E-Crime in Nigeria: Trends, Tricks, and Treatment.

Victor F. Balogun, M.Sc.[1] and Olumide O. Obe, M.Sc.[2]

[1]Department of Computer Science, University of Manitoba, Canada.
[2]Department of Computer Science, University Polytecnica of Bucharest, Romania.

E-mail: victobal@cs.umanitoba.ca[1]
voluobes@gmail.com[2]

ABSTRACT

The unprecedented spate of e-crime in Nigeria in recent times is quite alarming, and the negative impact on the socio-economy of the country is highly debilitating and of great concern. Numerous governmental and private initiatives have been deployed in order to curb and combat this menace. Recent reports revealed that there has not been significant reduction in this despicable art despite the various measures employed so far. Nigerian computer criminals are daily devising new ways of perpetrating this illegal trade and the existing methods of tracking these criminals are no longer suitable for to deal with their new tricks. The victims as well show increasing naivety and gullibility at the prospects incited by these fraudsters. This paper examines the trends, peculiarities, and reasons for the upsurge in e-crime in Nigeria. It further highlights these emerging tricks, possible infrastructures to be deployed for its treatment, and the implications of using such mechanisms.

(Keywords: e-crime, cyberspace, telephony crime, hacking, e-commerce, e-mail scams, internet fraud)

INTRODUCTION

Society is increasingly relying on new information technologies and the Internet to conduct business, manage industrial activities, and engage in personal communications. While these technologies allow for enormous gains in efficiency, productivity, and communications, they also create a vulnerability to those who wish to take advantage of new situations (Vatis, 1998).

The exponential growth of the Internet and its global acceptance is generating increasing security threats. The Internet creates unlimited opportunities for commercial, social, and educational activities as well as blossoming haven for societal miscreants to perpetrate their insidious acts.

E-crime is to Internet what noise is to signal propagation on bounded media; the more the signal boosts, the greater the boost in the noise. The trend is increasing astronomically each day and none can predict the next dimension. The effects usually require Herculean efforts to trace.

It attracts attention globally because its impacts are ubiquitous. Most popular today are the internet fraud schemes such as those perpetrated through e-mail, telephone, chat rooms, message boards, or web-sites. The critical elements involved are fraudulent solicitations and transactions, as well as the presence of unwitting victim. The chief of the FBI's financial crime section testified that in more than 80% of the FBI's Computer Crime Investigations, the Internet has been used to gain illegal access to systems (Brey, 2001). The speed and accessibility of the Internet are added advantages for the fraudsters and allow them to make their money quickly.

It is increasingly clear that e-crime is a growing and costly form of criminal enterprise. An anonymous survey by the FBI recorded instances of electronic thefts of up to US $500 million (Tedeschi, 2003). Systematic and proactive steps have to be taken in order to curb this menace before it totally ravages and crumbles the economy globally.

E-CRIME DEFINED

E-crime or electronic crime is any crime accomplished through the knowledge or use of

electronic devices like computers, phones, and other handheld devices. Brenner and Susan (2001) further explained that Cyber Crime, or e-crime, consists of specific crimes dealing with computers and networks and the facilitation of traditional crime through the use of computers.

While, nobody knows the true extent of electronic crime, the frequency of this type of crime is estimated to be 40 times greater when compared with classical crime. This criminal act spreads with great agility and through a variety of forms because it uses a technology with enormous possibilities and applications.

Many e-crimes, about 80% remain practically undiscovered. Those that are detected often go unreported, because businesses fear that they can lose more from negative publicity than from the actual crimes. By conservative estimates, businesses and government institutions lose billions of dollars every year to computer criminals. According to the FBI, the average computer crime is worth about 600,000 dollars – far more than most other crimes. A single case of computer fraud cost the Volkswagen Company in Germany more than 260 million dollars in 1984. Pirated CDs of computer software are peddled daily in the popular market called Computer Village in Ikeja, Lagos, Nigeria. Much has been done by the law enforcement agents and even Microsoft has gotten a presence in the market. But this illegal act is still perpetrated underground.

FORMS OF E-CRIME

E-crime comes in different forms and the perpetrators are constantly devising new ways of conducting their nefarious acts. The forms considered below are not meant to be exhaustive but they are meant to portray some of the different taxonomies of e-crime.

Hacking

This is a general term for e-crimes like illegal access, defacing, hijacking, bombing, denial of service attack, diddling, super zapping, eavesdropping, etc. Some Internet users think that hacking is harmless fun and even quite clever, but it can be a serious invasion of privacy and a significant threat to e-commerce. The Information Security Advisory Group estimates that world-wide, there are now some 100,000 hackers or crackers. White-hat hackers test computer security at the request of organization, black-hat hackers' act privately to break into systems, and grey-hat hackers straddle both worlds. In 1990 hackers broke into and defaced several web-sites, including the U.S. Department of Justice, U.S. Air Force, CIA, NASA, and others (Sandeep, 2004). In 1991, when a security breach occurred at the research facility of a major U.S. automobile manufacturer, the company lost $500 million worth of designs for future cars and suffered in the marketplace because its design fell into the hands of competitors. A report by the General Accounting Office finds Defense Department computers sustained 250,000 attacks by hackers in 1995. In 2000, even Microsoft fell prey to hackers (Handbook of Cyber Law, 2000).

Pirating

Digital technology makes it very easy to perfectly copy creative products such as music or films and the Internet provides a free and almost anonymous means of transmitting or exchanging these pirated materials around the world. According to research from the Business Software Alliance (BSA), an international organization that represents leading software and e-commerce developers (www.bsa.org), global software piracy is an $11.8 billion problem that's only getting bigger (Privacy journal, 1996).

Cyber Stalking

There is no universally accepted definition of 'cyber stalking' yet. It is generally considered as the use of the Internet, e-mail, or other electronic communications device to stalk or harass a person. Stalking is defined as repeated harassing or threatening behavior. Cyber stalking is a form of harassment that makes use of modern technology like cell phones, fax machines, and other devices to pursue their victims. Cyber stalking is now considered a crime in many places and as a crime its definition has varied with the locale or country. A single push of a button and a cyber-stalker is able to send repeated, threatening, or harassing messages at regular or random intervals, even if he is not physically present at the computer. Due to the anonymity of the Internet, a perpetrator's identity can be completely

concealed. In addition, cyber-stalking has led to offline incidents of violent crime. For example, a South Carolina woman has been stalked for several years via e-mail by unknown person who has threatened her life, threatened to rape her daughter, and posted her home address on e-mail making it openly available to anyone with access to the Internet (Toronto Star, 1995). It has been estimated that approximately 20,000 people stalk someone each year (Economics Times, 2004). Seven states have passed statutes that include stalking by computer (Times of India, 2004).

Illegal Trading

This is the use of Internet facilities like chat rooms, bulletin boards, newsgroups, and web-sites to transact trades that are classified as illegal (e.g. fake drugs, human trafficking, etc.).

Cyber Squatting

The term which was derived from 'squatting' which refers to the act of reserving a particular Internet domain name for the purpose of selling it at a higher price later. Though a domain name serves a purely technological function of locating website in cyberspace, the desire for prestigious business addresses in cyberspace has created a rush to register business names of an entity. Common examples of cyber squatting include the reservation of sites that include the names of celebrities or companies. This guarantees the cyber squatters a profit whenever a celebrity or company decides to set up an official web-site and needs that domain name. Panasonic and Hertz are some well-known victims of cyber squatters.

Fraud

This involves activities like packet reading, obtaining confidential information, auction fraud, investment fraud, escrow services fraud, etc. It is very common on the Internet for fraudsters to trick users of certain sites (e.g. banks, building societies, etc.) into disclosing their passwords or other confidential information needed to access their accounts. It is usually done by sending e-mail to customers advising them to check or confirm their password by clicking onto a realistic but fake website and then supplying their confidential details. This information can then be use to fraudulently transfer money from the individual's account.

Money Laundering

This is the illegal transfer of public funds into private accounts via the Internet. Italian policymakers believe that the Sicilian Mafia is laundering vast sums of money in cyberspace by its use of on-line trading and banking. Money laundering is a very common type of e-crime in Nigeria.

Theft of Communication Services

This is fraudulently obtaining employee's access code, or using the available software on the Internet to gain access into an organization's telephone switch board. The possibility arises however, that offenders may target victims in other countries at times when it is impossible for personal telephone verification checks to be undertaken. Funds could be for instance electronically debited from accounts at night when a company is closed and when transaction could not be immediately identified. A similar problem arose with the early types of ATMs which permitted accounts to be overdrawn during night time hours when the machine was "off-host" (Chapman & Smith, 2001).

Phishing

Phishing is an act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in order to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web-site where they are asked to update personal information such as password and credit card, social security, and bank account. According to a study by Gartner, 57 million Internet users in the US have received letters through e-mail, which have been identified to be Phishing attacks (PC Quest, 1999).

PERPETRATORS OF E-CRIME

Today the computer has replaced both the gun and the pen as the weapon of choice for many criminals. Contrary to what the movies suggest, perpetrators of e-crime are though prevalent in the developing nations of the world, Nigeria inclusive, cut across every race and gender. E-

criminals include students, amateurs, terrorists, and company insiders – clerks, cashiers, programmers, computer operators, and managers – who have no extraordinary technical ingenuity.

Some are trusted employees with no criminal records who are tempted by an opportunity, such as the discovery of a loophole in system security, tempted by greed, financial worries, or personal problems. While others are ex-employees seeking revenge on their former bosses, corporate or international spies seeking classified information, or high-tech pranksters looking for a challenge. Organized crime syndicates are even turning to computer technology to practice their trades.

Sometimes entire companies are found guilty of computer fraud. For instance, a particular company in Nigeria through her various nefarious program and services like Quiz Shows on a National TV station, promised thousands of naira to winners of the displayed questions. Deductions of N100 were made per attempt from several thousands of callers whereas only one call would be allowed to sail through. Another instance can be seen in the case of Equity Funding, Inc., which used computers to generate thousands of false insurance policies that were later sold for over $27 million.

REVIEW OF E-CRIMES THAT ARE PECULIAR TO NIGERIA

There is no doubt that e-crime is an image nightmare for Nigeria. The recent decision with former Nigerian President, Olusegun Obasanjo on setting up a working group, the Nigeria Cyber Crime Working Group (NCWG), is an indication that cyber crime is a source of concern and embarrassment for the nation. The Internet creates unlimited opportunities for commercial, social, and educational activities. But as we can see with cyber crime the Internet also introduces its own peculiar risks.

Instances of Cyber Crime

The instances reported here ranges from fake lotteries to the biggest internet scams. Elekwe, a chubby-faced 28-year-old man made a fortune through the scam after two years of joblessness despite having diploma in computer science. He was lured to Lagos from Umuahia by the chief of a fraud gang in a business centre. He has three sleek cars and two houses from his exploits. In July 2001, four Nigerians suspected to be operating a “419” scam on the internet to dupe unsuspecting foreign investors in Ghana were arrested by security agencies. Their activities are believed to have led to the loss of several millions of foreign currencies by prospective investors. Two young men were recently arrested after making an online purchase of two laptops advertised by a woman on her website under false claims. They were arrested at the point of delivery by government officials.

Mike Amadi was sentenced to 16 years imprisonment for setting up a website that offered juicy but phony procurement contracts. The man impersonated the EFCC Chairman, but he was caught by an undercover agent posing as an Italian businessman. The biggest international scam of all was committed by Amaka Anajemba who was sentenced to 2½ years in prison. She was equally ordered to return $25.5 million of the $242 million she helped to steal from a Brazilian bank.

On recent internet scam case was reported on the Sunday PUNCH newspaper of July 16, 2006 involving a 24-year-old Yekini Labaika of Osun State origin in Nigeria and a 42-years-old nurse of American origin, by name Thumbelina Hinshaw, in search of a Muslim lover to marry. The young man deceived the victim by claiming to be an American Muslim by the name, Phillip Williams, working with an oil company in Nigeria and he promised to marry her. He devised dubious means to swindle $16,200 and lots of valuable materials from the victim. The scammer later was sentenced to a total of 19½ years having been found guilty of eight-counts against him. Incidences like these are on the increase. Several young men unabated are still carrying out these illegal acts successfully, ripping off credulous individuals and organizations.

Instances of Telephony Crime

The rate of e-crime on the side of telephony is increasing at an alarming rate in Nigeria. The advent of Global System for Mobile Telecommunication (GSM) in Nigeria has brought with it its own scams. Many victims have been duped through “send me credit” practice in the country. There was a case of a

woman in Ibadan who was asked to pay a sum of five thousand naira to a swindler in order to clear goods sent by her son from South Korea. The swindler impersonated the woman's son on the phone. The swindler asked that the money should be sent in the form of a recharge card for his phone. This was done without notice until it dawned on her that she has been duped. A similar thing happened to the head of Department of Computer Science of the Federal University of Technology in Nigeria. However, luck ran against the swindler when the head of the department asked for the account number of the swindler to pay the amount to in Osogbo in Osun State of Nigeria. The case was reported to the police and the swindler was traced through the supplied account number.

In 2004, the Inspector General of the Nigerian Police, Mr. Tafa Balogun, was tricked by fraudsters to the tune of millions of Naira equivalent of MTN recharge cards. The perpetrators called the Inspector General on his mobile phone and pretended to be Rtd. General Ibrahim Babangida, hence requesting recharge cards bi-weekly for a period of close to six weeks. It was the General's aides who eventually cautioned him that the General would not personally be requesting recharge cards in this absurd manner. The fraudsters were eventually located and arrested.

In another case, there was an instance of a professor at the Lagos State University, who was sent a message that he has won ₦1 million in an ongoing MTN promotion. In the message, a phone number of fake staff of MTN was given to be contacted. On calling the said number, the staff congratulated the professor for being one of the lucky winners. He now asked the winner to text his contact address in which the check of ₦1 million would be sent to 33354, in which an automated system responded by requesting for recharge cards worth ₦6,000 to cover the cost of the courier that will deliver the check. He parted with the sum and the check was never delivered. So many other instances had gone unreported.

E-Crime Statistics in Nigeria

It seems impossible to tell how much has been lost due to e-crime in Nigeria because a lot of this crime go unreported, however, we present here some of the global and local documentations recorded on e-crime in Nigeria. The latest statistics released in March, 2007 by Ultrascan Advanced Global Investigations, a Dutch private investigation firm that has been studying advanced fee fraud (419) scams worldwide for a decade, showed that companies and individuals in the United States were defrauded of about $720 million last year alone. The United Kingdom has the second highest losses at $520 million, while Spain and Japan were tied for third with about $320 million in losses. The report further stated that in March last year, Luiz Gottschalk, the respected founding chairman of the Psychiatry Department at the University of California at Irvine, USA, fell victim to the trick and lost $3 million to some people purported to be in Nigeria.

Recently, a report indicated that Nigeria is losing about $80 million yearly to software piracy. The report was the finding of a study conducted by Institute of Digital Communication, a market research and forecasting firm, based in South Africa, on behalf of Business Software Alliance of South Africa. The American National Fraud Information Centre reported Nigerian money offers as the fastest growing online scam, up to 900% in 2001. The Centre also ranked Nigerian cyber crime impact per capita as being exceptionally high.

Impact of E-crime in Nigeria

Tunji Ogunleye, an ICT security consultant and a member of Nigeria Cyber Crime Working Group (NCWG) disclosed that the rate of e-crime in Nigeria has outgrown the rate of Internet usage in the country. He said Nigeria is the 56th out of 60 countries in embracing Internet usage but third in the fraud attempt category. The impact of e-crime on Nigerian citizenry is already detrimental. Global corruption bodies, such as Transparency International has listed Nigeria as one of the most corrupt countries in the world. It is no gainsaying that Nigerian cyber crime has the potential to impact technological growth which is a key requirement for productivity improvement, and ultimately socio-economic growth because: International financial institutions now view paper-based Nigerian financial instruments with skepticism. Nigerian bank drafts and checks are not viable international financial instruments.

Nigerian ISPs and e-mail providers are already being black-listed in e-mail blocking blacklists systems across the internet. Some companies are blocking entire Internet network segments and traffic that originate from Nigeria. Newer and more sophisticated technologies are emerging that will make it easier to discriminate and isolate Nigerian e-mail traffic.
Key national infrastructure and information security assets are likely to be damaged by hostile and fraudulent unauthorized use.

No one knows to what extent the Internet crime activities will damage the Nigerian Economy. It is becoming foreseeable that it is beginning to have drastic economic and financial impact. International Banks often delay Nigerian Financial transactions, pending proper verification and foreign investors often consider Nigeria as an unattractive market.

Reasons for the State of E-Crime in Nigeria

We are tempted to ask why there is such an upsurge of e-crime in Nigeria and what are the factors that made Nigerians so vulnerable to e-crime? Considering the present economic recession and political upheavals in the country, the reasons are not far-fetched and they include the following:

Unemployment: The spate of unemployment in Nigeria is alarming and growing by the day. Companies are folding up and financial institutions are going bankrupt. The federal government has proposed a mass sack of government workers to the tune of 33,000. Companies are also embarking on mass sacks of staff. Financial institutions have put unreasonable age barriers on who is eligible to apply for jobs and embarked on mass lay-offs of staff based on ad-hoc decisions.

Poverty Rate: On the global scale, Nigeria is regarded as a third world country. The poverty rate is ever increasing. The rich are getting richer and the poor are getting poorer. Insufficient basic amenities and an epileptic power supply have grounded small scale industries.

Corruption: Nigeria was ranked third among the most corrupt countries in the world. Until 1999, corruption was seen as a way of life in Nigeria.

Gullibility/Greed of the victims: Most victims of e-crime express some degree of gullibility and/or greed. They typically do not carry out any thorough investigation before venturing into transactions. Because of greed, the victims never share with others the seemingly fortune changing transaction they have just discovered until they fall into the trap.

Lack of Standards and National Central Control: Charles Emeruwa, a consultant to Nigeria Cyber Crime Working Group (NCCWG), said lack of regulations, standards and computer security and protection act are hampering true e-business. Foreign Direct Investment (FDI) and foreign outsourcing are encouraging computer misuse and abuse.

Lack of Infrastructure: Proper monitoring and arrest calls for sophisticated state of the art Information and Communication Technology devices.

Lack of National Functional Databases: National database could serve as a means of tracking down the perpetrators of these heinous acts by checking into past individual records and tracing their movements.

Proliferation of Cybercafés: As a means of making ends meet, many entrepreneurs have taken to establishment of cybercafés that serve as blissful havens for the syndicates to practice their acts through night browsing service they provide to prospective customers without being guided or monitored.

Porous Nature of the Internet: The Internet is free for all with no central control. Hence, the state of anarchy presently experienced.

Get-Rich Syndrome: In Nigeria today, almost everybody, especially the youth, wants to get rich with little or no effort at all. This get rich quick mentality has fueled the current trends in e-crime.

DIFFERENT WAYS E-CRIME HAS BEEN ADDRESSED

In London on the 14th of October, 2005, the government of Nigeria and the Microsoft Corporation signed a Memorandum of Understanding defining a framework for co-operation between Microsoft and the Economic

and Financial Crimes Commission (EFCC) of Nigeria to fight cyber crime. This agreement is the first of its kind between Microsoft and an African government and this will help to support the Nigerian government's effort to create a safe legal environment for technology development and enforce laws that will help to attract investment and ensure sustainable economical development.

This open and collaborative approach to working with the Nigerian government to combat issues such as spam, financial scam, phishing, spyware, viruses, worms, malicious code launches and counterfeiting is a key example of how public-private partnership efforts have been made.

The Nigerian government has launched and is enforcing the Nigerian Cyber Crime laws aimed at ensuring the security of computer systems and networks and the protection of critical ICT infrastructure in Nigeria through the Nigerian Cyber crime Working Group (NCWG). This group is made up of all key law enforcement (the Nigerian Police, National Security Adviser, Department of State Services), security/intelligence (EFCC, National Intelligent Agency), ICT agencies of government (Nigerian Communication Commission), plus major private organizations in the ICT sector (like Internet Service Provider's Association of Nigeria, NITDA).

The working group engages in a public education program, building institutional consensus amongst existing agencies, providing technical assistance to the National Assembly on cyber crime and in the drafting of the Cyber Crime Act; laying the groundwork for a cyber crime agency that will eventually emerge to take charge of fighting cyber crime in Nigeria, and collaborating with global cyber crime enforcement agencies at fore-front of fighting cyber crime.

In the 2005 Computer Crime and Security Survey conducted by the CSI and FBI, participants from different African countries resolved to establish African Information Security Association (AISA) at the end of the conference with a view to promoting knowledge and creating awareness about computer security and cyber crime on the continent. It was resolved in a communiqué that AISA would serve to promote global best practices in information, computer and internet security, campaign against cyber crime, conduct annual survey on information security, promote legislation and regulations and create linkages and networks in Africa.

EMERGING E-CRIME METHODS AND TRICKS

New forms of Nigerian e-mail scams include the following:

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.

Fake Web Sites: The scammer opens a fake online bank and directs the victim to the site which shows a multi-million dollar deposit when the victim expresses doubts. Common in Nigeria are the cases of University admission and visa scams where unsuspecting persons apply for University admission through a fake web site and even make payments online. Thousands of people have been defrauded over the Internet through these means.

American Soldier in Afghanistan or Iraq: The scammer requests personal and financial information of the victim in order to deposit funds from the treasure of terrorist currency he claimed to have discovered.

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

by an interested buyer from Nigeria or another African country. The scammer then sends the victim a check or money order for an amount much larger than the asking price of the item. The victim is then asked to deposit the difference back to the scammer. If the victim does not wait for the bank to verify the check, he can end up losing thousands of dollars.

Lotteries: Some corporate organizations in Nigeria garner millions of viewers to send text messages or to call in answers to a displayed question on TV. The amount charged for such calls or text message (SMS) from the viewers amounts to millions of Naira while the amount to be won might just be 10,000 Naira.

Donation Solicitations: The victim receives an e-mail requesting "donations" to fight an evil government or dictatorship in Africa. The scammer requests that the victim provide bank account information so that the "donation" can be directly withdrawn from the bank.

Reshipping: Many Nigerians have come up with ingenious schemes to dupe Americans into willingly cooperating with rip-offs. Those schemes are known as "reshipping" and often start at a single chat web site. In a chat room, a scammer establishes a relationship with a potential victim. He then persuades the victim to agree to receive merchandise that he buys online, and then reship it to Nigeria. Once she agrees, the criminal uses stolen credit card information to buy goods online and have them shipped to America. The victim rewraps the merchandise and ships it to an address in Nigeria (Mickinley, 2005).

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.

Impersonating Relatives/Acquaintances in Distant Locations: Victims receive phone calls from someone who claim to be a relative in a distant location like the United State of America either requesting help, or the cost of shipping consignments to them.

Phreaking: This type of crime involves the theft of telecommunication services, instances of which have involved using cereal box toy whistles to imitate telephone call signals, and more recently cloning mobile sim cards. Many homes in Nigeria are now connected to DSTV products through a self made cord, which when attached to a video player, has the capability of connecting to several stations in DSTV television.

INTRICACIES OF THESE EMERGING TRICKS

Although greater expertise in e-crime is an important goal for law enforcement agencies to achieve, there are a number of factors that make the detection and investigation of some forms of e-crime extremely difficult. In effect, although many computer based crimes are merely conventional criminal acts that have involved a computer, there are some that have no conventional similarity (Thompson, 1989). Criminal acts of this kind denote a number of complicating features that computer systems and information technology bring to the area of criminal investigation. These include:

• The speed and power of modern information technology complicates the detection and investigation of computer crimes. For example, communications networks now span the globe and a small personal computer can easily connect to sites that are located in different hemispheres or continents. This raises very significant problems in terms of jurisdiction, availability of evidence, co-ordination of the investigation and the legal framework(s) that can be applied to criminal acts that occur in this context.

• New technologies create new concepts that have no legal equivalence or standing. For example, computer viruses may or may not cause damage to infected systems - some are quite benign (although many benign viruses still cause unintentional damage). Nevertheless, a virus utilizes the resources of the infected system without the owner's permission. Hence, even a benign virus may be variously interpreted as a system penetration, a piece of electronic graffiti or simply a nuisance prank. The major point however, is that the legal system and therefore the definition of computer crime itself is reactive and unable to encompass behaviors or acts that involve new computational concepts.

• Information has several unique and abstract properties - for example its capacity to still be in

the owner's possession after it has been copied or stolen. The last decade has seen the legal system struggle with the implications of this in a computer based context. Clearly, conventional notions of copyright, patent rights, and theft have been strained when applied to software and computer based information, basically because existing concepts of theft and break-in for example, relate to common notions of permanent deprivation or removal (theft) or physical damage (break-ins). Neither of these concepts bears much relationship to computer break-ins or the theft of information held on such systems. Hence, the legal system is currently coming to terms with these new concepts and their relationship to the existing criminal law system.

• A related property of digital information is the ease and extent to which it can be transformed and translated. That is, a piece of information (i.e., a program) can be represented in a huge variety of informational forms. It can be represented as program text (source code), executable code (binaries), or it can be transformed in a large number of ways - mathematically, by encryption, or by conversion to say a holographic image or a piece of music. As long as the method(s) of transformation are known, the music, image, or encrypted text can be translated back to its original form. Therefore, the informational form in which information exists may eventually have no legal status. Instead, some measure of its value or functionality as information itself may eventually determine its legal and commercial position.

This malleability of information has implications in terms of system break-ins where information may not be destroyed (as in corrupted or erased) but is encrypted or made temporarily inaccessible. Such actions can hardly be classified as theft or even malicious damage. In addition to the informational form in which information exists, there is the physical form in which it is stored, such as on hard or floppy disks, magnetic tape, paper tape, computer printouts etc. These too create classification problems for the legal system since it may apply different legal frameworks to different forms of physical representation even when exactly the same information is being held.

Thompson (1989) has also identified a number of factors that further complicate the detection, investigation and prosecution of e-crime:

• E-crimes are generally of low visibility and therefore are difficult to detect;

• E-crimes can be committed over large distances, which cross interstate and international jurisdictional boundaries;

• A large proportion of computer related crimes are 'inside jobs';

• Once the crime has been detected, discovering and understanding the method used by the offender in a technologically complex computer crime can be difficult;

• The ability to obtain physical evidence is generally more difficult than other commercial crimes;
• Computerized information, which is of evidentiary value can easily be altered or destroyed, often leaving no trace of tampering;

• Issues involving the admissibility of evidence in court is further complicated in the computerized environment;

• The technological aspects of a computer related crime can be difficult to present in simplified terms to a court.

Risk Involved in Tracking down Offenders

The FBI estimated that electronic crimes are running at many billions of dollars a year. Some estimates say that only 17 percent of companies victimized report these intrusions to law enforcement agencies, as they are concerned with protecting consumer confidence and shareholder value. They say reporting cyber crimes expose them to leaks and that there is no substitute for constantly enhancing their own defensive electronic security (Webster and Borchgrave, 1999). We here analyzed some of the problems and risks involved in tracking down perpetrators of e-crime.

Difficulties in Carrying out Investigations: The investigation of computer crimes within any given country is difficult enough. The needs to ensure that evidence is available, secured and free from tampering, and admissible, are also challenging. When an international cross-border element is added to the mix, the legal, evidentiary, and jurisdictional problems become even more diverse. In order to secure the

cooperation of a corresponding agency in a foreign country, a law enforcement agency would first need to know exactly who to contact. Having opened a channel of communication with the appropriate authority in a foreign state, the investigating agency has to contend with divergent degrees of expertise in different countries. Legal impediments may also impede co-operation.

Apathy of Some Countries to E-Crime: According to a recent study, many countries are not even minimally prepared to deal with e-crime. Only nine out of fifty-two countries whose laws were studied had been sufficiently geared up for e-crime prosecutions.

Difficulty in Bringing the Offender to Trial: Even where there is international cooperation in locating and apprehending a suspect, the state in which the "victim" computers are located may still have significant problems in securing the suspect for trial.

Obtaining Witness Cooperation: One of the major impediments that face investigators relates to securing the cooperation of complainants and witnesses. It is no news that the victims of e-crime are reluctant to report them to police. Ernst & Young (2003) found in its recent 8th Global Survey of business fraud, that only one quarter of frauds reported in the survey were referred to the police and only 28% of those respondents were satisfied with the resultant investigation.

Identifying Suspects: Investigators of e-crime are most of the time faced with the problem of identifying the right suspects. This can lead to considerable problems when the wrong person is arrested. Digital technologies enable a person to disguise his identity in a wide range of ways making it difficult to know with certainty who was using a computer from which illegal communication came. This problem is more prevalent in business environments where multiple people may have access to a personal computer and where passwords are known and shared.

Problems of Encryption: A difficult problem that faces e-crime investigators borders on data that have been encrypted by accused persons who refuse to provide the decryption key or password.

Locating and Securing Relevant Material: Considerable difficulties arise in locating and securing electronic evidence as the mere act of switching on a computer may alter critical evidence and associated time and date records. It might also be necessary to search through vast quantities of data in order to locate the information being sought.

SUGGESTED METHODS OF CURBING EMERGING TRICKS

Since the rate and varieties of e-crime is daily on the increase, a proactive rather than reactive approach has to be deployed in order to tackle this problem. Here we present a highlight of safety rules that can be adopted by an individual or corporate organization in order to combat e-crime. We also make suggestions of different infrastructures that could be put in place for our cyberspace in Nigeria and other places to be well positioned to withstand the threat posed by e-crime.

E-crime Safety Rules

- Educate yourself, the members of your family, and the members of your entire organization on basic online safety rules. There are lots of resources on the Internet that give practical advice which can be applied to all electronic encounters like text messaging, use of mobile phones, e-mailing, etc.
- Don't buy product from or patronize companies that you are not familiar with.
- Wait to receive written material on any transaction.
- Set up basic virus protection and possibly a firewall on your personal computer to control what sort of material comes into your home and what access others have to your personal information.
- Avoid downloading shareware and freeware.
- Don't open e-mail attachments form anyone you don't trust.

- Scan attachments with an antivirus tool before opening attachments from people you don't trust.

- Avoid clicking buttons inside pop-up windows that invite you to close the window. Instead, close the window by clicking on the x in the corner of the window or by putting your cursor on the upper frame of the window where the title of the web page resides and hit Alt+F4.

- Always check out unfamiliar companies and the personalities of those involve.

- Pay only after delivery.

- Don't give your credit numbers.

- Do not reply to any letter asking you to send money or banking information.

- Avoid any offer of an opportunity that appears too good to be true.

- Be careful of businesses conducted out of post office box or mail drop.

- Be cautious of those that will not reveal their identity on the phone, who will ask you to make a guess of who they are.

- Receipts of ATM, credit statement and bank statement should be well destroyed even when they are no longer needed.

- If different billing and shipping addresses are provided in the order, contact the customer by phone or e-mail to ascertain the reason for the different addresses. When a response is received, consider the response in the context of all of the results from your order scrutiny checklist.

- Use a delivery carrier that requires signatures on delivery and provides copies of the signatures for your records.

Possible Infrastructures for E-Crime Treatment in Nigeria

There are several infrastructures which are being put to use in developed countries which could be imbibed in Nigeria in an attempt to tackle e-crime, these include the following:

Address Verification System: Address Verification System (AVS) checks could be used to ensure that the address entered on your order form (for people that receive orders from countries like United States) matches the address where the cardholder's billing statements are mailed.

Interactive Voice Response (IVR) Terminals: This is a new technology that is reported to reduce charge backs and fraud by collecting a "voice stamp" or voice authorization and verification from the customer before the merchant ships the order.

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.

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.

Use of Biometric means of Identification: Biometric means like fingerprint scanners could be used to identify the user of a computer system. This will require that all computers should have biometric user authentication system when logging-on. DNA samples can also be gathered from keyboards which can be used to identify an individual with a particular computer.

Use of Video Surveillance Systems: The problem with this method is that attention has to be paid to human rights issues and legal privileges.

CONCLUSION

As the general population becomes increasingly sophisticated in their understanding and use of computers and as the technologies associated with computing become more powerful, there is a strong possibility that computer-based crimes will become more common. Nigeria is rated as one of the countries with the highest levels of e-crime activities. E-crime must be addressed seriously as it is affecting the image of the country in the outside world. All the stakeholders must put their hands on deck to exterminate this monster called e-crime. To combat this trend, it is clear that law enforcement agencies must become more sophisticated in their understanding and application of information technology in order to both prevent computer based crimes and to adequately investigate them once they have been committed.

In this paper, we suggested various ways through which emerging e-crime activities in Nigeria could be curbed and we have analyzed several infrastructures that could be deployed in order to fully treat these tricks. These are not to serve as once and for all therapies. The battle against e-crime must be a continuous one if Nigeria and other countries that have been ravaged by this crime are to regain their lost image and take their rightful place in the economic scene in the world. There is much work to be done on electronic crime by individuals, nations and groups of nations. However, given the acknowledge existence of e-crime havens and the pervasive nature of the information technology, many of the solutions suggested in this paper rely on regional or global cooperation.

REFERENCES

1. Brenner, J.K. and Susan, W.Y. 2001. "Is There Such a Thing as 'Virtual Crime'?". *Cal. Criminal Law Rev*. 1(4).

2. Brey, P. 2001. "Disclosive Computer Ethics". In: R. A. Spinello and H. T. Tavani (eds.). *Readings in Cyber Ethics*, Jones and Bartlett: Sudbury, MA.

3. Chapman, A. and Smith, R.G. 2001. "Controlling Financial Services Fraud". *Trends and Criminal Justice*. no. 189. Australian Institute of Criminology: Canberra, Australia.

4. Ernst & Young. 2003. *8th Global Survey of Business Fraud*. www.resourceshelf.com/2006/06/30/recently-released-2006-ernst-young-globalfraud-survey/

5. *Handbook of Cyber Law*. 2000. "It is Time to Act". Macmillan India, Ltd.: New Delhi, India. 147.

6. Mickinley, E.D. 2005. "The Reshipping Scam". www.IntenertRetailer.com

7. *PC Quest.* 1999. "A Cracker Breaks in Pokhran".

8. *Privacy Journal*. 1996. "SSN's For sale Online". 4.

9. Sandeep, D. 2004. "Bid to Block Anti-India Website Affects Users ". *The Hindu*. New Delhi, India.

10. Tedeschi, B. 2003. "Cybercrime, They Just Don't Mention It". *The Age*. http://www.theage.com.au/articles/2003/01/30/1043804447447.html

11. *The Economic Times*. September 11, 2004. 1.

12. Thompson, D. 1989. "Police Powers - Where's the Evidence?". *Proceedings of the Australian Computer Abuse Inaugural Conference*.

13. *Times of India*. 2004. "Online Lotteries Bring Bumper Worries".

14. *Toronto Star*. 1995. "Scam Artists Await Unwary Travelers". F-19.

15. Vatis, M. 1998. "Congressional Statement of the Director National Infrastructure Protection Center". Senate Judiciary Subcommittee Papers. Washington, D.C. www.fbi.gov/pressrm/congress98/vatis0610.html

16. Webster, W. and Borchgrave, A. 1999. "Cyber Crime, Cyber Terrorism, Cyber Warfare: Averting an Electronic Waterloo". CSIS Publications: New York, NY.

ABOUT THE AUTHORS

V. F. Balogun is currently a Computer Science doctoral student at the University of Manitoba, Canada. He holds a B.Tech. degree from the Federal University of Technology, Akure, Nigeria and an M.Sc. Degree in Computer Science from the University of Lagos, Nigeria. His research interests are virtual reality systems, decision support systems, computer graphics applications, *ad hoc* networking, and mobile computing. He is currently working on designing

efficient routing protocols for wireless mesh networks and investigating research issues in cognitive radio networks.

O.O. Obe is currently a doctoral student at the University Polythecnica of Bucharest, Romania. He holds a B.Tech. degree in Computer Science from the Federal University of Technology, Akure, Nigeria and an M.Sc. degree from the University of Lagos, Nigeria. His research interests include software engineering, genetic algorithms, and artificial neural networks. He is currently working on oblivious querying over data with heterogeneous structure.

SUGGESTED CITATION

Balogun, V.F. and O.O. Obe. 2010. "E-Crime in Nigeria: Trends, Tricks, and Treatment". *Pacific Journal of Science and Technology*. 11(1):343-355.