International Journal of Scientific Engineering and Technology
(Engineering Collection-Innovative Research Publication Journals)
https://dx.doi.org/10.22624/AIMS-22667

ETHICAL HACKING AND CYBER SECURITY IN NIGERIAN TELECOMMUNICATION INDUSTRY

Sarumi, J.A & Ibraheem Abdul-Raheem

Department of Computer Science

Lagos State University of Science & Technology

Ikorodu, Lagos State, Nigeria

E-mail: jerrytechnologies@yahoo.co.uk

ABSTRACT:

The issue of cyber security is one that has been discussed by many people in various perspectives, most coming at it from different sides than the others. Cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries as the United States. The illegal act may be targeted at a computer network or devices e.g., computer virus, denial of service attacks (DOS), malware (malicious code). However, ethical hacking has been used by various telecommunication companies to cover the loophole and this study is identifying the problems and providing an overview on the issues and the solutions. Cybersecurity through ethical hacking plays an important role in the ongoing development of telecommunication industry, as well as Internet services. Enhancing Cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being (Odinma, 2013). Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.

An ethical hacker is a computer and networking expert who systematically attempts to penetrate a computer system or telecommunication network on behalf of its owners for the purpose of finding

https://dx.doi.org/10.22624/AIMS-22667
security vulnerabilities that a malicious hacker could potentially exploit (Okonigene & Adekanle, 20016).

Ethical hackers use the same methods and techniques to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security (Laura, 2015). The purpose of ethical hacking is to evaluate the security of a network or system's infrastructure. It entails finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible. Vulnerabilities tend to be found in poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures. One of the recent examples of ethical hacking occurred in the 2010, when the United States government used groups of experts called "red teams" to hack its own computer systems (Laura, 2015). It has become a sizable sub-industry within the information security market and has expanded to also cover the physical and human elements of an organization's defenses. A successful test doesn't necessarily mean a network or system is 100% secure, but it should be able to withstand automated attacks and unskilled hackers.

The exceptional outbreak of cyber-crime in Nigeria in recent times was quite alarming, and the negative impact on the socio-economy of the country is highly disturbing. Over the past twenty years, immoral cyberspace users have continued to use the internet to commit crimes; this has evoked mixed feelings of admiration and fear in the general populace along with a growing unease about the state of cyber and personal security (Oliver, 2010). This phenomenon has seen sophisticated and extraordinary increase recently and has called for quick response in providing laws that would protect the cyber space and its users.

Nigerian cyber criminals are daily devising new ways of perpetrating this form of crime and the existing methods of tracking these criminals are no longer suitable for dealing with their new tricks (Adebusuyi, 2018). The victims as well, show increasing naivety and gullibility at the prospects incited

https://dx.doi.org/10.22624/AIMS-22667
by these fraudsters. This paper seeks to give an overview of ethical hacking and cyber-security in Nigerian telecommunication industry, outline some challenges and proffer solutions.

KEYWORDS: CYBERSECURITY, ETHICAL HACKING, TELECOMMUNICATION, CHALLENGES, INFRASTRUCTURES, VULNERABILITIES.

INTRODUCTION

1.1 BACKGROUND TO THE STUDY

Cybersecurity through ethical hacking plays an important role in the ongoing development of telecommunication industry, as well as Internet services (Odinma, 2013). Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being (Odinma, 2013). Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.

An ethical hacker is a computer and networking expert who systematically attempts to penetrate a computer system or telecommunication network on behalf of its owners for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit (Okonigene & Adekanle, 20016).

Ethical hackers use the same methods and techniques to test and bypass a system's defenses as their less-principled counterparts, but

https://dx.doi.org/10.22624/AIMS-22667

rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security (Laura, 2015). The purpose of ethical hacking is to evaluate the security of a network or system's infrastructure. It entails finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible. Vulnerabilities tend to be found in poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures. One of the recent examples of ethical hacking occurred in the 2010, when the United States government used groups of experts called "red teams" to hack its own computer systems (Laura, 2015). It has become a sizable sub-industry within the information security market and has expanded to also cover the physical and human elements of an organization's defenses. A successful test doesn't necessarily mean a network or system is 100% secure, but it should be able to withstand automated attacks and unskilled hackers.

Deterring cybercrime is an integral component of a national cybersecurity and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and

https://dx.doi.org/10.22624/AIMS-22667

activities intended to affect the integrity of national critical infrastructures (Adebusuyi, 20018). At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens.

The exceptional outbreak of cyber-crime in Nigeria in recent times was quite alarming, and the negative impact on the socio-economy of the country is highly disturbing. Over the past twenty years, immoral cyberspace users have continued to use the internet to commit crimes; this has evoked mixed feelings of admiration and fear in the general populace along with a growing unease about the state of cyber and personal security (Oliver, 2010). This phenomenon has seen sophisticated and extraordinary increase recently and has called for quick response in providing laws that would protect the cyber space and its users.

The first recorded cyber murder was committed in the United States. According to the Indian Express, January 2002, an underworld don in a hospital was to undergo a minor surgery. His rival went ahead to hire a computer expert who altered his prescriptions through hacking the hospital's computer system. He was administered the altered prescription by an innocent nurse, this resulted in the death of the

https://dx.doi.org/10.22624/AIMS-22667

patient. Statistically, all over the world, there has been a form of cyber-crime committed every day since 2006. Prior to the year 2001, the phenomenon of cyber-crime was not globally associated with Nigeria. This resonates with the fact that in Nigeria we came into realization of the full potential of the internet right about that time. Since then, however, the country has acquired a world-wide notoriety in criminal activities, especially financial scams, facilitated through the use of the Telecommunication facilities. Nigerian cyber criminals are daily devising new ways of perpetrating this form of crime and the existing methods of tracking these criminals are no longer suitable for to deal with their new tricks (Adebusuyi, 20018). The victims as well show increasing naivety and gullibility at the prospects incited by these fraudsters. This paper seeks to give an overview of ethical hacking and cyber-security in Nigerian telecommunication industry, outline some challenges and proffer solutions.

In 2014, the National Assembly of Nigeria made a bold move in the war against cybercrime when the Senate passed the Cybercrime Bill. This feat in addition to the cyber security strategy and policy documents introduced by the Office of the National Security Adviser (NSA) are attributes that will strengthen cyber security.

1.2 STATEMENT OF THE PROBLEM

https://dx.doi.org/10.22624/AIMS-22667

The issue of cyber security is one that has been discussed by many people with various perspectives on the issue, most coming at it from different sides than the others. Cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries as the United States. The illegal act may be targeted at a computer network or devices 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 the computer network or device". However, ethical hacking has been used by various telecommunication companies to cover the loophole and this study is identifying the problems and providing an overview on the issues and the solutions.

1.3 OBJECTIVES OF THE STUDY

The following are the objectives of this study:

1. To examine the issues of ethical hacking and cyber security in Nigeria telecommunication industry.
2. To examine the solutions to the issues of ethical hacking and cyber security in Nigeria telecommunication industry.

https://dx.doi.org/10.22624/AIMS-22667

3. To determine the level of effectiveness of ethical hacking and cyber security in Nigerian telecommunication industry.

1.4 RESEARCH QUESTIONS

1. Is ethical hacking and cyber security practiced in Nigeria telecommunication industry?
2. What are the solutions to the issues of hacking and cybercrime in Nigeria telecommunication industry?
3. What is the level of effectiveness of ethical hacking and cyber security in Nigerian telecommunication industry?

1.6 SIGNIFICANCE OF THE STUDY

The following are the significance of this study:

1. The findings from this study will educate the stakeholders in the telecommunication industry and the general public on how ethical hacking can be used in cyber security to protect against cybercrime.
2. This research will be a contribution to the body of literature that explained the effect and solution of cyber security in the telecommunication industry, it will also be an empirical literature for future research in the subject area.

https://dx.doi.org/10.22624/AIMS-22667

1.7 SCOPE/LIMITATIONS OF THE STUDY

This study will cover the issues and solution relating to ethical hacking and cyber security in the Nigerian telecommunication industry.

LIMITATION OF STUDY

Financial constraint- Insufficient fund tends to impede the efficiency of the researcher in sourcing for the relevant materials, literature or information and in the process of data collection (internet, questionnaire and interview).

Time constraint- The researcher will simultaneously engage in this study with other academic work. This consequently will cut down on the time devoted for the research work.

https://dx.doi.org/10.22624/AIMS-22667

LITERATURE REVIEW

2.1 INTRODUCTION

The vast growth of Internet has brought many good things like electronic commerce, email, e-taxi, easy access to vast stores of reference material etc. As, with most technological advances, there is also other side: criminal hackers who will secretly steal the organization's information and transmit it to the open internet. These types of hackers are called black hat hackers. So, to overcome from these major issues, another category of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers. So, this paper describes ethical hackers, their skills and how they go about helping their customers and plug up security holes. Ethical hackers perform the hacks as security tests for their systems. This type of hacking is always legal and trustworthy. In other terms ethical hacking is the testing of resources for the betterment of technology and is focused on securing and protecting IP systems. So, in case of computer security, these tiger teams or ethical hackers would employ the same tricks and techniques that hacker use but in a legal manner and they would neither damage the target systems nor steal information. Instead, they would evaluate the target system's security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them.

https://dx.doi.org/10.22624/AIMS-22667

Ethical hacking is a way of doing a security assessment. Like all other assessments an ethical hack is a random sample and passing an ethical hack doesn't mean there are no security issues. An ethical hack's results are a detailed report of the findings as well as a testimony that a hacker with a certain amount of time and skills is or is not able to successfully attack a system or get access to certain information. Ethical hacking can be categorized as a security assessment, a kind of training, a test for the security of an information technology environment. An ethical hack shows the risks an information technology environment is facing and actions can be taken to reduce certain risks or to accept them.

2.2 THEORETICAL FRAMEWORK

The Internet is one of the fastest-growing areas of technical infrastructure development. Today, information and communication technologies (ICTs) are omnipresent and the trend towards digitization is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings. Electricity supply, transportation infrastructure, military services and logistics – virtually all modern services depend on the use of ICTs. Although the development of new technologies is focused mainly on meeting

https://dx.doi.org/10.22624/AIMS-22667

consumer demands in western countries, developing countries can also benefit from new technologies. With the availability of long-distance wireless communication technologies such as WiMAX5, 3G & 4G Internet and computer systems that are now available for less than 30,000 Naira, many more people in developing countries should have easier access to the Internet and related products and services. The influence of ICTs on society goes far beyond establishing basic information infrastructure. The availability of ICTs is a foundation for development in the creation, availability and use of network-based services. E-mails have displaced traditional letters; online web representation is nowadays more important for businesses than printed publicity materials; and Internet-based communication and phone services are growing faster than landline communications. The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries. ICT applications, such as e-government, e-commerce, e-education, e-health and e-environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. ICT applications can facilitate the achievement of millennium development targets, reducing poverty and improving health and environmental conditions in developing countries. Given the

https://dx.doi.org/10.22624/AIMS-22667

right approach, context and implementation processes, investments in ICT applications and tools can result in productivity and quality improvements. In turn, ICT applications may release technical and human capacity and enable greater access to basic services. In this regard, online identity theft and the act of capturing another person's credentials and/or personal information via the Internet with the intent to fraudulently reuse it for criminal purposes is now one of the main threats to further deployment of e-government and e-business services. The costs of Internet services are often also much lower than comparable services outside the network. E-mail services are often available free of charge or cost very little compared to traditional postal services. The online encyclopedia Wikipedia can be used free of charge, as can hundreds of online hosting services. Lower costs are important, as they enable services to be used by many more users, including people with only limited income. Given the limited financial resources of many people in developing countries, the Internet enables them to use services they may not otherwise have access to outside the network.

International Journal of Scientific Engineering and Technology
(Engineering Collection-Innovative Research Publication Journals)
https://dx.doi.org/10.22624/AIMS-22667

CYBER SECURITY AND CYBERCRIME

3.1 INTRODUCTION

Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. The fact that the 2018 UN General Assembly resolution on cyber security addresses cybercrime as one major challenge the world id facing. Cyber security plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy. Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and

https://dx.doi.org/10.22624/AIMS-22667

international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cyber security thus requires a comprehensive approach. Cyber security strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime. The development and support of cyber security strategies are a vital element in the fight against cybercrime. The legal, technical and institutional challenges posed by the issue of cyber security are global and far reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation. In this regard, the World Summit on the Information Society (WSIS) recognized the real and significant risks posed by inadequate cyber security and the proliferation of cybercrime. The provisions of the WSIS Tunis Agenda for the Information Society, including the Annex, set out a plan for multi stakeholder.

https://dx.doi.org/10.22624/AIMS-22667

3.2 TYPES OF CYBER-CRIME

This study presents the types of cyber-crimes that have economic impact either directly or indirectly on the financial system of a nation or having cross border ripple effects. Longe & Chiemeke (2018) simplified the list of unintended consequences of ICT to include acts such as Phishing, cyber terrorism, electronic spam mails, cyber-stalking, and fake copy -cat websites. While some types of cyber-crimes are specific to Nigeria, other types, such as identity theft and false statements, cut across all countries.

3.2.1 PHISHING

According to Roger, phishing is simply a hightech identity theft that does not only steal personal information and identity from unsuspecting consumers, but also an act of fraud against the legitimate businesses and financial institutions that are victimized by phishing. Phishing is usually a social engineering crime pervasive in attacking organisations' or individuals' (customers') information systems (IS) in order to gather private information to be used against organisations to extract some benefit for the perpetrator through the anonymity of identity theft or identity deception acts (Rodger, 2018). According to recent estimates from the Anti Phishing Working group, phishing scams remain a

https://dx.doi.org/10.22624/AIMS-22667

relatively small percentage of spam sent worldwide today. Phishing attempts to pose significant dangers for unsuspecting victims. It has become one of the fastest-growing worldwide threats on the Internet. This rapid growth has made combating it a huge priority for electronic mail service providers, since phishing impacts every aspect of the Internet and computing and there is no single action from any one company or organization to solve the problem. The remedy can only come in a holistic fashion involving collaboration between technology innovation, industry, government, and user education as prescriptive guidance. To build systems shielding users from fraudulent websites, designers need to know which attack strategies work and why. What makes a web site credible? This question has been addressed extensively by researchers in computer-human interaction. Successful phishing must not only present a high credibility web presence to its victims; it must create a presence that is so impressive that it causes the victim to fail to recognize security measures installed in web browsers. Data suggest that some phishing attacks have convinced up to 5% of their recipients to provide sensitive information to spoofed websites. About two million users gave information to spoofed websites resulting in direct losses of $1.2 billion for U.S. banks and card issuers in 20013. If we hope to design web browsers, websites, and other tools

https://dx.doi.org/10.22624/AIMS-22667

to shield users from such attacks, we need to understand which attack strategies are successful and what proportion of users they fool. In an analysis of phishing attacks carried out in 20016, Rachna, Tygar, & Hearst found that good phishing websites fooled 90% of participants. Existing anti-phishing browsing clues are ineffective and 23% of participants in the study did not look at the address bar, status bar, or the security indicators.

Perpetrators target both document categories to secure personal identifying information. Often they obtain a 'set' of point of information documents in order to present themselves as 'legitimate customers' to deceive the target organisation's authentication and verification processes to commit identity fraud. Increasingly, the mode of attack for the fraud, especially the identity fraud perpetrator, is tending to rely on electronic commerce or mechanical/digital devices to initiate the identity theft or identity deception act. This is to some extent enabled by Internet adoption. For example, 74% of United States (US) adults were online in May 2016, up from 77% in 2017, according to e-Marketer. In phishing e-mail messages, the senders must gain the trust of the recipients to convince them to divulge their personal information. To gain this trust, fraudsters "spoof," or mimic, a reputable company. The companies spoofed most often are financial services- Internet

https://dx.doi.org/10.22624/AIMS-22667

organizations such as the commercial bank in Nigeria, Jumia Online store, PayPal, etc. Retailers and Internet service providers are also targeted. These phishing e-mails are usually mass mailed (Warner, 20014). Many of the recipients are not customers of the spoofed companies and may quickly realize that the e-mail is fraudulent, or may believe that the e-mail was mistakenly sent to them and ignore the e-mail. Fraudsters rely on the responses from the few recipients who are customers of the spoofed company and who fall victim to the scam. According to Longe, Mbarika, Korouma, Wada, & Isabalija, the scammers claim to be from reputable companies and go to great lengths to emulate the company's visible branding. Their fraudulent e-mails often contain the company's logo and use similar fonts and color schemes as those used on the company's web site. Some of the fraudulent e-mails simply reference images from the legitimate company's site. The main link in a fraudulent e-mail sends the recipient to the fraudulent phishing web site, but many fraudulent e-mails include other links that send the recipient to sections of the real company's web site. To further convince the recipient that the e-mail originated from the reputable company, the scammers use a "from" e-mail address that appears to be from the company by using the company's domain name (e.g., @gtbank.com, @jumia.com.ng). Phishing

https://dx.doi.org/10.22624/AIMS-22667

e-mails also try to assure the recipient that the transaction is secure in hopes of gaining the recipient's trust. The following are assurances that were included in fraudulent e-mails: "Remember: GTbanl will not ask you for sensitive personal information (such as your password, credit card, bank account numbers, social security number, etc.) in an e-mail." This e-mail then sends users to a fraudulent web site that asks for personal and account information while promising that the information is submitted via a secure server. The phishing perpetrators could then notify the victim of a "security threat." Such a message may be welcomed or expected by the victim, who would then be easily induced into disclosing personal information. The number of unique phishing websites detected by APWG during the second half of 20018 saw a constant increase from July to October with a high of 27,739. In Nigeria, the most recent phishing attacks were on the customers of Inter-switch, which remains the organization with the highest customer base in electronic transactions. The Nigeria Deposit Insurance Corporation (NDIC) disclosed in its 20017 annual report and statement of account that underhand deals by bank staff, among others, resulted in attempted fraud cases totaling over N10.01 billion (over 65 million USD) and actual losses of N2.76 billion (13 million USD) in 20017. With the present situation in the world economy and the appropriate

https://dx.doi.org/10.22624/AIMS-22667

technology, fraudulent action is most likely to increase and phishing remains one of the main means of performing “fraud without borders.” The extent of readiness to stem phishing in Nigeria needs to be determined because fraudulent activities emanating from these nations have far-reaching consequences beyond her borders.

3.2.2 Cyber Terrorism

According to the U.S. Federal Bureau of Investigation, cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents". Unlike a nuisance virus or computer attack that result in a denial of service, a cyber terrorist attack is designed to cause physical violence or extreme financial harm. According to the U.S. Commission of Critical Infrastructure Protection, possible cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems. Apart from that, there is another dimension to cyber terrorism – the use of cyber infrastructure to launder money for financing physical terrorism. In 20012, FBI officials reported that Al Qaeda terrorist cells in Spain used stolen credit card information to make numerous purchases. According to Wilson (20018), cyber terrorism is said to have taken place when the

https://dx.doi.org/10.22624/AIMS-22667

effects of a widespread computer network attack is unpredictable and might cause enough economic disruption, fear, and civilian deaths, to qualify as terrorism. At least two views exist for defining the term cyber terrorism.

These are;

(1) Cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals.

(2) Cyber terrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage. The terrorist's use of the Internet and other telecommunications devices is growing both in terms of reliance for supporting organizational activities and for gaining expertise to achieve operational goals. Tighter physical and border security may also encourage terrorists and extremists to try to use other types of weapons to attack. Persistent Internet and computer security vulnerabilities, which have been widely publicized, may gradually encourage terrorists to continue to enhance their computer skills, or develop alliances with criminal organizations. They will also probably consider attempting a

https://dx.doi.org/10.22624/AIMS-22667

cyber-attack against the nation critical infrastructure. Cybercrime has increased dramatically in past years, and several recent terrorist's events appear to have been funded partially through online credit card fraud. Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money and for the smuggling of arms and illegal drugs. These links with hackers and cybercriminals may be examples of the terrorists' desire to continue to refine their computer skills, and the relationships forged through collaborative drug trafficking efforts may also provide terrorists with access to highly skilled computer programmers.

3.2.3 Electronic Spam Mails

These are unsolicited bulk e-mail to multiple recipients. They can be commercial, political, or religious. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, web search engines, and blogs. Spamming is popular because the advertisers have no operating costs beyond the management of their mailing lists and it is difficult to hold senders accountable for their mass mailings. As a result, costs such as lost productivity and fraud are borne by the public and by Internet service providers that have been forced to add extra capacity to cope

https://dx.doi.org/10.22624/AIMS-22667

with the deluge. A good example is 419 (also known as Yahoo Boys) mails or the Nigerian advance fee frauds which in 2016 was estimated to have cost unsuspecting clientele over five billion dollars. These mails emanate in a triangle called the "The Nigerian Connection" mostly in Europe and in some parts of Africa, “The 419 (also known as Yahoo Boys) Coalition, 20015.” The Nigerian Scam, according to published reports, is the third to fifth largest industry in Nigeria. It is the 419 Coalition view that, in effect, the elites from which successive governments of Nigeria have been drawn are the scammers. Therefore, victims have little recourse in this matter. Monies stolen by 419 (also known as Yahoo Boys) operations are almost never recovered from Nigeria. Most 419 letters and e-mails originate from or are traceable back to Nigeria. However, some originate from other nations, mostly also West African nations such as Ghana, Cameroon, Togo, Liberia, Sierra Leone, Ivory Coast (Cote D’Ivoire), etc. The effects of such scams have immense effects with confirmed losses of millions of dollars annually (Herald Tribute, 20017). According to Longe and Longe, governments have tried to come up with policies to try to curtail this menace. Nigeria, through the EFCC, banned night browsing. This is because most fraudulent activities are perpetrated at cyber cafés at nights. For now, there are no quantitative data to measure the effect of this action on the

https://dx.doi.org/10.22624/AIMS-22667

reduction or otherwise of cybercrime in Nigeria. Apart from the availability and usage of Internet facilities in cyber cafes for pornography and other cybercrimes, the evolution of fixed wireless facilities in Nigeria, for instance, has added another dimension to the cybercrime problem. Nigeria therefore enjoys a dubious distinction of being the source of what is now generally referred to as '419' mails, named after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that prohibits advance fee fraud. These crimes are similar to theft and the likes that have existed for century's offline even before the development of high-tech equipment. Progress in the fight against Internet pornography has been moving at a very slow pace in Africa. A majority of public internet access point deals with the problem in unorthodox manners such as placing notices on cyber cafe walls warning against browsing pornographic sites and other spamming activities. Those with some technical expertise resort to the use of content filters which are downloaded and installed to filter unwanted Internet content.

3.2.4 Cyber Stalking

Stalking in the physical sense generally involves harassing or threatening behavior in which an individual engages repeatedly, such as following a person, appearing at a person's home or place of business,

https://dx.doi.org/10.22624/AIMS-22667

making harassing telephone calls, leaving written messages or objects, or vandalizing a person's property. According to Ellison and Akdeniz cyber stalking refers to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. This term is used interchangeably with online harassment and online abuse. A cyber stalker does not present a direct physical threat to a victim, but follows the victim's online activity to gather information and make threats or other forms of verbal intimidation. The anonymity of online interaction, they argued, reduces the chance of identification and makes cyber stalking more common than physical stalking. Although cyber stalking might seem relatively harmless, it can cause victims psychological and emotional harm, and occasionally leads to actual stalking. Cyber stalking is becoming a common tactic in racism and other expressions of hate. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing website (e.g., blogs) and e-mail. The availability of free email and website space, as well as the anonymity provided by these chat rooms and forums, has contributed to the increase of cyber stalking as a form of harassment. Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim's immediate family; and still others require only that the alleged stalker's course of

https://dx.doi.org/10.22624/AIMS-22667

conduct constitute an implied threat. While some conduct involving annoying or menacing behavior might fall short of illegal stalking, such behavior may be a prelude to stalking and violence and should be treated seriously. The nature and extent of the cyber stalking problem is difficult to quantify. Indeed, current trends and evidence suggest that cyber stalking is a serious problem that will grow in scope and complexity as more people take advantage of the internet and other telecommunications technologies. Important advances can only be made if industry, law enforcement, victims, service providers, support groups, and others work together to develop a more comprehensive and effective response to this problem. Ultimately, however, the first line of defense will involve industry efforts that educate and empower individuals to protect themselves against cyber stalking and other online threats, along with prompt reporting to law enforcement agencies trained and equipped to respond to cyber stalking. Physical stalking, online harassment, and threats may be a prelude to more serious behavior, including physical violence.

For example, in Nigeria, hateful speech is widely perpetrated through online media.

Offensive and hateful speech has been a challenge in Nigeria. If it has to do with the Nigerian Civil War, Igbo nationalists take offense with the

https://dx.doi.org/10.22624/AIMS-22667

rest of the country; if it is about Boko Haram and its alleged sponsors, self-appointed defenders of the North are up in arms with equally self-appointed defenders of the South; if it has to do with resource control and oil politics, the North squares off against the South. The Igbos and the Yoruba, rival major ethnic groups, frequently pick on each other.

Hate and offensive speech profiling reached a pinnacle in the country in June 2017, when a coalition of Northern youth groups issued a Kaduna Declaration which, apart from calling the Igbos unprintable names, gave all Igbos in the North three months (until October 1, 2017) to leave. The reaction stemmed from harsh pro-Biafra rhetoric of Nnamdi Kanu, leader of the Indigenous People of Biafra. While it is true that Nnamdi Kanu had engaged in a form of rhetoric offensive to many people, the quit notice given to the Igbos in the North triggered competitive quit notices to vacate.

Though the notices were later withdrawn, they led to palpable fears that the situation could degenerate to a Rwanda-like genocide unless the tide of free-flowing offensive and hate speech in the country was stemmed.

The hate speech bill in Nigeria has prescribed death by hanging for any person found guilty of any form of hate speech that results in the death of another person. The bill—in early stages of becoming law—seeks the

https://dx.doi.org/10.22624/AIMS-22667

establishment of an independent commission to enforce hate speech laws across the country. For offenses such as harassment on grounds of ethnicity or race, the bill recommends that the offender be sentenced to "not less than a five-year jail term or a fine of not less than 10 million naira (about $277,000), or both."

3.2.5 Fake Copy-Cat Web Sites

One recent trend in on-line fraud is the emergence of fake 'copy-cat' web sites that take advantage of consumers what are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster's personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud.

https://dx.doi.org/10.22624/AIMS-22667

3.3 EFFECTS OF CYBER-CRIME ON TELECOMMUNICATION COMAPNIES

According to Reuter's media briefs from Cameroon, British prime minister, cyber-crime costs the British economy some 27 billion pounds a year. On the other hand, the Economic and Financial Crimes Commission Report ranks Nigeria as third among the top ten sources of cyber-crime in the world. It is estimated that after the United States with 65 per cent of cyber-criminal activities and the United Kingdom with 9.9 per cent, Nigeria is the next hub of cyber criminals in the world with 8 per cent. The growth of online telecommunication further presents enhanced opportunities for perpetrators of cyber-crime. Funds can be embezzled using wire transfer or account takeover. Criminals may submit fraudulent online applications for bank loans; disrupt e-commerce by engaging in denial of service attacks, and by compromising online phone calling systems. Identity takeover can also affect online banking, as new accounts can be taken over by identity thieves, thus raising concerns regarding the safety and soundness of financial institutions. Therefore, unless crime detection and prevention are confronted collectively, Nigeria like any other country will remain warm breeding grounds for cartels of such criminal activity. A global effort to combat this crime is of essence. Financial fraud is one of

https://dx.doi.org/10.22624/AIMS-22667

America's largest growth industries, creating annual losses of $189 billion. The cost of application fraud alone, they argued, is more than $35 billion a year. This is by far more damaging than delinquent or bankrupt accounts, fraud losses which are generally three times higher than normal charge off rates. This situation poses a real and constant threat to profitability and may raise the price of goods and services for consumers. They further argued that by far, the greatest threats are from ecommerce fraud, identity theft and international criminal organizations, all of which are becoming more widespread and sophisticated every day. As e-commerce continues to grow, it will become an even bigger attraction for criminals. The report indicated that identity theft is escalating at 40% a year and is particularly problematic compared with more traditional forms of financial fraud. Greater access to credit, an abundance of information, faster electronic communications, and intense competition among financial institutions make it easier than ever for perpetrators to steal identities and falsify information. The existence of cyber-crime and its effects require the formulation of appropriate policies to address them. The next section presents existing policies on cyber- related crime in Nigeria.

https://dx.doi.org/10.22624/AIMS-22667

3.4 CYBER-CRIME POLICY IN NIGERIA

There is presently no law that is specific to cyber-crime in Nigeria. However, this is not to say that cyber criminals are free to operate in the country. There are general laws that are not specifically related to cyber-crime but are being enforced to deal with the crime. Some of these laws are: The Nigeria criminal code, Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2004, and the Advance Fee Fraud and other Related Offences Act 2006. The Nigeria Criminal Code Act 1990 The Criminal Code Act of 1990 (Laws of the Federation of Nigeria, 1990) criminalizes any type of stealing of funds in whatever form, an offence punishable under the Act. Although cyber-crime is not mentioned in the Act, it is a type of stealing punishable under the criminal code. The most renowned provision of the Act is Chapter 38, which deals with “obtaining Property by false pretenses Cheating.” The specific provisions relating to cyber-crime is section 419, while section 418 gave a definition of what constitutes an offence under the Act.

https://dx.doi.org/10.22624/AIMS-22667

RESEARCH METHODOLOGY

4.0 INTRODUCTION

This chapter states the various methods used in research, as well as the population of the study, and sampling techniques used in determining the sample size for the research. How data was collected and analyzed is also discussed in this chapter.

The main objectives of this research were achieved through quantitative methods, as inferential statistics were used to measure the level of accuracy and validate responses from the respondents in accordance to the objectives of the research.

4.1 STUDY AREA

The study was conducted in Ikeja, Lagos state. Lagos is a state in Nigeria. It is located in the coastal southern part of the country, lying between latitudes 4°32′N and 5°33′N, and longitudes 7°25′E and 8°25′E. Lagos is one of Nigeria's 36 states, with a population of over 19million people and more than 10 million people in diaspora. The state's capital is Ikeja, with over 8million inhabitants. Lagos has an airport (murtala muhammed International Airport). Lagos state is

https://dx.doi.org/10.22624/AIMS-22667

home to the Ibom E-Library, a world-class information center. Along with English, the main spoken language is majorly yoruba.

4.2 RESEARCH DESIGN

The research design used for this study was the descriptive research design. Since data characteristics were described using frequencies and percentages, and no manipulations of data or variables were necessary, the researcher chose this research design. The researcher discarded other alternatives such as the causal and explanatory research designs, because accurate findings and data analysis may not be achieved.

4.3 POPULATION OF THE STUDY

The population for this study is made up of employees of Nigerian telecommunication commission, Internet Service Providers company and telecommunication company. The population figure for the study was 32 respondents, comprising of respondents in the Nigerian telecommunication commission Internet Service Providers company and telecommunication company.

https://dx.doi.org/10.22624/AIMS-22667

4.4 POPULATION SIZE AND TECHNIQUE

Since the population for the study was not large, and data could be collected from all the respondents, the researcher adopted the census sampling technique to successfully complete the study. All 32 respondents were used for this study.

4.5 DATA COLLECTION METHOD

Data for this study was collected from the respondents through the use of questionnaires. Questionnaires were shared to all 32 respondents of the organization, and field surveys through responses to questions in the questionnaire served as the main source of primary data for this study.

Other information was collected from text books, journals and other secondary sources of data.

4.6 DATA ANALYSIS

Various analytical tools and software such as pie charts, bar charts, tables, and Statistical Package for Social Science (SPSS) software were used in analysing data for this study.

Data collected were analysed using frequencies and percentages. These frequencies and percentages enabled the researcher to clearly

https://dx.doi.org/10.22624/AIMS-22667

represent true data characteristics and findings with a great deal of accuracy. Interpretation and analysis of data was also used to describe items in tables and charts used for this study.

4.7 LIMITATION

Since this study is a descriptive research, validation of data characteristics and variables described maybe limited to some extent as other statistical tools such as arithmetic mean, variance, standard deviation, and the central limit theorem were not applied to further prove the accuracy of findings in this study. The researcher only used descriptive statistical tools such as frequencies and percentages to describe data characteristics and findings.