CYBER CRIME AND ITS ECONOMIC IMPACT IN NIGERIA

1ENOGHOMWANSE ADESUWA
Computer Science Department
School of Science
Federal College of Education (Technical)
Asaba, Delta State.

&

2MADAKI SUNDAY DAVID
Computer Science Department
School of Science
Federal College of Education (Technical)
Asaba, Delta State
Email- 1debbietupsy@yahoo.co.uk, 2
sunnymaky7@yahoo.com
Mobile no- 08033244994, 07013700341

Abstract
Nigeria has begun to experience one of its difficult times when cybercrimes started to escalate day by day and causing loss of billions of dollars since then. Nigeria being one of the countries whose economic infrastructure is at the peak of developing has to do more in terms of fighting cybercrime before it damages the economic growth of the country. Foreign investors are finding Nigeria among the suitable places to invest and build Industrial Technology (IT) industries due to its sudden growth and acceptance of information technology and other technological advancements. This research work is to find out and discuss the trending cyber crimes that have surfaced in
Nigeria’s financial dealings from the last few years to date as well as the impact they make in Nigeria’s economy. Based on that, this paper has covered a range of contemporary cyber threats and attacks that are crippling Nigeria’s financial institutions and other agencies whose services rely on the internet platform. The paper also highlighted some challenges and solutions of cyber crime. Based on this study, the researchers recommended among others that security agencies should keep up with technological and security advancements for compliance monitoring and enforcement.

**Keywords:** Cybercrimes, Economy, Cyber-attacks, Nigeria.

**Introduction**

Cyber crime and security of information on Cyber space has become enormous challenge in key economic sector of the economy. According to (Michael, 2015) cybercrime is any crime committed or facilitated via the internet. It is moreover defined as any activity involving computers, devices, internet, be it local or global. It is important to note, cybercrime should not be confused with other conventional crimes, cyber crimes are unique because of what is involved in the act. This is why cyber crimes are being treated in a unique and specific way in the court of law. Perhaps, cyber crimes as the name implies are tricky in nature. Their approach is extremely dangerous and could cause huge loss and sometimes even cost lives.

Moreover, the widespread of cybercrime has necessitated many countries to adopt or make laws known as Cybercrime Acts. This law is only applicable to matters pertaining cyber-related crimes. Nigeria is one of the few countries that have recently passed the cybercrime Act into the law known as Cybercrime Act of 2015. Cybercrimes are dynamic phenomena that are complex and sophisticated in their nature (Shehu, 2014). Their complexity contributes to making them far beyond
comprehension. As time goes by new forms or types of cyber-attacks are emerging depending on how fast new technology evolves, new threats also evolve and new counterfeit must also be put in place in order to combat the attacks. So, in order to be able to discuss cybercrimes, there is need to specifically understand certain terminologies that are linked with cybercrimes in general, such are threats, vulnerabilities, and risk.

- **Threat:**
  According to (Mattord, 2015) threat is something that has the potential to cause harm, threats are specific to a certain number of environments, but particularly in cyber security, investigators refer to threat as anything that has the potential or capability of undermining the system’s integrity.

- **Vulnerabilities:**
  Vulnerabilities are weaknesses or mistakes that could jeopardize the entire system.

- **Risk:**
  Risk is when there is a likelihood of something bad to happen to the system. Most cybercrime cannot be treated under one umbrella, such attacks do occur in various forms and styles.

**What is Cyber Crime?**
Odinma (2017) states that cybercrime is any legal acts perpetrated in, on or through the internet with the intent to cheat, defraud or cause the malfunction of a network device which may include a computer, phone etc. The illegal act may be targeted at a computer network or device e.g. computer virus, denial of service attacks (DOS), malware(malicious
code). The illegal act may be facilitated by computer network or devices with target independent of computer network or device, particularly in Nigeria with over 90% of criminals coming from this sector. Wrong value system has been identified as the key factor encouraging cyber crime in Nigeria and the desire to get rich quick without working for it. The absence of enabling law makes policing even more difficult.

Categories of Cyber Crime

- **Hacking:** Hackers make use of the weaknesses and loop holes in operating systems to destroy data and steal important information from victim’s computer. It is normally done through the use of a backdoor program installed on the machine. A lot of hackers also try to gain access to resources through the use of password hacking software. Hackers can also monitor what a person does with the computer and can also import files on computer. (Shehu, 2014) asserted that a hacker could install several programs on a user system without the persons knowledge such programs could also be used to steal personal information such as passwords and credit card information, important data of a company can also be hacked to get the secret information to the future plans of the company.

- **Cyber-Theft:** Cyber-theft is the use of computers and communication system to steal important information in electronic format. (Schaeffer, 2019) stated that hackers crack into the systems of banks and transfer money into their own bank accounts, this is a major concern as larger amounts of money can be stolen and illegally transferred. Credit card fraud is also very common, most of the companies and banks don’t reveal that they have been the victim of cyber-theft because of the fear
of losing customers and stakeholders. Cyber-theft is the most common and the most reported of all cyber-crime because it can quickly bring experienced cyber-criminal large cash resulting from very little effort.

- **Viruses and Worms:** Viruses and worms is a very major threat to normal users and companies, viruses are malicious computer programs designed with the intension to cause the system to malfunction or misbehave. It is named virus because it spreads from one computer to another like a biological virus. A virus must be attached to some other program or documents through which it enters the computer (Strassmann, 2016). A worm usually exploits loop holes in softwares or the operating system.

- **Spamming:** Spamming involves mass amount of emails being sent in order to promote and advertise products and website. Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes not only in regards to bandwidth consumption but also to the amount of time spent downloading/eliminating spam mail (Shehu, 2014). Spammers are also devising increasingly advance techniques to avoid spam filters such as permutation of the emails content and use of imagery that cannot be detected by spam filters.

- **Financial fraud:** These are commonly called “phishing” scams and involve a level of social engineering as they require the perpetrators to pose as a trustworthy representative of an organization, commonly the victims bank.

- **Cyber harassment:** Electronically and intentionally carrying out threatening acts against individuals. Such acts include cyber-stalking.
Cyber laundering: It is an electronic transfer of illegally-obtained movies with the goal of hiding its source and possibly its destination.

Website cloning: One recent trend in cyber-crime is the emergence of fake websites that take advantage of consumers who are unfamiliar with the internet or who do not know the exact web address of the legitimate company that they wish to visit (Schaeffer, 2017). The consumer believing that they are entering credit details in order to purchase goods from the intended company is instead entering details into fraudster’s personal database, the fraudster then is able to make use of this information at a later stage either for its own or to sell to others interested in perpetrating credit card fraud.

Online charity: Another aspect of cyber crime common in Nigeria is where fraudulent people host websites of charity organizations for money, donations and materials to those organization that do not exist (Shehu, 2014). Unfortunately inheritance of millions of dollars has been exploited through this means.

Lottery scam: Allowing users believe that they are beneficiaries of an online lottery that is in fact a scam

Cyber Crimes in Nigeria
It is undoubtedly true that Nigeria as a country has witnessed a drastic transition from its old ways of managing things to a digital or rather computer age. This shift from classical ways of doing things to contemporary ones which usually comes with a price. These sudden changes do come along with the unexpected or unanticipated problems that we today call cyber crimes or electronic crimes. These crimes from the last few years have caused massive damage and loss in both the public and private sectors of Nigeria. Lack of awareness and
ignorance has also played a role in the manifestation of these attacks, this is because the country’s policy cares less about research and development, much focus is giving to building infrastructure and awarding contracts while the security of the country is at risk. Nigeria could not provide any genuine cyber law from the last 20 years until recently after countless incidents of scam known as 419. Although the cyber crime act had recently been passed by the lawmakers, yet the act does not sufficiently cover every aspect of the situation. Cyber crimes are more complicated than one could ever imagine, it is as important as any aspect of the country. However, as new threats are emerging, the law making body should always work hand in hand with research and educational institutes to ensure that the cyber laws are updated and amended as new crimes are being discovered. Currently if we are to analyze the occurrence of these events, it can conclude that most of the cyber attacks that took place (based on several reports by different agencies across the country and even beyond the country) were as a result of loopholes or attack vectors that open door to the attacker to easily gain access to the assets.(Okonigene and Adekunle, 2009).

Sometimes it happened accidentally while in the majority of cases happened as a result of mismanagement and human errors, while sometimes as a result of ego and desire to cause harm. Consequently, these cyber breaches in question are motivated by certain predictable and unpredictable elements. Massive increase in cybercrimes has been witnessed especially from 2014 to 2016 which clearly indicates that cyber crimes are moving drastically from one level to the next and therefore some measures must be put in place to combat this sudden upturn. In accounting for these events however, from 2010 to 2016, the Nigerian law enforcement agencies on different
occasions were said to have reported a number of 5,834 cases of cybercrimes which resulted in the loss of over $14,918,002. However, the report further reveals that 48.6% were females, 46% were males and the remaining 5.5% were anonymous. In most of the cases, the method or instruments of the attacks used included phishing and spamming with 4.4%, Phone hack with 16.3%, Social network attack with 13.2%, Internet fraud with 9.8%, text message with 4.2%, and impersonation with 1.3% (Scam watch 2016). Hence, billions of naira are lost to cyber theft, the majority of which were either caused by software vulnerability, unawareness, carelessness or direct attack on assets with the intention to cause implicit damage. Similarly, the Central Bank of Nigeria in a recent report reveals that over 20 billion naira has been stolen due to online crimes. This reason has led to the closure of many businesses across the country and perhaps scared away many foreign investors from investing in both the private and the public sector. The most recent statistics unveiled that most of the stolen information and assets in many organizations are due to negligence and mismanagement by administrators of those firms and 60% of former employees are said to have been the reason of several reported cases of cyber security breaches including leaking sensitive information to competitors and perpetrators in exchange for money. It is also important to acknowledge the report of the Nigerian Police Special Fraud Unit; the agency in their latest report opines that they have discovered new techniques of cybercrimes which are currently being used by the scammers (Odeyemi, 2014). A recent prediction by the Central Bank with the Chief Audit Executives of Banks with the motto “Changing Business Environment” says “Losses due to cybercrimes across all sectors have been estimated globally to hover between $400 to $550 billion in 2015”. It was said that
the figure could increase to about $2 trillion dollars by the year 2019-2010.

**Impact of Cyber-crimes in the Economy of Nigeria**

- **Information loss:**
  According to (Alese, 2014) information is the most sensitive assets for every country and even organizations including private and public. Information can be anything, it can be findings of a research conducting by the government which contains highly confidential content, it can be a payroll for security personnel and security contractors as well as top government officials whose information if leaked could jeopardize their work especially if such information is sold to perpetrators or competitors with malicious intent, this could cause a massive loss of money and reputation of the country or organization.

- **Disruption of business:**
  Thompson (2014) asserted that internet being the platform used by almost all the business firms is more exposed to this situation than any other sector in Nigeria. They are targeted mostly because of their daily transactions through e-money systems. Due to several security breach cases, many were forced to shut down their online businesses due to fear of being attacked. Conversely, a lot of foreign investors have declined offers to invest in Nigerian firms due to insecurity reasons. Hence, many e-commerce and e-businesses have suffered a drastic breakdown in the last few years.

- **Loss of reputation:**
  Reputation loss means a situation whereby a country loses its respect by investors and other international governing bodies. When people are not confident about their capability, then it becomes very difficult to achieve
anything. The loss of reputation is one of the greatest disasters as per as cyber crimes are concern. Every year more than 51 countries are suffering from loss of reputation (Shehu 2014). On a similar note, Nigerian’s President Muhammad Buhari also uttered the same statement in an interview with Telegraph that “Nigeria’s reputation for crime has made the country unwelcome in abroad”.

Loss of lives:
The use of computerized machines and chips is now becoming rampant especially in developed hospitals. Patients are put under observations using monitoring machines that are directly connected to computers. Chips are planted inside the body including the heart to monitor heart beat rates. Malicious people do take advantage of these advancements by hacking the devices and cause indirect death among the patients. Sometimes, they hack into the prescription menu and alter the prescriptions that are prescribed by doctors; thereby misguiding the doctors from given proper medications to the patients (Odeyemi, 2014) and this has resulted in killing many patients due to drug overdose

- Interruption of service:
A major DOS or DDOS attack could cause a massive breakdown of an entire infrastructure, there was a situation were the Nigeria’s electoral body was hacked using DOS attack. And also several cases of cyber attacks crippling an entire system for days Alese (2014), some for months and some forever, take Twitter DOS attack of October 21st, 2016 for instance, SoundCloud, Spotify, and several others.

Challenges of Cyber Crime
Olumide, 2015 stated that the rate of cyber crime in Nigeria has outgrown the rate of internet usage in the country. He further
stated that Nigeria is 56th out of 60 countries embracing internet usage. Why is there such an upsurge of cyber crime in Nigeria and what are the factors that made Nigerians so vulnerable to cyber crime.

- **Domestic and international law enforcement**: A hostile party using an internet connected computer thousands of miles away can attack internet-connected computers in Nigeria as easily as if it was next door. It is often difficult to identify the perpetrator of such an attack and even when a perpetrator is identified criminal prosecution across national boundaries is problematic.

- **Unemployment**: The state of unemployment in Nigeria is alarming and growing by day, companies are folding up and financial institutions are going bankrupt, companies are also embarking on mass sacks of staff. Financial institutions have put unreasonable age barriers on who is eligible to apply for jobs and embarked on mass lay-offs of staff based on ad-hoc decisions.

- **Poverty Rate**: On the global scale, Nigeria is regarded as a third world country. The poverty rate is ever increasing the rich are getting richer and the poor are getting poorer. Insufficient basic amenities and an epileptic power supply have grounded small scale industries.

- **Lack of standards and national central control**: Lack of regulations, standards, computer security and protection act are hampering through e-business, foreign direct investment and foreign outsourcing are encouraging computer misuse and abuse.
• **Lack of Infrastructure:** Proper monitoring and arrest calls for sophisticated state of the art information and communication technology devices.

• **Lack of National Functional Database:** National database could serve a means of racking down the perpetrators of these heinous acts by checking into past individual records tracing their movements.

• **Proliferation of Cyber cafes:** As a means of making ends meet many entrepreneurs have taken to establishment of cybercafés that serves as a blissful havens for syndicates to practice their acts through night browsing service they provide to prospective customers without being guided or monitored.

• **Porous Nature of the Internet:** The internet is free for all with no central control hence, different forms of Cyber crime is committed using the internet.

**Solutions to Cyber Crime**

• **Education:** Cyber rime in Nigeria is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols hence, we need to educate citizens that if they are going to use the internet they need to continually maintain and update the security on their system. We also need to educate corporations and organizations in the best practice for effective security management. For example, some large organizations now have a policy that all systems must meet strict security guidelines (Laura, 2017). Automated updates are sent to all computers and servers on the internal network and no new system is allowed online until it conforms to the security policy.
Establishment of Programs and Information Technology (IT) forums for Nigerian youths: Since the level of unemployment in the country has contributed significantly to the spate of Cyber Crime in Nigeria, the government should create employment for these youths and set up IT laboratories and forums where these youths could come together and display their skills (Laura, 2017). This can be used meaningfully towards developing IT in Nigeria at the same time they could be rewarded handsomely for such novelty.

Address Verification System: Address verification system (AVS) checks could be used to ensure that the address entered on your order form (for people that receive orders from countries like United States) matches the address where the card holder’s billing statements are mailed.

Interactive Voice Response (IVR) Terminals: This is a new technology that is reported to reduce charge backs and fraud by collecting a “voice stamp” or voice authorization and verification from the customer before the merchant ships the order.

IP Address Tracking: Software that could track the IP address of orders could be designed, this software could then be used to check that the IP address of an order is from the same country included in the billing and shipping addresses in the orders.

Antivirus and Anti Spyware Software: Antivirus software consists of computer programs that attempt to identify and eliminate computer virus and other malicious software (Alese, 2014). Anti-spywares are used to restrict backdoor program, Trojans and other spywares to be installed on the computer.

Firewalls: A firewall protects a computer network from unauthorized access. A network firewall typically guard
an internal computer network against malicious access from outside the network.

- **Cryptography:** Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient. (Schaeffer, 2017) stated that a number of cryptographic methods have been developed and some of them are still not cracked.

- **Cyber Ethics and Cyber Legislation Laws:** Cyber ethics and cyber laws are also being formulated to stop cybercrimes. It is the responsibility of every individual to follow cyber ethics and cyber laws so that the increasing cybercrimes will reduce (Laura, 2017). Security software like anti viruses and anti-spy wares should be installed on all computers in other to remain secure from cybercrimes. Internet service providers should also provide high level of security at their servers in other to keep their clients secure from all types of viruses and malicious programs.

**Conclusion**

Nevertheless, it is equally important for us to understand and acknowledge the undoubted fact that the problem of cyber fraud has now become global in both scope and impact (Michael, 2015). Hence, it is not a question of why Nigeria, or why Nigerians; it is a global issue that requires helping hands from across the globe coming together to fight it. And one of the ways for combating it is by conducting research in the areas of cyber security, cyber crimes, and by unveiling the crimes as well as proposing techniques to mitigating them, another contributing factor is the law enforcement agencies. In light of that, the agencies involved needs to improve, increase and circulate awareness programs that could help people understand
the nature of these crimes, their impact and how to mitigate or even end them.

**Recommendations**
Based on the conclusions above, the following recommendations are made:

- Cyber café operators should keep unique information of all their customers to enable monitoring of their activities, they should maintain a good database for all their customers in order to check cybercrimes.
- Government security agencies should keep up with technological and security advancements for compliance monitoring and enforcement of (1) above.
- Government should create a security awareness culture involving the public ISPs, Cybercafés government security agencies and internet users. Also in terms of strategy it is crucial to thoroughly address issues relating to enforcement.
- Government should address the issue of value-orientation among the various stakeholders of the internet especially the youths.
- Government should adopt good policy measures to create jobs to properly engage our youths in meaningful and legitimate means of livelihood.
- Government regulatory agencies should provide a foundation for verification of citizen’s identification needed to safeguard cyber cafés security.
- Operators who do not conform to regulatory standards should be shut down.
- A draft of cybercrime bill to the national assembly, should be urgently passed into law for the purpose of criminal investigation.
References