A Situation Analysis on Cybercrime and its Economic Impact in Nigeria

Muhammad Ubale Kiru
Lovely Professional University
Phagwara, Punjab, India

Sulaiman Isyaku Muhammad
Federal University, Dutse
Jigawa, Nigeria

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. The need to address this issue has become paramount before more damage is done. 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 IT industries due to its sudden growth and acceptance of information technology and other technological advancements. Thus, the critical objectives of this research work are 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 Nigeria's economy. Based on that, this paper has covered a range of contemporary cyber threats and attacks that are crippling Nigeria's financial institutes and other agencies whose services rely on the internet platform. Furthermore, recommendations on how to identify these threats are enumerated as well as the countermeasures or approaches to mitigating them.

Keywords

Cybercrimes, Economy, Cyber-attacks, Nigeria.

1. INTRODUCTION

According to [1], 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; meanwhile, cybercrimes are unique because of what is involved in the act. This is why cybercrimes 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 [2]. 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, readers have to specifically understand certain terminologies that are linked with cybercrimes in general, such are threats, vulnerabilities, and risk. (1) Threat according to [3] "is something that has the potential to cause us harm". Although he said 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. (2) Vulnerabilities on the other hand are weaknesses or mistakes that could jeopardize the entire system. Moreover, (3) risk is mentioned when there is a likelihood of something bad to happen to the system. Another key player in this discussion is the concept of detection which is part of this review. Detection according to [3] is the ability to identify the occurrence of any activity that seems illegitimate to the user and which requires the user to decide whether to respond to it appropriately or not. Detection, however, includes monitoring and analysis of events based on a received alert from part of the security systems. Detecting threats can sometimes be done with the support of intrusion detection systems, firewalls, proxy logs, event monitoring software, and tools are that specifically designed for that purpose.

According to CompTIA, most cybercrime cannot be treated under one umbrella, such attacks do occur in various forms and styles. Researchers basically categorize cyber-attacks into physical attacks, software-based attacks, network-based attacks, social engineering attacks and web application based attacks. Directly or indirectly, all the aforementioned attacks are done with a destructive intent.

1.1.Physical attacks

These are types of attacks carried out without the use of the internet or network channel that are connecting devices or computers through the target. Physical attacks are further categorized into natural attacks such as natural disasters, man-made attacks such as theft of devices like computers, tablets, PDAs and other similar handheld devices. In the recent years, physical attacks are becoming more prominent as the attackers are now equipped with mini devices which if attached to the target machine could cause harm such as key loggers and microchips.

1.2.Software-based attack

This is a type of attack that occurs on the software system and depends on the vulnerability of the software system. The attacks can either be launched at the application level, operating system level or protocol level. Their occurrence is often resulted by loopholes that are caused by human error and failure to improve or upgrade the software. The attackers use malicious codes to cause anomalies within the functional levels of the software. The major key players in software-based attacks include backdoor, rootkits, viruses, worms, Trojans, logic bombs, spyware, and macros.

1.3.Network-based attacks

Network-based attacks are considered one the most advanced types of attacks. They are referred to as network-based because they involve a sophisticated use of the internet or network in conducting such attacks. The attacker hides behind his computer and remotely accesses other people's computers without having any physical contact. The most prominent network attacks include social network attacks, DoS attacks, session hijacking, wireless device attacks, evil twining, blue jacking, war driving and so on.

1.4.Social engineering attack

In explaining social engineering attack, researchers can say that, it is a method or technique used by the attacker to influence as well as persuade the target to reveal sensitive information about their personal life, workplace or something they might be working on which requires confidentiality. Furthermore, social engineering includes the use of tricks, deception, lies and maneuvers to gain the trust of the victims and later the attacker uses that information he or she gained and attack the victims. An example of information that could be stolen through social engineering includes credit card information, passwords, security policies, staff information and much more. However, some example of social engineering includes spoofing, impersonation, hoaxing, whaling and many more.

1.5.Web application attacks

Web application attacks are closely associated with the network-based attack. This is because web applications are usually hosted on the networks, even though some of the web apps work offline, yet they require a certain amount of connection to be able to synchronize with other components of the application such as the database and web server. So, web application attacks are the types of attack that allow the attacker to directly or indirectly cause damage to the web application using the network as the gateway to the target. Most web application attacks are carried out directly using IP addresses, DNS and DHCP servers, password directory, and database of the web application. Some of the attacks on web application include SQL injection, web duplicate, password attacks, information theft such as credit card information, cross-site scripting, zero-day exploits, cookies and header manipulation.

2. THEORETICAL BACKGROUND

2.1.Cybercrimes in contemporary Nigeria

In the words of the famous Chinese Army General, Sun Tzu Wu who wrote *The Art of War* (a military treatise that emphasizes the importance of knowing yourself as well as the threat you face) he says "If you know the enemy and know yourself, you need not fear the result of a hundred battles". [4] added that "To protect your organization's information, you must know yourself; that is, be familiar with the information to be protected and the systems that store, transport, and process it; and know the threats you face". 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 usually comes with a price. These sudden changes do come along with the unexpected or unanticipated problems that we today call cybercrimes 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. It can be said that Nigerians' lack of awareness and ignorance about these electronic crimes 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. It will surprise the reader that, 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 cybercrime act had recently been passed by the lawmakers, yet the act does not sufficiently cover every aspect of the situation. Cybercrimes 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 [5] that open door to the attacker to easily gain access to the assets. 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. As a result, a survey was conducted recently by [6]. Their survey reveals the common motivating factors that are shaping the growth of cybercrimes from the last few years (see figure 1).

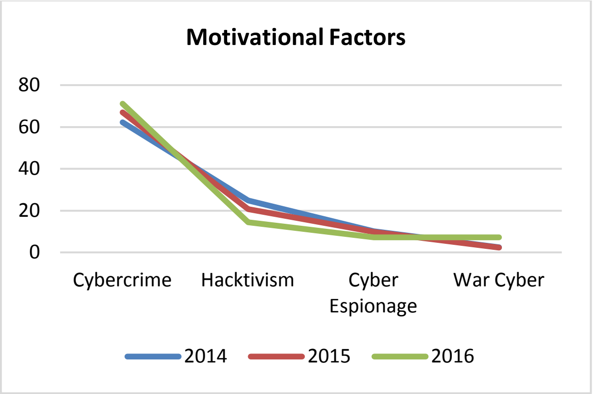

Figure 1

Based on the above chart, massive increase in cybercrimes has been witnessed especially from 2014 to 2016 which clearly indicates that cybercrimes 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 $14, 918,002. However, the report further reveals that 48.6% were females, 46% were males and the remaining 5.5% were anonymous. In most of the cases, however, the method or instruments of the attacks used included phishing and spamming with 4.4 %, Phone hack with 16.3%, Social network attack with 13.2%, Internet fraud with 9.8%, text message with 4.2%, and impersonation with 1.3$ [7].

In reporting a similar scenario, a research by[8]suggests that billions of naira were 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. He added that a report shows that "The general distribution of cyber-attacks is that 50% are hacktivism, 40% are cybercrimes, 7% are cyber espionage and 8% are cyber warfare" [9].

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 [10]. 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. Two most appealing ones include share scams –where a stranger will call you from nowhere and tries to offer you shares in a company that never existed. Next is affinity fraud –this type of attack is specifically targeting members of groups such as religious or ethnic groups to lure them into traps which will result in defrauding them [11].

More importantly, a survey by Symantec which was conducted on twenty thousand (20,000) victims of cybercrimes across twenty-four (24) countries reveals that 69% of selected population was victims of cyber-attacks at least once or twice in their life. The report added that in every 1 second fourteen (14) victims are attacked, which means more than one million attacks are being carried out every day [12]. Similarly, a statistical report by a group called the Gartner group proposes that out of the 400 websites which were audited, 97% of them were found vulnerable and therefore open to any type of attack [13]. However, more than 50% was as a result of poor implementation or lack of proper upgrades and failure to conduct vulnerability checks more often.

A recent prediction by the Central Bank Governor Mr. Godwin in [14] while speaking at the Quarterly Meeting of 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”. He added that the figure could increase to about $2 trillion dollars by the end of 2019.

2.2.Effects of Cybercrimes to the country

2.2.1. Information loss

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.

2.2.2. Disruption of business

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.

2.2.3. 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 your capability, then, it becomes very difficult to achieve anything. According to McAfee report dated June 2014, it states that 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 [15]. 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”.

2.2.4. Loss of lives

Many reports from the US have revealed that several murders were committed as a result of medical equipment being hacked [16]. The field of medicine has now advanced if compared with ten years back. 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 theprescriptionmenu and alter the prescriptions that are prescribed by doctors; thereby misguiding the doctors from given proper medications to the patients. And this has resulted in killing many patients due to drug overdose [17], [18].

2.2.5. Interruption of service

A major DoS or DDoS attack could cause a massive breakdown of an entire infrastructure. Earlier, the researchers have cited a situation in which the Nigeria’s electoral body was hacked using DoS attack. Readers have also seen how several cases of cyber attacks have crippled an entire system for days, some for months and some forever, take Twitter DoS attack of October 21st, 2016 for instance, SoundCloud, Spotify, and several others.

3. THE DIMENSION OF CYBERCRIMES IN NIGERIA

In analyzing the dimension of cybercrimes in Nigeria, one can be able to understand that many factors that contribute to what is seen as cybercrimes today. Now entities are not even bothered by attacks coming from the outer world anymore, attacks could come from both insiders and outsiders. What is meant by insider attack is “attack performed by disgruntled or malicious employee”. While outsider attack means “attack performed by a malicious individual, not within the organization” [5]. In shading more light on insider attacks, they are considered one the biggest threats to any system, as they are well aware of the system’s infrastructure as well as schematics of the organizations. They have full access and privileges, and they can easily collide with outsiders to install a backdoor that could compromise the organization’s infrastructure. Also, they are difficult to identify especially if they are at the top of the managerial hierarchy of the organizations. Moreover, they are extremely good in erasing their trace as they attack. One important thing worth mentioning is the fact that they can embed a malicious code in the system that could cause serious damage after they have left the organization.

In contrary, outsider attacks are much easier to manage if compared with insider attacks. When a proper check on the systems in done, the administrators can be able to block any future occurrence of such attack. Sometimes if lucky the attacker can even be traced by law enforcement agencies just as it happened in the famous EFCC cases of Elekwe and Yekini Labaika who scammed a Brazilian Bank and forced it to be closed completely [19].

3.1.Classification of Cyber Attackers

3.1.1. Black Hats

As mentioned in CEHv8, black hats are the types of attackers who possess extraordinary computing skills but use the skills in a malicious or destructive way. Their aims have always been the idea to destroy, damage, steal and vandalize people's assets. The majority of the black hats work at night or in hidden places in order to avoid being caught easily [5].

3.1.2. White Hats

The above-named attackers are the exact opposite of black hats. However, they are individuals with high-tech skills in security, hacking, and forensics. They mostly use their skills to defend attacks from coming in. They are mostly registered with organizations and institutes that deal with cyber security.

3.1.3. Gray Hats

Here, gray hats combine the attributes of white hat and black hat. This means that they could sometimes hide on the offensive side and sometimes the defensive side. Meaning, they can help secure your system and at the same time help the black hats find vulnerabilities in your systems.

3.1.4. Suicide Hackers

This category of hackers are said to have emerged recently. They could be individuals or group who are capable of bringing down any system or critical infrastructure for a course. By course it means, it might be a revenge, punishment or warning. And something strange about them is that they are not afraid to go to jail for their action. This is why they are called suicide hackers and they are extremely dangerous.

3.1.5. Script kiddies

Script kiddies are usually individuals with fewer skills and expertise in hacking who often compromise systems using sophisticated tools that they don't even understand. In this category, individuals can be found who are keen and curious to know how things work, therefore use their little knowledge to create damage.

3.1.6. Spy hackers

These are individuals who are highly skilled and equipped. Their knowledge of hacking is superb. They are mostly working for private companies or even the government. They are specifically hired to spy on people's assets or personal life.

3.1.7. Cyber terrorists

This group of attackers is considered the most dangerous of all groups. They consist of individual or group who are skilled, and whose major goal is to destroy people or government agencies. They are highly organized, and have the entire infrastructure they require to launch any type of attack. The majority of their targets are transportation systems, ventilation systems, hospitals, security and law enforcement agencies and so on.

3.1.8. State-sponsored hackers

This category of attacks are individuals who are extremely skilled who are often recruited by the government in order to gain top secret information or cause damage to systems that seems to pose a direct or indirect threat. A vivid example is China, Russia, and the USA. They often engage in cyber wars which result in exposing lapses of one another.

4. THE TRENDING CYBERCRIMES IN NIGERIA, THEIR IMPACT AND COUNTERMEASURES

4.1.Insider attacks

An insider attack also known as disgruntled insider attack is an example of an attack that is being carried out by an inside employee. This is regarded as one of the highest levels of cyberbreach; because an insider always has privileges and access to the system directly, unlike an outsider. So the act involves using access privileges to violate the rules and cause massive damage to the organizations [5]. According to [5], 60% of attacks occur from behind the firewalls based on a survey. And it was extremely difficult to identify the suspected insiders. Their intention has always been financial gain or revenge against the organization they work for. In Nigeria, an EFCC report shows that majority of traced advanced fee frauds were conducted by malicious insiders, the majority of which were bankers and government agents.

4.1.1. Countermeasures

CompTIA security is one of the leading institutes that provide services in security related matters has proposed the following measures for handling insider attacks.

4.1.1.1. Separation and rotation of duties

By separating employees from one another would minimize the chances of colliding to hatch any plan, and we can be able to manage them properly. Also rotate duties, meanwhile, do not allow one person to be managing one system or unit for a long time. This could help slow down their personal agenda if there is one.

4.1.1.2. Least privileges

In every organization, there must be an organizational hierarchy starting from the boss at the top down to junior staff. Do not allow everyone to have full access to the system. Let the junior staff always check with their seniors before implementing or carrying things out. This idea will help limit the degree of damage they could cause. In order to achieve this, consult with your system manager or administrator to come up with a better technology. However, in some cases, users can use user rights assignments option and security policy management console for limiting user privileges.

4.1.1.3. Access control

By implementing access control, you are limiting most of the users from accessing certain assets and resources within the organization. Of course, some assets are not to be seen by everyone. Make it in such way that, only what the employee needs that is assigned to them. Access control can be achieved at many levels. Users can set access control on the firewall systems, on the computer machines, websites and so on.

4.1.1.4. Mandatory Vocation

In highly advanced organizations, members of staff are periodically sent on a mandatory vacation. This will allow them to conduct checks and vulnerability search on the employee's computers or office. This has helped greatly in the past; many loopholes are often discovered during the checks.

4.1.1.5. Logging and auditing

Create a log that monitors all the activities of the employees. Areas to set log auditing include, log in and log out, access to the internet, access to certain server machines or computers, and access to web pages.

4.2.Scam (419 or Yahoo!)

The Nigerian scam is also known as 419 scams. According to [20]Nigerian scam predates the internet itself. It has been carried out for decades. Though, then, the attackers used to pose as Bank account managers who asked targets to help them transfer a huge amount of money by paying little charges which in the end will go back to the attacker. But recently it has changed in terms of approach; now we have different styles such as romance scams, where the attacker uses Facebook or their email to start relationship with foreigners and afterward collect a huge amount of money from them. Another form of scam is bank representatives who use their skills of social engineering to call the victims and pose as their account supervisor and lure them to releasing their credit card information. Next is the stranded traveler scam: here the attacker sends messages to the victim's friends on Facebook requesting them to send money as he or she is stranded in the middle of nowhere without money. Others which cannot be mentioned in details include Ghana scams, medical alert scams, weight loss claims, mystery shopper scams, pay in advance credit scams, pyramid scheme scams, church scams, invisible home improvement scams and many others.

4.2.1. Countermeasures

In order to tackle the Nigerian scams, we need to introduce awareness programs on both radio and TV stations where talks will be given to enlighten people on how to identify such scams. Another recommendation is by always being sensitive and overprotective of personal information. Moreover, always contact the authorities for confirmation of any anonymous claim. Furthermore, looking at it from a technical perspective, it is advised to install Anti-Scam software such as Kaspersky internet Security, Norton Internet security, Scrubkit, Risk IQ, iPensatori and much more.

4.3.Spam and Phishing attacks

Spams are typically considered unwanted grouped messages that are sent to the victim in bulk and which are by default filtered by the email server so as to protect the user. But if looked at in the other way round, spams are unsolicited emails that contain malicious codes or illegitimate advertisements that could lure the victim into a trap. While phishing on the other hand is an attempt to obtain user's sensitive information including bank details, master card information, company information, and many others by diverting the user to a fake website or by sending links to fake websites. The attackers usually pose as legitimate operators of the fake company seeking the user to confirm his or her information and it is considered very common in Nigeria. The EFCC has recently arrested several individuals on the same occasion, who posed as the staff of GTbank, Diamond Bank or First Bank. Another incident of phishing is when the attacker creates a carbon copy of an original bank site, as soon as the victims click on the link, the attack takes down whatever details the victim types on the site or page. Another most recent Phishing scam as reported by Symantec is the SMS Phishing scam, where the attacker obtains the phone number and email address of the victim, then they send an SMS pretending to be an email service provider, to the victims notifying them of a possible breach in their email account. A link for password reset will be attached with the SMS, as soon as the victim clicks on the link, it redirects him to a fake website which was earlier created by the attacker. As soon as the victim types his previous and new account details, it is visible to the attacker. Hence, the account becomes under the control of the attacker.

4.3.1. Countermeasures

For Spam attacks, the best recommendation to a non-technical person is to always cross check messages received from genuine as well as fake sources. It is very difficult to differentiate between the two, yet, if studied carefully, a fake message or email is easy to identify. However, most spams will start by congratulating you for a prize or gift you did not earn. Secondly, they are always asking for personal questions. Thirdly, the sender's information such as name is always misspelled, for instance, Microsoft is spelt as Microsotf. Looking at the situation from a technical perspective the following tools are recommended for counterfeiting spams: AEVITA Stop Spam Email, SpamExperts Desktop, SpamEater Pro, Spam Weasel and many others [21].

Phishing attack, the first step to be taken is to visit anti-phishing sites where you will be able to find lists of fake websites. Copy the links and add them to your spam filters so that such websites could be blocked as soon as they try to redirect you there. The best remedy for Phishing attack is the use of phishing detection tools. These tools would help isolate fake websites or links from genuine ones. They can also send notification or alerts to users cautioning them about the phished sites. Some of the Examples of anti-phishing tools include Netcraft, phishtank, GFI Mail Essential, SpoofGuard and so on [22].

4.4.Social Network

These types of attacks are peculiar to social networks such as Facebook, Twitter, WhatsApp, Instagram and many others. This act involves gathering confidential information about users, creating groups to allow extraction of information, imitating and copying the behavior of victims' friends, false identity claim, and identity theft or impersonation. Usually, the imposters approach the victim in disguise and solicit for friendship. In more than average of such cases, they pose as former friends. After having a good time with the victim, they begin to send nude pictures or uttering vulgar words that are easily inviting. Social network attacks might even escalate sometimes, as several cases of murder were reported more often. The victims end up meeting with their online fake lover, after meeting they end up dead or robbed. Readers can find lots of similar examples in that regard, amongst the famous social network frauds include 'bag of rice fraud', where the attacker posed as a businessman who sales food items, they offer a good price to the victim knowing that there is ascarcity of rice in the market, and later defraud the victims. Car auction is also another new form of fraud where an anonymous person poses as a 'Custom Officer' who will offer you a chance to get a 3 Million naira car for about six hundred thousand naira. Later they rob the victims or even kill them. It is important to note, social network attacks are directly linked to attacks on businesses and organizations. Intruders could trace an employee of an organization, by so doing, they can use him to get to the organization by sending him malicious malware that could open a door for them.

4.4.1. Countermeasure

To avoid social network attacks, you have to dig deep into a person's identity before accepting their friend request. You can do that by searching their names on Google search engine, or by looking at their friends, who they follow and who follow them. Abstain from people who request you to help them transfer money or buy something from them. As for employees, do not allow staff to access social network using company computers or download software. Also, avoid sharing details of deceased people, as people can easily impersonate them and avoid sharing details about your personal life on social networks, as the attackers could use your personal information to launch a brute force attack on your system. Revealing your personal information online always makes you an easy target.

4.5.Google attacks

Many of the readers would be surprised to know that Google search engine is a great tool for launching cyber-attacks. Looking at it critically, the intention of Google as a search engine is not to be used as a weapon of destruction rather as a search engine. Unfortunately many have turned the power of Google engine from a searching tool to nasty thing. Some of the possible attacks that could be launched using Google search engine include reconnaissance, foot printing, vulnerability and exploit search. All the mentioned activities are used as tools for finding and gathering information about possible targets. To be more specific, exploit search is used for identifying networks and systems which are having vulnerabilities that could be exploited. An exploit is a weakness of a system that can open door for any possible attack into the system. However, it is revealed that there are thousands of websites that publish hundreds of exploits every day. These exploits are posted by black-hat hackers who want other hackers to have access to those exploits. Locating exploits is very easy especially if the attackers know what they are doing. The main source of exploits come from systems that are unpatched, security devices with loose configuration, systems with programming error and reckless staff who do not manage their systems properly [23].

4.5.1. Countermeasures

The Internet in its nature is designed to cache users' information on the internet. Therefore, it keeps track of users' information whether known or unknown, and this information can be used maliciously by the attackers. According to [23], the best way to address Google hack is to choose which part of your system should be exposed and which should be kept from the public cyberspace. To do that, users have to enforce solid security policies on the infrastructure. Without a good security policy, users could easily be compromised. Secondly, they propose that for the information to be secured online, users have to hide certain directory structure of the systems, so that internet users could not lay their hands on them. They further recommend a small text file named Robot.txt which helps prevent the internet from caching your information. More about robot.txt could be found on www.robotstxt.org/wc/norobots.html.

4.6.Online theft

Online theft is generally referred to as 'Yahoo! or 419' in Nigerian context. Such practitioners are called Yahoo Boys. Going deep into it, online theft or cyber theft is one of the popular and most prominent types of cyber-attack. It basically involves any type of breach which enables the attacker to steal information or assets without the knowledge of the owner. It also includes breaking into databases to steal customer's credit card information, computer passwords, money from bank accounts, and so on. It is mentioned by [13] that most of the victims are banks, computer companies like Microsoft, Online Sellers and Email service providers like Yahoo! and Google. However, the most reported cyber theft in Nigeria is the stealing of Debit card information and illicit transfer of money from victims' bank account to the target's account. In a recent report by the EFCC, a 40-year-old Mike who is alleged head of a network of 40 individuals who were behind global scams worth $60 million across the world was nabbed by the agency in the southern city of Port Harcourt. According to Interpol, his operations include using malware to compromise sent emails to the victims, as well as romance scams. Interpol added that in one scam alone, the victim was conned into paying about $ 15.4 million [24].

4.6.1. Countermeasures

Online theft is very sophisticated that no one can avoid it completely. Starting with credit card theft, this type of theft can occur in the following ways: (1) either by physically stealing the credit card or (2) by stealing the credit card information. The best approach to this is to always report missing credit cards immediately. The second approach is to be extra careful before inserting your credit card into ATM machines, as recently it has been discovered that small chips are fixed or attached to the ATM card slot, as soon as you slot the card it copies the card's information. To avoid that, always pull back the ATM card slot in the machine to make sure that no external cover is attached. As for other forms of theft especially internet thefts, use strong passwords and endeavor to change your passwords regularly. Also, care to install a genuine operating system and antivirus. Moreover, avoid typing your confidential information directly using the computer keyboard, alternatively, use logical keyboard (for example Logitech software). This tool would hide all the keys pressed from the intruders.

4.7.Social Engineering attack

As mentioned in the beginning of the paper, social engineering attack in its earlier days was not more of an attack that involves the use of sophisticated network tools or computers. However, the social engineering attack of this generation combines the use of programmed tools as well as trickery. So basically social engineering is the act of convincing people to reveal personal or confidential information, something they wouldn't normally do for you, through deception, lies, and tricks [25]. According to EC-Council "Social engineers depend on that fact that people are unaware of their valuable information and are careless about protecting it". Generally speaking, social engineering starts with the attacker researching about the target or victim, after that they select their victims based on certain attributes and fulfillments, thereafter they develop an intimate relationship with the victims and finally exploit the relationship after gaining all their trust.

The most common type social engineering attacks in Nigeria include traveler who has lost his money and wants to go back home, soliciting money for charity organizations, soliciting money to buy Quran for educating children in Islamiyya schools especially in the Northern part of Nigeria. Another one is that which the attacker sends a Facebook message telling you that he or she is involved in an accident, so needed money to call home. It is evident that, in the recent case of one Idris Obaro who got nabbed by EFCC in December 2016. Obara used his social engineering skills and posed as a head of finance in the Ministry of Petroleum Resources. He lured the complainant into believing that he can get a job for him in the ministry and later agreed to pay the sum of N300,000.00 as a fee for employment [26]. Similarly, one Tonweringha Oyintonbra was arraigned by the same agency over the allegations that he defrauded one Izabela where he posed as a trader representing Yoshinaka Corporations, thereafter convinced her to pay about 53,000 Euros into a partnership, in the end, he disappeared.

4.7.1. Countermeasures

These days more than half of cyber-attacks depend on social engineering. This is because many are unaware of the tricks behind it. The best remedy is to introduce a program where enlightenment lectures are given on security policies, trending social engineering tips and how to handle them. Also, endeavor to enforce password policies to avoid guessing and brute force attacks. Use physical security tactics by introducing ID cards, uniforms and so on. Also, escort the visitors anytime they come in to avoid tailgating and access to restricted areas. Hire good helpdesk officers, as report shows that helpdesk officers are the most vulnerable part of an organization as far as social engineering is a concern. Finally, shred or burn sensitive documents to avoid dumpster diving [27].

4.8.DoS and DDoD

Both attacks are treated almost the same, although they differ in their ways of operation. Both the attacks are carried out with the intention to halt operations and services from running in order to achieve one or two benefits. Here, the victim's system is flooded with multiple requests that are initiated from acompromised system known as a zombie which send requests that are beyond the capacity of the system to deliberately crash the system or network. In most of the cases, the targets are large organizations or service providers, and the attack might turn out to be a diversion for bigger attacks. These attacks could be terrorist attacks, attacks on airports, telecoms and so on. DoS attack is not prominent in Nigeria, but some traces of it were found in the telecom giant MTN where their entire network failed for several hours. The most recent DoS attack was reported by the Independent National Electoral Commission (INEC) on March 2015. INEC confirmed that hackers had pulled down their websites for several days and indeed confirmed it was a DoS attack [28].

4.8.1. Countermeasure

DoS and DDoS attacks are often difficult to detect, and it is believed that there is still no immediate technique for stopping it[3]. However, DoS and DDoS can easily be detected as soon as users find abnormalities and noticeable deviation from the normal network traffic statistics. The following suggestions say that in times of such attack, configure TCP protocol to intercept and validate all incoming connection requests that seem suspicious. Configure logs that could monitor any slight change in the usual traffic. This can be achieved by using tools like NetFlow Analyzer, D-Guard Anti-DDoS firewall. Also, implement a load balancing system which will absorb traffic. And lastly, implement a honeypot. A honeypot is a configuration that is done on an isolated system that has all the properties of the target machine. This could help divert the attention of the attack and end of thinking they are attacking the real server [29].

4.9.Malicious Software attack

Software attacks occur when the attacker designs, alters and deploys a particular software for the purpose of creating a malfunction or anomalies in the software [4]. Several cases of cyber-attacks reveal that malicious code attacks occur as a result of software programming bugs that were planted in the system along time ago by the programmer or the company that carried out the design of the system, or by a disgruntled employee of the organization. This will give the malicious attacker access to the software any time in the future. Many surveys proved that malware is the key player and a suitable weapon for the majority of the attacks carried out on software. In a nutshell, malwareare programmable codes or components designed purposely to damage, destroy, deny access and or cause the target system to work based on how the attacker wants [4].

It has been discovered recently that websites owners are using a technique known as Drive-by Download (DbD) to hack visitors. Here, a malicious software program that is embedded within the website is installed on the victim's computer so that information such as IP address, MAC address, and other sensitive information could be stolen. And this information is used to conduct botnet attacks or use the victim's computer to carry out bigger attacks such as DoS attack. As revealed by a Google security report (2016), in every 20 websites 2 are involved in this crime.

4.9.1. Countermeasure

In counterfeiting this problem, ensure to secure the design and development process of the software from low-level employees, meaning only a few personnel will have access to the program. Make it necessary to hire a different programmer to conduct different bug testing such as runtime error testing, program transformation testing, and other similar security tests. Another solution is to obfuscate the code. Code obfuscation according to [3] is the deliberate act of creating the source codes which are difficult for human beings to understand. This could help in hardening the chances of penetrating through the system. Other steps to be taken in mitigating software attacks especially DbD attack is to disable all options on the browser which can give access to cookies and other temporary browsing files that could retain some information.

4.10. Cyber Espionage and Trespassing

Both terms are often used interchangeably to refer to an act of security breach or activity that gives the attacker unauthorized access to confidential information that does not belong to him. Both the attacks can be conducted electronically as well as physically. One example of espionage is known as shoulder surfing, this describes an instance whereby the attacker tries to oversee what the victim is doing over his shoulder especially during ATM machine withdrawals. Another type of this attack is dustbin diving. Here, the attacker searches for any sensitive information in dustbins and recycle cans where disposed papers are being thrown after use. Hence, such disposed information might be useful to an outsider with malicious intentions.

4.10.1. Countermeasures

Espionage, in general, is very difficult to detect; because you might not know who is up to you. But the best practice is to be extra cautious whether you are under attack or not. Take for instance shoulder surfing. Always ask the person standing beside or next to you to excuse you before accessing the ATM, because it's your right to have privacy. The second issue is duster diving. Do not tier papers, instead, shred them or burn them. Moreover, do not keep quite when you found such, always report to the nearest police station. As for trespassing on property, ensure to install surveillance cameras in every angle of the building so that you have a full coverage of what is going on day and night. Nowadays there are cameras with motion sensors; there are even cameras that look exactly like light bulbs. You can install such types for disguise.

4.11. Cyber hijacking - Session hijacking and keyloggers.

Session hijacking simply means the exploitation or capturing of a valid computer session that is actively going on between two or more users. Hijacking enables the attacker to steal information that is being transmitted over the network between two or more end-users. It can take place at both network level and application level. Types of hijacking include TCP/IP hijacking, IP spoofing, blind hijacking, and Bluetooth jacking.

Keylogger attack on one hand is the act of hijacking victims' keystrokes in form of alphabets and numbers. The attacker uses both software and hardware to steal all the words and phrases that are typed by the victims on their computers. They are able to do that by installing keylogger software into the victim's system or by plugging a removable device that could steal the information. Moreover, keylogger attack is one the most prominent cyber-attacks in Nigeria. It often takes place in cyber cafes and computer centers or rather business centers as people call them.

4.11.1. Countermeasures

The best countermeasure for cyber hijacking is to ensure that your communication channels are secured using the appropriate protocol such as SSL, IPsec, PPP, VPN and L2TP. These protocols are aiding in encapsulating any message that is sent over the network between the server and the browser, so that even if they got hijacked, they will look encrypted and difficult to break. Also minimize connecting to your system remotely unless necessary [30]. As for keylogger attacks, always check your keyboard plug point for any suspicious devices. Run a keylogger check using any of the anti-keylogger software such as Zemana Antilogger, SpyShelter and much more. Also, ensure to use Virtual Keyboards when typing sensitive information.

4.12. Device theft - Phone theft, drives

Device theft is the act of stealing handheld devices in form of mobile phones, PDA machines, Palm tabs, Tablets and many others for financial or fraudulent benefits. Device theft in Nigeria is one of the disturbing stories that are frequently heard in almost every police station in the country on daily basis. There is perhaps a small mobile phone market in a place called Palm Centre where such thefts are done expertly and mercilessly. Although in most of the reported cases, the theft is done for financial benefits, not with intention to hack or cause damage. While in few cases it is done to steal information such as pictures, text messages, emails and mobile contacts. Perhaps the theft of hard drives and pen drives is rare, yet they happen once in some few occasions.

4.12.1. Countermeasures

It is very difficult to stop device thefts because thieves are always one step ahead of the owner. The best way to handle device thefts is to implement a GPS tracker on the device. For Apple (iPhone, IPad) devices, it is already in-built and embedded within the devices, all you have to do is to configure it from 'icloud.com'. For Android devices, you have two options, you can download an app from Google store for tracking devices, or you can use Google device Manager that is located in the following link'www.Google.co.in/ android/devicemanager'. This platform will give you all the help you need to track your devices. For hard drives, always go for drive encryption, so that the content of the drive becomes useless to the attacker. And to do that, go to Google and type "how to encrypt my drive" many helpful options will appear.

4.13. Spoofing and forgery

These days the computer seems to be the best tool for forgery. The key player here is spoofing. Spoofing is basically an instance whereby the attacker or intruder sends a message that looks like it is coming from a trusted system. This is achieved when the intruder forges his IP address into a trusted IP address to make the mail server believe that the message is authentic and is coming from a verified source. This usually happens when the intruder stays in between two or more trusted end-users who engaged in an exchange of message, data or information, and then hijacks their IP address and then get it spoofed. Spoofing works on two major things, viz, MAC address and IP address. The most prominent types of spoofing apart from the earlier mentioned include impersonating someone's identity on social networks. According to Facebook (2016) 50 million impersonated accounts are deleted every year after confirming they don't belong to the original users. However, most of the victims of impersonation include celebrities, politicians, and deceased people.

4.13.1. Countermeasure

Security specialists believe there is not a way for detecting or identifying spoofed message manually. Perhaps nowadays using the latest routers and firewalls can really work against IP and MAC spoofing. They are so smart enough to detect such attacks.

4.14. Cyber Extortion

Information extortion is one of the oldest types of cyber-attacks, especially in developed countries. So, extortion is when an attacker (insider or outsider) steals sensitive information from victims and threaten to expose the information unless compensation is given or some agreement is reached between the attacker and the victims. Extortion is more common among Bankers, Doctors, therapists, and police. The aforementioned players by nature are having direct access to the victims' information. Most of that information is related to health, previous crimes, looted money and other social problems. Therefore, extortion always ends with blackmail, bullying, and defamation. This issue is mostly found in southern part of Nigeria. Among the techniques used in extortion includes hacking victims laptop cameras and their photos are taken mostly in their rooms while having their private times. Another example is mobile phone call hijacking which is mostly conducted by employees of telecommunication companies. Next is what is referred to as bluejacking. Bluejacking has just surfaced in Nigeria, meaning, it was not a practice until recently when sophisticated mobile phones emerged. Bluejacking occurs when the victims forget to switch off their Bluetooth, therefore the attacker tries to search for any open Bluetooth. As soon as the signal is detected, the attack uses software to pair the two phones. Hence, whatever the victims say, they record instantly. The last example in this category is cyber pornography that is becoming more rampant these days. Many celebrities and famous people are subject to this type of attack. The attackers often steal the photos of the victims through several ways. In most of the cases, the victims take their phones to charge their battery in public places, while some, use laptops that happen to have Picasa picture software installed on them, as soon as a phone is attached, Picasa copies all the photos that are stored on the phone and save it in the system. More importantly, a charging point malware attack known as Juicy Jacking is also at large. The attacker scouts for a public place like Airports and Train stations where people plug their phones for charging. As soon as the phone or device is plugged, a malicious malware is transmitted through the USB cable of the charger. At last, it sends the entire important document in the device.

4.14.1. Countermeasures

Sometimes users cannot prevent cyber extortion from happening. Although, the best practice is to avoid revealing personal details on the internet and social networks in general. Also, it is a good practice to regulate the amount of content a mobile phone should have such as pictures and personal secrets. Instead of storing such types of data on the phone's drive, always go for cloud storage such as Google drive, DropBox, iCloud, OneDrive and so on. Furthermore, do not charge your phone in public places using UBS cable; instead use a charger, because nowadays, there are charging points that embed a malware that steals your information while charging.

Next is cyber pornography; not all cyber pornographies of victims are true, so don't panic. In most cases, the attackers fix the picture of the victim into a naked body of someone who is into pornography, thereby making it look like they are the ones. So, do report such acts as quickly as possible. Although the imposters do threaten the victims if they report to the police, yet, it is better to report than to handle it alone, as most victims were found dead afterward.

4.15. Collaborative Insiders attack

A collaborative insiders attack usually takes place due to collaboration between Bank employees and Telecoms Company employees, where both parties gather all the victim's details and try to steal his money through a false confirmation via mobile call. In this attack, a bank employee will draft a cheque with the name and signature of the victim. Then collaborate with another employee that is working in a telecoms company where the victim is subscribed to. The telecoms official will temporarily block the victim's number and divert the call to another phone. As soon as they attacker present himself at the bank counter to cash out, a call is made to the victims mobile for verbal confirmation, this usually comes officially from the Bank. Therein, the fake owner would answer the call and give confirmation to approve the withdrawal. This form of cyber hack had happened in the past and is still happening.

4.15.1. Countermeasure

The bottom-line here is to collaborate with your bank account manager. If you don't have one, request the bank to assign one to you. Request your account manager to call you twice on two different numbers to confirm any transactions. This solution will be easier to reduce the chance of the attack. However, the banks should also ensure that personal details of their customers are only visible to some selected high-ranking employees. This can be done through implementation of something known as 'View policy' in database management system, that is, only financial information will be visible, any other information such as home address, mobile number, spouses, and children should will not appear. Lastly, telecoms companies should ensure the same strategy, i.e. only certain employees should have access to performing such operations; otherwise these could damage the reputations of the companies as well as compromise the safety of others.

4.16. Backdoor Attack

Here, the attacker uses a technique known as backdoor that is capable of carrying a payload which is accompanied by a legitimate software or file which is installed on the victim's system. After which access is giving to the attacker remotely. An example of the payload includes subseven and back orifice [4]. In Nigeria, this type of attack is often found in Internet cafes. They use anybody who wants software to be shared with them as the easy targets. The agent capable of carrying the payload is a pen driver, in other words, flash drive. The shared software usually has a backdoor embedded in it, as soon as you launch the software or application, the backdoor is simultaneously installed in the background. By background it means, it is invisible to the user. Another agent as well as tool for carrying such attack is the Trojan horse. A Trojan if successfully installed on the victim's system allows the attacker to take control of the system. The attacker has visual access to the victim's system; they can control and manipulate the system, as long as the system remains online.

4.16.1. Countermeasures

The first measure to be taken is to avoid using free online software programs, as majority contain Trojans and back doors, scan your emails before opening or downloading attachments, block all unnecessary ports that are not in use, monitor your internet traffics. More so, the best way to handle a backdoor attack especially when Trojans are involved is to scan for any suspicious open ports and running processes using Port Monitoring tools like 'Ice Sword' or 'CurrPort and TCPView', scan your computer registry using tools like 'SysAnayzer', 'Registry Shower' and 'All-seeing Eyes', and scan for any suspicious network activities using tools like Capsa Network Analyzer. This is because Trojans can only work in the background; they hide within other computer services, thereby making it difficult to be detected. Other recommended tools for fighting Trojans include Trojan Hunter, Emisisoft Anti-Malware and so on [31].

4.17. Doxing

Doxing is one of the advanced hacking techniques in which the attacker gathers information about the target and publish it online with the aim of luring the victim into a trap, as soon as you read the information, an embedded malware is installed on your system. With that, they can know your where-about, have access to your financial records, and other sensitive information. This technique is nowadays popular among unauthorized online magazines.

4.17.1. Countermeasure:

In order to stop Doxing, always make sure your anti-virus is up to date and has what it takes to detect such embedded malware even before visiting the sites.

4.18. Proxy attacks

The use of foreign and domestic proxy servers to launch attacks under the feet of some countries have contributed immensely by making it difficult for law enforcement agencies to be able to track criminals and try them in a court of law. This is due to the fact that the proxies are created through some target countries other than the country of the attacker. Sometimes the attacker forms a ring-like structure of ten to twenty proxies which are set in different countries. By so doing the attacker creates a diversion that looks like the attack is coming from a known location, while in reality, they are triangulating the attack so as to become invisible to radar. The inability of the agencies to detect this attack is what makes it difficult for EFCC to be able to arrest and try criminals in Nigeria due to lack of evidence. As a result, several cases were left unsolved and the perpetrators are still at large.

4.18.1. Countermeasures

The proxy attack is advanced and sophisticated in nature; it is even difficult for agencies like FBI and CIA to track down. The best solution is to have a joint force that could bring organizations like Internet Assigned Numbers Authority (IANA), Proxy services providers and government agencies under one roof. The collaboration of the respected bodies will help in figuring out who is behind the attack. Until and unless there is such joint force, proxy attacks would be very difficult to trace due to border barriers and other bureaucratic issues.

4.19. Software piracy and copyright crimes

Software piracy is basically the distribution of unauthorized as well as illegally acquired software copies or the modification of a software program without the prior knowledge of the inventor or owner of the software [13]. As far as software piracy is concerned, India, Nigeria, and China are in the forefront in software piracy. Microsoft in 2015 reported that a multi-year investigation by Chinese police in collaboration with the US FBI led to uncovering of two of the world’s largest piracy markets in Shanghai and Shenzhen in China who were responsible for the distribution of up to $2 billion of software. As a result, 1000 customers were sent notifications notifying them that the software they purchased were indeed pirated [32]. Back in Nigeria in 2010, the Nigerian Communication Commission (NCC) in a joint raid with Microsoft reveals that, the premises of one Genuss investment limited, a leading figure in computer resell at Computer Village located in Ikeja, Lagos, recovered over five thousand software programs belonging different software vendors across the globe including Windows XP disks, Microsoft Office, and many others [33].

4.19.1. Countermeasures

It is basically tedious to stop piracy, as new strategies are being developed, the perpetrators are also doing their best to break us. [34] Recommends the use of a mechanism to stop piracy known as Digital right manager. DRM “restricts the use of digital files by unauthorized user in order to protect the concentration of copyright holders“. Moreover, “it controls file access, copying, modification, and deletion”. Other tools to use for software piracy include CrypKey and DF_ProtectionKit [34].

5. 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 [19]. 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. Nigeria is actually lacking in this regard. Government should at least give a little priority to this area by establishing a cyber crime handling division within the police or as an independent entity. Hire professionals and experts in areas of cyber security, forensics investigation, incident handling and other crucial branches of cyber security that could add more weight to the agency. Moreover, when looking at the scope of cyber crimes in Nigeria from another point of view, one could tell with absolute certainty that illiteracy and lack of good governance are playing a sigficant role in the failure to manage the situations carefully. If awareness programs are to the introduced it would surely help those victims handle themselves to some degree. So that a shift of responsibility will be established between those fighting the crimes among the law enforcement agencies and common people. In light of that, the researchers urge the agencies involved 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. The recent Wannacry outbreak has caused Nigeria a lot due to unawareness and lack of proper handling approches. The researchers believe with the above suggestions a lot of the cases will be cut down significantly.

6. ACKNOWLEDGEMENT

This is to acknowledge that this research has not been funded or supported by any funding agencies be it private, government or academic. It is the intention of the researchers to conduct a review of this research area. Therefore, the researchers acknowledge that it is purely our work and none of the primary or secondary data comes as support from any organization.

7. REFERENCES

[1] National Crime Prevention Council, “Cybercrimes,” *Bur. Justice Assist.*, pp. 1–4, 2012.

[2] A. Y. Shehu, “Emerging Issues in Cyber-Crime: Causes, Implications and Effects for the Legal Profession,” *Online J. Soc. Sci. Res. ©2014 Online Res. Journals Full Length Res. Artic.*, vol. 3, no. 7, pp. 169–180, 2014.

[3] K. Michael, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, vol. 31. 2012.

[4] M. E. W. H. J. Mattord, *Principles of Information Security Fourth Edition*, 4th Edicat. Cengage Learning, 2012.

[5] EC Counsil, “CEHv9 - Module 01 - Introduction to Ethical Hacking.” 2014.

[6] R. Al Halaseh and J. Alqatawna, “Analyzing CyberCrimes Strategies: The Case of Phishing Attack,” *2016 Cybersecurity Cyberforensics Conf.*, pp. 82–88, 2016.

[7] ScamWatch, “Nigerian Scams,” 2016.

[8] O. J. Olayemi, “International Journal of Sociology and Anthropology A socio-technological analysis of cybercrime and cyber security in Nigeria,” *Int. JOurnla Sociol. Anthropol.*, vol. 6, no. 3, pp. 116–125, 2014.

[9] D. D. Odeyemi, “Cybercrime Event,” 2013.

[10] B. K. Alese, A. F. Thompson, K. V Owa, O. Iyare, and O. T. Adebayo, “Analysing Issues of Cyber Threats in Nigeria,” *Proc. World Congr. Eng.*, vol. I, 2014.

[11] PSFU, “Understanding Fraud and ways to recognize it,” 2016.

[12] J. Jang-Jaccard and S. Nepal, “A survey of emerging threats in cybersecurity,” *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2014.

[13] A. Razzaq, A. Hur, H. F. Ahmad, and M. Masood, "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications," *2013 IEEE Elev. Int. Symp. Auton. Decentralized Syst.*, pp. 1–6, 2013.

[14] P. Okafor, "Nigeria: Global Cybercrime Loss to Hit U.S.$1.5 Trillion By 2019," *Vanguard Newspaper*, Lagos, Nigeria, Dec-2016.

[15] J. Armin, B. Thompson, D. Ariu, G. Giacinto, F. Roli, and P. Kijewski, "2020 cybercrime economic costs: No measure no solution," *Proc. - 10th Int. Conf. Availability, Reliab. Secur. ARES 2015*, pp. 701–710, 2015.

[16] ICIT, "Hacking Health care IT in 2016," 2016.

[17] B. Filkins, "Health Care Cyberthreat Report," *... , compliance nightmare horizon. Bethesda, MD ...*, 2014.

[18] J. Niccolai, "Thousands of medical devices are vulnerable to hacking, security researchers say," *PC World*, Sep-2015.

[19] F. Ibikunle and O. Eweniyi, "Approach To Cyber Security Issues in Nigeria: Challenges and Solution," *Int. J. Cogn. Res. Sci. Eng. Educ.*, vol. 1, no. 1, pp. 100–110, 2013.

[20] O. Toppol, "Nigerian Email Scam, Phishing Attacks & More: Beware of Your Inbox," *BlogDog*, May-2015.

[21] E. Bash, "Ethical Hacking and Countermeasures: Spamming," *PhD Propos.*, vol. 1, pp. 5–20, 2015.

[22] EC-Council, *Ethical Hacking and Ethical Hacking and Countermeasures v6 Module LVI : Phishing Attack*. 2013.

[23] J. B. Johnny Long, Bill Gardner, *Google Hacking for Penetration Testers*, Third Edit. Elsevier, 2016.

[24] BBC, "Online fraud: Top Nigerian scammer arrested," *bbc London*, London, Aug-2016.

[25] J. D. Demott, A. Sotirov, and J. Long, *Gray Hat Hacking , Third Edition Reviews*. 2011.

[26] EFCC, "Job Scam," *EFCC Media & Publicity Unit*, 2016. .

[27] EC-Council, *Ethical Hacking and Countermeasures: Social Engineering Attacks*. 2013.

[28] C. Ebuzor, "Anti-hack team over-rides hackers DDOS(Denial of service) attack on INEC's website," *Pulse Nigeria*, 2015.

[29] EC-Council, *Certified Ethical Hacker v7: Denial of Service Attacks*. Ec-Council, 2015.

[30] EC-Council, *Certified Ethical Hacker v7: Module on Session Hijacking*, Edition 7t. Ec-Council, 2014.

[31] EC-Council, *Certified Ethical Hacker v7: Module on Trojans and Backdoors.* Ec-Council, 2014.

[32] C. Microsoft, "Piracy Report of 2014," 2014.

[33] E. Okonji, "Nigeria: NCC Raids Computer Village Over Software Piracy," *All Africa*, Lagos, Jun-2010.

[34] EC-Council, *Ethical Hacking and Countermeasures v6 . 1 Module L : Software Piracy and Warez Exam 312-50*. Ec-Council, 2013.