Journal of Finance, Business and Management Studies
Volume 4, Number 1, 2024, pp. 21 – 33
ISSN 2583-0503
Published by RGN Publications

http://www.rgnpublications.com

Relationship Between Cybercrime and the Nigerian Economy: Causes, Implications and the Path Forward

Nathan Udoinyang[a,*], Reuben Daniel[b] and Abroad E. David[c]

[a] *Department of Economics, Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt, Rivers State, Port Harcourt, Nigeria*
[b] *Department of Social Studies, College of Education Warri, Nigeria*
[c] *Department of Curriculum Study/Computer Science, College of Education Warri, Nigeria*

ARTICLE INFO

Keywords:
Cybercrime
Nigerian economy
Causes
Implications and Path forward.

JEL: G1, K14
DOI: 10.26713/jfbms.v4i1.2667

ABSTRACT

This research examined the relationship between cybercrime and the Nigerian economy: Causes, implications and path forward. Data from banks and her clients was gathered for this research using a survey approach. Access Bank, First Bank, GT Bank, UBA, and Zenith Bank are some of these banks. In order to get the effects from experts, the University of Port Harcourt's Bursary Department, Ignatius Ajuru University of Education's Computer Science Department, and others were selected. The random sampling approach was used in order to get a sample size of 300 from the intended population. To collect the required data, a self-structured questionnaire titled Cybercrime and the Nigeria Economy: Causes, Implications, and Path forward (C.N.E.C.I.P.F.) was filled out. A total of 300 questionnaires were personally administered to the respondents, 260 copies were retrieved and used for data analysis and interpretations using a simple percentage procedure with aggregate criterion of 50%. Reviewing the causes of cybercrime in Nigeria among others are: Urbanization and civilization; unemployment; poor implementation of cybercrime laws and inadequate equipped law enforcement agency; corruption etc. Our findings also review that the implications of cybercrime on Nigeria's economy are: disruption of business operation; loss of revenue; monetary losses etc. Although cybercrime cannot be completely eliminated, it may be lessened in intensity, according to the research's findings. The research also made a number of recommendations and concluded that to reduce the extent of cybercrime in Nigeria to a minimum, there is a need for citizens, businesses, and the government to actively collaborate.

1. Introduction

The growth of the Internet and seamless access to computer aided technology has created various opportunities for work and business activities, as well as for those taking advantage of the Internet revolution to engage in illegal activities. The introduction of information communication technology and online communication

[*] Corresponding author
Email(s): `nathannathanudoinyang@gmail.com` (N. Udoinyang); `reubendaniel@944gmail.com` (R. Daniel); `dataabroad@gmail.com` (A. E. David)
Orcid(s): 0009-0008-2457-3045 (N. Udoinyang)

has led to a dramatic increase in incidents as well as the emergence of new trends and patterns of Internet-enabled criminal activities. However, the rise of the Internet in Nigeria has come with an unintended consequence, global notoriety as a haven for cybercrime. In the 90s, fraud in Nigerian society was popularly referred to as 419 in reference to the penal code that framed the criminal justice system in Nigeria. At the time, individuals arrested in connection with that law were labeled '419ers'. Then came the Internet, shortly after which a number of tech-savvy contrarians successfully exported the 419 concept. While the popular 419 reference has been expanded to include cybercriminals, the name 'Yahoo-Yahoo' is the most familiar informal usage in Nigeria to refer to people who commit online (cybercrime) scams.

Cybercrime is one of the most prevalent forms of criminal conduct in Nigeria. Spam emails, emails used to launder money, and well-written but phony company partnership offers are just a few of the ways Nigerian hackers are notorious for tricking people all over the globe into falling for their fake schemes. Yahoo Yahoo is the most prevalent vernacular appellation for criminal conduct that happens online in Nigeria. The phrase "yahoo boys" is typically used to refer to the criminals that are involved in advance fee fraud schemes (419) that are often referred to as "yahoo yahoo." Most of the time, it involves using email to trick victims who aren't aware of the situation, particularly via a Yahoo account or Yahoo Messenger. As a result, the nation has established a name for itself as the source of what are now called "419" emails. Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) prohibits advance fee fraud, which is the basis for these letters. There are many tactics that the "yahoo boys" use in order to find victims. Many of these con artists hang out at computer cafes, where they spend the evenings browsing the web and sending phishing emails to unsuspecting victims. Individuals who go by the name of "yahoo boys" have exploited a great deal of foreigners, especially women, who are searching for partners online. These guys appear as though they are ready for a committed relationship before starting to take advantage of their susceptibility. Some of them could even be able to persuade their victims to help them get residency permits or travel documents to the country in which they now live. Once they successfully achieved their goals, they would cut off all connection with the victim and go to another target.

In other cases, con artists would use stories of harsh living circumstances, natural disasters, fatalities in the family, personal injuries, or other hardships to pique their victims' interest and keep them involved in their schemes. In addition, the victims are requested to make payments to help them get over their alleged financial obstacles. Most victims just tend to their wounds and go on with their lives. Some victims, on the other hand, are very resentful and report their experiences to the appropriate authorities. These authorities often apprehend and punish the accused, or they sometimes accept bribes substantial amounts of money from the suspects in exchange for their release. The problem has become worse as some non-Nigerians who are apprehended for cybercrimes often pretend to be Nigerians before being thoroughly investigated and having their place of origin confirmed.

Olumide Adegbolu, a young Nigerian musician better known by his stage name Olu Maintain, released the hit song "Yahooze" in 2007. This song does a good job of illustrating how severe the problem of cybercrime is in the country. The song, which has generated a lot of controversy, describes a lavish lifestyle that includes pricey beverages, extravagant vacations, and extravagant modes of transportation that is, if the singer is able to "hammer out" (get) one million dollars and convert it into Naira and use it for transportation. A young man must be a con artist if he is able to dream of living such a lifestyle and make such a significant sum of money, critics said, calling the song a praising of internet fraud, popularly known as "Yahoo Yahoo." Olu Maintain has sharply disputed this, claiming that the song just reflected his ascent to fame and the changes money has brought about in his life. It is evident that the song and the debate surrounding it represent the current way of thinking for a large number of young people in Nigeria. A large number of Nigerian youth have been involved in the "yahoo yahoo" sector because to their ambition to acquire and drive expensive cars and lead ostentatious lives.

In 2022, Ramon Olorunwa Abbas a 41-years-old Nigerian also known by his Instagram handle, 'Ray Hushpuppi' was sentenced to 135 months in prison (11 years and 3 months) by the United State District judge Otis D. Wright II, for school financial scam, business Email compromise fraud and other Cybercrime and was order to pay $1,732,841 in restitution to two fraud victims. It happens sometimes that you go into a cybercafé and find most of the customers are young males, mostly in their 20s, 30s, or early 40s who are browsing the internet for potential victims.

Furthermore, there is a habit known as “night browsing,” when people use the internet to do business while staying online all night. There is a fee associated with this service. The men often collaborate to practice their companies so that they may learn from one another and enhance their ventures. Most of them use their laptops, which they also possess, to conduct their illegal activities. Unfortunately, it seems that the stringent policies that many financial institutions and businesses that carry out online transactions have put in place in recent years have caused a setback for Nigerian hackers. Some of the most vulnerable among them have been compelled to use spiritual practices in order to enhance their businesses in order to meet this objective. The platform in question is called “Yahoo Plus.” It’s an upgraded version of Yahoo Yahoo, where the “yahoo boys” use spiritual charms and traditional spiritual techniques like voodoo or juju to hypnotize their victims into complying with their wishes and giving them whatever amount of money they desire. The Yahoo guys participate in esoteric rites that are linked to increasing their capacity to deceive others. It is feasible to guarantee that the cybercriminal hypnotizes his victims by using conventional spiritual strategies like voodoo or juju/charm, which raises the possibility that the con artist will be successful in hypnotizing his victims. It can be guaranteed that the victim will keep sending money from wherever in the world after this is completed. This accomplishment was attained by the use of several strategies. The Yahoo boy seeks guidance from a spiritualist, witch doctor, or diviner who confers with the “oracle” or the “gods” to answer his questions. He is then given a selection of ceremonies to lead and perform. Examples of this include the customs of sleeping in cemeteries, bringing body parts, and spending a set number of days in a coffin. Stated differently, he entices his victims who are mostly always women by lavishing them with a share of the stolen money so they may buy flashy and high-end stuff. This is done for the Yahoo Yahoo’s benefit, not because the Yahoo guy loves the victim. He may abduct the person, murder them, and then remove the needed body part. Some even get instructions to engage in sexual relations with virgins during the ceremonies. Most of the time, these avaricious people kidnap, rape, and sometimes even kill young girls, especially those in their teens and college years. Sleeping with mad or pregnant women is one of the other rituals that are practiced. Furthermore, the yahoo man can be told not to take a bath for a few days to several months since it might have severe effects.

Another “yahoo” crime that is quite common in Nigeria is phishing. Phishing is a kind of cyberattack that often involves sending an email to a victim that seems to be coming from a reliable source, such a bank, to the recipient, who is uninformed of the email’s true origin. Phishing involves sending the recipient an email asking them to validate their personal information by visiting a phony website via a link in the email. After obtaining the data, the hacker will have access to the victim’s financial information. According to Richards (2016), there was a rise in the quantity of phishing emails sent in 2015 by people thought to be Nigerian hackers. When the Central Bank of Nigeria (CBN) announced the deadline for Bank Verification Numbers (BVN), the volume of these emails peaked. Cybercriminals bombarded bank customers who were not paying attention with phishing emails. The purpose of the emails was to tell the recipients that their accounts would be blocked; nevertheless, when they divulged their personal details, the hackers took advantage of their login credentials.

Longe *et al*. (2008) [8] said that the internet and technology developments have significantly changed how information is distributed, reproduced, controlled, and disseminated. Arora (2016) [2], on the other hand, noted that information can now be sent quickly and cheaply across long distances in the globe because to computer networks’ rapid transmission speeds. The number of people utilizing the internet rose to 3.8 billion in 2017, accounting for 51% of the world’s population of 7 billion, after falling to 2 billion in 2015. Cybersecurity Ventures projects that by 2022, there will be 6 billion Internet users worldwide, or 75% of the 8 billion people who are expected to inhabit the planet. Additionally, it is projected that by 2030, there will be over 7.5 billion Internet users worldwide, or 90% of the projected 8.5 billion inhabitants on the planet (Morgan, 2017 [21]). Cybercrime encompasses any illicit activity involving the use of computers, whether as a means to an end or as a means of committing particular crimes. The probe includes elements of computer sabotage, espionage, manipulation, and unlawful use of a computer equipment. Cybercrime continues to be a major concern for all businesses worldwide and a major issue for humanity as a whole, according to Morgan (2017) [21]. Globally, attacks on the internet have enormous consequences. Cybersecurity Ventures, for example, projected that by 2021, cybercrime will have cost the world's population $6 trillion yearly a $3 trillion increase from the first projection in 2015. This would be more lucrative than the worldwide trade in all major illicit substances combined, and it would mark the biggest transfer of economic wealth in the history of the planet. According to Cybersecurity Ventures' "2017 Crime Report," which is the most prominent research and publishing company covering the worldwide cyber market, cyber-attacks are the kind of crime that is growing at the fastest pace in the US. They also mentioned how these attacks are becoming more complicated, widespread, and expensive.

Cyberattacks have resulted in a large number of computer users having their privacy breached; this may include the disclosure of private photos, login passwords, or medical details (Choo *et al.* 2007 [14]). Symantec (2016) [11] claims that these types of attacks have been effective in tricking victims into downloading malicious files and programs. Cybercriminals have a number of tools at their disposal to gain illegal access to people's PCs or company networks. Attacks may be passive or active, for example, a web-based attack that waits for a user to visit a malicious website in an attempt to infect the user's system with dangerous software, or a brute-force attack that obtains the user's password. Attacks might take two different forms. There are several reasons why this type of attack could be conducted, such as monetary gain, stealing confidential data, network disablement, setting up a command and control (C&C) server, or using the system as a springboard for additional attacks (Cruz, 2013 [5]; Global Forum on Cyber Expertise (GFCE), 2020 [16]; Harvy, 2017 [17]). The main element influencing the efficacy of cyberattacks is the general public's lax security habits, which have the potential to expose their sensitive and private information. Having strong passwords alone won't protect you from cybercrime since websites might have their data hacked.

According to a story that appeared in the daily Tope Omogbolagun Punch on November 22, 2023, the Senate is grumbling about the $500 million that cybercrime costs them each year. Senator Godswill Akpabio, the Senate president, is cited as stating this. They engaged in a wide range of illegal activities, such as fraud, harassment, cyberterrorism, identity theft, hacking, and more. Therefore, in Akpabio's opinion, the establishment of a thorough legislative framework by the government to prevent, investigate, pursue, and punish cybercriminals is of the highest national and economic significance. These crimes not only cost the nation a great deal of money, but they also compromised our privacy, interfered with vital infrastructure, and reduced public confidence in digital systems. They resulted in large financial losses as well. Furthermore, Senator Salisu elucidated the significance of the Cybercrime (Prohibition and Prevention) Act (Amendment) Bill, 2023 revision from a national perspective. According to him, the goal of the modification was to strengthen existing rules and address emerging dangers in order to make the legislation more effective. As a result, he challenged all of the participants, requesting that they elevate the topic of cybercrime by contributing a multitude of perspectives, a richness of knowledge, and experience. Every year, fraudulent activities using the internet cause losses exceeding 0.8% of Nigeria's GDP. Nigeria is ranked sixteenth among worldwide victims of cybercrime, according to a study released by the Federal Bureau of Investigation in 2023.

The majority of cybercrime in Nigeria is committed by both younger and older people, according to Ibikunle and Eweniyi (2013) [7]. The bulk of young people who commit cybercrime, however, are students at the several universities around the country, as well as recent graduates who are still jobless and pupils who have left school. They investigate the freedom that people have to do astounding crimes online, which has an impact on the socioeconomic advancement of business organizations in Nigeria. These offenses consist of stealing, deception, and theft. Cyberattacks may threaten the very survival of over eighty percent (80%) of Nigerian e-businesses and guarantee their continuous existence. The increasing frequency of cybercrimes and the resulting financial consequences are directly linked to this vulnerability. There may be illegal activities in the computer and Internet domains. Our economy, way of life, and society are all greatly impacted by this kind of illegal conduct. This may be attributed to the fact that our society is evolving into an information culture, which is defined by the information sharing that occurs online. As findings, cybercrime is a significant security concern impacting the country's commercial enterprises. This has led to a decline in the competitiveness of the majority of Nigeria's corporate organizations and the loss of important data related to those companies. These losses have negative effects on people, businesses, and the government. Some of these effects include revenue losses, business disruptions, lower profits and increased operational costs, and deficiencies in welfare. This research paper will examine the relationship between cybercrime and Nigeria's economy from 2003 to 2023, as well as its causes, effects, and future prospects. This is a reaction to the ongoing, everyday rise in cybercrime.

2. Literature Review

Most Cybercrimes Practice in Nigeria

According to Maitanmi *et al*. (2013) [10] the following is a list of some of the most prevalent categories of cybercrime that are perpetrated in Nigeria:

Yahoo Attack: Because it is the section of the Nigerian criminal law that forbids offenders of this sort, Yahoo Attack also known by its other name, 419. The usage of email addresses collected from Internet access points via the use of email address harvesting software also referred to as web spiders or email extractors distinguishes this. These technologies allow email addresses to be automatically extracted from online content. Nigerian scam letters employ a variant of the advance fee approach. This tactic involves an email from Nigeria offering the receiver the chance to split a substantial amount of money that the sender who poses as a government official is trying to smuggle out of the nation. This method has resemblance to the recently popular imitation fraud.

Hacking: Here, Nigerian hackers are taking part in brainstorming sessions to try to break security codes for websites selling e-marketing products, money point cards, and e-commerce websites.

*Software Piracy:*This the unlawful duplication and distribution of software, video games, audio files, movies, or videos to uninvited parties.

The word *"pornography"* refers to a broad category of images, videos, and movies with varying degrees of sexual content. Because of the internet's widespread growth of pornographic websites, there is now a free market for this illegal conduct. This is among the most prevalent forms of cybercrime in Nigerian educational institutions.

Credit Card and ATM Fraud: When consumers submit their credit card information online or when they use an ATM card to withdraw cash, hackers may obtain those details. When customers enter their credit card details on the merchant's website, this might occur. By assuming the identity of the cardholder, hackers have the power to use this credit card fraudulently.

A denial of service attack is an act of fraud wherein the perpetrator overloads the victim's email account or system's capacity with unsolicited messages, therefore impeding the victim's ability to receive or provide legally entitled services.

Criminal Activity on Internet Relay Chat (IRC) Servers: IRC servers are chat rooms where people may assemble and converse with one other from all over the world. It is used to arrange meetings with other criminals. Hackers use the application to share strategies and talk about vulnerabilities they have discovered.

Distribution of Viruses: A virus is a computer program that inserts a duplicate of itself into a file, usually an executable program, to infect that file. File transfer is the means by which viruses proliferate. There are many different types of viruses, and each one requires human participation, humans are often unaware of how they spread.

"Phishing" is the word used to describe the act of copying goods and e-commerce websites in order to trick unsuspecting users. This is a sophisticated technology scam that often uses spur-of-the-moment emails to trick people into sending sensitive financial or personal information.

Plagiarism: The act of stealing someone else's ideas via the usage of public domains on the internet is known as plagiarism in the digital sphere. The act of pilfering ideas from other people and passing them off as one's own original work is so common in academic settings that it is accepted as standard procedure by both instructors and students.

Spoofing is the practice of having one computer on a network pose as another, usually with elevated access privileges, in order to gain access to other computers inside the network.

When a scammer uses *cyberstalking*, they follow the victim by sending them emails on a regular basis and using chat rooms often.

When a fraudster includes defamatory material in emails they send to others connected to the victim, or posts it online, it's called *cyber defamation*.

Salami Attacks: Using massive data collecting, salami attacks are ostentatious commercial scams or assaults against confidentiality.

As per the United States of America, what is cyber terrorism? The Federal Bureau of Investigation (searchsecurity.techtarget.com) defines *cyberterrorism* as a planned, politically motivated attack on information, computer systems, computer programs, and data that results in violence against non-combatant targets by sub-national groups or clandestine agents.

3. Theoretical Literature

Three theories "the control theory, the structural strain theory, and the cultural transmission theory" serve as the foundation for this research project. Together, these theories provide as the unifying element.

3.1. Control Theory

The foundation for the control theory's findings is the notion that deviation is the external manifestation of social control disintegrating. Advocates of this theory argue that temptations abound in life and that participating in criminal activity, like cybercrime, may be fulfilling or enjoyable for those who partake in it. The theory holds that people follow social norms because those who live in such societies have mechanisms in place to make sure that everyone in the community does as expected. The theory also said that there is a higher likelihood of deviation from the norm in circumstances when such mechanisms are insufficient. One of the idea's proponents, Durkheim, said that societies with strong social relationships are more inclined to exercise more control over its members and require obedience. However, low levels of compliance are likely to be encouraged by bad collective sentiments, which are the result of weak social ties and eventually give rise to deviant acts like cybercrime.

3.2. Structural Strain Theory

The primary tenet of the structural strain hypothesis is that people are under pressure to deviate, especially those who are socially disadvantaged. Social strain creates pressure on people to diverge, which leads to deviation. It is credited to R.K. Smith, an American sociologist. Meyer. According to Merton, the theory suggests that a perceived imbalance in the social structure may be the cause of various forms of criminal conduct, including cybercrime. The theory states that deviant behavior, which in this case refers to cybercrime, may occur on a large scale when a social system rigorously severely limits or completely closes direct connections to approved modes of achieving these goals for a significant portion of the citizenry, while a value system extols certain important critical success goals for the citizenry. The same society that creates opportunities and assures individuals of the means to take advantage of them also blocks access to achieving the means or goals, leading to a sense of confusion or anomie. Stated differently, opportunities are created by the same society. In these kinds of circumstances, people who feel abused turn to illicit acts that are not authorized, such stealing, banditry, kidnapping, and hacking, to achieve their goals.

3.3. Cultural Transmission Theory

The ‘differential association’ hypothesis, often called the cultural transmission theory, is predicated on the premise that abnormal behavior is picked up via social interaction. According to this hypothesis, people may learn criminal behaviors including cybercrime just as they can learn any other kind of activity. Edwin Sutherland, widely regarded as the father of this theory, asserts that abnormal, objectionable, or illegal behavior is obtained via “differential association” with certain people, including those who engage in illegal activity on the internet. “Birds of the same feather always flock together” and “he was a good kid until he started going out with bad guys” are two examples of how interactions with people who have a tendency to engage in criminal behavior can predispose otherwise law-abiding individuals to engage in criminal acts such as cybercrime, according to Bello (2017, page 178).

3.4. Empirical Literature

Ayub & Akor (2022) [4] conducted an examination of the patterns, trends, and effects of cybercrime in Nigeria. The study article, which uses secondary data sources, notes that Nigeria’s governments have attempted to combat cybercrime by passing and putting into effect the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 in 2015. The Nigerian police and the Economic and Financial Crimes Commission (EFCC) have detained and punished a significant number of cybercriminals in an ongoing fight against them. Nevertheless, despite the efforts of the authorities, the ongoing modifications to strategies and advancements in approaches have consistently impeded the capture of a significant number of cybercriminals. The report recommends that law enforcement personnel get retraining as well as continuous training in order to counter the danger. By putting firewalls in place, keeping personal information private, and refusing unsolicited notifications asking them to validate their login credentials or information, internet users may safeguard their computer systems.

In 2020, Message Magazine [20] will look at the issue of cybercrimes in Nigeria: Causes and Effects. According to their findings, Nigeria was expected to lose N250 billion ($649 million) annually due to cybercrime in 2017, but that amount dropped to N288 billion ($800 million) in 2018. Comparing this to the value of N250 billion in 2017, there was a notable rise. They recommend that the Nigerian government make a bigger effort to deal with this problem that impacts the whole nation.

In 2020, Victoria *et al.* [12] presents an analysis of cyber security flaws, procedures, and capacities in Nigerian online banking. This essay’s goal is to go over the findings of a research project on cyber security in Nigeria’s online banking industry. The industry’s cyber security capabilities and procedures are presented in the publication, along with the most notable cyber security breaches that have occurred. An online poll was conducted with one hundred seasoned people working in Nigeria’s banking and banking security services sectors. The data indicates that hacking, electronic spam messages, and viruses, worms, or Trojans, are the top three most common breaches. These findings imply that Nigerian cybercrime has evolved from low-tech, cyber-enabled crimes to high-tech, sophisticated breaches. The management of banking staff has provided enough support and training on the application of cyber security rules and procedures. The lack of cutting-edge technology to identify and address cyber security breaches and the low degree of regulatory compliance seem to be the main factors that have led to a decline in the cyber security expertise of the banks in our sample.

The work of Adesina (2017) [1] goals are to: (i) draw a link between cybercrime and poverty in Nigeria; (ii) look into the steps the Nigerian government is taking to prevent cybercrime; and (iii) offer possible solutions that could be put into practice to help lower cybercrime and alleviate poverty. The essay makes the case that the government need to put laws and initiatives into place that have the power to end and minimize poverty. However, these programs and policies must be wisely and successfully backed by actions. From the above empirical literature review, it is evident that a wide range of academics have studied cybercrime in their various works. For instance, Ayub & Akor (2022) [4] looked at the trends, patterns, and consequences of cybercrime in Nigeria; Message Magazine (2020) [20] looked into the causes and effects of cybercrimes in Nigeria; Wang *et al.* (2020) [12] looked at cyber security breaches, practices, and capability in Internet banking in Nigeria; and Adesina (2017) [1] looked into cybercrime and Poverty in Nigeria. This paper differs from others in that it examines the relationship between cybercrime and the Nigerian economy from 2003 to 2023, as well as the causes, implications, and future directions. Primary data and the survey method using a questionnaire to obtain information directly from banks, its customers, students, and experts from the bursary department and computer science department at the University of Port Harcourt and Ignatius Ajuru University of Education Port Harcourt, Rivers State are used.

4. Methodology

In this study, we used the survey technique as our method and the purposive research design approach as our research design. This action was taken to guarantee that the target population we were targeting could be reached. We chose to utilize the survey technique because our objectives are to assess how these dangers affect the economy and to get information from individuals who use computers, bank accounts, and the internet. The research used primary data, and its sample of interest was drawn at random from banks and their clientele. Access Bank, First Bank, GT Bank, UBA, and Zenith Bank are some of these banks. Furthermore, since students and instructors make up the majority of those who use computers and the internet, the Bursary Department, Computer Science Department, and Ignatius Ajuru University of Education were selected to get professional feedback. The random sampling approach was used in order to get a sample size of 300 from the intended population. A self-structured questionnaire titled Cybercrime and the Nigeria Economy: Causes, Implications, and Path forward (C.N.E.C.I.P.F.) was used to perform this study. The research utilized this questionnaire to collect data. The questionnaire was delivered to each responder in unique sets, totaling 300 copies. 260 of those were gathered and utilized for the analysis and interpretation of the data. This indicates that 86.7% of respondents to the survey completed it. In addition, the responses from survey respondents were compiled and assessed using the basic percentage approach.

5. Data Presentation and Discussion of Findings

Response of respondents of the causes of cybercrime in Nigeria

Table 1 shows the causes of cybercrime in Nigeria. From Table 1 it can be deduce that majority of the respondents anonymously agreed to the causes of cybercrime in Nigeria which constitute to an aggregate percentage of 76.5% to that of YES RESPONDENTS which is above the aggregate percentage criterion of 50% and also above the NO RESPONDENTS of 23.5%.

Response of respondents of the implications of cybercrime in Nigeria

Table 1 shows the causes of cybercrime in Nigeria. From Table 1 it can be deduce that majority of the respondents anonymously agreed to the causes of cybercrime in Nigeria which constitute to an aggregate percentage of 84.8% to that of YES RESPONDENTS which is above the aggregate percentage criterion of 50% and also above the NO RESPONDENTS of 15.2%.

Discussion of Findings

Findings from Table 1 shows that the causes of cybercrime in Nigeria are: Urbanization and civilization; high rate of unemployment; quest for quick wealth at the expense of one's life; poor implementation of cybercrime laws and inadequate equipped law enforcement agency; negative role model; corruption; gullibility/greed; poverty; proliferation of cyber café and the porous nature of internet and finally Abdulistic mentality i.e the act of making money without working. All the respondents agreed on all the causes of cybercrime in Nigeria as seen in table I which is in line with the empirical literature review of Ayub & Akor (2022) [4], Message Magazine (2020) [20], Wang *et al*. (2020) [12], and Adesina (2017) [1].

Findings from Table 2 shows that the implications of cybercrime in Nigeria are: Increase in the cost of operation of business as a result of increase in the cost of protection of cybersecurity technology, insurance premium and

Table 1
What are the causes of cybercrime in Nigeria?

S. No.	Items	Option	Frequency	%	Decisions
1	Urbanization and civilization has led to increase in cybercrime	Yes No	175 85	67.3 32.7	Agreed
2	High rate of unemployment	Yes No	257 3	98.8 1.2	Agreed
3	Quest for quick wealth at the expense of one's life	Yes No	259 1	99.6 0.4	Agreed
4	Law enforcement organizations are not sufficiently equipped, and laws relating to cybercrime are not being appropriately enforced	Yes No	196 64	75.4 24.6	Agreed
5	Negative role model	Yes No	177 83	68.1 31.9	Agreed
6	Corruption	Yes No	239 21	91.9 8.1	Agreed
7	Gullibility/Greed	Yes No	146 114	56.2 43.8	Agreed
8	Poverty	Yes No	203 57	78.1 21.9	Agreed
9	Other concerns include the spread of cyber cafés and the open nature of the Internet	Yes No	152 108	58.5 41.5	Agreed
10	Abdulistic mentality i.e., the act of making money without working	Yes No	186 74	71.5 28.5	Agreed
	Aggregate %			76.5/23.5	Agreed

(Source: Authors Field Work, 2024)

public relations support; disruption of business operation; altered business practices; reputational damage of the country's name; loss of revenue; loss of intellectual property; reduction in competitive edge; productivity losses and rising cost; retard financial inclusion; loss of confidence in the country's banking sector and monetary losses. All the respondents agreed on all the implications of cybercrime in Nigeria as seen in Table 2 which is in line with the empirical literature review of Ayub & Akor (2022) [4], Message Magazine (2020) [20], Wang *et al.* (2020) [12], and Adesina (2017) [1].

6. Recommendations

The Path Forward

Fighting cybercrime is a very challenging task. This is because, as technology advances, criminals become more cunning to thwart cyberattacks. They do this by devising fresh techniques for executing their fraudulent schemes. To prevent data loss due to cyber theft, individuals, businesses, and financial institutions are urged to put the following strategies into practice:

(i) It is advised to employ strong firewalls to stave against attacks and filter malware or potentially dangerous software.

(ii) It is important to develop and implement rules that will help organizations build and sustain a strong information technology infrastructure that will allow them to grow.

(iii) In order to detect vulnerabilities and take appropriate action to fix them, information technology infrastructure must be deployed to simulate attacks. Included are vulnerability assessments and penetration tests.

Table 2

What are the implications of cybercrime in Nigeria?

S. No.	Items	Option	Frequency	%	Decisions
1	Increase in the cost of operation of business as a result of increase in the cost of protection of cybersecurity technology, insurance premium and public relations support	Yes No	242 18	93.1 6.9	Agreed
2	Disruption of business operation	Yes No	226 34	86.9 13.1	Agreed
3	Altered business practices	Yes No	209 51	80.4 19.6	Agreed
4	Reputational damage of the country's name	Yes No	253 7	97.3 2.7	Agreed
5	Loss of revenue	Yes No	248 12	95.4 4.6	Agreed
6	Loss of intellectual property	Yes No	198 62	75.4 24.6	Agreed
7	Reduction in competitive edge	Yes No	205 55	78.8 21.2	Agreed
8	Productivity losses and rising cost	Yes No	191 69	73.5 26.5	Agreed
9	Retard financial inclusion	Yes No	179 81	68.8 31.2	Agreed
10	Loss of confidence in the country's banking sector	Yes No	243 17	93.5 6.5	Agreed
11	Monetary losses	Yes No	234 26	90 10	Agreed
	Aggregate %			84.8/15.2	Agreed

(Source: Authors Field Work, 2024)

(iv) To monitor and detect unusual traffic and intrusions within the implemented information technology infrastructure, IT workers should get regular training.

(v) The adoption of strict legislation and the penalties meted out to those who break it (v).

(vi) To ensure security, secure user interfaces must be implemented to make sure that only authorized users are allowed access to company networks.

(vii) Frequent updates and upgrades are necessary to keep software and apps current and compliant with the most recent worldwide best practices.

(viii) Effective and thorough coordination and cooperation amongst financial institutions. For example, funds are moved to or deposited into an account at a different financial institution when identity thieves use computers or other information and communication technology infrastructure to steal money from one person's account to another. In the case that these kinds of fraudulent transactions are found, the concerned organization must show effective collaboration.

(ix) Acquiring insurance coverage to compensate for damages resulting from cyberattacks and cybercrimes.

(x) Discussions on the kind, alleged origins, and frequency of cyberattacks need to take place in a forum designed to foster collaboration and information sharing.

(xi) To improve the capacity of Nigerian public and security officials to tackle cybercrime in a proactive and long-lasting way, workshops need to be held.

(xii) Boost the efficiency of operational risk management strategies across the board for the organization. The only sensible thing for institutions to do is to set up strong risk management systems that can outperform the level of knowledge shown by cyber fraudsters.

(xiii) In order to reduce cybercrime to a level that can be controlled, collaboration between individuals, corporate entities, and governmental bodies will be very advantageous.

(xiv) To ensure that policies, procedures, and guidelines that support security on internet service providers' infrastructure are followed, collaboration with telecom regulatory bodies is essential. This will facilitate the identification and tracking of activities linked to illicit cyber activity. It is expected that enforcing the use of Security Incident and Event Management (SIEM) would enhance the process.

(xv) Increased consumer education and public understanding of the importance of:

  (a) It's crucial to follow fundamental rules, such making sure every person's computer system has a certain anti-malware application or protection and staying away from computer software that was acquired illegally.

  (b) You should never provide someone you don't know your Personal Identification Number (PIN), bank account information, or email access due to the many security holes in systems. despite the product's intricate design and complexity.

  (c) Personal information must never be exchanged or disclosed to any individual as no network can guarantee security against hostile hackers 100% of the time.

  (d) You should disregard any unsolicited email or text message that asks for financial information of any type.

  (e) It is important to ensure end users are always aware of the requirement of maintaining cyber security, and there should be regular user awareness education offered.

For government

(i) Create employment opportunities.

(ii) Strict and proper implementation/enforcement of cybercrime laws and adequate equipped law enforcement agencies.

(iii) Zero tolerance against corruption starting from the corridor of power to the least citizen of the nation.

(iv) Those in the corridor of power should set clear example by being a leader of integrity and good role model to youth and citizen of the nation.

(v) Effective and efficient economic policy that will fight against poverty and hunger.

(vi) Raise the bar for digital security and protocols while maintaining the quality of products and services throughout the duration of the supply chain.

(vii) Encourage efforts to improve it so that everyone may benefit from enhanced cyber hygiene.

(viii) Install security measures that will stop non-state players, such as those in the private sector, from damagingly hacking networks for their own gain or the gain of hired allies.

(ix) It is essential that efforts be focused on creating and implementing suitable international regulations and putting policies in place to promote trust in cyberspace.

7. Conclusion

A cyber security breach is still one of the biggest security risks facing the banking industry in most developing communities, according to The Nerve (2016) [24]. The fact that cybercrime is done across international boundaries is one of the aspects that makes it difficult to properly enforce our laws. This is something that needs to be addressed. As a consequence of the fact that the majority of victims are typically foreigners, it is challenging for our courts to effectively achieve convictions even when direct evidence is offered. However, the burden of proof needs to be re-adjusted, and the Nigerian government, in concert with the international community, should work on finding a means to establish a unified international cybercrime law. However, although it is not feasible to totally and easily remove cybercrime, it is possible to lessen its effect. There would be a need for an active joint effort by citizens, commercial organizations, and the government in order to decrease the degree of cybercrime in Nigeria down to a minimal level.

Acknowledgement

I would like to utilize this occasion to convey my deepest appreciation to everyone who is involved for the accomplishment of this effort. As well as for their significant assistance and encouragement throughout the full process of study, I would like to convey my particular thanks to every one of the co-authors. Their wise advice and understanding considerably helped to the richness of the content. The culmination of this work would not have been possible without the knowledge and financial contributions of each and every one of them, and I would like to offer my greatest appreciation to each and every one of them.

References

[1] Adesina, O.S. (2017). Cybercrime and poverty in Nigeria. *Canadian Social Science*, **13** (4), 19 – 29, DOI: 10.3968/9394.

[2] Arora, B. (2016). Exploring and analyzing Internet crimes and their behaviours. *Perspectives in Science*, **8**, 540 – 542, DOI: 10.1016/j.pisc.2016.06.014.

[3] Alhaji, B.K., Hassan, A.S. & Mohammed, J.I. (2016). Information and communication technology, cybercrime and the administration of criminal justice system in Nigeria, In: Yusuf, Y.M. (ed.), *Current Themes on Nigerian Law and Practice*, University of Maiduguri, Maiduguri, Chapter 25, pp. 416–431.

[4] Ayub, A.O. & Akor, L. (2022). Trends, patterns and consequences of cybercrime in Nigeria. *Gusau International Journal of Management and Social Sciences, Federal University, Gusau*, **5**(1), 241–262.

[5] Cruz, A. (2013). Cybercrime and how it affects you. *Cyber Security Tips*, **7**(1).

[6] Cybercrime Act (2015). Laws of the federation of Nigeria. Lagos: Federal Government Press, Nigeria.

[7] Ibikunle, F. & Eweniyi, O. (2013). Approach to cyber security issues in Nigeria: Challenges and solutions. *International Journal of Cognitive Research in Science Engineering and Education*, **1**(1), 11 pages.

[8] Longe, I.O., & Longe, F. (2008). Implications of the Nigeria copyright law for software protection. *The Nigerian Academic Forum Multidisciplinary Journal*, **5**(1), 7–10.

[9] Ndubueze, P.N. (2017). *Cyber Criminology and Technology-Assisted Crime Control: A Reader*. Ahmadu Bello University Press Ltd., Zaria, Nigeria.

[10] Olusola, M., Samson, O., Semiu, A. & Yinka, A. (2013). Impact of cybercrimes on Nigerian economy. *The International Journal of Engineering and Science*, **2**(4), 45–51.
Impact of cyber crimes on Nigerian economy, *The International Journal of Engineering and Science* **2**(4), 45–51.

[11] Symantec (2016). *Cybercrime & Cyber Security Trends in Africa*. The Netherlands: Global Forum for Cyber Expertise (GFCE) Initiative, 95 pages.

[12] Wang, V., Nnaji, H. & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, **62**, 100415, DOI: 10.1016/j.ijlcj.2020.100415.

URLs

[13] Central Bank of Nigeria (CBN) (2015). *Guidelines on Electronic Banking in Nigeria*. URL: https://www.arca.network/lib/E-BANKING-Regulation-document.pdf.

[14] Choo, K.-K., Smith, R., & McCusker R. (2007). *Future Directions in Technology-Enabled Crime: 2007-09*. Research and public policy series no. 78. Canberra: Australian Institute of Criminology. URL: https://www.aic.gov.au/publications/rpp/rpp78.

[15] FBI (2011). Taking a trip to the ATM?. Retrieved from, URL: https://www.fbi.gov/news/stories/atm.

[16] Global Forum on Cyber Expertise (2020). Strengthening cyber capacity and expertise globally through international collaboration. Available on URL: https://thegfce.org/ accessed on January 2, 2022.

[17] Harvy, C. (2017). Types of malware and how to defend against them. Security planet. Available on: URL: https://www.esecurityplanet.com/malware/malwaretypes.html accessed on November 13, 2021.

[18] Ibrahim, U. (2019). The impact of cybercrime on the Nigerian economy and banking system. URL: https://nigeriareposit.nln.gov.ng/handle/20.500.14186/1255.

[19] Martins, J.O. (2013). Cybercrimes in Nigeria: The implication in our economy and social image. Retrieved on the 17th of July, 2017 from URL: https://www.acta-pac.org.

[20] Message Magazine (2020), Cybercrimes in Nigeria: Causes and effects. *Retrieved from* URL: https://www.messagemagazineng.com/en/newsroom/press-releases/2020-08-15-gartner-forecasts-.

[21] Morgan, S. (2017). 2017 Cybercrime report. Herjavec Group, accessed on February 7, 2022, URL: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.

[22] Punch Newspaper (2023). Senate laments Nigeria's loss of $500m annually to cybercrime. URL: https://punchng.com/senate-laments-nigerias-loss-of-50m-annually-to-cybercrime/.

[23] Richard, A.O. (2016). Putting the cybercrime law to test in 2016. Retrieved on January 6, 2016, URL: https://guardian.ng/features/focus/putting-the-cybercrime-law-to-test-in-2016/#google_vignette.

[24] The Nerve (2016). Nigeria financial service industry affected most by cybercrime - Cisco, retrieved from: URL: https://thenerveafrica.com/9310/cisco-says-nigeria-financial-services-industry-oneaffected-cybercrime/.