INTERNET HACKING, SHIELDING CONVENTIONAL CRIMES STRATEGIC REASONING

Dr. Emeka, J. Owan*

Ayuk, A. Achu*

Ezikeudu, C. Charles*

ABSTRACT

It is ostensibly so devoid of doubt in as much as trade holds the pad-lock to today and future local, economic, global and social growth and development. Perhaps, in conceptualizing human invention, e-trade posses a reasonable percentage of agreeable problems that seemingly overwhelms its applicably. The major thrust of the paper is to investigate some of these challenges and consternation. This research is in exhaustive, it is rather a tool for extensive investigation.

Keywords: Crime, internet, Cramming, Hacking.

* Department of Sociology, University of Calabar, Calabar

INTRODUCTION

Internet crime which encompasses a wide range of issues of illegality to include: cyber pornography, piracy, copyright, trademark violation, identity, sales of illegal and stolen goods to mention but just a few, to say the least has for now been a source of worry to criminologists, sociologists, psychologists and government of Nigeria, especially where there are no adequate laws and templates to address these concerns.

More so, the loss of socio-economic development in the advancement of society because of internet theft is incalculable. Inadequate trained personnel further compound the problem in internet security in Nigeria and amongst Nigerians. This is so because, computer related education in Nigeria is not encourage and even when thought, is more theoretical with no security emphasis and practical underpinnings as regard crime control vis-a-vis hacking.

No doubt, the advent of computer and its associated merits is commendable in all ramification (economic, academic, security, medicine, agriculture, communication, transportation etc). Therefore, a major issue of challenge in good governance relates to how effectively and efficiently these positive attributes of computer can be harnessed to bring into being, legitimate methods of transactions to ensure sustainable development and ordered society with checked criminality.

INTERNET SCAM

The issue of crime has always remained the by-product of invention or innovation in the society. Internet fraud activities emanated with the evolution of the technological advancement in our society today. The agreeable characteristics of the internet is its breath, speed and ease of operation and exploration. Based on this potent merit is what cyber criminals have dwelled on to strip – off users of heavy amount of resources.

It is pertinent to attempt a definition of what internet scam or crime is as the core of this study. Adebiyi (2004),sees it as "unlawful act using the computer as either a tool or target for both". While the telecommunication and postal offences Decree of defined internet scam as:

"any person who inter alia engages in computer fraud or does anything relating to fake payments whether or not the payment is credited to the account of an operator or the account of the subscriber is guilty of an offence".

More so, internet hacking (cyber crime) has also been considered as computer medicated activities which are either illegal or regarded as illicit by certain parties and which can be conducted through global electronic networks. Furthermore, it represent act committed by use of the internet (a host communicating with another host) which is classified as a criminal offence according to national law, (Adebiyi, 2004).

Criminal act on the internet range from fraud, pervasive pornography, pedophile rings, drug trafficking to cyber extortion, etc. The security and effect of cyber hacking on business society and government is unquantifiable. Annually, over $1.9 trillion is lost to internet criminals (Williams, 2009). Internet hacking is attracting the authorities for many reasons:

1. Electronic commerce, though with myriad of problems.
2. Money can be transferred through the internet, via online electronic payments, such as credit or cash cards, electronic money etc.
3. Fraud committed via the internet poses complicated enforcement and jurisdictional problems to investigative agencies and the judiciary.
4. Lastly, there is no internationally accepted method of verifying the integrity and accuracy of the information that flows through the web.

REASONS FOR COMPUTER HACKING

- Send spam.
- Launch a Dos – attack
- Create an unauthorized net
- Phishing attack
- Distribute illegal materials
- Obtain anonymity in order to:

Break into another computer (fame and pride/steal information/erase data/cause malfunctions etc).

- Obtain storage space for pirated goods.
- Cause malfunction on the system.
- Steal information
- Hack for pride and fame.

SPECIFIC ELEMENTS AND STAGES THAT ESTABLISH A PERPETRATOR OR AN ACCUSED

Just as the element of traditional crime must be fully present for an accused to be indicted, so also does cyber hacking has some specific elements and stages which the persecutor must establish to convict and accused. These stages include:

a) **Planning:** at this stage, the criminal carefully observes the pattern and trends of the target. This would include his data entry style, programme listing, systems documentation etc.

b) **Execution:** Most computer crimes are executed remotely, thereby eliminating the need for physical presence. Criminals execute their act by modifying application programmes or operating system, accessing control programmes etc.

c) **Concealment:** The criminal having executed his act, deliberately conceals it from being discovered. Cyber crime can be concealed by representing the act as an error or omission, performing the illegal act in conjunction with an authorized activity.

d) **Conversion:** The criminals has to convert the criminal object into tangible object of use to him. Conversion can take place in different means, sale of data without authority, destruction of data in cases of revenge, or in most cases for the financial gains.

CATEGORIES OF ELECTRONIC TRADE FRAUDS

- **Consumer – type fraud:** This is perpetuated through internet auction frauds, health care products sales and tourism services.
- **Investment – type fraud:** This is actualized through online payment and manipulation of data fraud and the usage of net fraud. It is achieved through manipulation of internet access services, international modern dialing and web cramming.

VARIETIES OF ELECTRONIC FRAUDS

- **Cyber Pornography:** This includes pornographic websites (including transmission of images of children; pornographic magazines using computers and the internet, dissemination of pornography).for example The American case of state of New York v. Buffnet and ISP pleaded guilty to the misdemeanor charge of knowingly providing access to child pornography. Investigation revealed that the ISP hosted a pornography newsgroup called “Pedo University”. The police warned the defendant but it refused to comply. After which it servers were leased and

it was made to remove the pictures and pay fine. The convention on the rights of a child guarantees the right of protection of children against pornography and obscenities.

- **Internet Matrimony:** Marriage and relationship are largely built on communication between two willing adults. The internet offers an unprecedented communication platform for such issues. The story was told of one Anastasia solovienva of former Soviet Union who was matched with an elderly man (Indle King Jr), who had been a former tug earlier convicted of violence upon his earlier internet gotten wife. Two years after the marriage, Anastasia was found dead, strangled and buried in a junkyard by her husband. Internet matrimony is gradually filtering into Nigeria with the recent report of an American woman who met her bricklayer husband in the chat room. Time will tell how well such marriages would work.
- **Identity Theft:** The criminal either steals the victim's information or card and goes ahead to pose to a seller that he is the owner for payment purpose. The Advance Fee Fraud and other fraud Related Offences Decree were enacted to ease the proof of this crime. Furthermore, the Economic and Financial Crimes Commission of Nigeria is now saddled with the responsibility of enforcing Decree No.13 1999.
- **Sale of Illegal or Stolen Goods:** The internet offers a gateway for the sale of goods through auction mail order or directly to the buyer. These goods include but not limited to hard drugs e.g cocaine, body parts (kidneys); by-product of endangered species, ammunitions, stolen goods etc. Section 472 of Nigeria Criminal Code criminalizes reception of stolen goods.
- **Piracy, Copyright Infringement, Trademark Violations:** The case of playboy enterprise in Co. v Frena operator of a bulletin board allowed its subscribers to upload and download digitized pictures copyrighted by "playboy" magazine. He was held liable for infringement notwithstanding that he claimed ignorance and promptly removed the pictures on knowing. A person could commit so many other intellectual property crimes. This includes software piracy, trademarks violations, theft of computer sources code etc. In Nigeria, the only regulation that can be construed to punish infringers is the Copyright Act or case laws.
- **E-mail Spoofing:** This is when an e-mail appears to originate from a source but which actually did not.
- **Cyber Defamation:** This was defined by Section 142 of Sharia Penal Code of Zamfara State, Nigeria as spoken or reproduced words by mechanical means intending to harm or knowing or having reason to believe that such imputation will harm the reputation of a person.

- **Cyber Stalking:** Here, stalking has been defined as the crime of following someone over a period of time in order to force them to have sex or kill them. Although no conventional definition has been proffered, yet cyber stalking has been defined as the use of the internet, e-mail or other electronic methods to stalk or harass a person.
- **Hacking:** Hacking is obviously an act of securing unauthorized access to a computer or computer network. Hackers are divided into two types viz: white-hat hackers and black-hat hackers. White-hat hackers are legally employed or independent contractors who hack to check the security of a system. Black-hat hacking is illegal, because such hacked do their activities to cause damage or steal information from the computer or network of a victim. Apart from the above classification, hackers have also been classified thus;
- **Code Hackers:** They can succeed in making the computer do nearly anything they want.
- **Crackers:** They take pleasure in circumventing operating systems and its security apparatus.
- **Cyber Punks:** They have perfected the act of cryptography.
- **Phreakers:** They use the internet to commit havoc on the telecommunication system e.g T.V. telephone etc.

HACKING

Hacking therefore involves penetrating computer system, which of course requires security procedures to be circumvented. The hackers have found a wide range of ways to achieve this. In most cases, these attacks are done for the challenge and challenge alone. The majority of hackers are not motivated by any sense of criminal imperatives, but only by a deep curiosity and a fascination with what they see in the ultimate computer 'game'.

Packet sniffing, tempest attacks, password cracking, buffer cover flow, E-mail interception, Trojans etc are means through which hackers perform their nefarious activities. Most developing countries have no sophisticated laws on which to successfully prosecute criminal hackers.

- **Internet Time Theft:** This is the unauthorized use of the internet time paid for another person.

- **Cyber Squatting:** This is the act of reserving a domain name on the internet, thereby denying true users of the name from using it. The cyber squatting use this in order to sell such names for "cut-throat prices".
- **E-mail Bombing:** The cyber criminal registers the victim's e-mail with so many mail service organizations thereby making the person receive hundreds of unwanted e-mails everyday from different quarters. This can make the Internet Service Provider to delete the victim from its service.
- **Denial of Service Attacks:** This usually involves a malicious flooding of commercial websites, causing them to crash and preventing genuine customers from patronizing the site. There is another variant called Distributed Denial of service attack. This is a concerted effort of different parts of the world towards one system or network. It is a little difficult to prosecute this crime. However, the European Convention on cyber crime has provided a leeway in its Acts.
- **Worm Attack:** G 'worm' is a self-replicating programme, which eats up space capacity within computers. Worms are found in network where they infect all the computers connected to the main server.
- **Virus Attack:** A computer virus as the name implies is analogous with medical viruses. A virus in cyber crime parlance is the computer 'machine code' that copies its code into a host programme when the programme is run. Viruses also duplicate themselves depending on the makeup. Viruses are contacted through the use electronic storage devices, down-loaded data from the internet or through file transfer on a selected network.
- **Trojan Horses:** Trojan horses do not usually replicate themselves; instead, they hide their true intent behind something benign. They can present themselves as games, programmes and screensavers. Trojan horses are designed primarily to give hackers remote control of the victims computer.
- **Logic Bombs:** These are malicious programmes that are primed to start operating at some point in the future; the trigger can be a specific data or event. A sacked network administrator in the US was changed after the planned a logic bomb in the system of the company. This cost the firm an estimate $10 million in damage.

CYBERCRIME CONVENTION: CRIMINAL LAW

- Illegal access (computer lutrusion).
- Illegal interception
- Data interference
- Misuse of devices (exploit and passions)
- Computer related forgery
- Computer related fraud.
- Offences related to child pornography
- Attempt/aiding/abetting and corporate liability.

POSSIBLE WAYS OF COMBATING CYBER HACKING(CRIMES): GOVERNMENT'S ROLE

Government world over has a major catalytic role to combat or curb cyber crime. Most developing nations today has no legislation to combat electronics commence frauds and cyber crimes. The starting point of any formidable fight against cyber crime is proper legislation. Government has to enact laws governing the carrying on of electronic commerce. The law should outline the major duties of each party and the liabilities faced by each party in case of negligence and/or breach of trust. For instance, in the US, though the laws governing electronic commerce are still emerging, there are responsibilities and liabilities placed on the credit card companies, the users and the banks respectively.

REGULATORY AUTHORITIES ROLE

The apex and central monetary regulatory institutions in its regulatory role shuold issue regulations on electronic banking. For instance, the Economic and Financial Crime Commission and other anti-graft bodies in Nigeria have issued regulations on electronic commerce and more particularly on electronic banking. The Deposits Insurance Companies all over the world needs to ensure a form of insurance of depositors. Central Bank of Nigeria could also promulgate standards for the practice of electronic banking. There should be a data repository of electronic fraudsters like ordinary fraudsters to helped foil credit card fraud in Nigeria.

TARGET'S ROLE

Banks and other targets of cyber crime can ameliorate the impact of conducting risk assessment, implementation of controls, policy formulation, customer screening, employee screening, due diligence, ethical and professional practice.

INTERNET FRAUD STATISTICS (HACKING) 2010

Total Loss

Overall: $9,209,196

Average loss $654

January – June Tope 10 Frauds

- Online Auctions 89%
- General merchandise 4%
- Nigerian money 8%
- Offers computer 2%
- Equipment/software work – at – home 5%
- Plan internet – 4%
- Service information/Ad – 2%
- It services travel/vacations – 05%
- Advance fee loans – 05%
- Prizes/sweepstakes 04%

Source: Wikipedia (2010)

PAYMENT METHODS OVERALL

- Money order – 29%
- Credit card – 33%
- Debit card – 15%
- Bank debit - 7%
- Cashier check – 3%
- Cash – 4%
- Other – 2%

Source: Wikipedia (2010)

RECOMMENDATIONS

Countries should provide their competent authorities involved in combating electronic fraud with adequate financial, human and technical resources. Countries should have in place processes to ensure that designated law enforcement authorities have responsibility for cyber crime investigations.

CONCLUSION

Cyber hacking (crime) is a major threat to the growth of internet based commerce and globalization. With over $2.6 billion lost to cyber crime every year, the least our nations can do is to proactively enact laws on internet transaction, regulation on this menace(cyber crime etc). Fellow nations have done this and much more. This has taken the lead today by shielding all other types of crime that was hitherto perpetuated. The world over cannot afford to sleep through the revolution especially in view of the active participation of all nation in internet base operations.

REFERENCES

The Laws Of The Federation Nigeria;Criminal Code Chapter 42.

Olufemi, D (2009). Cybercrimes, obsoleting the guns, bombs and knives.

Adebiyi,T (2004). Internet crime, capital market law. economic development journal.

Williams, P. (2004). Organized crime and cyber-crime: Implication for Business.

Internet Fraud – Wikipedia, the free encyclopedia.

en.wikipedia.org/wiki/internet_fraud.

en.wikipedia.org/wiki/category: Internet fraud.

www.fbi.gov/../internet-fraud.

Myjoyonline.com.

Home.rmci.net/alphae/419loal

www.sec.gov/../cyberfraud.htm

www.jidaw.com/.../security5.html

www.justiuce.gov/.../internet/

www.crimes-of-persuasion.com/crimes...

www..nigeriafraud.org/.

www.fraud.org/internet/intinfo.htm

news.bbc.co.uk/2/hi/Africa/3241710.stm

www.usa.govt/.../internet_fraud.shtml

www.scamdex.com/

www.scamwatch.gov.au/repotascam

www.rcmp-grc.gc,ca/.../index-eng.htm

www.odos.uiuc.edu/.../internet-fraud.pdf

simple.wikipedia.org/…/internet-fraud

www.fbi.gov/scams-safety/fraud.

www..Ic3,gov/crimeschemes.aspx.

www.nairaland.com/nigeria/topic -160.

www.financialnigeria.com/development.

Ifraudalert.org/

www.nrps.com/community/ifraud.asp.

www.usenbassey.gov/acs_abuja_scg

www.met.police.uk/fraudalert.

www.gistexpress,com/tag/internet-fraud.

www.adviceguide.org.uk/index/fraud.

Naijaupdate.com/fraud.

www.ccomstwanted.com/.../scam.htm