# Assessment of Cybercrimes and control measures and impact on Nigeria.

**Ejirefe Influence**

Institute of Governance and Development Studies Nasarawa State University, Keffi.

## Abstract

This paper looks at the relationship between the dangerous manifestations of cybercrimes and control measures in Nigeria. It relies absolutely on qualitative method via secondary data. It states that cybercrimes likeATM fraud and other fraudulent electronic transactions, identity theft, espionage, cyber bullying, spamming, phishing, copy write infringement or theft of intellectual property, computer virus and defacing of websites in Nigeria gives impression that the computer systems and its components encourages cybercrimes. It however argued that, in spite of the fraudulent practices and losses caused by the unauthorised users of the computer systems and it components, the technology has more positive impact. The paper also, highlights the causes and impact of cybercrimes as well as assessed the existing control measures in Nigeria. It also, noted that the control measures adopted in Nigeria so far are inadequate but hope was finally rekindled with the cyber Act, 2015 but implementation is weak. Nevertheless, it concluded that cybercrimes have become endemic and permanent eradication is impossible but can be reduced. The paper therefore, recommends additional and more effective control measures for the control of cybercrimes in Nigeria.

**Keywords:** Control measures, Cybercrimes, Cyber-Criminals, Cyber Security, Nigeria and Victims.

## Introduction

The existence of Information and Communication Technology in Nigeria is a welcome development but some few bad eggs called the ‘Yahoo boys’ i.e internet fraudsters have turned the technology into a device for fraudulent practices. They are damaging the reputation of the country. Cybercrimes is real, the earlier we discourage it, the better for all Nigerians. Apparently, the love for money and the lure for it by the criminal minded lazy youths and adults folks have eroded their sense of dignity and societal values. It is disheartening that instead of directing their thinking to productive ventures, they deliberately channelled it to cybercrimes.

Distance use to be a barrier till the internet helped us to bridge the gap. The use of internet has truly made the world a global village. This technology is a good thing that everybody wants to identify with to simplify life, ease of doing business and progress but has however brought about increased world-wide apprehension.

## Methodology

This paper relies absolutely on qualitative method via secondary data. The secondary data used include, internet sources such as online academic journals and online newspaper articles, act/legislation, physical journal and newspaper, conference paper and books.

## Clarification of Concepts

There are some concepts which are very important to the understanding of this paper. It is important they are properly clarified. Thus:

(i) **Control Measures**: These are the various strategies or devices put in place toidentify, monitor, and arrest and curtail the menace of cybercrimes. Instrument like legislations and the use of law enforcement agencies are the major control measures suggested in this paper.

(ii) **Cybercrimes**: There is no generally agreed definition of what constitute cybercrimes among experts. Cybercrimes also known as electronic crimes, internet crimes or computer crimes is viewed from different perspectives. Perhaps, one area of agreement among experts is that, it is a crime committed with the use of computer. For example, (Monisoye (2007) defined cybercrimes as unlawful acts wherein the computer is either a tool or a target or both. It can also be described as unlawful activity in which computer or computing devices such as smart phones, tablets, Personal Digital Assistants (PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal activity (Jeetendra, 2017). Williams (2013) asserts that, cybercrimes are any crimes that involve a computer and a network. In some cases, the computer may have been the target of the crime.

(iii) **Cyber Criminals**: Cyber criminals also known as Internet fraudsters or Yahoo boys are perpetrators of cybercrimes, either for self-aggrandisement or greed, retaliation or adventure.

(iv) **Cyber Security**: Cyber security is a unique aspect of security. Nonetheless, whether data or information can be very sensitive and vital to the individual, country, organisations and businesses. The proliferation and sophistication of cyber-attacks brought about the need for cyber security. Nate (2019) declares that, cyber security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. In fact, the core functionality of cyber security involves protecting information and systems from major cyber threats. Techopedia (n.d) also, defined cyber Security as the preventive methods used to protect information from being stolen, compromised or attacked. The protection of the computer systems which include the hardware, software or information from theft and destruction by anyone are part of the control measures assessed by this paper.

(v) **Victims**: Victims in this paper refers to the targets or people who suffer from the negative activities of the perpetrators of cybercrimes.

## Theoretical Framework

The Routine Activity Theory is used for the analysis of this paper because of its relevance to the Nigeria cybercrime situation. The Routine Activities theory presents a clear-cut explanation of why crimes occur. It states that, crime occurs in the presence of three key elements which are a suitable target, lack of a suitable guardian, and a likely motivated offender.The theory suggest that, if all three elements are available somewhere, there is the tendency for crime increase and conversely, if one of these elements is absent, then there is chances for crime decrease (Cohen & Felson, Felson & Clarke, as cited in Urgun & Daglar, 2016). Nwosu (2016) believes that, the involvement of Nigerian youth in cybercrime can best be situated in the

Routine Activity Theory - a sub-field of crime opportunity theory that focuses on situations of crimes. The basic assumption of the theory is that in order for crime to occur, victims and perpetrator of the crime must meet in a certain place and time where there is the absence of an effective or suitable guardian. The implication is that unemployment and poverty causes cybercrimes but not the only causes of criminal activity. It also suggests that reducing criminal opportunities help in reducing the occurrence of crime.

Meier and Meithe (as cited in Nwosu, 2016) confirmed that, the Crime Opportunity Theory suggests that offenders make rational choices by choosing targets that offer a high reward with little effort and risk. Therefore, those who commit crime as a result of their deviation from norms also look for opportunities that make the crime beneficial to them. The theory is therefore based on the simple idea that people look for opportunity, whether through legitimate means or otherwise, to gain what they desire. The origin of this theory lies in the presumption that in every society, there is always the concept of 'norms' and that of 'deviance' and when a standard lifestyle established by a society becomes unachievable; people become deviant in attempts to achieve that standard in order to continue to be perceived as being within the realm of norm.

Clearly, the occurrence of a crime depends on two things: the presence of at least one motivated offender who is ready or willing to engage in a crime, and the conditions of the environment in which that offender is situated, to wit, opportunities for crime. All crimes therefore require opportunity but not every opportunity is followed by a crime. Similarly, while a motivated offender is necessary for the commission of a crime, it is not necessarily enough. Many jobless youths in Nigeria are motivated offenders who converge in time and space with innocent victims that they prey upon. The victim can be a Nigerian or foreigner, provided they are on the web at the time of communication. Sadly, the advent of cell phones, laptops, i-pads, and several other hand-held electronic communication devices has made cybercrimes very cumbersome for police and other law enforcement agents to combat.

Even though, the Routine Activities Theory provides a simple and relevant insight into some of the cause cybercrimes in Nigeria, it also has some weaknesses. For example, Brunet (as cited in Urgun and Daglar, 2016) criticised the Routine Activities Theory due to the fact that most studies which test the theory are post hoc and descriptive. At this stage in its development, the theory is limited in its predictive capacity. Degamo (as in Urgun & Daglar, 2016) also believes the theory is plagued with theoretical discrepancies. Again, it merely assesses one crime or crime density in a location instead of looking at a string of inter-correlated crimes. Furthermore, despite the Routine Activities Theory describes the transition from place to network, it fails to address the issue of divergence in time between victims and perpetrators in cyberspace. Even though the interactions between the victims and the perpetrators in physical space happen in real time, it is not always the true situation with cybercrimes.

## History and challenges of cybercrimes in Nigeria

The history of cybercrimes in Nigeria started in the form of Advance Fee Fraud majorly perpetrated by unemployed youth. The perpetrators thrive on tricks. The scammer trickily mail out letters through couriers or fax machine informing potential victims in another country that he successfully starched away huge sum of money amounting to millions of dollars via corrupt means or over invoicing of government contract or other means, that he is looking for a genuine person (potential victim) who is willing to make his or her account available for the money to be deposited and would handsomely reward the potential victim for helping to get the money out. At the initial stage, it would look as if the scammer is harmless till he achieves his target. As time went by, the potential victim would receive another mail that requires him or her to invest a small amount of money as processing fees; once the potential victim agree and send the money, that small amount turns out to be the initial loss or just enough for the jobless scammer. Then, scammers were few but they are more these days and cybercrimes are more or less a huge industry in Nigeria. Punch (2019) asserts that, in Nigeria, the three-pronged introduction of the Internet, computers and the mobile phones gave rise to massive outbreak of cybercrimes.

In today Nigeria, the perpetrators of cybercrimes are highly sophisticated in their fraudulent practices more than ever before while their victims seem handicapped in protecting themselves and their organisations. PricewaterhouseCoopers (2016) assert in their survey that organisations rank cybercrime as the second most reported type of economic crime up from fourth place. In the survey, 32% of organisation admits they had been a victim of cybercrime and 34% expected to be a victim in the next 2 years. Only 37 had a plan to respond to the incidents of cybercrime. The Nigerian Communication Commission (NCC) reveals that Nigeria currently ranked third globally in cybercrime behind UK and US (NCC, 2017).

The internet increases the speed of communication. It has also made business transactions easy, enhances friendship, increases pain and loss. In Nigeria, it has brought about ATM fraud and fraudulent electronic transactions, internet time theft, theft of computer systems or parts, physically damaging a computer, identity theft, espionage, cyber bullying, spamming, phishing, copyright infringement or theft of intellectual property, computer virus and defacing of websites. Mosuro (2017) confirmed that in March, 2015 that the Independent National Electoral Commission (INEC) website was defaced as well as that of the Lagos State Government in December, 2015. Adedapo (2014) reveals that the Central Bank of Nigeria (CBN) estimated that about N40 billion was lost by Nigerian banks to cybercrimes in recent times. Monguno (as cited in Nwosu, 2016) argued that, no organisation or country can perform optimally under an atmosphere of fear and insecurity. Uncertainties and raised anxieties have therefore strained both the Nigerian economy and society. As at the second quarter of 2016, it was estimated that 88% of the total cybercrimes in Nigeria comes from card and mobile banking frauds, with fraudulent transfers accounting for 8% while internal fraud stood at 4%. Indeed, global tracking of cyber-attacks indicate that Nigeria is among countries with high cases of software piracy, intellectual property theft, and melware attacks. Nigeria is losing about N127 billion, which is 0.8% of the country's Gross Domestic Products (GDP), to cybercrime yearly (Shittu, 2016). This situation is a big challenge to the numerous advantages and the huge opportunities that internet brings, while harmonising and managing its associated risks.

Most individuals and organisations that make use of the internet globally have become victims of cybercrimes which affects the overall performance of businesses. These catalogues of fraudulent practices and losses committed via the computer and its components give the impression that the computer system and its components encourage fraudulent practices (cybercrimes). Nevertheless, this paper believes that the cyber space is good and big enough for everyone to operate even though the unauthorised users play it dirty on the cyberspace. This paper therefore, is set out to highlight the causes of cybercrime, impact and assessment of the existing control measures in Nigeria; and then suggest more effective control measures.

## Causes of Cybercrimes in Nigeria

Cybercrimes are universal crimes that know no boundaries. The cyber criminals are everywhere looking for opportunity and easy ways to make money on rich individuals, organisations and government. In spite of the many control measures put in place, they continue to increase in numbers and more sophisticated in their operations. This may be attributed to the faceless nature of the criminals and crimes.

Krazytech (2017) asserts that the vulnerability of computers gives hackers easy access to steal sensitive information. Hackers can steal access codes, relina images, etc that can fool biometric systems easily and bypass firewalls can be utilized to get past many security systems. Again, the anonymous nature of cyber criminals makes it difficult to catch them and when you do, sometimes evidence related to the crime is easily destroyed. This has become a very common and obvious problem which paralyzes the system behind the investigation of cybercrimes. Krazytech (2017) asserts further that the comparatively small space of the computer has the unique characteristics of storing data in a very small space and this makes it a lot easier for cyber criminals to steal data from any other storage and use it for own profit. Again, the computer runs operating systems and these operating systems are programmed millions of codes. The human mind is imperfect, so they can do mistakes at any stage. The cyber criminals take advantage of these gaps. Moreover, negligence is a characteristic of human conduct. So, there may be a possibility that protecting the computer system we may make any negligence which provides cyber criminals the access and control over a computer system.

Usifo (2017) declares that greed for money, corruption, peer pressure; the urge to make it big by any means possible as well as joblessness is a cause of cybercrimes in Nigeria. Oladeide (2018) asserts that the National Bureau of Statistics said the Nigeria’s unemployment rate increase from 18.8% in the third quarter of 2017 to 23.1% in the third quarter of 2018. Joblessness causes poverty and crime. No wonder that many of these jobless citizens find solace in cybercrimes.

## Assessment of Existing Control Measures of Cybercrimes in Nigeria

Perpetrators of cybercrimes are not spirit but human beings. The anonymous nature of the perpetrators is big challenge and tracing them requires a high degree of computer knowledge. However, the following are assessment of some of the existing control measures used by individuals, public and private organisations:

(i) Some victims of cybercrimes report to the police. Unfortunately, not every police man has what it takes to arrest and curtail cybercrimes.

(ii) Some security agents with good computer knowledge inspect cybercafé from time to time as possible way of catching the cyber thieves in the act. Through such checks some of the yahoo boys have been caught.

(iii) Some individuals and organisations keep their computers away from unauthorised users during and at the close of work, but then, there are reported cases of insider threat perpetrated by disgruntled employees.

(iv) As a defence mechanism, some individuals and organisations install security software like firewall, anti-virus and some other powerful monitoring system as a first line of defence. This is good, yet some unauthorised users still find a way to corrupt the system with virus.

(v) Some secure their data by using encryption for their most sensitive files.

As said, these control measures are good but not complete safeguard for all cases. An unauthorised user can be invisible or hacker with a high degree of computer knowledge does not need the identity of anyone before robbing or infecting a computer with a virus.

## Legislation on cybercrimes in Nigeria

Before the passing of the Cybercrime Act, 2015, there was no definite and reliable legislation designed to address the threat of cybercrime in Nigeria. This gap led to the proliferation of cyber-criminals popularly known as 'Yahoo boys'. The following are the most common of these laws:

The Economic and Financial Crimes Commission Act (2004): The Economic and Financial Crime Commission (EFCC) Actis a Nigerian law enforcement agency charged with the responsibility of preventing, investigating, prosecuting, and penalizing economic and financial crimes and enforcement of other laws and regulations relating to economic and financial crimes. Economic Crime as defined by Section 46 of the EFCC Act covers:

> “ the non-violent criminal and illicit activity committed with the objective of earning wealth illegally either individually, or in a group or organized manner, thereby violating legislation governing the economic activities of government and its administration to include any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting, and anyform of corrupt malpractices, illegal arms deal, smuggling, human trafficking, child labour, oil bunkering, illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and policy, open market abuse, dumping of toxic wastes, and prohibited goods, etc.” (www.nassnig.org/document/download/5762).

Though the Act did not specially mention the term 'cybercrime' but terms like 'fraud', 'money laundering', 'embezzlement' and ‘any form of corrupt practices’,’ foreign exchange malpractices', etc. It obviously covers cybercrimes and so the offence can properly be brought within, the EFCC Act, 2004.

The Criminal Code Cap. C 38 Laws of the Federation of Nigeria (2004) is a legislation meant to punish criminal acts in Southern Nigeria while the Penal Code (1959) is meant to punish criminal acts in the Northern states of the country. Under the Criminal Code, cybercrime like 'advance fee fraud' is a form of 'false pretence' as contemplated by Section 418 while a perpetrated internet scam is situated within Section 419 which describes activities which constitute false pretences. For example, Section 418 which defines the term false pretence states that:

> “Any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true is a false pretence.” (Www.wipo.int/edocs/lexdocs/laws/en/ng/ngo25en.pdf.).

On the other hand, Section 419 of the Criminal Code describes what amounts to obtaining goods by false pretences. It states that:

> Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years. If the thing is of the value of one thousand Naira or upwards. He is liable to imprisonment for seven years. It is immaterial that the thing is obtained or its delivery

is induced through the medium of a contract induced by the false pretence (Www.wipo.int/edocs/lexdocs/laws/en/ng/ngo25en.pdf.).

Obviously, these laws cannot adequately address most cybercrimes. For example, Section 419, advance fee fraud is a felony and a suspect could not be arrested without a warrant unless found guilty in a competent court of law or arrested while committing the offence. Unfortunately, cybercrimes are perpetrated from personal computers and in private which sometimes makes it difficult for the perpetrators of cybercrimes to be caught. Therefore, the criminal code is not enough to deter cyber criminals.

Also, the Advance Fee Fraud and other Related Offences Act (2006) is an act of the National Assembly that forbids and penalises certain crimes relating to Advance Fee Fraud and other fraud related crimes. Section 1 and 2 of the Act clearly stood against any kind of false pretence and with the intention to defraud or obtain from any person in Nigeria or abroad to confer a benefit on him or on any other person has committed an offence under this Act and as such is liable on conviction to imprisonment for a term of not more than 20 years and not less than 7 years without the option of fine. Waziri (2005) states that, once an unsuspecting or gullible foreigner or company responds to the scam, an advance fee are demanded in the form of local taxes such as the National Economic Recovery Fund (NERFUND), contract tax, and various legal charges. Sometimes the victim is invited to Nigeria to sign (fake) contract papers. Once the initial payment is made the deal is concluded, and the victim loses his money.

These laws lacks uniformity and therefore amount to conflict and confusion among officers of the police, Economic and Financial Crimes Commission, Independent Corrupt Practices and related offences Commission, etc in terms of implementation.

The Cybercrime Act (2015) brought about confidence and assurance in the fight against cybercrime. The objectives of the Act as provided for in Section 1 are: to provide an effective and unified legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; ensure the protection of critical national information infrastructure; and promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, as well as intellectual property and privacy rights.

The Act contains 59 sections and is a very vital breakthrough in the history of Nigerian legislation owing to its focus on the development of the emerging online financial and Information and Communication Technology sectors in the country. By virtue of its Section 22, the law permits for the interception of electronic communication by way of a court order by a Judge, where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings.

Also, this inspired legislation by virtue of section 3 gives the President the power to designate certain computer systems, networks, and information infrastructure vital to the national security of Nigeria or the economic and social well-being of its citizens, as constituting Critical National Information Infrastructure (CNII), and to implement procedures, guidelines, and conduct audits in furtherance of that. Examples of systems which could be designated as such include transport, communication, banking, etc.

Above all, this Act has obvious constitutional disposition given its penchant for the protection of the basic constitutional rights of citizens while targeting cybercriminals. The Act therefore, prohibits the distribution of racist and xenophobic material to the public through a computer system or network. It also forbids the use of threats of violence and insulting words to people based on race, religion, colour, and descent, national or ethnic origin. To further realise the need to protect the rights of citizens, this Act authorises service providers to keep all traffic data and subscriber information with utmost confidentiality to protect the individual's constitutional right to privacy, and this can only be processed, or retrieved, subject only to an order of the court of law.

The Cybercrime Act, 2015 also:

(i) Recommends death sentence for an offence committed against a system or network that has been designated critical national infrastructure of Nigeria that leads to the death of an individual.

(ii) By the Act, Hackers or internet fraudster if found guilty of unlawfully accessing a computer system or network, would be made to pay a fine of up to N10 million or jailed for 5 years.

(iii)Those who commit identity theft are punishable with imprisonment for a term of not less than 3 years or a fine of not less than N7 Million or both.

(iv) The offence of Child Pornography is punishable with a jail term of 10 years or a fine of not less than N20 Million or both as the situations permit. The offence institute acts like producing, procuring, distributing, and possession of child pornography.

(v)The Act also stipulates a punishment of 1-10 years and/or a fine of N2-N25 Million or both, as the case may be for the offence of Cyber-stalking and Cyber-bullying.

(i) The Act also provides a minimum of 2 years jail term or a fine of not less than N5 Million or both for cyber-squatting.

In spite of the sanctions contained in the Cybercrime Act (2015) the perpetrators of cybercrimes continue to increase. The simple reason is that, implementation of the act is weak. So, there is need for those in-charges of the implementation to be firm and active in the discharge of their duties without undermining the provisions of the act. Again, the implementation of the Cybercrime Act is domiciled in the office of the National Security Adviser and if well implemented, it will help to boost the online cashless initiative of Central Bank of Nigeria. Therefore, proper understanding of the law by the Judiciary and the Law enforcement agencies and implementation of the Act would strengthen cyber security and ensure reduction of cybercrimes in Nigeria.

## Impact of Cybercrimes on Nigeria

Cybercrimes impacted on Nigeria in the following ways:

(i) The fact that some Nigerians into cybercrimes has truly damage the reputation of Nigeria before the international community. Nigeria is currently ranked third in the world behind the UK and USA. No genuine businessman or woman or country wants to do business with a fraudster in any country.

(ii) Cybercrime causes financial loss to individuals and private companies, including the cloning of both private and public enterprises. Some persons have been duped via ATM cards and banks like First Bank and Zenith Bank plc. websites was cloned just to dupe innocent Nigerians and foreigners.

(iii) At the individual level their privacy has been distorted. Private emails are being hacked every now and then. People receive unsolicited messages in their phones and email. Some of the cyber criminals hack into some individual phones such that they pay for calls made by the cyber criminals. Cyber bullying, cyber terrorism, etc. All these undermine morality and individual freedom.

## Conclusion

The history of cybercrimes in Nigeria started in the form of Advance Fee Fraud.Today, the perpetrators of cybercrimes are highly sophisticated in their fraudulent practices more than ever before while their victims seems handicapped in protecting themselves and their organisations. It is abysmal that, cybercrimes are on the increase in spite of the legislations and sanctions contained in it. The perpetrators devise means to breach security, steal money and very important information physically and online. Some of the criminals go to the extent of damaging hardware and software. Individuals, private companies, public companies are negatively affected, including Nigeria's reputation. Some of the causes of cybercrimes range from joblessness, corruption to greed. The solution to all these is better control measures and thorough implementation.

## Recommendations

The following are recommended for more effective control measures:

(i) The various legislations so far has not deterred the perpetrators of cybercrimes. Youth unemployment seemed to be major precursor of cybercrimes. Therefore, government should focus more on creating jobs for the teeming unemployed youths in the country. This will assist to reduce cybercrimes.

(ii) For every cybercrime there is a perpetrator. Every perpetrator has the intent to commit crime but without the opportunity a crime cannot be committed. Therefore, it is crucial to train and strengthen the capacity of law enforcement agents to ensure the opportunity to commit cybercrimes are reduced by being technologically ahead of the cybercriminals in order to curtail their excesses.

(iii) Organisations should also filter properly during the process of selection, interview and recruitment of staff as well as motivate staff to dissuade them from committing cybercrimes.

(iv) Management should train employees on how to detect and detract potential cyber-attacks.

(v) Cyber security department should be established in our institution of higher learning and cyber security should be offered as a compulsory course at all levels to boost the knowledge of cyber security in the country.

## References

Adedapo, I. (2014). Managing online information security. *The Punch*, October p.10.

Advance Fee Fraud and other Related Offences Act, (2006). Retrieved from www.nigeria-law.org/Advance%20Fee%20Fraud%20and%20other%20Fraud%20Related%20offences%20Act%202006.htm.

Criminal Code Cap. 38 Laws of the Federation of Nigeria, 2004. Retrieved from www.wipo.int/edocs/lexdocs/laws/en/ng/ngo25en.pdf.
Cybercrimes Act, 2015. Retrieved from https://www.cert.gov.ng/file/docs/cybercrime-Prohibition-Prevention-etc-Act_2015.pdf.

Economic and Financial Crimes Commission (Establishment) Act, 2004. Retrieved from www.nassnig.org/document/download/5782.

Jeetendra, P., (2017). Introduction to cyber security. Retrieved from www.uou.ac.in/sites/default/files/sim/introduction-cybers security.pdf.

Krazytech (2017). Causes of cybercrime and preventive measures. Retrieved from https://krazytech.com.

Monisoye, O.A. (2007). Cybercrime in west africa: causes, implications and effect on the legal profession. annual conference of the Nigerian Bar Association, Ilorin. 26-31 August. P.2.

Mosuro, F., (2017). Cyber security- a matter of concern for Nigerian boards. Retrieved from www.mondaq.com.

Nate, L., (2019). What is cyber security? Definition, best practices and more.

Retrieved from https://digitalguardian.com/blog/what-is-cybersecurity..

Nigerian Communications Commission, (2017) Nigeria ranks 3rd in global internet crimes behind UK, US. Retrieved from https://www.premiumtimesng.com/news/top-news/241160-nigeria-ranks-3rd-global-internet-crimes-behing-uk-u-s-ncc.html.

Nwosu, U.W., (2016). Cybercrime in Nigeria's Receding Economy: The role of the legal system. A paper presented at the 1st International conference, organised by the School of Post-Graduate Studies in collaboration with College of Management and Social Sciences, on the theme: Investment in a receding economy, 28 November – 1st December, 2016 in Salem University Kogi State. pp. 104-117.

Oladeinde, O., (2018). Nigeria's unemployment rate rises to 23.1%. Retrieved from https://www.premiumtimes.com/news/headlines/301896-nigeria-unemployment-rate-rises-to-23.1/-nbs.html.

Penal Code Law, 1959.PricewaterhouseCoopers, (2016). Retrieved from htt://www.eccouncil.org.

Punch, (2019) Retrieved from https://punch.ng.com/youth-and-cybercrime-in-nigeria.

Shittu, A., (2016). Nigeria loses N127 to cybercrime-nsa will stop this. Retrieved from https://www.thecable.ng/shittu-nigeria-loses-n127bn-cybercrime-nsa-will-stop. Techopedia (n.d.) https://www.techopedia.com.

Urgun, U & Daglar., (2016). Examination of routne activities theory by the property crime. International Journal of Human Sciences. 13(1) 1188-1192.

Usifo, V., (2017). 12 Ways to Prevent Cybercrime and Internet Fraud in Nigeria. Retrieved from https://infoguidenigeria,com.

Waziri, F.M., (2005). Advance fee fraud, national security and the Law. Ibadan, Nigeria: BookBuilder Edition Africa.

Williams, J., (2013). What is cybercrime? Definition, types and examples. Retrieved from https://study.com/academy/lesson/what-is-cybercrime-definition-types-examples.html.