The Effect of Cybercrime on the Educational System of Nigeria

BY

AKPAN, E. Ebenezer, *Ph.D, FCICN, AP, PPGDCA, PHDCDPM*
Corporate Institute of Research and Computer Science
140 Ikot Ekpene Road
Uyo, Akwa Ibom State

AND

FRIDAY, Enobong Peter
Corporate Institute of Research and Computer Science
140 Ikot Ekpene Road
Uyo, Akwa Ibom State

ABSTRACT

The study was to investigate the effect of cybercrime on the educational system of Nigeria. Cybercrimes commonly committed by students include: hacking, unauthorized and illegal access to bank accounts, identity theft, phishing, spoofing, unauthorized reading of emails, desktop counterfeiting, pornography, cyber harassment, fraudulent conversion of property, chat room conspiracy, sending computer viruses, plagiarism, phreaking, and downloading unauthorized data. The study has fully shown that students' involvement in cybercrime has been necessitated for diverse reasons. If properly contained, it will have a positive effect on the nation. The government, family, and students all have a vital role to play in this contest. Collective action could better the interests of future existence, regain international reputation, and promote the nation's economy. The perpetrators of cybercrime are not farfetched; they are our brothers, friends, colleagues, distant relatives, and neighbours who can be tamed under appropriate circumstances with the right and positive communication, orientation, education, and empowerment. The study concluded that cybercrime poses a great risk to the economy and therefore the need to institute an effective risk management system and enhance the capacity to carry out forensic investigations to tackle it. Also, collaborative efforts of governments, corporate entities and the citizenry could play a vital role in checking cybercrime. One of the recommendations made was that the government should strengthen its security agencies, loaded with the difficult responsibility of fighting cybercrimes in Nigeria.

KEYWORDS: Effect, Cybercrime, Educational System and Nigeria

Introduction

Cybercrime (in a broader sense) is a criminal activity carried out using electronic devices (computers), the communication network (internet) and data with the sole purpose of extorting valuables from victims, once a weakness is exploited (Aghatise, 2011). Cybercrime is targeted at the victim once a weakness is exploited (Aghatise, 2011). Cybercrime is targeted at the victim’s computer, with the intention of spreading malware, obtaining illegal information, and gaining unauthorized access to make a profit or steal vital information from victims. Cybercrime is perhaps the most involved high-tech crime of the twenty-first century. As the internet and its associated technologies permeate more and more aspects of human activity, so do the vulnerabilities to cyber victimization. The internet revolution has created some new patterns of criminal activity hitherto unknown to humanity and also new, intriguing patterns of criminal victimization across the world. Cybercrime issues have become high profile, especially those that are related to hacking, copyright infringement, child pornography, and child grooming (Pitts, 2007).

Cybercrime appears to be a permanent feature of modern society. Despite the efforts of social workers, law enforcement agencies, and personal and criminal justice professionals to minimize it, the world is becoming a more terrible place. Where crimes such as homicide, kidnapping, robbery, assault, sex offences, child molestation, burglary, environmental crime, arson are crimes without a victim, economic crime, political crime and cybercrime are the order of the day. Cybercrime is defined as (i) a computer-aided crime originating in the Nigerian internet domain space; (ii) a computer-aided crime perpetrated by Nigerians located outside the Nigerian internet domain space. In collaboration with Nigerians within the Nigerian internet domain space, and crimes aimed at information and telecommunication technology (ICT) infrastructure in Nigeria, from any location (Nwannema & Unadi, 2011).

Cybercrime is a crime which involves the use of digital technologies in the commission of an offence, directed at computing and communication technologies in the commission of an offence, directed at computing and communication technologies. The modern techniques that are proliferating towards the use of internet activity result in creating exploitation and vulnerability, making it a suitable way of transferring confidential data to commit an offence through illegal activity (Ebelogu, Ojo, Andeh & Agu 2019). The activity involves things like attacking the information center data system, theft, child pornography built images, online transaction fraud, internet sale fraud, and also deployment of internet activities such as viruses, worms, and third party abuse like phishing, email scams, etc.

The contribution of the internet to the development of the nation has been marred by the evolution of new waves of crime. The internet has become an environment where the most lucrative and safest crime thrives. Cybercrime has come as a surprise and a strange phenomenon that now lives with us in the educational system of Nigeria. With each passing day, we have witnessed more and more alarming cases that are more shocking than the ones before. Their study investigates the effect of cybercrime on the educational system of Nigeria.

Concept of Cybercrime

Cybercrime is a crime that involves a computer and a network (Moore, 2011). The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may harm someone’s security and financial health (Bossler, & Berenblum, 2019). Cybercrime refers to the criminal activity that either targets or uses a computer, a computer network or a networked device. Cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations (Kaspersky Lab 2021). Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers. Halder and Karruppannan (2011) define cybercrimes as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly, using modern telecommunication networks such as the internet (chat rooms, emails, notice boards, and groups), and mobile phones (SMS/SMS).

Cybercrime is the crime (as theft, fraud, intellectual property violations, or distribution of child pornography) committed electronically. Cybercrime is defined as either a crime involving computing against a digital target or a crime in which a computing system is used to commit criminal offenses (Technopedia 2018). Cybercrime is broadly defined as any illegal activity that involves a computer, another digital device, or a computer network. Cybercrime includes common cyber security threats like social engineering, software vulnerability exploits and network attacks. It also includes criminal acts like hacktivist protests, harassment and extortion, money laundering, and more (Ngo-Lam, 2019). Cybercrime may also be referred to as computer crime. Cybercrime is the crime or illegal activity that is done using the internet. Cybercrime is any criminal activity that involves a computer, a networked device, or a network. Most cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images, or other materials. Some cybercrimes do both – i.e., target computers to infect them with a computer virus, which is then spread to other machines and, sometimes, entire networks. Thomas and Loader (2000) defined cybercrime as those computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.

According to Maat (2004), cybercrime encompasses all illegal activities where the computer, computer systems, information network, or data is the target of the crime and those known illegal activities or crimes that are actively committed through or with the aid of a computer, computer systems, information network, or data. Cybercrime is criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer, especially to illegally access, transmit, or manipulate data (Merriam-Webster 2019).

Types of Cybercrime

Computer viruses: The deliberate release of damaging computer viruses is yet another type of cybercrime. In fact, this was the crime of choice of the first person to be convicted in the United States under the computer fraud and abuse act of 1986. On November 2, 1988, a computer science student at Cornell University named Robert Morris released a software "worm" onto the internet from MIT (as a guest on the campus, he hoped to remain anonymous). The worm was an experimental self-propagating and replicating computer program that took advantage of flaws in certain e-mail protocols. Due to a mistake in its programming, rather than just sending copies of itself to other computers, this software kept replicating itself on each infected system, filling all the available computer memory. Before a fix was found, the worm had brought some 6,000 computers (one tenth of the internet) to a halt.

ATM fraud: Computers also make more mundane types of fraud possible. Take the automated teller machine (ATM) through which many people now get cash. In order to access an account, a user supplies a card and personal identification number (PIN). Criminals have developed means to intercept both the data on the card's magnetic strip as the user's PIN. In turn, the information is used to create fake cards that are then used to withdraw funds from the unsuspecting individual's account.

***Social-Hi jacking*:** This is a major problem all over the world. Many social networking pages have been hi-jacked by hackers who demand money in return for releasing the personal information of users. This has occurred on sites like Twitter, Facebook, and Instagram. These fraudsters go as far as sending messages from the authorized page to friends and family, requesting money or any other kind of assistance. Another common scenario also occurs when the fraudster creates a social page pretending to be someone else, especially celebrities.

Internet fraud: Schemes to defraud consumers abound on the internet. Among the most famous is the Nigerian, or "419", scam; the numbers are a reference to the section of Nigerian law that the scam violates. Although this con has been used with both fax and traditional mail, it has been given new life by the internet. In the scheme, an individual receives an e-mail asserting that the sender requires help in transferring a large sum of money out of Nigeria or another distant country. Usually, this money is in the form of an asset that is going to be sold, such as oil, or a large amount of cash that requires "laundering" to conceal its source; the variations are endless, and new specifics are constantly being developed. The message asks the recipient to cover some of the cost of moving the funds out of the country in return for receiving a much larger sum of money in the near future. Should the recipient respond with a cheek or money order, he is told that complications have developed; more money is required. Over time, victims can lose thousands of dollars that are utterly unrecoverable.

Hacking: while breaching privacy to detect cybercrime works well when the crimes involve the theft and misuse of information, ranging from credit card numbers and personal data to file sharing of various commodities-music, video, or child pornography-what of crimes that attempt to wreak havoc on the very workings of the machines that make up the network? The story of hacking actually goes back to the 1950s, when a group of phreaks (short for "phone freaks") began to hijack portions of the proliferation of computer bulletin board systems (BBSs). In the late 1970s, the informal phreaking culture began to coalesce into quasi-organized groups of individuals who graduated from the telephone network to "hacking" corporate and government computer network systems.

Causes of Cybercrime

Hassan, Lass & Maknde (2012), identified urbanization, high unemployment, quest for wealth, poor implementation of cybercrime laws, inadequately equipped law enforcement agencies, and negative role models as some of the causes of the proliferating cybercrimes in Nigeria. Akwara et al. (2013) examined in their study the relationships between unemployment, poverty, and insecurity in Nigeria. They found that unemployment causes poverty, and that a positive causal relationship exists between the latter and insecurity. Other causes of cybercrime, according to them, are corruption and the vulnerable nature of the internet. The main causes of cyber-crime in Nigeria are briefly discussed below.

Urbanization: Rapid urbanization in Nigeria, which manifests mainly through fast population growth, is a challenging issue for policy makers. The urban population grows at an annual rate of 4.3% (WDI, 2016). This is much higher than the sub-saharan Africa average and continues to put pressure on available resources in Nigerian cities. For instance, only 32.8% of the urban population had access to potable water supply during the period. According to Meke (2012), urbanization is beneficial only to the extent that it increases the availability of good jobs that have been created in cities, amidst a high population growth rate. The study held that urbanization is one of the major reasons that led to an increase in cybercrimes in Nigeria. He also noted that urbanization and crime move in tandem.

Unemployment: The unemployment rate in Nigeria is high and stood at 23.1% in the fourth quarter of 2018. The youth unemployment rate is currently above 47%. According to Okafor (2011), high unemployment in Nigeria comes with socio-economic, political and psychological consequences. This phenomenon encourages the development of street youths and urban urchins (‘area boys') that grow up in a culture that encourages criminal behavior.

Corruption: Nigerians have continued to occupy a despicable position in the global ranking for corruption. In 2018, Nigeria was ranked the 144th most corrupt nation in the world out of 176 countries surveyed by Transparency International. People celebrate wealth without questioning the source of such wealth. It is common to hear of people with questionable character and wealth being celebrated in society. This misguided disposition towards wealth encourages the get-rich-quick mindset that can be pursued through cybercrime.

Poverty: According to Jolaosho (2016), poverty refers to the inability to afford decent food, shelter, clothing and recreational activities. Hence, poverty is the absence of basic life essentials for the survival and comfort of mankind. A poverty-stricken person may unwittingly turn to crime for survival. About 50% of Nigerians live in extreme poverty as at 2018.

The root causes of cybercrime are not far-fetched. One only has to take a quick glance around society to observe illicit wealth acquisition and its display. This is coupled with the fact that the perpetrators are highly exalted. The problem is made worse by high youth unemployment, the absence of enforceable prohibitive laws, and the general laissez-faire attitude of individuals and businesses regarding cyber security (Hassan et al., 2012). Evidence has also shown that a significant proportion of these crimes are perpetuated by people in their youth. It is, however, worth noting that some of these attacks are also perpetrated within organizations. Many internet users are easily lured by unknown mail and web site addresses, falling victim to spyware and phishing.

Concept of Education

Education is the act or process of imparting or acquiring general knowledge, developing the powers of reasoning and judgment, and generally of preparing oneself or others intellectually for mature life (Dictionary 2021). Education may also be defined as a positive, conscious or unconscious psychological, sociological, scientific, and philosophical process which brings about the development of the individual to the fullest extent and also the maximum development of society in such a way that both enjoy maximum happiness and prosperity. Adhikary (2018) describes education as a process of development from infancy to maturity, the process by which he adapts himself gradually in various ways to his physical, social, and spiritual environment. Education refers to the discipline that is concerned with methods of teaching and learning in schools. According to Wikipedia (2018), education is the process of facilitating learning, or the acquisition of knowledge, skills, values, morals, beliefs, and habits.

Educational System of Nigeria

The Nigerian educational system has undergone major structural changes over the past 30 years. Before and after the 1960 Nigerian independence, the educational system at the primary and secondary levels mirrored the British system, i.e., 6 years of primary education, 5 years of secondary education, and 2 years of higher level/A levels. In 1973, the educational system was updated to the 6-3-3-4 (6 years' primary, 3 years' junior secondary, and 4 years' tertiary education), similar to the American system. In 1982, the first national policy on education was developed and adopted. Since this period, the educational system has witnessed a lot of changes and modifications at various levels. The following section gives a narrative of the educational system in Nigeria which also applies to Niger state. The scope of the educational transformation purposed in the state is limited to the primary and secondary schools. With the introduction of the 6-3-3-4 system of education in Nigeria, the recipient of the education would spend six years in primary school, three years in junior secondary school, and four years in a tertiary institution.

In 1982, Nigeria switched to the American system of six primaries, three junior secondaries, and three senior secondary grades, but the Nigeria examination system remained. to qualify for entry into junior secondary schools (JSS), senior secondary schools (SSS), and higher education. Nationwide examinations are held each year. Because exam scores determine a student's future educational choices, schools tend to stress memorization of facts rather than creative problem-solving. There are not enough senior secondary schools in Nigeria, so most students who finish JSS go into the workforce. Certain federal and state agencies plan and carry out special education programs. Teach in one of these programs. Mostly, though, the government encourages the integration of special education students into regular schools.

The ministries of social development, youth, and sport also run centers throughout the nation to help train people with special needs. There are three major categories of higher or tertiary education. One is post-secondary, which is non-university level training in technical and vocational fields. Students receive a certificate of training for completing work-oriented courses. The second type of higher education institution consists of higher technical but non-university level programs at technical colleges, polytechnics, and colleges of education. They usually offer a variety of options for students that lead to a National Diploma (HND) for four years of study. The third type of tertiary institution is the degree granting institution offering Bachelor’s and higher degrees.

Effect of Cybercrime on Educational System of Nigeria

The advent of social media has easily spread awareness of cybercrime among students in Nigeria. This has drastically increased the quest for participation in cybercrime, having seen the lavish lifestyle fluent on social media, clubs, and other social gatherings, not knowing the danger behind this wealth (Ogunjobi, 2020). Some youths go as far as withdrawing from school to join the pyramid of cybercriminals. Cybercrimes, whether ‘yahoo yahoo’ or ‘yahoo plus’ among students, have grievous consequences for the students themselves, the school, their parents, and society. Students who are blinded by sudden and unexpected affluence become deviant and arrogantly disrespectful of their schools. Some of them are snobs, and as such, they cannot associate with or live peacefully with their coworkers. The impact is adversely on their academics.

According to Oyebade (2019), the effect of the cybercrime acts among students is that they impugn their reputation, the integrity of their school, and that of their parents and guardians, as such students, when caught, are sometimes paraded before newsmen. It is unnecessary to say that cybercrime acts lead to the loss of money, valuable property, and vital information. In the case of Yahoo plus, it often results in the loss of body parts and precious lives as victims are maimed or gruesomely murdered for ritual purposes by students who use them to get spiritual or diabolic power. The far reaching consequence of this is on the economy. Evidence abounds of youths, mostly undergraduates, who have hacked into accounts of individuals and organizations. Unbridled involvement of youths and students in cybercrimes and other forms of financial crimes is affecting the reputation of Nigeria.

Conclusion

The study concludes that cybercrime poses a great risk to the economy, the need to institute an effective risk management system and enhancement of the capacity to carry out investigation to tackle it. Also, collaborative efforts of governments, corporate entities and the citizenry could play a vital role in checking cybercrimes. The study has fully shown that students' involvement in cybercrime has been necessitated for diverse reasons, and if properly contained, will have a positive effect on the nation. The government, family, and students all have a vital role to play in this contest. Collective action could better the interests of future existence, regain international reputation, and promote the nation's economy. The perpetrators of cybercrime are not farfetched; they are our brothers, friends, colleagues, distant relatives, and neighbors who can be tamed under appropriate circumstances with the right communication, orientation, education, and empowerment.

Recommendations

1. The government should strengthen its security agencies, loaded with the arduous responsibility of fighting cybercrimes in Nigeria.

2. The government should set up a mechanism to track and investigate the menace of cyber criminals within and outside institutions.

3. The government should intensify campaigns on cybercrime awareness among Nigerian students in order to make them understand that cybercrime is a criminal offence punishable under the criminal act, with the attendant adverse consequence of jeopardizing their educational accomplishments when convicted.

REFERENCES

Adhikary, M. C. (2018). Role of Teachers in Quality Enhancement Education and Human Development International *Journal of Humanities and Social Science Invention (IJHSSI)*, 7(12), 31-41

Aghatise, E. (20110. *Cybercrime definition*, "Computer research centre,

Akware A. F., Akwara N.F, Enwuchola J., Adekunle M. & Udaw J. E. (2013). Unemployment and Poverty: Implications for National Security and Good Governance in Nigeria. *International Journal of Public Administration and Management Research (IJPAMR)* 2(1).

Bossler, A.& Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice* 42(5):495-499.

Brush, K. (2021) *Definition of Cybercrime*. Available at: https://searchseecurity.techtarget.com/definition/cybercrime

Dictionary (2021). *Education*. Available at: https//www.dictionary.com/browse/education

Ebelogu C.U., Ojo S.D., Andeh C.P. & Agu E.O. (2019). Cybercrime, its Adherent Negative Effects on Nigerian Youths and Society at Large: possible Solutions. *International Journal of Advances in Scientific Research and Engineering*, 5(12).

Halder, D. and Karuppannan, J. (2011). *Cybercrime and the Victimization of Women*: Laws, Rights and Regulations. IGI Global publication.

Hassan A., Lass F. & Makinde J. (2011). Cybercrime in Nigeria: causes, Effects and the way out. *ARPN Journal of science and technology*, 2(7), 626-631

Jolaosho, A.O. (2016). *Some popular perception of poverty in Nigeria*, quoted in UNDP Human Development Report on Nigeria. Lagos: UNDP.

Kaspersky Lab (2021). *Tips on how to protect yourself against cybercrime*. Available at: https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

Maat, S. (2004). *Cybercrime*: A Comparative Law Analysis (Doctoral thesis), University of south Africa, Pretoria, south Africa p.239.

MERRIAM-WEBSTER (2019). *Cybercrime*. Available at: https://www.merriam-webster.com/dictionary/cybercrime

Moore, R. (2011) *Cybercrime*: Investigating High-Technology Computer Crime, Cleveland, Mississippi: Anderson Publishing.

Ngo-Lam, V. (2019). *Cybercrime*: Types, Examples, and What your Business Can Do. Available at: https://www.exabeam.com/information-security/cyber-crime/

Nwannema, C. & Unadia, O. *Indigenous Information Technology Capacity Development*. Lagos (ICADEV).

Ogunjobi, O. (2020). *The Impact of Cybercrime on Nigerian Youths*. Available at: https;//www.researchgate.net/publication/

Okafor E.E. (2011). Youth Unemployment and Implications for Stability of Democracy in Nigeria. *Journal of Sustainable Development in Africa*. 13(1).

Oybade, A.O. (2019). *Students and cybercrimes*: causes, effects and solutions. News Diary Online

Technopedia (2018). *Cybercrime*: What Does Cybercrime mean? Available at: https://www.technopedia.com/definition/2387/cybercrime

Thomas D, Loader B (2000). Cybercrime: law enforcement security and surveillance in the information age. Routledge, London. *J. Soc. Policy*, 30(1):300.

WDI (2016). World Development Indicator (WDI), International Bank for Reconstruction and Development/The World Bank; Washing D.C, USA.

Wikipedia (2018). *Education*. In Wikipedia, The Free Encyclopedia.