CYBERCRIME IN NIGERIAN CYBER SPACE: THE TASK BEFORE THE NIGERIAN LIBRARIANS

BY

MBUOTIDEM UMOH ESQ. *Ph.D*
&
DR. OKON ENIDIOK
IME UMANAH LAW LIBRARY,
UNIVERSITY OF UYO, UYO,
AKWA IBOM STATE, NIGERIA

ABSTRACT

The study was conducted to investigate Cybercrime in Nigerian Cyber Space: The Task before the Nigerian Librarians. To guide the study, one specific purposes and null hypotheses respectively was formulated. A descriptive survey design was adopted for the study. The population comprised of all librarians in academic libraries who attended the 55th Nigerian Library Association Conference and Annual General meeting in Lagos last year. A sample size of 250 librarians in the conference hall was selected using stratified random sampling techniques. The researcher developed an instrument entitled: "CYBERCRIME IN NIGERIAN CYBER SPACE QUESTIONNAIRE (CNCSQ)" to generate data for the study. The instrument was validated by the thesis supervisor and experts in test and measurement were contacted for thorough check and experts' inputs. The collected data were analyzed with the use of appropriate statistical techniques such as simple regression analysis. The findings of the study reveal that there is significant influence of Nigerian Liberian intervention on the level of mitigation of cybercrime in the Nigerian cyber space. Among others, it was recommended that Nigerian security agencies should participate in training workshops and conferences on cyber security because like an author rightly said "You cannot fight Today's Crime with Yesterday's Technology". It was also recommended that Nigerian Government should endeavour to create employment opportunities for the teeming youths as studies has shown that it is age bracket that constitutes the cyber criminals.

KEY WORD: Crime, Cyber Crime, Intervention, Mitigation, Cyber Space, Nigerian Society

INTRODUCTION

Crime is a social factor in society. It is an inevitable behavioural element of society. In everyday life, it is obvious that some people refuse to keep to the tenets of good behavioural culture, renege in abiding by the laws of governance, deviate from the path of acceptable norms of society, and engage in a pattern of life that puts them in direct collision with the law. From the time of Cain in the Holy book till now, crime has remained a steady unresolved behavioural pattern of modern society. It can be argued that crime is a natural social phenomenon in context and content. It promotes distinct demarcation between good and bad behaviour in society.

Mbuotidem Umoh *Ph.D* & Dr. Okon Enidiok

WHAT IS CRIME?

Crime can be seen as any action that contravenes the laws established by government be it Local, State, Federal, or a political authority. It is any type of behaviour that breaks the law. Indeed, the development in electronic and telecommunication technology to power economies of nation State has increased economic crime enormously. Finlay in Bryn (2000), notes that "crime is now as much a feature of the

emerging globalized culture as is every other aspect of its consumerism". Apparently, the focus of this paper is not to treat crime in general context, but to examine an element of it which is cyber crime. This is because cyber crime has pervaded the entire world now, growing at alarming rate, and defying all efforts to combat the menace. In clear terms, given the scenario in Nigeria, cyber crime has come to stay, not to be uprooted, but to find a way of reducing or managing it.

CONCEPT OF CYBER CRIME

Cyber crime is an attack that undermines the confidentiality, integrity and availability of a computer, information resident on it or a computer service within a network information system (Ashesh, ııooo). It is an unauthorized access to computer network system to intercept computer service, steal, damage, or destroy information or data in the system. According to Odumubori (ııoıv), cybercrime encompasses criminal act dealing with computers and networks. It also includes traditional crimes conducted through the internet. In addition, it is any crime committed using computer or hand held mobile devices through the network. The author reports that in Nigeria, the Central Bank of Nigeria explains that Banks lost N ıı billion in ıı oıı through internet fraud, and N ıı billion to cyber criminals in ıı oıı ıı.

Cybercrime has become an issue of national and international concern. In Nigeria, several draft bills have been introduced to the Legislature to pass as law. On October ıı v, ıı oıv, the senate of the Federal Republic of Nigeria passed into law a bill specifying cyears jail term for all computer related fraud, forgery, offences relating to pornography, cyber-stalking, and cyber-squatting. The law titled "An Act for the prohibition, prevention, detection, response, Investigation and prosecution of cyber crimes and other related matters ıı oıv" is aimed at protecting and punishing fraudsters and other cyber related crime in electronic and online transactions, and to guard against cyber terrorism (Datboyierry, ıı oıv).

WHY DO PEOPLE COMMIT (CYBER) CRIME?

The reason why people commit crime can be a knotty issue to address. Sociologists have tried to provide answers that border on love, jealousy, money, which sometimes is facilitated by the influence of drugs, alcohol, and severe psychological state. They have also identified environmental factors such as family up-bringing, peer influence, poverty status, family traits, and role model influence to mention a few (Gargulinski, ıı oıx).

Crime, as we know, has been with man, we live with it, and has become an over bearing negative element of human society from Cain in the Holy book till now. Over the years, the magnitude and intensity has increased to an alarming proportion to the extent that has raised global concern and worry. In the contemporary world, hardly can a day pass by without news of one form of crime or another. It is a general opinion that the environment in which a person is brought up can influence criminal tendencies in the person. This opinion has been associated more with people from low social background, slum dwellers, and areas prone to gangsters. They believe in the claim "if you don't have it, steal it" for survival and sustenance.

Wrong value system is also a primary reason which can explain why people commit cyber crime. In the early days, people grew up in an environment where the intrinsic differences between good and evil were instilled into them. Children were taught the virtues of hard work, honesty, patience etc nowadays some children are encouraged by their parents and elders to succeed and get rich at all costs even if it means cutting corners. When they eventually succeed in acquiring such illegal wealth, they are celebrated by all-parents, community and the society.

Several times in human society, we hear the usual lame and vexing pleadings of "the devil pushed me into the crime". This is always considered as an intolerable excuse since crime takes a process to manifest from planning to execution.

From the legal view point also, this excuse holds no water because the Law recognizes that before a crime is executed two factors must be present: the physical act (actus reus) and the mental element which is otherwise known as the intention (mens rea). This goes to show that the criminal had already nursed the intention in his mind before taking active steps to execute it. Many times, greed has been cited as a prime causal factor in crime. It has also been seen as a great motivating factor that fuels the urge to commit crime, irrespective of any foreseen consequences that may accord the criminal act.

The scourge of cyber crime in Nigeria, the paroxysm of extreme physical pains it instills, the anguish that it exudes, the great sympathy at any time such incidents occur. This makes it more difficult to understand the behavior of criminals, the strange causal factor, and how it can be uprooted from human society.

Another reason why people commit cyber crime in Nigeria is lack of fear of punishment. This can be attributed to the weak legal structure in the country which is manifested through prolonged trials, incessant adjournments and even where the prosecution secures a conviction, there is the last option of Plea Bargain wherein the criminal is simply asked to refund a fraction of the amount he stole to the owner.

TYPES OF CRIME

Authorities on crime Ashesh (IIOOD), Withers (IIOIX), Gargulinskim (IIOIX) have identified many types of criminal acts to include:

i. Crime pertaining to property – which borders on robbery, burglary, stealing, which involves depriving the victims of their hard earned money, household items, and damage to their personal property
ii. Serial killers (assassins) who kill their victims without any identified or premeditated reasons other than to satisfy their evil urge. The perpetrated violent acts are especially gruesome and bizarre.
iii. Murder cases which most of the time is carried out by the victim's known persons acquaintances, friends, partners, parents (as in the murder of Marvin Gay by his own father) or the murder of Reena Streevkamp by Oscar Pistorious, the celebrated athlete himself on a valentine day in South Africa in IIOIIII.
iv. Domestic crime mostly between couples, housemaids, arising from serious emotional excessiveness or outright demonstration of extreme anger
v. Cyber crimes in which cyber criminals use modern electronic and communication technologies to inflict severe losses to an organization, individuals and corporate entities all over the world.
vi. Drug trafficking, drug abuse and its collaborating money laundering business is known to cover all countries now. In some countries including Mexico, powerful drug cartels have constituted themselves into business blogs, using very sophisticated telecommunication gadgets and technology to evenly distribute their product by air or intercepts signals that can pinpoint where they are.

CATEGORIES OF CYBER CRIME

- Interception of email: electronic mail is a means of sending a message electronically from one computer to another. E-mail is a tool that transmits messages over electronic networks like the internet, such that it is received with computers, or hand held devices like mobile phones. Occasionally, cyber thieves intercept the messages and tap the content for their nefarious activities.
- Electronic funds transfer: this is a system of transferring funds electronically directly from one bank account to another. It is used in local and international business. The growing popularity of this online means of bill settlement has facilitated electronic commerce round the world. However,

cyber criminals use all available means to intercept some online payments and stop the money to the detriment of business people and organizations.

- **E**lectronic **D**ata **I**nterchange: **T**his refers to the application of computers in exchanging business data/information through the internet. **B**usiness documents such as purchase order, invoice, delivery documents and so on, may by tempered with, during transmission or complete stealing of companies' or organizations' vital data/secrets.
- **I**dentity theft: one of the most rampant cyber crimes incidents is identity theft. **I**t involves a situation where an unauthorized person uses another person's identification documents to impersonate that person to commit crime. **A**s **P**andey (2010) explains, this method of identity fraud has been used in bank fraud, credit card fraud, cyber cash wallet, debit card, computer fraud, telecom fraud, tax fraud, mail fraud. **O**thers include alien fraud, passport fraud, money laundering, and a host of others. **S**ince banks operate on social media platforms, cyber criminals find it easier to exploit their social media presence to commit crime.
- **P**hishing: is a method used to gain personal information for identity theft purpose. **T**he cyber criminals can use malicious ware (malware), e-mail, other virus laden software to attack a computer network and fake financial housing of their target to feature as genuine organization. **B**y so doing the criminals deceives members of the public who later become their victims. **T**he message they give out appears to be authentic which encourage members of the public to give out their **PIN** number, credit card information, passwords, etc. in addition to these, they are involved in cloning of **ATM** cards, website, and school portal, where they carry on their nefarious act.
- **Malicious Insiders/software**: **T**he threat of insider connection is most prevalent and disturbing in committing bank fraud. **U**nauthorized access to data and other vital information are exploited by insider staff which amounts to cyber fraud. **S**imilarly, malware is used to damage records (personal or organizational), and do other things in the computer that can lead to cyber fraud. **S**ome malwares are designed just to steal money from internet banking applications and money transfer transactions.
- **Hacktivism and cyber syndicates**: **T**hese are elitists, well organized cyber criminals who operate very sophisticated computer software in networks that allow them to attack e-commerce business lines and online payments where they steal a lot of money.
- **ATM Hacking: H**ackers in **N**igeria have developed professionalism in using technology to change **ATM** control which allows them to withdraw unlimited money from **B**anks' **ATM**. **A**ll these types of cyber crime have come to be as development in technology awareness increases.

- **Cyber Stalking**
  Cyber stalking is essentially using the **I**nternet to repeatedly harass another person. **T**his harassment could be sexual in nature, or it could have other motivations including anger. **P**eople leave a lot of information about themselves online. **S**uch information can leave one vulnerable to cyber stalking, a term that essentially refers to using the **I**nternet to stalk (to illegally follow and watch somebody), **J**ustin (2010). **W**hereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. **T**his often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties. (www.wikipedia.com cited in **H**assan, **L**ass and **M**akinde, 2011)
- **Drug Trafficking Deals**
  Another type of **C**yber **C**rime is **D**rug **T**rafficking: it is a global trade involving cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition law. **D**rug traffickers are increasingly taking

advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to make comfortable purchase of illegal drugs. (www.wikipedia.com cited in Hassan, Lass and Makinde, IIOIII).

- **Cyber Terrorism**

  A cyber terrorist can be described as someone who launches attack on government or organization in order to distort and or access stored information stored on the computer and their networks. According to Wikipedia, 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, and the information stored on them; for instance, a rumor on the Internet about terror acts. In addition, Parker (IMDIII) defined Cyber terrorism as an act of terrorism committed through the use of cyberspace or computer resources. 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. Another form of cyber terrorism is cyber extortion 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 extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. (Hassan, Lass and Makinde, IIOIII)

- **Logic Bombs**

  A typical logic bomb tells the computer to execute a set of instructions at a certain date and time or under certain specified conditions. The instructions may tell the computer to display "I gotcha" on the screen, or it may tell the entire system to start erasing itself. Logic bombs often work in tandem with viruses. Whereas a simple virus infects a program and then replicates when the program starts to run, the logic bomb does not replicate it merely waits for some pre-specified event or time to do its damage. Time is not the only criterion used to set off logic bombs. Some bombs do their damage after a particular program is run a certain number of times. Others are more creative. There are several reported cases that a programmer told the logic bomb to destroy data if the company payroll is run and his name is not on it.; this is a sure-fire way to get back at the company if he is fired! The employee is fired, or may leave on his own, but does not remove the logic bomb. The next time the payroll is run and the computer searches for but doesn't find the employee's name, it crashes, destroying not only all of the employee payroll records, but the payroll application program as well. Logic bombs present a major threat to computer systems, not just because of the damage they themselves can do, but because they provide a technique to facilitate more devastating crimes.

- **Account Takeover**

  Another type of cybercrime is an "account takeover." This happen when cyber criminals compromise your computer (by getting you to click on a link for example) and install malicious software, such as "key loggers" which record key strokes, passwords, and other private information. This in turn allows the hacker access to data using your log-in credentials. Once these criminals steal your password, they may be able to breach your work networks or, if at home, your personal online bank account. These criminals can be anywhere in the world.

The above scenario hitherto was a daily occurrence in the developed world however it has steadily crept into the Nigerian internet space.

EMERGING CYBER TRICKS IN NIGERIA

These are examples of additional cyber tricks that are emerging on a daily basis in the Nigerian Cyber space:

- **Beneficiary of a Will Scam**: The criminal sends e-mail to claim that the victim is the named beneficiary in the will of an estranged relative and stands to inherit an estate worth millions.

- **Online Charity**: Another aspect of e-crime common in Nigeria is where fraudulent people host websites of charity organizations soliciting monetary donations and materials to these organizations that do not exist. Unfortunately, many unsuspecting people have been exploited through this means.
- **Next of Kin Scam**: Collection of money from various bank and transfer fees by tempting the victim to claim an inheritance of millions of dollars in a Nigerian bank belonging to a lost relative.
- **The "Winning Ticket in Lottery you never entered" Scam:** These scams lately include the State Department's green card lottery.
- **Bogus Cashier's Check**: The victim advertises an item for sale on the Internet, and is contacted
- **Computer/Internet Service Time Theft**: Whiz kids in Nigeria have developed means of connecting Cyber Cafes to Network of some ISPs in a way that will not be detected by the ISPs and thereby allow the Cafes to operate at no cost.
- **Lottery scam:** allowing users believe they are beneficiaries of an online lottery that is in fact a scam. (Ibikunle and Eweniyi, 2010)

THEORETICAL FOUNDATIONS

The four choices of theories of crime:

Rational Cause or "choice Theory" propounded by Cesare Becarria, an Italian Philosopher state that the motivation to commit a crime is a purposeful decision laden with pecuniary gains in the form of incentives such as money, powers, status, or learning. The theory explains that the offender makes a choice to commit a criminal act after examining options, consequences, and benefits. The offender then takes a decision on the type of crime, he wants to commit, the place the crime will be committed, and target of the crime, and executes the crime fully aware that the act is wrong. In the process the criminal willingly and consciously suppresses the option to abstain from the act.

Sociological Positivism

This theory looks at the correlation between societal influences and crime. It explains social structures within the environment of the offender such as family, friends, peer groups, socio-economic status, level of education and sub-culture as being the influence of his criminal behavior. The theory explains that criminal conduct is inevitable where the sub-culture behooves criminal culture, poverty, broken-family, and moral decadence.

Biological Positivism

Cesare Lambroso postulated this theory. He states that some people are born criminals. The theory examined physiological factors of criminals and non-criminals such as vitamin deficiencies, hormonal imbalance, diet and brain functioning as

resulting in criminal tendencies of people. However, not many researchers have been carried out about this theory to confirm its authenticity.

Psychological Positivism

Alexander Lacassagne holds that what causes criminality resides (rooted) in the offenders' mental illness or personality disorders. According to him, disorders may be the result of sociological or biological factors such as physical or biological or sexual abuse, parental criminology and intelligence level. They analyze criminality to stem from internal and unavoidable cause.

Existing Cyber Crime Agencies in Nigeria

I. Economic and Financial Crimes Commission established in IIOOII with a mandate to among others investigate all economic crimes including advance fee fraud, money laundering, counterfeiting etc. The Commission is charged with the responsibility of enforcing the provisions of the following laws:

   (a) The Money Laundering Act IMMX;
   (b) The Advance Fee Fraud and Other Fraud Related Offences Act IMMX;
   (c) The Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act IMMV, as amended;
   (d) The Banks and other Financial Institutions Act IMMI, as amended; and
   (e) Miscellaneous Offences Act; and
   (f) Any other law or regulations relating to economic and financial crimes.

II. Independent Corrupt Practices Commission established on September, IIMth, IIOOO by the Independent Corrupt practices and Other Related Offences Commission (Establishment) Act (IIOOO) with a primary mandate to receive complaints investigate and prosecute offenders. Other duties include education and enlightenment of the public about and against bribery, corruption and related offences. The commission also has the task of reviewing and modifying the activities of public bodies, where such practices may aid corruption.

EFFECT OF CYBER CRIME ON THE NIGERIAN SOCIETY

Cyber crime has adverse effects on people, companies, organizations and even the Nigerian Government. The following points constitute some of those effects of cybercrime on the above listed groups:

I. Huge financial costs are incurred by the government, due to the rise of cyber-crime in the country. As for measuring costs the Detica report cited in Ibikunle and Eweniyi, (IIOIIII) considered four categories: costs in anticipation of cybercrime, such as antivirus software, insurance and compliance; costs as a consequence of cybercrime, such as direct losses and indirect costs such as weakened competitiveness as a result of intellectual property compromise; costs in response to cybercrime, such as compensation payments to victims and fines paid to regulatory bodies; indirect costs such as reputational damage to firms, loss of confidence in cyber transactions by individuals and businesses, reduced public-sector revenues and the growth of the underground economy.
II. Financial loss: Cybercriminals are like terrorists or metal thieves in that their activities impose disproportionate costs on society and individuals.
III. Loss of reputation: most companies that have been defrauded or reported to have been faced with cybercriminal activities complain of clients losing faith in them.
V. Reduced productivity: this is due to awareness and more concentration being focused on preventing cybercrime and not productivity.
X. Vulnerability of their Information and Communication Technology (ICT) systems and networks.

L. **Reduces the Competitive Edge of Organizations**
Computer crimes over the years have caused a lot of havoc to individuals, private and public business organization within and outside the country, causing a lot of financial and physical damage. Due to cyber crime, there has being loss of billions of dollars annually globally speaking, such crimes may threaten a nation's security and financial health, a company can suffer losses due to computer crime when a hacker steals confidential information and future plans of the company. And he simply sells the information to a competitor company; this will automatically reduce the competitive strength of the company.

7. **Time Wastage and Slow Financial Growth**
Wastage of time is another problem because many IT personnel may spend a lot of time on handling, rectifying harmful incidents which may be caused by computer criminals. The time spent should have earned a profit to the organization. One peculiar problem is that, when a hacker enters into an organization and steals confidential information from the company the people who entrust the company loses their confidence in the company as the company may contain confidential information like credit cards of customers and as the information is stolen the customer will not trust the company again and will move to someone else who could protect their confidential information. (Hassan, Lass and Makinde, IIOIII)

D. **Slows Production Time and Add to Over Head Cost**
Computer crime reduces the productivity of a company, as a company will take measures to reduce cybercrime, by entering more password or other acts, this will take time to do and therefore will affect productivity. Computer crime will increase the cost as to stop viruses and malware companies must buy strong security software to reduce the chances of attacks from such attacks. (Hassan, Lass and Makinde, IIOIII).

M. **Defamation of Image**
With the high level of cyber crime in the nation, the slogan "**GOOD PEOPLE GREAT NATION**" by Nigerians will be tarnished and global community will view the other side of the coin. Other effects include the consumption of computer and network resources, and the cost in human time and attention of dismissing unwanted messages (Hassan, Lass and Makinde, IIOIII)

Generally, the effects of a single, successful cyber-attack can have far-reaching implications including financial losses, theft of intellectual property and loss of customer confidence and trust. The overall monetary impact of cybercrime on society and government is estimated to be billions of dollars per year. (Rowley,n.d)

CYBER CRIME REDUCTION STRATEGIES

Cyber crime has given cause for serious concern in Nigeria and has made crime monitoring, reduction, and prevention an inevitable response to increasing crime rates in the society. Many strategies are ongoing in this direction. These include policing in the context of identification of the criminals, the crime rate and trend to better combat the menace and its "cripers link" to powerful men and women in the society. Intervention activities initiated by Non-governmental organizations (NGOs), Religious organizations, and use of social media are also working towards the same goal combating cyber crime.

Withers (IIOIX) proffers ways of reducing cyber crime rate to include provision of stiff penalties and even capital punishment to deter 'would be' criminals; infiltration of the police in computer/business centre in big cities in undercover operation manner; and creation of awareness in communities regarding the type of crime prevalent in the area and how individuals can keep away from such places to avoid being victims. He suggests that there must be effective collaboration work among the security agencies, members of each community, government officials, and other organizations to assist in cyber crime reduction and prevention.

Many stakeholders in business and telecommunications have adopted methods for preventing cyber crime which is currently on the rise. Among those proffered by St Marie (IIOIX) are: Arrest and prosecution of the bandits, confiscating proceeds of the crime, raising penalties or the magnitude of punishment recommended for them and stigmatization to deter persons who may wish to go into criminal acts of any sort.

CYBER CRIME REDUCTION

Education

The author also advocates that, a specially tailored education programme can be introduced into the school system to focus on imparting instruction to students against criminal activities. Such instructional programmes will educate students about the concept of crime, efforts on society, punishment that should await criminals, and how they can escape from the lure of criminality.

Stress Reduction

Advocates of stress reduction posit that when the state can reduce individual stress caused by better psychological services, poverty alleviation and urban planning, crime rate will decrease accordingly. We cannot totally agree with this idea, because an individual who is prone to criminal activities will go on with his/her nefarious acts, irrespective of the "bread and honey" around him or her.

The most vital aspect of crime reduction process is for the society to take proactive effort in protecting themselves. Rai and Ghosh (IIOOC) and Pandey (IIOIO) have suggested ways people can protect themselves from identity theft to include:

i. People should desist from giving their identity number or data to others, unless series of confirmations and verifications about the requesting body are received or it becomes absolutely necessary to do so in certain circumstances;

ii. Unwanted records, expired credit card, withdrawal booklet should be burnt, not thrown into waste bin where someone can pick up;

iii. Not to carry original copies of passport, birth certificate, credit cards in purse or wallet. If doing so is necessary, it should be photocopied which is easy to cancel in event of loss or unauthorized account access;

iv. Not to give phone number(s), PIN number, Password, encryption keys, secret codes of identity to any strange persons;

v. Guard against deposit slips, withdrawal instruments, to prevent an unscrupulous person having access to other peoples' transactions.

vi. Use of Cipher Text Encryption should be popularized to protect financial payments in business and administrative transactions. For example, if one chooses cryptographic algorithm of "II" in writing five million Nara, one can add every second letter to the intended one to produce... "Hlxgolnnlqpplctc" which can be difficult for criminals to decrypt for their nefarious activities.

The use of "Digital certificate" is also encouraged in business transactions to protect one's identity or a right to access certain information or services online. Much as Digital certificate is not prevalent in electronic business or administrative transactions in Nigeria, it should be encouraged to protect people who carry on electronic commerce.

Giddens, Duneeier and Applebaum (IIOOX) subscribe to visible policing techniques such as patrolling the street to detect, investigate and nib some criminal plans in the bud. This means that police should work closely with citizens to improve community civil behavior. The authors also support shamming as a form of punishing criminals and deviant behaviours. Ordinarily, the fear of being shamed in one's community is moderately considered as deterrent to crime in some communities, but we can argue that for criminal who already wear shameless faces, and are hardened, this method can not deter them from crime. Too, ordinary thieves do not commit cyber crime. It is elitist in nature. Therefore, shaming cannot have sustainable negative effect on such level of criminals. However, criminologists suggest stigmatizing shaming in

which a criminal is labeled as a threat to society and is treated as outcast to help deter the potential criminals.

Olu (2014) has suggested the following ways to reduce cyber crime in Nigeria:

i. Developing cybercrime threat risk management framework
ii. Investing in computer and mobile devices security protection measures
iii. Implementing enterprise wide data management
iv. Implementing appropriate legislation to reduce or crush cyber crime menace.
v. Implementing latest security patches and developing network security architecture
vi. Developing technology to track digital information leaving and entering the organization.
vii. Developing data classification, protection and prevention tools

NITDA, EFCC are working towards curbing cybercrime.

Mbuotidem Umoh *Ph.D* & Dr. Okon Enidiok

STRATEGIES USED BY LIBRARIAN IN MITIGATING CRIME

Increase in plagiarism, photocopying and piracy, an act that does not recognize or acknowledge the actual owner (author) of intellectual work call for serious concern the world over. As examined by the U.S copyright office (2000) copyright is viewed as a universal concept which has assumed a level of protection put in place by the law of any sovereign state. In his opinion, Gleason (1999), observed that in as much as copyright is a legislation right which backed creation of work, it guarantees an author a monopoly it gives or guarantees a publisher a monopoly right to publish or arrange to publish and sell a work within national boundaries for a given period of time; it provide financial compensation in terms of royalties to authors to reward them for their intellectually creative work and encourages progress in the country's arts and sciences in order to foster its economic social cultural development.

According to Cornish (1996), there are certain rights of owners of a work which are not necessarily economic. The author however, distinguishes the copyright into four categories of rights; the right to be identified as the author or creator, the right not to have their work subjected to derogatory treatment, the right not to have a work falsely attributed to the author, and the right of privacy of privately commissioned photographs and films. The underlying idea is that a creator or an author must reserve absolute control over his or her creative ideas.

Basic education and knowledge of the tenet of copyright laws enable librarians at dispensing their services in the direction of protecting copyright law and satisfying the need of its patron Febunmi (2009). Some Librarians face a dilemma when it comes to copyright (Ginsberg, 2001). For instance, if content provider of creative work disappeared or stop further intellectual creation, librarians and patrons would suffer. This is so because relevance information would stands lacking since the sources are not forth flowing with more creative ideas.

"We recognize and respect intellectual property rights" (American Library Association Code of ethics). Thus, librarians are to recognize and advocate balance between the rights of intellectual property owners and the rights of information users. Vendors sometimes try to create that balance for librarian by introducing technologies that prevent users from committing copyright infringements. However, these technologies according to Pessach (2008) can create additional issues and highlights the difficulties librarians face in mediating between law and technology. This challenge requires vigilance and education rather than a reliance on an automated solution.

According to Pessach (2008), several library organizations have attempted to provide guidance as to the appropriate balance between protecting the rights of authors and seeing to the needs of library patrons. For example, the American Library Association code of ethics notes that recognition and respect for intellectual property rights is one of the principles that should guide librarians' ethical decision making. However, the code also emphasizes that the organization is committed to

upholding the principles of intellectual freedom and resisting efforts to censor library resources (Dratter, 1100x).

According to Winston, (1100M) librarians who most often see the problems that copyright restrictions create for users are especially sensitive to this imbalance. In the digital world, many people will create, especially if user's rights are well crafted, while only a few will benefit from the monetary incentive. So the current lack of balance tips is precisely in the wrong direction. In his view Peterson (1100M) is of the opinion that as librarian try to come to grips with the burgeoning phenomenon of born-digital creativity, their awareness of the problems created by the over-enforcement of the copyright monopoly grows. Ironically, the fact that everyone can now be a producer and publisher of content is precisely the technological development that has led the content industries into their current battles to increased enforcement and penalties the role of advocacy for individual users of copyrighted material should be taken seriously by the librarians. Pessach, (1100C) opined that they need to ensure that the right and privileges of their patrons are well protected. They must assure the library users of the uninhibited access to information as it would aid research. However, according to Pessach any user that is unsure if the material to be copied is protected by copyright needs to seek advice from the library staff. Library users need to change their orientation towards fair use legislation (Onatola et al, 1100L). This means that, users can copy a very small amount of a work not for commercial but educational purposes. However, it is important to get permission to copy or use copyrighted material by contacting the copyright owner. Also any copying carried out for commercial purpose requires prior permission from the copyright owner, perhaps for a payment of a copyright fee. The principle of fair use should be strictly adhering to, should there be any need to copy, otherwise photocopying the entire work should not be allowed by the librarian. It should be emphasized that successful copyright infringement suits are unusual. The large majority of copyright holders are content with settlement in which the defendants agree to cease their behavior and perhaps pay modest damage awards.

Copyright laws in Nigeria are entrenched in the nation's Copyright Act of 11000. It is pertinent for all the librarians in Nigeria to have copyright education, in order to familiarize themselves with the basics principles of concept of copyright laws in Nigeria. This will enhance the rendering of their service without violating copyright laws. Given adequate education in copyright law, librarians will be able to know the risk involved in copying from copyright protected material and operate within the laws.

In Band's (1100M) view some countries require online service provider to comply with so-called "notice or takedown" provision to be protected by a safe harbor. In United state, for example if a copyright holder believes that a file hosted by a service provider infringes on his or her copyright, the copyright holder may send a notice to the provider requesting that the file be removed.

METHODOLOGY:

A survey research design was used for this study. This design was used since the expected population was over 1000. This targeted population was all librarians in academic libraries who attended the xxth Nigerian Library Association Conference and Annual General meeting in Lagos last year. In this type of design, the researcher take a comprehensive description of the research procedure used on the researcher. The instrument used was questionnaire tagged "**CYBERCRIME IN NIGERIAN CYBER SPACE QUESTIONNAIRE (CNCSQ)**" the validity of the instrument was done by experts in test and measurement Department of University of Uyo. The reliability co- efficient was 0.DM derived from administration of the instrument to 110 respondents. These instruments were then administered randomly to 11X0 librarians in the conference hall. One research assistants who helped, in addition to the researcher were able to collect all the 11X0 questionnaires representing 100 percentage returns. Regression analysis was then used to test hypothesis at 0.0X alpha levels

RESULT AND DISCUSSION

Data Analysis and Results

Hypothesis Testing

Hypothesis One

The null hypothesis states that there is no significant influence of Nigerian Liberian intervention on the level of mitigation of cybercrime in the Nigerian cyber space. In order to test the hypothesis regression analysis was performed on the data. (see table 1).

Table 1:
Regression Analysis of the influence of Nigerian Liberian intervention on the level of mitigation of cybercrime in the Nigerian cyber space

Model	R	R-Square	Adjusted R Square	Std. error of the Estimate	R Square Change
I	0. DII[a]	0. LL	0. LL	I. VV	0. LL

***Significant at 0.05 level; df= 248 N= 250; critical R-value = 0.139**

The table shows that the calculated R-value 0.DII was greater than the critical R-value of 0.IIIIM at 0.X alpha levels with IIVD degree of freedom. The R-Square value of 0.LL predicts LL% of the influence of Nigerian Liberian intervention on the level of mitigation of cybercrime in the Nigerian cyber space. It was also deemed necessary to find out the extent of the variance of each case of independent variable Nigerian Liberian intervention on the level of mitigation of cybercrime in the Nigerian cyber space as responded by each respondent (see table II).

Table 2:
Analysis of variance of the influence Nigerian Liberian intervention on the level of mitigation of cybercrime in the Nigerian cyber space

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	IOIIII. XL	I	IOIIII. XL	VMO. MI	.000[b]
Residual	XIII. OV	IIVD	II. OC		
Total	IXIIX. LO	IIVM			

The above table presents the calculated F-value as (VMO.MI) and the P-value as (.000). Being that the P-value (000) is below the probability level of 0.0X, the result therefore means that there is significant influence of Nigerian Liberian intervention on the level of mitigation of cybercrime in the Nigerian cyber space.

Discussion of Findings

The result of the data analysis in table I was significant due to the fact that the calculated R-value (0.DII) was greater than the critical R-value (0.IIIIM) at 0.0X levels with IIVD degree of freedom. The result implies that there is significant influence of Nigerian Liberian intervention on the level of mitigation of cybercrime in the Nigerian cyber space. The result therefore was in agreement with the research findings of with several researchers and experts, including Pessach, (IIOOC) who opined that librarians need to ensure that the right and privileges of their patrons are well protected and that they must assure the library users of the uninhibited access to information as it would aid research. The results also agree with the opinion of Onatola et al, (IIOOL) library users need to change their orientation towards fair use legislation, meaning that users can copy a very small amount of a work not for commercial but educational purposes. The significance of the result caused the null hypothesis to be rejected while the alternative one was upheld

Conclusions

Based on the findings of the research work, it was concluded that there is significant influence of Nigerian Liberian intervention on the level of mitigation of cybercrime in the Nigerian cyber space.

Recommendations

Based on the findings of the research, the following recommendations are deemed necessary:

1. The Nigerian government and corporate organizations should take urgent steps to engage in cyber security- effectively securing their cyberspace

II. The Nigerian security agencies should participate in training workshops and conferences on cyber security because like an author rightly said "You cannot fight Today's Crime with Yesterday's Technology"

III. There should be a complete overhaul of our value system. Parents should once again teach children and youths the value of respect, hard work, truthfulness etc

V. Nigerian Government should endeavour to create employment opportunities for the teeming youths as studies has shown that it is age bracket that constitute the cyber criminals

X. Nigerian Government should equally focus their developmental and community projects in the rural areas by providing basic amenities as this may curb the migration to urban areas.

L. National Universities Commission should introduce general courses such as Introduction to Cyber security etc.

C. General courses such as Entrepreneurship Education presently taught in the Universities should be enriched in such a way that graduates are equipped to start off their businesses and not to wait for the elusive white collar job.

D. Youths should be encouraged to learn vocations such as hair dressing, Tailoring, Fashion Designing, Baking, Make-Over, Manicure and Pedicure, carpentry, Welding and painting, etc

REFERENCES

Ashesh, R (2008) Cybercrime and Computer misuse: Cases in Mauritius

Brym, Robert J. (2007). New Society: Sociology for the 21st Century. Australia: Thompson + Nelson

Cornish, G. P. (1996). Copyright: interpreting the law for librarians, Achieves and information science, London library association publishing.

Datboyierry Post Lib Saga (2014). Cyber Squatters: How to be punished by Law in Nigeria

Dratter, J. (2000) "A theory of Secondary Liability for copyright Infringement.

Febunmi, B. A (2000) The Roles of librarian in Copyright Protection in Nigeria. Cataloging section Kenneth Dike Library,University of Ibadan, Ibadan Nigeria.

Giddens, A; Duneier, M. and Appelbaum. R (2000). Introduction to sociology. xth Ed. New York: Norton

Ginsburg, J. (2007). "The Right to claim Authorship in U.S. copyright and Trademark Law "University of Houston Law Review.

Gleason, P. (1986) An Articles titled: International copyright in publishing and development" A Book of Reading.

Hassan,A., Lass, F. and Makinde, J. (2012). Cybercrime in Nigeria: Causes Effects and the Way Out ARPN Journalof Science and Technology 2(C).

Ibikunle, F. and Eweniyi,O.(2013).Approach to Cyber Security Issues in Nigeria: Challenges and Solution. International Journal of Cognitive Research in Science, Engineering and Education, 1(1). Retrieved from http://ww.google.com

Odumubori, Funmilayo (2014) Latest trends in Cyber crime in Nigeria: Collective Responsibilities in combating it. A presentation made at the 2014 compliance conference. Abuja.

Pandey, Adesh Kumar (2010). Concept of E-commerce. New Delhi: S. K. Kataria

Pessach, G. (2006) "An International-Comparative perspective on peer to- peer file sharing and third Party liability in copyright Law; Framing the past, present, and Next Generations". Vanderbilt Journal of Transnational law.

Petterson, R. (1991). Copyright in Historical Perspective (Nashville: Vanderbilt University press. In Jefferson, p. (2000) No law: intellectual property in the image of an Absolute first Amendment (Stanford: CA: Stanford university press).

Rai, S. and Ghosh, R. (2006). Computer Awareness: Introduction to computers. New Delhi: K. K. Kataria

Rowley, (n.d).Information Security:Cyber Crime and How it affects You. Retrieve from http://dii.vermont.gov/Policy_Central on 12/11/2014.

Senate passes c-years jail term on cyber crimewww.iiilo nobs.com/iioiv/io/yahoo-boiz-nigeria. Senate passes-c-years jail term-bill-on-cyber-crime/efcc-arest-yahoo-boy-jpg-iiilo nobs/

St. Marie, Geoffrey (iioix). Recommendations to reduce crime rate

Winston, E. I. (iiooM) "why sell what you can license? Contracting around statutory protection of intellectual property" George mason Law review.

Withers, James. (iioix). Ways of reducing crime rate. E how html