guide the study. Routine Activity Theory (RAT) The routine activity theory is one of the theories of rational choice and criminology that have been used extensively in research to explain criminal inclinations. Cybercrime is a type of these criminal inclinations. Even as cybercrimes are perpetrated online, they are criminal and as such RAT could be used to explain cybercriminal behavior. The theory has three constructs: suitable target, offender, and absence of suitable guardian. This theory was proposed by Cohen and Felson in 1979 (Felson & Cohen, 1979) in their article titled “Social Change and Crime Rate Trends: A Routine Activity Approach”. The theory attests that “Crime occurs when there is an intersection in time and space of a motivated offender, an attractive target, and a lack of capable guardianship.

Empirical Review

Lakshmi and Ishwarya (2015) did a study on the impact of cybercrime in the financial institution. The aim of their study was to establish and to come up with a conceptual framework of how the criminal activities being conducted online are affecting the financial institutions in Nigeria. 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 financial institutions anticipate is the fact that these activities may lead to loosing of customer trusts hence losing business as some may opt to other financial institutions.

Another study done on the issue relating to cybercrime and how it is not the only concept to be worried about. Their study focused mainly on two case studies, one of the studies 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 financial institutions. The study found out that there are many consequences and costs that financial institutions face from poor implementation of legal requirements and security measures. The study presented several options and solutions required in tackling policy strategies for future development.

Maitanmi, Ogunlere and Ayinde (2013) focused on the effect of cybercrime on finances of the financial institutions. The main objective of their study was to discuss the problem of cybercrime in the financial institutions. 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 financial institutions 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 Ndible (2016) they did a paper on the economics of cybercrime. According to their study, online criminal activities take place because of a number of idle nuisance hackers. The paper identifies that the financial 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 fraud. The institutions must be willing to incur security costs for this to take full effect and secondly the study suggested that to tackle cybercrime, the financial institution must first understand the economic perspective.

Methodology

Research Design

The research design used here is the survey design. It is chosen because of its popularity as the best available method to the management and social services researchers. Also, it is known for its benefit of being cost effective in comparison with the amount of information gathered with little stress. It is important to note that the survey method may involve all or some people. Hence, the association concepts of population and sampling will be used.

Sources of Data

There are two main sources of data for this study. These were secondary and primary sources.

Primary Data

This will be a representative of the actual data that will be obtained for the purpose of the research study. It will include raw facts such as answered questionnaire. This type of data will be collected and then analysed to get the information required. Questionnaires and semi structured interview guide will be used as the major data collection instruments.

Secondary Data

This consists of already published materials in books, journals, and unpublished academic dissertation.

Population of the Study

The population (Administrative Division, Capacity Development Division, The Research and Publication Division, Networking and Collaboration Division and Cadets Division) of this study is made up of employees of three zonal offices of Economic and Financial Crimes Commission, in Anambra (60), Enugu (90), and Imo (50) States, totaling 200. The population is made of male and female between the ages of 26 and 48. These organizations were chosen because of data available and ease of access to the EFCC for questionnaire completion. The selection of the organization was done through random sampling.

Determination of Sample Size

This study adopted Purposive sampling (also known as judgment, selective or subjective sampling). It is a sampling technique in which researcher relies on his or her own judgment when choosing members of population to participate in the study (Joel 2011). Purposive sampling is a non-probability sampling method and it occurs when "elements selected for the sample are chosen by the judgment of the researcher. Researchers often believe that they can obtain a representative sample by using a sound judgment, which will result in saving time and money". This study adopted purposive sampling which implies the use of the entire population. Hence there was no need for sample size determination.

Sampling Technique

The strategy of administration consisted also of direct appeal to respondents to complete the questionnaire promptly. In some restricted case, a telephone approach was used to get at respondents who could not be reached directly. These strategies yielded a significant return of appropriately completed questionnaire.

Method of Data Collection

The instrument used in collecting data was a structured questionnaire which was organized in sections reflecting the research questions.

Validity of the Instrument

Content validity was adopted. Copies of the instrument for the study were given to three research experts of ESUT Business School for validation. They vetted them in terms of appropriateness of content, clarity of words and relevance to the objective of the research. Various corrections and recommendations made by the experts were implemented accordingly. Specifically, the validators made some grammatical corrections, reframed some items, cancelled some items, and added others. Thus, the instrument which had 26 items ended up with 22 valid items. Consequently, the validators recommended that the instrument be used for the study.

Reliability of Research Instrument

Instrument used was first given to a certain group of workers from the organizations under study to complete. It was later collected from them and evaluated. Same questionnaire was given to another group of workers to complete which was later retrieved from them. In all, it was observed that degree of understanding of the questionnaire was the same across board, suggesting consistency of the instrument.

Method of Data Analyses

The main method of analyzing data collected in this study will be the simple percentage for testing the questionnaire. The formular for percentage is given as:

$$\frac{a}{b} \times \frac{100}{1}$$

where; a = numerator (number of respondents to an item).
b = denominator (total respondents in sample),

Data Presentation

This section presents data in tables for ease of understanding. Data presentation is defined as the process of using various graphical formats to visually represent the relationship between two or more data sets so that an informed decision can be made based on them. Data is presented and analyzed below:

Table 1: Analysis of Questionnaire Return

Alternatives	Frequency	Percentage
Questionnaires Distribution	200	100
Returned Questionnaire	150	75
Dropped Questionnaire	50	25
Questionnaire Applied	**150**	**75**

Source: Field Survey 2022

The sample of this study was drawn from members of staff of the organizations under study. The questionnaire administration covered a period of three weeks considering the nature of the population. The entire sample frame was effectively covered in the exercise. However, following logistic problems occasioned by the disperse nature of the population, follow up on all the respondents was not effectively sustained resulting to fifty questionnaires not returned. In all therefore, 150 questionnaires were correctly completed and returned, representing 75% of the questionnaire distributed.

Analysis of Responses to Questionnaire

Table 2: Qualification of Respondents

S/N	Proposition	Responses	Frequency	%
1	Highest level of academic qualification	WAEC/OND	71	47.3
		B.Sc./ Equivalent	41	27.3
		Master's degree	38	25.3
		Total	150	100

Source: Field Survey 2022

Above table shows that 47.3% of the respondents has WAEC/OND qualification. 27.3% holds B.Sc./equivalent while 25.3% holds Master's degree. This goes to show that the respondents are well informed and educated people.

Table 3: Increase in Cybercrime in the Southeast

Cybercrime is on the increase in the financial institution in Southeast	*Response*	*Frequency*	*%*
	Strongly agree	30	20
	Agree	70	46.5
	Disagree	20	13.3
	Strongly disagree	30	20.2
	Indifferent	0	0
	Total	150	100

Source: Field Survey 2022

Question was asked to ascertain whether cybercrime is on the increase in the southeast or not. 20% of the respondent strongly agree that cybercrime is on the increase in financial institutions in the Southeast. 46% also agree to above claim. On the other hand, 13.3% disagree while20.2% strongly disagree.

Table 4: Cybercrime and Sustainability of Financial Institution

Cybercrime hampers the sustainability of Financial Institutions

Response	*Frequency*	*%*
Strongly agree	60	40
Agree	54	36.2
Disagree	15	10
Strongly disagree	20	13.3
Indifferent	1	0.5
Total	150	100

Source: Field Survey 2022

Table 4 shows that 40% of the respondents strongly agree that cybercrime hampers the sustainability of financial institutions. 36.2% also agree. On the other hand, 10% disagree while 13.3% strongly disagree. 0.5% of the respondent were indifferent.

Table 5: Frequency of Bank Verification Number Scam

Bank Verification Number Scam is common in the financial institution

Response	*Frequency*	*%*
Strongly agree	60	40.1
Agree	50	33.3
Disagree	20	13.3
Strongly disagree	20	13.3
Indifferent	0	0
Total	150	100

Source: Field Survey 2022

Table 5 shows that 40.1% of the respondent strongly agree that bank verification number scam is common in the financial institution. 33.3% also agree. 13.3% disagree while another 13.3% strongly disagree.

Table 6: Effect of BVN Scam on Profitability of the Financial Institution

Bank Verification Number Scam negatively affects the profitability of the financial institution.

Response	*Frequency*	*%*
Strongly agree	60	40
Agree	54	36.2
Disagree	15	10
Strongly disagree	20	13.3
Indifferent	1	0.5
Total	150	100

Source: Field Survey 2022

Table 6 shows that 40% of the respondent strongly agree that bank verification number scam affects the profitability of the financial institution. 36.2% also agree. On the other hand, 10% of the respondent disagree while 13.3% strongly disagree. 0.5% of the respondent were indifferent.

Table 7: Effect of Phishing on Customer Base of Financial Institution

Phishing affects the customer base of the financial institution negatively

Response	*Frequency*	*%*
Strongly agree	60	40
Agree	54	36.2
Disagree	15	10
Strongly disagree	20	13.3
Indifferent	1	0.5
Total	150	100

Source: Field Survey 2022

It can be seen from above table that 40% of the respondents strongly agree that phishing affects the customer base of the financial institution. Similarly, 36.2% agree. 10% disagree. 13.3% disagree. 0.5% remained indifferent.

Table 8: Effect of Cybercrime on the Confidence of Customers

Increasing cybercrime in the financial institution affects the confidence of the customers

Response	*Frequency*	*%*
Strongly agree	50	33
Agree	60	40
Disagree	10	6.7
Strongly disagree	25	16.7
Indifferent	5	3
Total	150	100

Source: Field Survey 2022

Table 8, 33% of the respondent strongly believe that the increasing cybercrime in the financial institution negatively affects the confidence of the customer. 40% of the respondent also agree. On the other hand, 6.7% disagree while 16.7% strongly disagree. 3% of the respondent were indifferent.

Table 9: Performance of the EFCC in Fighting Cybercrime

EFCC is living up to expectation in fighting cybercrime in the financial institution.

Response	*Frequency*	*%*
Strongly agree	42	28
Agree	7	4.6
Disagree	50	33.3
Strongly disagree	51	34.1
Indifferent	0	0
Total	150	100

Source: Field Survey 2022

It can be seen from above table that 28% of the respondent strongly agree that EFCC is living up to expectation in fighting cybercrime in the financial institution. 4.6% agree. 33.3% disagree. 34.1% strongly disagree.

Test of Hypotheses

In this section, the hypothesis proposed will be tested using chi-square statistical technique at 5% level of significance.

Hypothesis I:

H_0: The extent to which bank verification number (BVN) scam has affected the profitability of financial institutions in Southeast is low

H_1: The extent to which bank verification number (BVN) scam has affected the profitability of financial institutions in Southeast is high

Step II: The test statistics is $X^2 = \frac{\sum(O-E)}{E}$

Step III: Level of significance used is 5% i.e., 0.05
Step IV: The degree of freedom is df = K – 1 = 2-1 = 1
Step V: The critical value is $X^2 = 3.841$
Step VI: Computation of the test statistics

Alternative Response	***O***	***E***
Strongly Agree	25	25
Agree	30	25
Disagree	5	25
Strongly Disagree	90	25
Indifferent	0	25
Total	150	150

Source: Field Survey 2022

$$X^2 = \frac{\sum (O-E)^2}{E}$$

$$X^2 = \frac{(25-25)^2}{25} + \frac{(30-25)^2}{25} + \frac{(5-25)^2}{25} + \frac{(90-25)^2}{25} + \frac{(0-25)^2}{25}$$

$$X^2 = 0 + 1 + 16 + 16.9 + 25$$

$$X^2 = 58.9$$

Step VII: 58.9 > 3.841
Step VIII:

Decision:
We can see that the value of calculated X^2 is greater than the table value of X^2. We therefore reject the null hypothesis and accept alternate hypothesis thus the extent to which bank verification number (BVN) scam has affected the profitability of financial institutions in Southeast is high.

Summary of Findings
The following are the summary of findings in line with the objective of the study:

i. Bank Verification Number Scam negatively affects the profitability of the financial institutions in the Southeast, Nigeria (76.2%). This is because scammed customers are prone to closing their bank accounts consequent upon the loss, they incurred by means of cybercrime.
ii. Phishing negatively affects the customer base of the financial institutions in the Southeast, Nigeria. (76.2%). This is because loss to the financial institution's customer is an indirect loss to the financial institution.

Conclusion
The rising spate of cybercrime globally and its attendant negative consequences has continued to call for immediate actions. As technology advances, novel methods are used to perpetrate cyber related crimes. Nigeria and Southeast in particular, is not immune to these attacks. It is expected that the cost of cybercrime may continue to increase as the convergence of IT and finance (FINTECH) becomes obvious globally and with the rise of crypto currency and the anonymity of transactions. There is therefore the need to take proactive steps to curb the menace. Cybercrime poses a great risk to the financial institutions, hence the need to institute an effective risk management system and enhancement of the capacity to carry out forensic investigation to tackle it. Also, collaborative efforts of governments, corporate entities and the citizenry could play a vital role in checking cybercrimes. Cyberspace is a challenging environment that is fast and continuously evolving. Hence, the challenge is for those charged with the responsibility of security in various quarters to be abreast of developments in the cyber world. The economic vitality of the financial institutions largely depends on a stable, safe, and resilient cyberspace.

Recommendation

Cybercrime cannot be easily and completely wiped out but can be reduced. However, collaborative efforts of individuals alongside with government intervention could go a long way to minimize it to a reasonable level. The following are recommendations of the study:

i. Financial institutions' customers, on their part, should ensure proper security controls and make sure they install the latest security updates on their computer systems and carefully select the sites they visit while the financial institutions should make it a practice to always educate their customers of the ways to avoid cybercrime attacks.
ii. The EFCC and other law enforcement agencies need to beef up their cybercrime fighting skills and abilities by continuous engagement in learning and development practices and adoption of more modern cyberspace fighting equipment.

Suggestion for Further Studies

It is suggested that further studies should be carried out on the Practicability of Enforcement of Laws Relating to Conviction of Cyberspace Criminals in Nigeria.

References

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

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

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

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

Ndible, N. (2016). Practical Application of Cyber Crime Issues. Retrieved May 6, 2016, from http://ijma3.org/Admin/Additionals/ Cybercrime/Nibal%20Idlebi%20Presentation.pdf

Okeshola, F. B., & 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.

Parthiban, L., & Raghavan, A. R. (2014). The effect of cybercrime on a Bank's finances. *International Journal of Current Research and Academic Review, 2*(2), 173–178. Retrieved February 2014, from www.ijcrar.com

Wada, F., & Odulaja, G. O. (2014). Electronic Banking and Cyber Crime In Nigeria – A Theoretical Policy Perspective on Causation. *Afr J Comp & ICT, 4*(3)

Iroegbu, E. (2016). Cyber-Security: Nigeria Loses over N127bn annually through Cybercrime. Retrieved June 9, 2016, from http://www.thisdaylive.com/index.php/2016/04/18/cyber-security-nigeria-loses-over-n127bn-annually-through-cybercrime/

Jolaosho, A. O. (1996). Some Popular Perceptions of Poverty in Nigeria. Quoted in UNDP Human Development Report on Nigeria. Lagos: UNDP.

Justin, P. (2010). Top Five Computer Crime and How to Protect Yourself from Them. Publication of Justin Plot.

Landwher, C. E., Bull, A. R., McDermott, J. P., & Choi, W. S. (1994). A Taxonomy of Computer Program Security Flaws. *ACM Computing Surveys, 26*(3), 211–254.

Laura, A. (2011). Cyber Crime and National Security: The Role of the Penal and Procedural Law.

Lewis, A. J. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies, Washington, DC.

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

NBS (2012). Nigeria Poverty Profile, 2010. National Bureau of Statistics, Abuja.

Okafor, E. E. (2011). Youth Unemployment and Implications for Stability of Democracy in Nigeria. *Journal of Sustainable Development in Africa, 13*(1).

Okeshola, F. B., & 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), 98–113.

Saul, H. (2007). Social Network Launches Worldwide Spam Campaign. *New York Times*.

Theohary, C. A., & Finklea, K. (2015). Cybercrime: Conceptual Issues for Congress and U.S Law Enforcement. Congressional Research Service Report.
Wada, F., & Odulaja, G. O. (2012). Assessing Cyber Crime and its Impact on E-banking in Nigeria Using Social Theories. *African Journal of Computing & ICTs, 5*(1), 69–82.
WDI (2016). World Development Indicator (WDI). International Bank for Reconstruction and Development/The World Bank; Washington D.C, USA.