FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 3 No. 1, March, 2019, pp 249 – 257

CYBER CRIME AND THE SOCIOLOGICAL IMPLICATION IN THE NIGERIA'S TERTIARY EDUCATION SYSTEM

Suleiman A. A.

Department of Educational Foundations, Federal University Dutsin-Ma, Katsina State

Correspondence author: saahmad@fudutsinma.edu.ng

ABSTRACT

The global infrastructure on information renders a vast and unlimited access for a lot of organizations and individuals to do bulk of activities. This made it on the increase among anonymous hoodlums termed as 'cyber criminals'. The nature, type, mode, count, cost, and dynamical sophistication of such attacks are seriously increasing and it is so alarming. Nigeria is even rated 3rd globally in cyber crime; although, it is a global phenomenon. Recently, one of the popular social sites Facebook, was hacked upon which 50 million accounts including that of the company's chief executive were victims. There are limited academic write up and researches carried out on cyber security and cyber threat, which made it looks more professional than academic. This paper as a conceptual and discursive examines the categories, types, modes of cybercrime and the sociological implications of these kinds of crimes on or with cyber space which seems to be a serious threat to our entire security. The paper discusses on such activities in relation to universities system in Nigeria and outlined on the laws, measures and recommendations to address the cyber crime and cyber security in the country.

Keywords: Cyber Crime, Sociology, Education, Nigeria

INTRODUCTION

One of such eminently important commodity to any individual or society is a 'knowledge' which is mainly referred to as 'education'. It is a milestone or cornerstone and bedrock for any kind of development. Nigeria provides education system in three levels of institution i.e.: primary, secondary and tertiary levels. They are compartmentalized set of courses classified into formal, informal and non-formal training. Tertiary level specifically has three major components Polytechnics, Colleges and Universities which all are engine for the countries educational, economic, social, political and cultural growth. Education either formal or informal, be it a primary or tertiary is the aggregate of all processes by which an individual develops the ability, attitude and other forms of behavioral positive values of and to the society in which he/she lives.

Nigeria's universities as tertiary institutions are regulated by the National Universities commission (NUC). It is essentially a service and regulatory body which provides such unique services and regulatory activities to all the Nigerian university system and the nation at large. The provision of these services ensures an efficient and balanced coordinated development of the universities in the country in the public, state and privately owned institutions. It has to facilitate and flourish the tripartite mandates of Nigerian universities viz: 'teaching', 'research' and 'community service'.

NUC as dynamic regulatory agency is a catalyst for positive change and innovation for the of quality service delivery in quality universities to have a quality education in Nigeria. As of this report there are 165 recognized universities in Nigeria by NUC (43 Federal, 47 State and 75 Private). For ascertaining viable quality, and ICT capabilities and affordability the NUC work in synergy with other bodies like Tertiary Education Trust Fund (TETFund) Nigeria Communication Commission (NCC), Nigeria Information Technology Development Agency (NITDA).

The former Executive Secretary, of TETFund Dr. Baffa Bichi once called for the establishment of a statutory committee to be known as State Services Higher Education Board of Advisors (SSHEBA), with membership of key stakeholders from Information Technology Experts, Intelligence Corps (IC) and Higher Education Institutions (HEIs) as a way of strengthening the relationship between them and to enhance on the total security of the system from all angles. (NUC, 2018)

The Executive Secretary National Universities Commission (NUC), Prof. Abubakar Rasheed has said that there are 1.9 million students in Nigerian Universities. The information as contained in the 2017 universities' statistical digest was presented at a two-day retreat for governing council members of the Nigerian universities in Abuja on Tuesday, May 8, 2018. He also said that 51,000 people are currently engaging in academic work (teachers and support) in various universities across the

country. Akinbayo, (2018) in his view added that "it was a discouraging statistics that ought to be improved upon considering the above population which stands at 1:37 student teacher ratio."

Going by the Nigeria's university population of about 2 million students; the level of Internet connectivity has been quite appreciating considering the more access point of the mobile device around. Most universities were in one way or the other connected to network by microwave, wireless radios and fiber optic terminations this is beside the individualized subscribed data plans on mobile devices from commercial mobile companies. World Internet statistics website (2018) shows that Nigeria's Internet access stands with total numbers of 98,391,456 users which is almost 49.1% of the total population in the country of 195,875,237 people. The penetration of the Internet into areas is 50.2% of the population. The Nigerian Communications Commission, (NCC), in their magazine the communicator reported that the number of active mobile phone subscribed lines in the country rose to 144 million in December 2017. The report further showed that there was an increase of 2,731,273 lines, from 142 million recorded in November 2017. The Commission's report further indicated the active mobile phone lines raised to 144,631,678 in December compared to 141,900,401 in November 2017. (NCC, 2018; Premium Times Newspaper, 2018)

The global information infrastructure creates unlimited opportunities for commercial, social and other human activities. However, it is increasingly under attack by cybercriminals; as the number, cost, and sophistication of attacks are increasing at an alarming rate. Cyber criminals take full advantage of the anonymity, secrecy and interconnectedness provided by the Internet, therefore attacking the very foundations of our modern information society. There are chunks of online and cyber activities in the universities among both academic, non academic as well as students. Most universities have online accessibilities from application for admission, content delivery, and students' assessment, up to graduations as well as alumni, linkages and collaboration through researches, socializations and sharing of resources.

The cutting edge technological development of the internet and the widened accessibility of ICT tools and modern computing technologies created and offer dynamic opportunities for vast of activities, as well as making the users to decide to engage legal, semi legal and to some extend illegal activities. There are limited academic researches on cyber security and cyber threat considering it as a recent and on growing paradigm; it is more professional than academic. The rise of information technology and online communication has not only warrant for, and produced a substantial increased in the incidence of criminal activities, but has equally resulted in the emergence of variety of online criminal acts; which is becoming a serious danger if not curb. The President of the Cyber Security Experts Association of Nigeria (CSEAN) as quoted in Vincent, (2017) has stated that "Nigeria faces a chronic shortage of cyber security professionals that will be able to combat the rising wave of cyber crime activities in the country." He further viewed that "Nigeria with an estimated population close to 200 million, the number of certified cyber security professionals in Nigeria is 1800 persons. Considering the rate of experts and the rate at which financial cyber crime is ravaging the country, it is too dangerous compared to other countries."

OBJECTIVES

This is a conceptual and theoretical discursive paper sets to identify and discuss the type, mode and sociological implication of cybercrime in Nigeria's Universities.

The specific objectives set to guide the study are as follows:

- To discuss the extent of mode of cybercrime in Nigerian Universities.
- To discuss the extent of types of cybercrime in Nigerian Universities.
- To discuss on the sociological implication of cyber crime in Nigerian Universities.
- To highlight on laws and measure set on cyber crime in Nigeria.

RESEARCH QUESTIONS

The research questions set for this study are as follows:

- To what extent is mode of cybercrime in Nigerian Universities?
- To what extent are types of cybercrime in Nigerian Universities?
- To what extent are the sociological implications of cyber crime in Nigerian Universities?
- To what extent are laws and measure set on cyber crime in Nigeria?

Meaning of Cybercrime

Computer crime and or cybercrime, is any crime that involves a computer and a network. Oxford dictionary defines "it as any criminal act carried out by means of computer or internet". Unlike a normal crime the cyber crime is a kind of crime that happens in cyberspace, that is, happens in, on and with the world of computing tools and the Internet. Cyber crime is becoming a wide global phenomenon. It has a seriously, potentially and severe impact on peoples' lives and society at large; in polity, economy, culture and so on; this is because the world is already an information society where cyberspace it the hub city center. Concept of cybercrime is very historical. Its advent has been a boon to people users i.e. teachers, students, doctors, patients,

buyers, sellers, lawyers, and criminals. Massive digitization and unprecedented interconnectivity help in that respect thus, the repercussion will be on all. These forms of criminal activities were classified, categories as they are perpetuated. Cyber criminals are out there trying to do anything to make money and steal useful information. Recently Facebook, as one of the most popular social networking site was hacked upon which about 5% (50 million accounts) of its subscribers including that of the company's chief and top executives were victims. As the world is becoming more digitized, there are openings up for more and more types of cyber crime. Recently, at the time of this report, China in October 2018 from the back door used tiny micro chip to hack, infiltrate and infect thousands of commercial companies in America including Amazon, Apple, and Bloomberg. This threat was termed as the 'the big hack'. (Bloomberg Business week, October 5, 2018) The fear is what would have been the consequences of this devastation if this was turn to be a global warfare across the whole world?

Classification of cyber crime

To clearly understand the classifications of cyber crime, we have to consider the categories, types and dimensions of the cybercrime as identified by Maitanmi et al., (2017).

Cyber crimes against persons:

These are cyber crimes committed against persons include: such as harassment by use of a computer, e-mail phishing, posting, dissemination, trafficking, and distribution, of obscene materials, pornography, and indecent exposure. It could also be any act to harm, frighten, and dehumanize someone. It is just any action or attempt that threatens and undermines another person.

Cyber crimes against property

The other class is against all forms of property. These include computer vandalism (destruction of others' property), transmission of harmful programmes such as virus or denial of the entire service.

Cyber crimes against government

The next is related to government. Cyber terrorism and cyber warfare are distinct kinds of crime in this category. Internet has been medium used by individuals and groups to threaten the international governments or to terrorize the citizens of a country. This is cyber terrorism when an individual cracks into a government or military site facilities.

Types of cyber crime

Cyber crime has been categorized by AIC (2006) as cited in Odumesi, (2014) as follows:

1. Offence against the confidentiality, integrity, and availability of computer data and system such as illegal access, illegal interception, data or system interference and illegal devices.
2. Computer related offences like computer related forgery and computer-related fraud
3. Content-related offences (child porn, bully, and pedophile
4. Offences related to infringements of copyright and related right.

Upon these three categories Maitanmi et al., (2017); Gérôme, (2017) also reported that there exist other bulk of types of cyber crime in various dimension and modes; the most common are as follows:

Phishing Scams

Phishing scams are attempts by scammers to trick one into giving out personal information such as bank account numbers, passwords and credit card numbers. Attackers use a brute force approach for the password cracking. Mode of email, text message, phone call and social media profiles are used in this, pretending to be a legitimate business, bank, company, or internet associate. Scammers on this get hold of one's information that 'unauthorised or suspicious activity has been happening on his/her account, one may be ask to update details on systems, to fill out a survey, to win a prize but the motive is to lead one to get access to email address, phone number, password, bank keys and more. Maitanmi et al., (2017)

Online Scams

Online scams are basically scams that happen online. It is tricking one into giving out personal details online by an ad popping up telling that one has won something and asking for ATM, card details to pay for shipping. You will never receive anything but bunch of noticing weird transactions coming from your bank account. A hacker uses 'search engine optimization' (SEO) poisoning to attack users. (Horshpreet, 2018)

Malware

Malware is the contraction of malicious software onto a system. It's software written with the intent of causing harm to data and devices. Malware is a create types of viruses such as a worm, roolkit, adware trojan, bot and spyware. Malware is often done through a range of viruses that will get into one's computer, tablet, and phone and destroy it or just cause havoc. (Horshpreet, 2018)

Email Bombing

Email bomb is another form of internet abuse. This is an overload of cluster emails directed to one email address; this will cause the person receiving the emails server to become sluggish, stack or even crash. Mostly this not necessarily for stealing anything but to have server runs down or instill real pain and hard work to fix. (Horshpreet, 2018)

Virus Dissemination

This is similar to bomb email but it is particularly sneaky form of cyber crime. It not only gets a piece of malware onto one part

of the victim's system, but it spreads across other pieces of software. the new mail if not quarantine proper is sent to a sandbox, the next time it is open a piece of undiagnosed and infected software get install on to the device and continue again and again. (Gérôme, 2017)

Logic Bombs

A logic bomb is also like the one above but act in the same way as a virus. But on this a small program or sections of the program are triggered on a certain date or time which may only affect a certain percentage of disk space (sector or track) and filled it or remove some files and so on. A program could then delete critical sections of source code, plugins thereby rendering that software redundantly useless. This type of crime is most commonly done and installed by insiders who already had access to the system physically or virtually. (Horshpreet, 2018)

Theft

Internet theft is not like physical one, it is the broad term use for a theft that happens over the internet. This is in many ways i.e. fake emails, fake ads, viruses and snooping. The aim of this is to steal personal information and use it to steal form victim's bank account or online purchases using those details. (Horshpreet, 2018)

Social Media Spamming & Hacking

Social media hacking is often done as a joke, a lot of big people and celebrities are hacked. It's an invasion of privacy. Unwarranted content that can be distressing is shared one's account so that it can be reported and shut down or cause public disgust on you. It also appears in fake account and becomes friends or followed by the average person. It can be done to spread malicious links created with the intent to harm, mislead or damage a user or their device. (Maitanmi et al., 2017)

Electronic Money Laundering

Money illegally generated can be laundered before it can be spent or invested. One way to launder money is electronically between banks called "wire transfer". Previously it seemed difficult of impossible to monitor but today due to screen wire transfers tremendous of transactions from banks to banks are clamping down on the basis of suspicious activity. Some institutions, universities, hospital, military hardware companies, consultants, connive in this kind of activities. (Maitanmi et al., 2017)

Software Piracy

Now on internet, one can find free online a lot of audio-visual resources such as document, movie, song or software. Those materials although free they are mostly pirated and come with a range of risks such as: trojans, viruses, worms and malware.

Data Diddling

Data diddling is the action of skewing data entries in the user's system. This includes adjusting financial figures up or down marginally, or it could be more complex and make an entire system unusable. (Gérôme, 2017)

Slicing Attack

Slicing attack, sounds funny, it's a technique used to steal online money or resources in tiny bit at a time with an un-noticeable difference to the bank account. It will go different alternate time and from different sources which accumulates to a considerable amount over time. (Maitanmi et al., 2017)

Hacking

In this hacker is an intruder who accesses a computer system without permission. Hackers do it for various motives and reasons i.e. for greed, fame, fun, power and or curiosity, it make cyber criminal to break into systems and steal personal information of corporation, banking, financial data. Most hackers are programmers and have an advanced understanding of computers. (Maitanmi et al., 2017)

Cyber Stalking

Cyber stalking is found across the world its common with teenagers and young adults. The victim is mostly subjected to online harassment in forms of messages and emails. This is to make miserable of the victim or exert control over the victim, just like ordinary stalking. (Maitanmi et al., 2017)

Cyber Bullying

Cyber bullying is similar to cyber stalking, but here messages can be harmful, abusive, and offensive. It is by posting online images and videos to offend the victims, excluding online, and or making fake accounts and share distressing, abusive and obscene content and making request. (Gérôme, 2017)

Identity Theft

This is the most common types of cyber crime. It occurs by creating fraud for financial gains. Culprit steals identity information of others such as credit card information, addresses, email addresses and more. With this information they pretend to be someone else and create new bank accounts. (Gérôme, 2017)

Child Soliciting & Abuse

Child soliciting and abuse is a type of cybercrime where criminals solicit children via chat rooms for the purpose of pornography. It forms of sexual abuse towards children. (Maitanmi et al., 2017)

Ransomware

Ransomware is like kidnapping, but done online. Attacker snatch and get hold of computer network and encrypts files to deny access for the actual owner using 'denial of service (DoS) system' until the attacker is paid ransom before the service is release. Companies and organisations are more vulnerable to

this. Other advance way is the Zombies attack from which infected computers are used to make up what is call a botnet. The zombies are used to deploy a 'distributed denial of service (DDoS)'attack. Maitanmi et al., (2017)

Cyber Terrorism

Cyber terrorism is to launches attack on government or organization in order to distort and or access stored information stored on the computer and their networks. A cyber-terrorist is someone who intimidates a government or to advance his or her political or social objectives by launching computer-based attack against computers, network system, and the information stored on them.

It means that any act intended to instill fear by accessing and distorting any useful information in organizations or government bodies using computer and Internet is generally referred to as 'cyber terrorism'. Cyber terrorism is in various forms cyber extortion is one in which a website, e-mail server, computer systems is put under attacks by hackers for denial of services, demanding for ransom in return. Cyber criminals and extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. It is also an intentional or unintentional attempt or action on computers and network or other devices to cripple any government effort in achieving anything by mode of remote or close access by self or by proxy. (Gérôme, 2017)

Cyber Laws in Nigeria

The chairman of the Senate Committee on ICT, Abdulfatai Buhari, at the subcommittee on Cybercrime report once said that there is a need to review the current cyber crime laws to reflect the global trend and to prepare the country for impending dangers. It is not clear how safe the Nigeria's cyberspace is. The developed world is been attacked day in day out, what of a developing country like Nigeria? Thus, there is a need for us to strengthen our cyberspace. The lawmaker said it is wrong to call an individual a "yahoo boy" as no law recognizes such designation. There is the need of who handles cybercrime which for now we don't have any solid law (on cybercrime) in this country today. (Busari, in premium times October 31, 2017) there are bulk of cases on cyber crime and online fraud and scam involving local residents and foreigners lodge with the economic and financial crime commission (EFCC) but irregular legislation halted the cases and rendered them pending and lingering. (Halderand & Jaishankar, 2011)

Nigeria has no clear legislation against these crimes. Economic and Financial Crime Commission (EFCC) is seen as the body that cyber crime and its vices are under its jurisdiction. It is the body empowered by government to fight all forms of financial crimes including cyber crimes in Nigeria. They are working together with the cyber crime prevention working group. It is further believed that cyber laws need to be updated in Nigeria. The federal and state government needs to update the criminal code laws. The National Assembly as the legislative body must urgently modify/amend certain sections of the criminal code to deal with cyber crimes. Cyber crimes are being perpetuated on daily basis leading to serious crimes. Cyber laws are not clearly stated and it varies from country to country; thence, that cross jurisdiction made the laws difficult to harness. This may even result to the tendency of 'technology apocalypse'.

The significance of cyber legislation cannot be overemphasized in our contemporary Nigerian society. As a way to minimize the menace, NCC on their part use various ways for awareness, training and legislations. On their social media outfit Facebook page 'CyberAware' to be precise NCC constantly post reminders and 'cyber security tips' to people on how to be free from cyber attacks. Some of the tips states "*regularly update your software", ignore any mail with suspicious links or attachments", don't believe anything you read online thus don't share or use"* and so on.

As outlined below by legislative unit of public affairs of NCC published on their journal 'the communicator', (1st quarter edition April 2018) the imperativeness of cyber legislation in Nigeria could be viewed from the following perspectives:

- Establishment of legal and regulatory framework
- Establishment of institutional framework for coordination and implementation;
- Standards and regulations;
- Capacity building
- Compliance &enforcement;
- Emergency response & readiness;
- Public enlightenment
- International cooperation and institutional framework.

The unit further recommends on the following to mitigate it.

- Capacity building
- Cooperation between actors (private or public)
- Establishment of institutional framework for coordinating cyber security efforts
- Enactment of related bills to strengthen the cyber security framework

Sociological implication of cyber crime in Nigerian universities

Using connected electronic devices sharing information on network has become an integral part of our daily lives. All types of organizations, use them be it financial, medical, and education institutions. Cyber criminals nowadays mainly take full advantage of the anonymity, secrecy and interconnectivity provided by the Internet, thereby getting chances of attacking a lot of victims in this our modern global information society. Agents responsible for law enforcement took it hard to identify, recognize, apprehend, and prosecute such culprit along sociologists who on one hand trying searched for origin, nature, motive and implications of such cyber crimes activities. Psychologists and psychiatrists are also on the tract of studies that can assist both culprit and victims along the sociologists to find a well-positioned gaze and befitting law to guide and deal with the issue related communal influences and interpretations of cyber crime. (Odumesi, 2014) Experts in cyber security have documented multiple of cyber crime happenings of various nature and levels; from which billions, of dollars every year got robbed. Many of the victims and culprits altogether of such online financial misdeed fell into other sociological fallouts and crises to some extent jail or even death. In October 2018 it was reported (Premium times, 4th October, 2018) that the senior special assistant (SSA) to the president on Diaspora Abiki Dabri Erewa stated that twelve (12) Nigerian students in Benin republic were detained in relation to cyber crime. In view of this as well, NCC boss Professor Umar Garba Dambatta disclosed at the Nigerian Bar Association (NBA) conference in Lagos that a report placed Nigeria as the 3rd in global internet crimes behind UK, US. The statement further said that N127 billion was lost to cyber crime in 2015 alone in Nigeria. Although there are benefit in using cyber space the risk are also high. Thus, it needs to be managed well because for now, the cyber laws are not favourable. One big problem is that, there are no easy ways of identifying and verifying the owner of card use in some transactions and business; whereas there are no clear punishments for the offenders. (Ngugi, 2005)

From the documented cases around the universities, cyber crime in those academic institution universities in particular has been an issue of concern especially in the Nigerian system (Folashade, 2013). In his study carried out at Ahmadu Bello University Zaria he stated that 93.7% of the respondent heard about cyber crime. He therefore identified some ways, means and places university students indulge in those activities. He reported that 86.5% of the culprits are youth. From his study also 80% have indicated that cyber café are mostly used for such activities. In his report 78% of the respondents have indicated that they use social media, 8.9% use pornography, 17% used spamming. As for the techniques used Folashade further said that 87% of the respondents age that they do password cracking, 53.3% use key loggers, 53% used network sniffer. When interviewed the respondents mentioned that some use design puzzle or game to link to the victims profile. Some use phone call and text messaging to lure their victims. Others indicated ATM fraud and so on.

This form of criminality is presumed by some students as a kind of pride to have been a hacker to cheat, dupe and defraud others online unnoticed. Most of those involve in the act around the institutions are not high class top experts in the cyber activities they are merely amateur attackers who are mainly termed as 'white hat hackers'. It is very prevalent among themselves, and to some extent other people around and outside the universities. This is one of the means of survival to some of the students. Cyber extortionists increasingly perpetuate their attacking on personalities' financial status, especially top civil servants, politicians and appointees as well as corporate companies and big organisations' website pages and other networks links aiming at, crippling their ability to operate and perhaps demanding for payments in order to restore back the service. It is clear that some students with the ICT capabilities and efficacy took that advantage against other students and their families especially those well to do, to extort them through some money deals that appears genuine but actually is fraud. (Premium times, 4th October, 2018)

Other methods rampant among students in Nigerian universities such as 'link jacking', 'like jacking' and 'tag jacking' are use to lewd victims into a serious danger. Some other culprits use 'call jacking' by calling victims mobile phone number or text messages once it was pick then the billing software run and continue to charge the account as you are making calls sometimes charging you for making international calls. (Odumesi, 2014) This sociologically affects the victims into changing their profiles, subscriber identification module (SIM) card or the phone itself. Some victims get seriously disturb and sometimes into drugs out of frustration (Odumesi, 2014; Gérôme, 2017).

The Economic and Financial Crimes Commission, (EFCC), on Wednesday, February 3, 2015 arraigned the trio of Solomon Uchendu, Ndubisi Agu and Uchendo Chikwadu before Justice D. V. Agishir of the Federal High Court sitting in Enugu, Enugu State for offences bordering on obtaining by false pretence and Advanced Fee Fraud. The suspects, who were living at 4, Coal City University Close, Independence Layout, Enugu, were arrested by operatives of the EFCC following intelligence report over their alleged involvement in Internet crime.

One of the suspects, Solomon, who is currently undergoing the mandatory National Youth Service Corps, NYSC, in Akoko, Ondo State, confessed that he had about seven different email accounts registered with different names. (EFCC Media & Publicity, 2018)

In a Vanguard News Paper of November 2018 it was reported that Cyber crime extends into the academic pursuit and activities as well, especially on the malpractices that occur on the evaluation processes in the universities. The EFCC acting Head, Media and Publicity, Mr. Tony Orilade, made it known on the paper that they apprehended some suspects, who were 24 university students between 19 and 37 years of age all concerning cyber fraud.
(Vanguard News Paper November, 2018)

With the advancement and proliferation of online content delivery and assessment as well as e.learning platform give avenues for the malpractices which are all modes of cybercrime. It occurs among students themselves, or between them and their staff or teaching or non-teaching status. Connectivity devices; i.e. Bluetooth, Infrared, Xender; other mobile multimedia devices; i.e. smart watches, eye glasses, ear pieces; social media and negligence among examiners warranted for that. Poor and un-practice digital efficacy, low level of orientations, poor audit trail and security on school portals and websites, poor staff and student data management and insincerity are the major factors responsible for the frequent occurrences of the cyber criminality in our tertiary institutions. Intellectual property theft, plagiarism and publication favoritism became rampant among academics and their students. Internal cyber threats could have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices i.e. servers and server rooms as well as other connectivity. Internal users may not have better hacking skills than external attackers. Both internal users and external users can access the network devices through the Internet. A well designed security implementation should require authentication before corporate data is accessed, regardless of whether the access request is from within the corporate campus or from the outside network. (Ngugi, 2005; Halderand & Jaishankar, 2011)

Cyber bullying and cyber victimization is characterized as the undertaking by which a one-by-one or assembly of persons is aimed at for cheating, abusing, attack or intimidating one another. It is poorer than in-person bullying because the perpetrators can conceal behind a cloak of anonymity in which victims expressed the harshness and trauma as too injurious. Some cyber bullying victims commit suicide after the pains of unrelenting attacks. Universities environments witness such acts among the students of various genders. Those with low morale and low sprit or those with a deviant orientation were mainly the victims. Students with cultist attitude usually were predators among the students, while others who are intellectually higher, financially vibrant fall as their prey. There are other ways called 'cultist surveillances' this is by watching a victim to identify his or her cultist camp or gender relation so as to clamp him down. Others use 'academic pseudo-politics'; this is where a lecturer would ruin a student or a colleague if he belong and relating to another lecturers or administrators camp. In all of these it ends up in result manipulations and fees alterations as well as lewd to commit an online error that would render you held responsible and accountable. Other culprits used business centers around or at far and sometimes a porous university's network to perpetrate on their victims (Gérôme, 2017).

Cyber-pornography expressly refers to progeny pornography on the internet, usually engaging those less than 18 years of age. Un-noticed various websites have become repositories of such sex related and explicit images of young children, where the pictures are acquired and traded. Cyber pornography has expanded in the world. Countries like Great Britain have been impacted high; it has been turn into a large-scale enterprise at expense of young children which is quite horrifying our societies. A newer pattern of cyber porn is used to engage online groups i.e. 'second life,' where created avatars, or three-dimensional (3D)simulations, are shrewd and be used in the online environments and more especially video sharing platforms. It is quite devastating to the future of the victims and their families. In many countries it is abolished, thus virtual progeny pornography is illicit, while the regulation is much less clear in other countries. It is rampant now in universities among students, lecturers recording and holding victim to ransom of illicit pictures recorded consciously or otherwise. Online video sharing and multimedia platforms offer those avenues where students use to create among themselves with anonymous what is call amateur recording porn clips and sell to porn companies to make earnings. (Gérôme, 2017)

In May 2018, the website for sharing adult-orientated works of fiction known as *Adult-FanFiction.Org* had 186,000 records exposed in a data breach. The data contained names, email addresses, dates of birth and passwords in plain text. In February 2018, a massive collection of almost 3,000 alleged data breaches was found online. It had previously been seen in *Have I Been Pwned*, http://www.haveibenpwnd website. This is a website that can be use to check if a particular email account or website is hacked. Some files consisting of more than 80 million unique email addresses had not previously been seen. In June 2017, the online playlists service known as 8Tracks suffered a data breach which impacted 18 million accounts which was not secured using two-factor authentication". Therefore, with such challenges serious challenge is being posed to the society.

Another serious cyber threat is Hacktivism. This is a term used to describe cyber attacks carried out by people who are considered social, political or ideological extremists. Hacktivists attack people or organizations that they believe are enemies to the hacktivist agenda. Students now a day use social media to protest on any un-desirable policy and happening in their institutions. (Folashade, 2013) Several episodes around Nigerian universities were a testimony. Students with poor performance can cause havoc using such

medium. Others use the medium to commit a lot of fraud of which a lot were apprehended (EFCC Media & Publicity, 2018).

Way Forward

From the discussions and consideration of the report from (EFCC Media & Publicity, 2018; NCC, 2018; Folashade, 2013) here are some recommendations made to reduce the adverse effect of those cybercrime threats on personal, organizational or societal bases:

- Identify agencies that will have primary authority and responsibility to investigate and prosecute cyber crime;
- Enact and pass into law legislation with clear interpretation covering aspect of cyber crime;
- Enforcing the enacted laws on all perpetrators and guilty of committing such cyber crimes alongside creation of cyber police and policing;
- Harmonise those laws on cyber crime to facilitate and reflect international cooperation in preventing it;
- Provide training, workshops, seminar and media adverts on cyber crime along multilateral cooperation and needs;
- In liaison with agencies and organization there is the need to set 24/7 exchange of information among local and global stake holders and perhaps establish national computer and cyber crime resource center under national information and communication development agency NITDA;
- In conjunctions with expert organizations and association i.e. cyber security experts association of Nigeria CSEAN there is a need to be organising awareness, orientation and seminars on how to combat cyber crime among the general public both education and legal framework;
- Measures, including setting up of a Voluntary Fund, to support victims;
- Organization to employ methods to ensure confidentiality of information, data encryption, two factor authentication and username ID and password;
- Organisation should ensure the 'CIA triad 'components: confidentiality, integrity, and availability; which is good for information security for the organization;
- For personal or organizations a good and strong password is advice: so user should not use dictionary words or names in any languages. They should use if possible ten and above combination of letters, numbers, special characters, symbols such as: ! @ # $ % ^ & * ( );
- To prevent malicious software from monitoring user activities, collecting personal information, and producing unwanted pop-up ads on a user computer it is strongly recommended that anti spare ware be install and have constant update?
- Proper and perfect use on all school portals and sites of audit trail, visit counter and IP tracker, vulnerability scanner, infection monkey testing, virtual invigilator, web-guard, web-shield, strong firewalls, antivirus, anti malware, and so on,
- Boosting robust compulsory and constant ICT training and retraining among staff and students on adversaries and new challenges. Use need to think like the criminals themselves in order to avert the cyber crime.
- Use of secure and highly configure network with constant update is advice with levels of authentication and authorization is recommended. Constant verification using some pwned/hacking site like (*https://haveibeenpwned.com*) is recommendable.
- User needs to ignore any email, test messages or calls requesting for any information unless one is aware of it. So also be aware of transaction on online shopping and purchases especially those require payment before delivery.

REFERENCE

Akinbayo, W. (2018). National Universities Commission NUC says there are 1.9m students in Nigerian universities. https://www.pulse.ng/communities/student/nuc-says-there-are-1-9m-students-in-nigerian-universities-id8355649.html

Bangabandhu, S. M. (2015). Cyber Laws: *Presented at the Department of Sociology, Science and Technology University* (BSMRSTU)

Bloomberg Business week, (October 5, 2018). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. https://cacm.acm.org/news/231636-the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-u-s-companies/fulltext

Busari, K. (October 31, 2017). Premium times paper report: Nigeria's-cybercrime-act-needs-review-senate-committee. https://www.premiumtimesng.com/news/more-news/247851-nigerias-cybercrime-act-needs-review-senate-committee.html

EFCC, (2018). EFCC Arraigns Youth Corps Member, Two Others for Cybercrime. Published by EFCC Media & Publicity, on 4th January, 2014 at http://efccnigeria.org/efcc/index.php/news/1160-efcc-arrains-youth-corps-member-two- others-for-cybercrime/

Folashade, B. O. (2013). Nature, causes and consequences of cyber crime in tertiary institution in Zaria, Kaduna State Nigeria. American journal of contemporary research. vol. 3 (9).

Gérôme, B. (2017). Cyber-Resilience a New Pillar of Cyber Security Strategy. Partner Cyber Security & Digital Trust

Horshpreet, K. (2018). Cyber crime among students. Slide share resources. http://www.slideshare.net/mobile/june21/harsh/cyber-crime-among-student.

Halderand, D., Jaishankar, K. (2011). Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global

NCC, (February 7, 2018). Active mobile lines in Nigeria hit 144 million in December –. Agency Report. https://www.premiumtimesng.com/news/more-news/257906-active-mobile-lines-nigeria-hit-144-million-december-ncc.html

NCC, (2018). A Summary of the Legislation on Cybercrime in Nigeria. The Communicator Journal Magazine. 1st Quarter edition (issue 24). April 2018. Published by Legislative Unit, Public Affairs Department, NCC. https://www.ncc.gov.ng/thecommunicator/index.php?-cybercrime-in-nigeria

Ngugi, M. (2005). Legal week: Law on Cyber Crime Overdue, available at *www.crimeresearch.org*

NUC, (2018). Dr. Bichi Advocates for State Services Higher Education Board of Advisors. https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview

https://nuc.edu.ng/dr-bichi-advocates-for-state-services-higher-education-board-of-advisors/

Maitanmi, O. Ogunlere, S., Ayinde, S., Adekunle, Y. (2017). Crimes and Cyber Laws in Nigeria. The International Journal Of Engineering And Science (IJES). Volume 2, Issue 4 Pages 19-25. www.theijes.com

Odumesi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology. Vol. 6(3), pp. 116-125, DOI: 10.5897/IJSA2013.0510 http://www.academicjournals.org/IJSA

Premium Times News Paper, (2018). https://www.premiumtimesng.com/news/more-news/257906-active-mobile-lines-nigeria-hit-144-million-december-ncc.html

Vanguard, (2018). EFCC arrests 24 undergraduates, others over cyber crime On November 15, 2018 read more at:

https://www.vanguardngr.com/2018/11/efcc-arrests-24undergraduates-others-over-cyber- crime/

Vincent, N. (2017). Hack It Like the NSA...Or, How to Exploit MS17-10.*Cyber security Experts' Newsletter*

World internet statistics, (Sept, 2018). Global Internet usage-Nigeria. http://www.World-internet-statistics/nigeria

https://csean.org.ng/

https://haveibeenpwned.com/