The Implications and Remedies of Student Involvement in Cyber-Crime: Empirical Survey of the Students of Tertiary Institutions in Imo State

BY

IWUJI, Florence Ijeoma, *Ph.D*
Department of Curriculum and Instruction
Alvan Ikoku Federal College of Education
Owerri, Imo State

AND

AMAH, Kanu Ogbonnaya, *Ph.D*
Department of curriculum and Instruction
Alvan Ikoku Federal College of Education, Owerri,
Owerri, Imo State

ABSTRACT

The study sought access the implications and remedies of student involvement in cyber-crime: empirical survey of the students of tertiary institutions in Imo State. Ex-post facto research design was adopted for the study. The study was conducted in Imo State. The population of the study comprised of all the tertiary institution students, lecturers and stake holders in Imo State. Simple random sampling technique was used to select 3 tertiary institution. From each institution 40 students and 10 lecturers and was randomly selected. 15 stake holders were also selected from the ministry of education for the study. And this gave a total of 165 respondents that constituted the sample size for the study. The Main Instrument used in this study was a questionnaire titled "Implications and Remedies of Student Involvement in Cyber-Crime Questionnaire (IRSICCQ)". Face and content validation of the instrument was carried out by an expert in test, measurement and evaluation from Imo State University. Cronbach Alpha technique was used to determine the level of reliability of the instrument. The reliability coefficient obtained was 0.78 and this was high enough to justify the use of the instrument. The researcher subjected the data generated for this study to appropriate statistical techniques such as percentage analysis for answering the research question and simple regression analysis for testing the hypotheses. The test for significance was done at 0.05 alpha levels. The study revealed that there is significant influence of the implications of students' involvement in cybercrime on the educational sector of Nigeria. There is significant influence of the implications of students' involvement in cybercrime on the Nigeria economy. Hence, the study concluded that certain precautionary measures should be taken by students while using the internet which will assist in challenging this major threat Cybercrime. One of the recommendations was that federal and state government, as well as educational communities should intensify campaigns on cybercrime awareness among Nigerian undergraduate students in order to make them understand that cybercrime is a criminal offence punishable under the criminal act with attendant adverse consequence of jeopardizing their educational accomplishment when convicted.

KEYWORDS: Implications and Remedies, Student Involvement, Cybercrime, Tertiary Institutions and Imo State

Introduction

Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government (Dennis, 2019). Internet has been the revolutionary invention of the 20th century. It successfully shrunk the world into a much smaller place by bringing the citizens and nations closer together in terms of enhanced communication and prompt exchange of ideas and information (Saroha, 2014). Keeping aside its advantages, internet has also raised numerous security concerns which found place in highest levels of official and governmental discourses. Such crimes threaten a nation's security and financial health. These issues surrounding these type of crimes have become high-profiling cases around the world (Tanwar, 2016).

In Nigeria, cybercrimes seem to be perpetrated by people of all ages ranging from young to old, but in most recent instances the young appear to be the worst offenders. Akpan (2016) reported that cybercrime has put the Nigerian students in a serious quest for money other than the real deal of getting university education. Several youths engage in cybercrime with the aim of emerging as the best hacker, or as a profit making venture since the tools for hacking in our modern world has become affordable by many. Ngozi (2016) submitted that the rate at which Nigerian youths are involving in one form of cybercrime or the other calls for urgent concern. Going by the nature that cybercrime can tarnish the image and reputation of organizations, institutions and individuals, it becomes very imperative; however, to investigate level of student involvement in cyber-crime, its implications and remedies.

Statement of the Problem

The fundamental purpose of education is to prepare of students for the future. Students are now flourish in the modern, fast-paced, high-tech world and as such, must have information seeking capacity and technology skills. The means of acquiring this literacy must be embedded in learning programmes and be part of student’s educational experience. However, Nigerian students are now aware of the cybercrimes carried out with the aid of internet and a computer system. Some of them are now master-minds such a crime. Victims of cybercrime usually the gullible, go through serious pains (emotional/psychological) as they are duped of their hard earned money by fraudsters, who may even be their own children/relatives. And this have led to many cases of death through suicide arising from cybercrime. Moreover, the prevalence of cybercrime gives a country a bad image. It also threatens a nation’s security and financial health. Students are now taking pleasure in defrauding public and private organizations as well as their fellow students. Hence, this study is therefore set out to find out student involvement in cyber-crime: its implications and remedies.

Objective of the Study

1. To find out the implications of students’ involvement in cybercrime on the educational sector of Nigeria.

2. To examine the implications of student involvement in cybercrime on the Nigeria economy.
3. To proffer the remedies that can mitigate student's involvement in cybercrime

Research Questions

1. What are the implications of students' involvement in cybercrime on the educational sector of Nigeria.
2. What are the implications of student involvement in cybercrime on the Nigeria economy.
3. What are the remedies that can mitigate student's involvement in cybercrime

Research Hypotheses

$H0_1$: There is no significant influence of the implications of students' involvement in cybercrime on the educational sector of Nigeria.

$H0_2$: There is no significant influence of the implications of students' involvement in cybercrime on the Nigeria economy.

Concept of Cyber Crime

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some 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 (Brush, Rosencrance and Cobb, 2020). Halder and Karuppannan, (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 or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups), and mobile phones (SMS/MMS). Thomas and Loader (2000), conceptualised 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". Maat (2004), proposed a definition for cybercrime which 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 crime that are actively committed through or with the aid of computer, computer systems, information network or data. Cyber Crime is broadly defined as any illegal activity that involves a computer, another digital device or a computer network.

Types of Cyber Crime

Cybercrime ranges across a spectrum of activities. At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or individual (Dennis, 2019). Also at this end of the spectrum is the growing crime of identity theft. Midway along the spectrum lie transaction-based crimes such as fraud, trafficking in child pornography, digital piracy, money laundering, and counterfeiting.

Internet fraud: Internet fraud is a type of cybercrime fraud or deception which makes use of the Internet and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance (Warf, 2018). Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace. It is, however, differentiated from theft since, in this case, the victim voluntarily and knowingly provides the information, money or property to the perpetrator (Brenner, 2009). It is also distinguished by the way it involves temporally and spatially separated offenders. Internet fraud can occur even if partly based on the use of Internet services and is mostly or completely based on the use of the Internet (Fisher and Lab, 2010).

ATM fraud: Computers also make more mundane types of fraud possible. In recent years, there has been proliferation of ATM fraud across the globe (Jain, 2017). Through the automated teller machine (ATM) 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 well 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 (Dennis, 2019). The number of ATM fraud has continued to increase due to negligence in the handling of ATM cards by bank customers. Most bank customers compromise their bank account details including their personal identification number to fraudsters (Jain, 2017).

Cyberbullying: This involves the use of communication technologies to harass people. Cyber harassment mostly affects children and teenagers but can also target adults. Some forms include cyber extortion, distribution of embarrassing pictures, delivery of threatening messages, cyberbashing to mock people and impersonating victims (Sabillon, Cano, Cavaller and Serra, 2016).

Prohibited/Illegal Content: This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network.

Cyberlaundering: Cybercrime that comprises financial transactions using funds from criminal activities. Cyberlaundering is based on e-payments, digital money and illegal hardcash that is converted to illegal e-money.

Identity theft: This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud (Panda Security, 2019). Identity theft leads to identity fraud that exploits additional crimes like financial identity theft, business identity theft, criminal identity theft and money laundering.

Hacking: Hacking becomes illegal once is used for unauthorized access to computer systems. Cybercrime is consummated once criminal hacking takes place. Illegal hacking activities are usually part of organized crime networks, specific motives and a high degree of sophistication.

Spam, steganography, and e-mail hacking: E-mail has spawned one of the most significant forms of cybercrime—spam, or unsolicited advertisements for products and services, which experts estimate to comprise roughly 50 percent of the e-mail circulating on the Internet. Spam is a crime against all users of the Internet since it wastes both the storage and network capacities of ISPs, as well as often simply being offensive. Yet, despite various attempts to legislate it out of existence, it remains unclear how spam can be eliminated without violating the freedom of speech in a liberal democratic polity. Unlike junk mail, which has a postage cost associated with it, spam is nearly free for perpetrators—it typically costs the same to send 10 messages as it does to send 10 million.

Cyberextortion: A crime involving an attack or threat of an attack coupled with a demand for money to stop the attack. One form of cyberextortion is the ransomware attack. Here, the attacker gains access to an organization's systems and encrypts its documents and files -- anything of potential value -- making the data inaccessible until a ransom is paid. Usually, this is in some form of cryptocurrency, such as bitcoin.

Cryptojacking: An attack that uses scripts to mine cryptocurrencies within browsers without the user's consent. Cryptojacking attacks may involve loading cryptocurrency mining software to the victim's system. However, many attacks depend on JavaScript code that does in-browser mining if the user's browser has a tab or window open on the malicious site. No malware needs to be installed as loading the affected page executes the in-browser mining code.

Cyberespionage: A crime involving a cybercriminal who hacks into systems or networks to gain access to confidential information held by a government or other organization. Attacks may be motivated by profit or by ideology. Cyberespionage activities can include every type of cyberattack to gather, modify or destroy data, as well as using network-connected devices, like webcams or closed-circuit TV (CCTV) cameras, to spy on a targeted individual or groups and monitoring communications, including emails, text messages and instant messages.

Software piracy: An attack that involves the unlawful copying, distribution and use of software programs with the intention of commercial or personal use. Trademark violations, copyright infringements and patent violations are often associated with this type of cybercrime.

Cyberstalking: This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically, cyberstalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety (Panda Security, 2019).

Phishing: This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer. Cybercriminals are becoming more established and many of these emails are not flagged as spam. Users are tricked into emails claiming they need to change their password or update their billing information, giving criminals access.

Rate of Students' Involvement in Cybercrime

The findings showed that students are involved in cybercrime in many areas such as; online drug trafficking; cyber stalking; email hacking; hacking of organizational account; identity theft; encrypting of files using public-key; online spam sending; floatation of illegal business proposal; cybercrime with direct contact through phone; the use of remote administrative tools and online child sexual abuse material (Amini-Philips, 2018). The students in their various responses have shown that they have been involved in one form of cybercrime or the other in their various institutions. Ngozi (2016) reported that the quest for money has made Nigerian youths to deeply involve themselves in cybercrime. She further found out that most of these students are deeply involved in cybercrime alongside their counterparts in the school. Denga (2011) in his own study disagreed vehemently with the findings of Ngozi, when he stated that undergraduates are fully occupied with academic and vocational activities that can make them associate with cyber theft. Ben (2017) in his study reported that up to 90% of undergraduate students are very much involve in cybercrime and its activities. Adanma (2017) as well vigorously disagreed with Ben, as she concluded that the level of undergraduate student involvement in cybercrime is still not fully ascertained. Odo & Odo (2015) investigated the extent of involvement in Cybercrime activities among students' in tertiary institutions in Enugu state of Nigeria. Their findings showed that students of higher institutions in Enugu state are involved in cybercrime. It also showed that students' involvement in cybercrime is dependent on gender and Institution type.

Prevalence of Cyber Crime in Nigeria

At the turn of 21st century, Nigerian internet infiltration levels have increased rapidly. According to Bengal, Babatope and Bankable, (2012) the number used to be less than 5% in 2002-2003, and later stood at over 30% by the end of 2012 and this growth is only equanimeous to speed up. At the end of the first quarter of 2016 (January-March 2016), Nigeria rated the 16th highest ranked country moving up two places from 18th position in the previous quarter. Developing nations especially the Africans countries were highly represented in the upper rankings and Nigeria was surpassed by a handful of other African countries, including Namibia and Malawi in second and fourth spots respectively (The news, 2016). However, the rise of the internet in Nigeria has come with a non-deliberated consequence and global notoriety becomes a safe haven for cyber fraudsters. Back in the 90s, fraud in Nigeria society was popular called 419 in reference to section 1(3) of the advance fee fraud and other related offenses Act No. 14 of 2006 penal code that framed the criminal justice system in Nigeria. Consumer Reports State of the Net (2007) shows that more than $7 billion cost of cybercrime on U.S consumers was estimated and also, The Internet Crime Compliant Centre (2012), reported that victims had losses over $500,000. In 2012, the Internet Crime Complaint Centre (IC3) received 289,874 consumer complaints, with losses of $525,441,110 (Ndubueze, 2013). To appraise the prevalence of cybercrime in Nigeria, quantitative research was employed in collecting information around losses in terms of money, time and material incurred by citizens through cybercrime. According to Bengal et al, (2012), the prevalence appraisal a survey was used to estimate how many of Nigerian's 48.3 million internet users experienced the loss. This was used to compute the estimated loss for Nigeria. This led to the estimated Nigerian consumer loss of #2,146,666,345,014.75 ($13,547,910,034.80) to cybercrime in 2012. The reported case ranges from fake lotteries to the biggest internet scams (Bengal, et al 2012).

Causes of Students' involvement in Cyber Crimes

The root implications of cybercrimes are not far-fetched. One only has to take a quick glance around the society to observe illicit wealth acquisition and its display. This is coupled with the fact that; the perpetrators are highly exalted (Akwara et al., 2013). The problem is made worse by the 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) 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 proliferated cybercrimes by students in Nigeria.

Unemployment: Unemployment rate in Nigeria is high and stood at 23.1% in the fourth quarter of 2018. Youth unemployment rate is currently above 47%. According to Okafor (2011), high unemployment in Nigeria comes with socioeconomic, 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: Nigeria has continued to occupy 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 the Transparency International in 2017 (Transparency International, 2017). 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.

Urbanization: Rapid urbanization in Nigeria which manifests mainly through the fast population growth is a challenging issue for policy makers. 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. According to Meke (2012), urbanization is beneficial only to the extent of availability of good jobs that have been created in cities, amidst high population growth rate. Meke's study also showed that that urbanization is one of the major reason that led to increases in cybercrimes by students in Nigeria. He also noted that urbanization and crime move in tandem.

Poor Implementation of Cybercrime Laws and Inadequately Equipped Law Enforcement Agencies: According to Laura (2011), African countries have received intense criticism for inadequately handling of cybercrimes due to inadequate infrastructure and competence of assigned law enforcement agencies. The private sector also lags behind in protecting itself from cyber savvy criminals, Nigeria inclusive. There is no sophisticated hardware to forensically track down cyber criminals. In some instances, the laws regarding cybercrimes are circumvented by criminals. It is worth noting that law enforcement agencies in Nigeria such as the EFCC and ICPC have successfully prosecuted cybercrime offenders over the years. Nevertheless, much improvement can still be made (Okafor, 2011).

Quest for wealth: Carnal instinct that quests for wealth is another cause of cybercrimes in Nigeria. For any business to succeed, it is expected that, the rate of returns on the investment grow at a geometric rate, with minimal risk. Cyber criminals desire to invest minimal capital in a conducive environment that would reap maximum gains as they strive to become rich using the quickest means possible.

Implications of Cybercrimes

Cybercrimes Implications on the Nigerian Economy

The implication of cybercrime has been, and is still being felt by all governments and economies that are connected to the Internet. Criminals uses the Internet, computers and other digital devices to facilitate their illegal activities as long as the financial gains outweigh the consequences when caught (Olusola, Samson, Semiu and Yinka, 2013). Knowing about the quantity of Cybercrime as well as the economic impact is vital for both governments as well as businesses which could be a necessary tool to adjust the legal and regulatory frameworks as well as institutional capacities. According to Vladimir (2005) internet is a global network which unites millions of computer located in different countries and open broad opportunities to obtain and exchange information but it is now been used for criminal purposes due to the economic factors. Nigeria a third world country is faced with so many economic challenges such as poverty, corruption, unemployment amongst others, thereby, making this crime thrive. According to the Nigerian Communication Commission (2016), cybercrime and espionage cost the global economy upwards of 500bn annually and are the main contributors for dragging down economic growth across the world. A study by the security firm McAfee and the Centre for Strategic and International Studies (CSIC) revealed that the US, the world's largest economy loses about $100bn (€76bn, £65bn) from cybercrimes and espionage, including loss of key business data and intellectual property (Mathew, 2014). According to the PTI Contents (2009), over 80% of the companies' surveyed acknowledged financial losses due to computer breaches. The approximate number impacted was $450 million. As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy.

Cybercrimes Implications on the Nigerian Educational Sector

Societies all through time have always relied on the education for guidance (Ozturk, 2008). Chimombo (2015) postulates that education has always served to cultivate the innovative capabilities of individuals in a society and this has created opportunities for improvements in the economic, political, societal and moral outlook of individuals in a nation. Nations seeking to stimulate national development have invested in education (Ozturk, 2008). However, it is imperative to note that the Nigerian educational system has face terrible challenges occasioned by cybercriminals. These activities have negatively impacted on the advancement of the nation's educational sector (Ololube, 2016). In the Nigerian educational context, vouchers are inflated, ghost workers employed, supplies of educational materials faked, and this has pave way to an increase in cybercrime activities. Many researchers have established that about 21 billion US dollars has been lost between the years 2005 to 2006 to illicit as well as unlawful fraud by cybercriminal in educational sector (Mumuni and Sweeney, 2013). Nwaokugha and Ezeugwu (2017) highlighted that student involvement in cybercrime activities in the educational sector negatively impacts social equality, merit and competence as it becomes rampant in the school campus. They further observed that these criminal acts in the educational sector has drained the quality of educational system, and influences the moral advancement in the society, hence impeding the sustainable development of the country (Abraham, 2011).

Remedies to Students' involvement in Cyber Crime

Prevention is always better than cure. Students should take certain precautions while operating the internet and should follow certain preventive measures for cybercrimes which can be defined as:

Education: Cybercrime in Nigeria is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols; hence, government of every nation needs to educate students and the society at large on use of internet and the need for continual maintenance and updating the security on their system.

Establishment of Programs and IT Forums for Nigerian Youths: Since the level of unemployment in the country has contributed significantly to the spate of e-crime in Nigeria, the government should create employments for these youths and set up IT laboratories/forum where these youths could come together and display their skills. This can be used meaningfully towards developing IT in Nigeria at the same time they could be rewarded handsomely for such novelty.

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

Antivirus and Anti Spyware Software: Antivirus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software. Anti-spywares are used to restrict backdoor program, Trojans and other spy wares to be installed on the computer.

Cryptography: Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient (Schaeffer, 2009).

Cyber Ethics and Cyber Legislation Laws: Cyber ethics and cyber laws are also being formulated to stop cyber-crimes. It is a responsibility of every individual to follow cyber ethics and cyber laws so that the increasing cybercrimes will reduce. Security software like antiviruses and anti-spywares should be installed on all computers, in order to remain secure from cyber-crimes (Laura, 2011). Internet Service Providers should also provide high level of security at their servers in order to keep their clients secure from all types of viruses and malicious programs.

Methodology

Ex-post facto research design was adopted for the study. The study was conducted in Imo State. The population of the study comprised of all the tertiary institution students, lecturers and stake holders in Imo State. Simple random sampling technique was used to select 3 tertiary institution. From each institution 40 students and 10 lecturers and was randomly selected. 15 stake holders were also selected from the ministry of education for the study. And this gave a total of 165 respondents that constituted the sample size for the study. The Main Instrument used in this study was a questionnaire titled "Implications and Remedies of Student Involvement in Cyber-Crime Questionnaire (IRSICCQ)". Face and content validation of the instrument was carried out by an expert in test, measurement and evaluation from Imo State University to ensure that the instrument has the accuracy, appropriateness and completeness for the study under consideration. Cronbach Alpha technique was used to determine the level of reliability of the instrument. The reliability coefficient obtained was 0.78 and this was high enough to justify the use of the instrument. The researcher subjected the data generated for this study to appropriate statistical techniques such as percentage analysis for answering the research question and simple regression analysis for testing the hypotheses. The test for significance was done at 0.05 alpha levels.

Results

Research Question One: The research question sought to find out the remedies that can mitigate student's involvement in cybercrime. To answer the research question percentage analysis was performed on the data, (see table 1).

Table 1: Percentage analysis of the remedies that can mitigate student's involvement in cybercrime

REMEDIES	FREQUENCY	PERCENTAGE
Education	24	14.55
Establishment of Programs and IT Forums for Nigerian Youths	32	19.40
IP Address tracking	33	20
Antivirus and Anti Spyware Software	11	6.67*
Cryptography	29	17.58
Cyber Ethics and Cyber Legislation Laws	36	21.82**
TOTAL	**165**	**100%**

**** The highest percentage frequency**
*** The least percentage frequency**
SOURCE: Field survey

The above table 1 presents the percentage analysis of the remedies that can mitigate student's involvement in cybercrime. From the result of the data analysis, it was observed that the tagged "cyber ethics and cyber legislation laws" 36(21.82%) was rated by the highest percentage of the respondents as a remedy of student's involvement in cybercrime, while "antivirus and anti-spyware software" 11(6.67%) was rated by the least percentage of the respondents as a remedy to student's involvement in cybercrime.

Hypotheses Testing

Hypothesis One: The null hypothesis states that there is no significant influence of the implications of students' involvement in cybercrime on the educational sector of Nigeria. In order to answer the hypothesis, simple regression analysis was performed on the data (see table 2).

TABLE 2: Simple Regression Analysis of the influence of the implications of students' involvement in cybercrime on the educational sector of Nigeria

Model	R	R-Square	Adjusted R Square	Std. error of the Estimate	R Square Change
1	0.77a	0.59	0.59	1.17	0.59

***Significant at 0.05 level; df= 163; N= 165; critical R-value = 0.197**

The above table 2 shows that the calculated R-value (0.77) was greater than the critical R-value of 0.197 at 0.5 alpha levels with 163 degrees of freedom. The R-Square value of 0.59 predicts 59% of the implications of students' involvement in cybercrime on the educational sector of Nigeria. This rate of percentage is moderately positive and therefore means that there is significant influence of the implications of students' involvement in cybercrime on the educational sector of Nigeria. It was also deemed necessary to find out the influence of the variance of each class of independent variable as responded by each respondent (table 3).

TABLE 3: Analysis of variance of the influence of the implications of students' involvement in cybercrime on the educational sector of Nigeria

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	324.32	1	324.32	235.64	.000b
Residual	224.35	163	1.38		
Total	548.67	164			

a. Dependent Variable: Educational Sector
b. Predictors: (Constant), Cybercrime

The calculated F-value (235.64) and the P-value as (.000b). Being that the P-value (.000b) is below the probability level of 0.05, the result therefore means that there is significant influence exerted by the independent variables i.e. cybercrime on the dependent variable which is educational sector. The result therefore means that there is significant influence of the implications of students' involvement in cybercrime on the educational sector of Nigeria. Therefore, the result is cognate to the research findings of Vladimir (2005) who asserted that internet is a global network which unites millions of computer located in different countries and open broad opportunities to obtain and exchange information but it is now been used for criminal purposes due to the economic factors. Nigeria a third world country is faced with so many economic challenges such as poverty, corruption, unemployment amongst others, thereby, making this crime thrive. The significance of the result caused the null hypotheses to be rejected while the alternative was accepted.

Hypothesis Two: The null hypothesis states that there is no significant influence of the implications of students' involvement in cybercrime on the Nigeria economy. In order to answer the hypothesis, simple regression analysis was performed on the data (see table 4).

TABLE 4: Simple Regression Analysis of the influence of the implications of students' involvement in cybercrime on the Nigeria economy

Model	R	R-Square	Adjusted R Square	Std. error of the Estimate	R Square Change
1	0.73a	0.53	0.53	1.45	0.53

***Significant at 0.05 level; df= 163; N= 165; critical R-value = 0.197**

The above table 4 shows that the calculated R-value (0.73) was greater than the critical R-value of 0.197 at 0.5 alpha levels with 163 degrees of freedom. The R-Square value of 0.53 predicts 53% of the implications of students' involvement in cybercrime on the Nigeria economy. This rate of percentage is moderately positive and therefore means that there is significant influence of the implications of students' involvement in cybercrime on the Nigeria economy. It was also deemed necessary to find out the influence of the variance of each class of independent variable as responded by each respondent (see table 5).

TABLE 4: Analysis of variance of the influence of the implications of students' involvement in cybercrime on the Nigeria economy

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	380.70	1	380.70	181.87	.000b
Residual	341.20	163	2.09		
Total	721.90	164			

a. Dependent Variable: Nigeria Economy
b. Predictors: (Constant), Cybercrime

The calculated F-value (181.87) and the P-value as (.000b). Being that the P-value (.000b) is below the probability level of 0.05, the result therefore means that there is significant influence exerted by the independent variables i.e. cybercrime on the dependent variable which is Nigeria economy. The result therefore means that there is significant influence of the implications of students' involvement in cybercrime on the Nigeria economy. Therefore, the result is cognate to the research findings of Nwaokugha and Ezeugwu (2017) who stress that student involvement in cybercrime activities in the educational sector negatively impacts social equality, merit and competence as it becomes rampant in the school campus. And these criminal acts in the educational sector drains the quality of educational system, and influences the moral advancement in the society, hence impeding the sustainable development of the country (Abraham, 2011). The significance of the result caused the null hypotheses to be rejected while the alternative was accepted.

Conclusion

The study concluded that since users of computer system and internet are increasing worldwide, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by students while using the internet which will assist in challenging this major threat Cybercrime. Therefore, the study reveals that there is significant influence of the implications of students' involvement in cybercrime on the educational sector of Nigeria. Also that there is significant influence of the implications of students' involvement in cybercrime on the Nigeria economy.

Recommendations

Based on the findings of the study, the following recommendations was considered necessary:

1. Federal and state government, as well as educational communities should intensify campaigns on cybercrime awareness among Nigerian undergraduate students in order to make them understand that cybercrime is a criminal offence punishable under the criminal act with attendant adverse consequence of jeopardizing their educational accomplishment when convicted.

2. Government should set up a mechanism to track and investigate the menace of cyber criminals within and outside the institutions. After all, majority of undergraduates live within the larger society and it is more difficult to monitor the development of these students.

REFERENCES

Abraham, N. M. (2011). Functional education, militancy and youth restiveness in Nigerias Niger Delta: The place of multi-national oil corporations (MNOCs). *African Journal of Political Science and International Relations*, 5(10), 442-447.

Adanma, J. (2017). Awareness level of undergraduate students and cybercrime among undergraduate students in South-East zone of Nigeria. *Journal of Social Media Review*, 5(3), 20-29

Akpan, C. (2016). University students and cybercrime: An indispensable critical review. *Journal of Sociology*, 2(2), 181-186.

Akwara A. F., Akwara N.F, Enwuchola J., Adekunle M. and 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), Vol. 2, no. 1.

Amini-Philips, C. (2018). Awareness and Involvement in Cybercrime among Undergraduate Students in Universities in Rivers State, Nigeria. *International Journal of Humanities and Social Science Invention (IJHSSI)*, 7(3), 39-43

Ayo, E. (2010). Convergence and Policy Issues in ICT sector. In G.O. Ajayi (Ed) Proceedings of Workshop on National Information and Communication Infrastructure, Policy, Plans and Strategies. Abuja, Nigeria. Pp. 28-50.

Ben, F. (2017). Cybercrime awareness level of students: The media role. *Journal of Social Development*, 4(2), 92-101.

Bengal, S., Babatunde, S, and Bankable, F (2012). *Economic Cost of Cybercrime in Nigeria*. University of Toronto. Monk School of Global Affairs

Brenner, S. W. (2009). *Cyberthreats*: The Emerging Fault Lines of the Nation State. Oxford University Press.

Brush, K., Rosencrance, L. & Cobb, M. (2020). Cybercrime. Available at: https://searchsecurity.techtarget.com/definition/cybercrime

Chimombo, J. P. (2005). Issues in basic education in developing countries: An exploration of policy options for improved delivery. *Journal of international cooperation in education*, 8(1), 129-152.

Consumer Reports State of the Net (2007). *U.S. Nationally Representative Survey of more than 2000 America Households*. Consumer Reports National Research Centre

Denga, A. (2011). *Youths and cyber theft*. Lagos: Ademola Publishers

Dennis, M. A. (2019). *Cybercrime*. Encyclopedia Britannica. Available at: https://www.britannica.com/topic/cybercrime

Fisher, B. S. and Lab, S. (2010). *Encyclopedia of Victimology and Crime Prevention*. Thousand Oaks, CA: SAGE Publications. p. 493.

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

Hassan A. B., Lass F. D. and Makinde J. (2012): Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology*, 2(7), 626–631.

Jain, S. (2017). *ATM Frauds-Detection & Prevention. International Journal of Advances in Electronics*, 4(10), 82-89.

Laura, A. (2011). *Cyber Crime and National Security*: The Role of the Penal and Procedural Law", Research Fellow, Nigerian Institute of Advanced Legal Studies.

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

Mathew, J. (2014). *Cybercrime Cost global economy $500bn annually*. International Business Times retrieved from: http://www.ibtimes.co.uk/cybercrime-csic-mcafee-hacking-493506

Meke E.S.N. (2012). *Urbanization and Cyber Crime in Nigeria*: Causes and consequences.

Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

Mumuni, A and Sweeney, G. (2013). *Public Interest litigation for the right to education*: the SERAP V. Nigeria case. In G. Sweeney, K. Despota and Lindner (eds) Global Corruption Report: Education. New York Routledge.

Ndubueze, P. N. (2013). Social Values and the Yahoo Boys' Subculture in Nigeria: Towards a Paradigm Shift for National Value Re-Orientation. *The Nigerian Journal of Sociology and Anthropology,* Vol. 11, No 1

Ngozi, S. (2016). Students' perception of cybercrime and its implications. *Journal of Social Development*, 4(2), 50-57.

Nigerian Communication Commission (2016). *Final Report on*: Effects of Cyber Crime on Foreign Direct Investment and National Development. Retrieved from: https://www.ncc.gov.ng/

Nwaokugha, D. O. and Ezeugwu, M. C. (2017). Corruption in the education industry in Nigeria, Implications for national development. *European Journal of Training and Development Studies*, 4(1), 1-17.

Odo, C. R. and Odo, A. I. (2015). The Extent of Involvement in Cybercrime Activities among Students' in Tertiary Institutions in Enugu State of Nigeria. *Global Journal of Computer Science and Technology: Information & Technology*, 15(3), 1-6

Okafor E.E. (2011). Youth Unemployment and Implications for Stability of Democracy in Nigeria. *Journal of Sustainable Development in Africa*, Vol.13, No. 1.

Ololube, N. P. (2016). Education fund misappropriation and mismanagement and the provision of quality higher education in Nigeria. *International Journal of Scientific Research in Education*, 9(4), 333-349.

Olusola, M., Samson, O., Semiu, A. and Yinka, A. (2013). Impact of Cyber Crimes on Nigerian Economy. *The International Journal of Engineering and Science (IJES)*, 2(4) 45-51

Ozturk, I. (2008). *The role of education in economic development*: a theoretical perspective. Available at SSRN 1137541.

Panda Security (2019). Types of Cybercrime. Retrieved from: https://www.pandasecurity.com/

PTI Contents (2009). India: A major hub for cybercrime. Retrieved from: http://business.rediff.com/

Sabillon, R., Cano, J., Cavaller, V. and Serra, J. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security*, 4(6), 165–176

Saroha, R. (2014). Profiling a Cyber Criminal. *International Journal of Information and Computation Technology*, 4(3), pp. 253-258

Schaeffer, B. S. (2009). *Cyber Crime and Cyber Security*: A White Paper for Franchisors, Licensors, and Others.

Tanwar, U. K. (2016). Cyber-Crimes and their Impacts: A Review. *IJRSI*, 4(1), 451-452

The Internet Crime Compliant Centre (2012). *2012 Internet Crime Report*. Internet Crime Compliant Centre. Retrieved from: https://www.ic3.gov

The news (2016). *Cybercrime*: Nigeria's Ranking gets Worse. Retrieved from: www.thenewsnigeria.com.ng

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

Transparency International (2017). *Corruption Perceptions Index 2016*. Retrieved from: https://www.transparency.org/

Warf, B (2018). The SAGE Encyclopedia of the Internet. SAGE Publications.

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