CURRENT TRENDS AND PATTERNS IN INTERNET CRIME

BY

FASANMI, FOLUSO HANNAH

PGD/MCS/2006/1200

A PROJECT SUBMITTED TO DEPARTMENT OF MATHEMATICS/COMPUTER SCIENCE FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF POSTGRADUATE DIPLOMA IN COMPUTER SCIENCE.

JANUARY, 2009.

CERTIFICATION

I hereby certify that this project work titled "CURRENT TRENDS AND PATTERNS IN INTERNET CRIME" is the original work of FASANMI, FOLUSO HANNAH

With registration number PGD/MCS/2006/1200 and has never been presented for the award of any degree or certificate in the past.

Dr. A. Isah
Supervisor

-- ---

Date

Dr. N. I. Akinwande
Head of Department

Date

DEDICATION

This project is dedicated to the Glory of God for his Mercy shown on me through the period of this project work.

ACKNOWLEDGEMENT

My deep and sincere gratitude is to God, the creator who has been the source of my strength and inspiration. I wish to appreciate my supervisor Dr. A. Isah who despite his busy schedule rendered invaluable contribution and constructive criticism that aided at all the stages of this work.

Iam also grateful to the head of department in person of Dr. N. I. Akinwande and all the staffs of the department for their positive impact in my life. May the almighty God reward them.

To my father and Mother, I say a thank you for all your support and understanding, and for being available to me when it matters most.

TABLE OF CONTENTS

ABSTRACT

This project is an appraisal on cybercrime and the changing nature of trends in the crime. Secondary data as compiled by IC3 2007 through complaints forwarded through a public website, ***www.lookstoogoodtobetrue.com***, was analyzed using descriptive statistics. This work also educates consumers with various consumer alerts, tips, and description of fraud trends all over the World. The study also shows only few fraud reports is available for Nigeria.

CHAPTER ONE

GENERAL INTRODUCTION

1.1 Introduction

Over the past three decades, the technology of computers and communications systems has developed so rapidly that it has become difficult to foresee the associated social impact it will have on our lives. This amazing new technology is profoundly acting and changing the functioning of the societies worldwide. The issue of personal privacy and what is perceived to be an increasing invasion of it by advancement in technologies have raised publics concerns. Most individuals regard privacy as a basic right, but the problem is that people have different interpretations and thresholds on what they regards as private and when/where that privacy is jeopardized or invaded.

1.2 What is Computer or Cyber Crime?

Computer crime, cyber crime, electronic crime (e-crime) or hi-tech crime generally refers to criminal activity where a computer or network is the target or place of a crime. These categories are not exclusive and many activities can be characterized as falling in one or more category. Additionally, although the term computer crime/cyber crime is more properly restricted to describing criminal activity in which the computer or network is a necessary part of the crime, this term is also sometimes used to include traditional crimes, such as fraud, theft, blackmail, forgery and embezzlement in which computers or networks are used to facilitate the illicit activity.

A common example, when a person intends to steal information from or cause damage to a computer or computer network. This can be entirely virtual that is, the information only exists in digital form and the damage, while real, has no physical consequence other than the machine ceases to function. In some legal systems, intellectual property cannot be stolen and the damage must be visible. The vast majority of computer crime is no more than traditional criminal activity perpetrated using computer technology, whether blackmail, harassment, financial fraud, piracy or terrorism, the list goes on. The power and flexibility of modern computer systems coupled with global communication potential facilitate certain types of crime including distribution of child pornography. No matter which medium is used to perpetrate the crime, the crime itself remains the same.

Some terms frequently used are often not helpful in the description of computer crime. These include; White collar crime, Computer misuses, Computer abuse, Computer fraud, Computer related crime, IT fraud, and Internet abuse. Yesterday's computer criminal was typically thought of as a mysterious hacker figure, usually a highly intelligent but socially maladjusted teenager, using arcane knowledge to crack codes and gain access to top-secret of military installations. By these standards, the computer criminals of today would be totally unrecognizable. The entry level to work with computer systems used to be a computer science degree, along with access to a secure mainframe

computer installation. Today, it is provided virtually from birth. Games consoles and computer games now link to the internet as standard and from there the world awaits. The widespread adoption of these entry-level to computer systems has led to a correspondingly rapid development of software that is powerful and user friendly. The technical capabilities of the user have increased, with the ability to use a computer as a prerequisite for most jobs.

Furthermore a computer can be the tool used to plan or commit an offense such as larceny or the distribution of child pornography. The growth of international data communications and in particular the Internet has made these crimes both more conspire or exchange data with fewer opportunities for the police to monitor and intercept. This requires modification to the standard warrants for search telephone tapping etc.

Computer crime can broadly be defined as criminal activity involving the information technology infrastructure including illegal access (unauthorized access), illegal interception)by technical means of non public transmissions of computer data to or from within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data) systems interference (interfering with the functioning of a computer system by imputing, transmitting, damaging, deleting, deteriorating,

altering or suppressing computer data), misuse of devices, forgery (ID theft) and electronic fraud.

Computer is a tool and like any other tool, can be used by people who intend to cause damage or carry out some form of illegal activity. The nature of today's Internet and computer networks means that criminal activity can be carried out across national borders. This can create problems over the jurisdiction of those investigating the crime and over differences in the law of the relevant countries where the crime took place. An activity deemed criminal in the home country of the target of the crime for example, may not be considered so in the country from which the offending action was launched.

There are number of ways in which computers can be used for crime, notably among them are:

(i) To commit real-world" crimes, such as forgery, fraud or copyright piracy; just like any other technical device, these types of computer-enabled crime are not usually prosecuted using other relevant laws rather than computer or cyber crime law.

(ii) To damage or modify other computerized systems; these are the types of activity that are usually prosecuted using computer crime legislation.

(iii)Using for activities that cannot be prosecuted but that skate around the edges of legality, to the frequent frustration of law makers and security

consultants, these sorts of activity cannot be legislated against because they often employ everyday, lawful means on the Internet.

Computer and the Internet is complex, but they function on a very narrow set of technical principles. This provides great flexibility but makes it very difficult to legislate against certain types of activity without affecting others. Privacy entails an individual's right to control the collection and use of his or her personal information. Even after that information is disclosed to others with the consent of that individual. When information is disclosed to a doctor, a merchant, or a bank, one expects that the professionals or companies will collect the information they needed to deliver a service and use it for that sole purpose. In the event where the information is to be used for other purposes, individuals expect to be information about it and the right object to its further use.

While privacy was also a problem in manual systems, modern computer communication technology makes it economical to store and process large volumes of data, permits complex correlations at high speed, allows rapid access from distant locations and thus, makes technically feasibility for physically decentralized systems to become centralized logical.

1.3 Existing Technologies

1.3.1 Surveillance cameras

Surveillance cameras are setup in peculiar places and are often illusive in the sense that individuals don't realize that they are being filmed. For the most part these cameras are setup with good intensions namely for the benefits of public safety. They can be a vital tool in preventing or solving crimes. The problem is not that the individual is being filmed, but usually it's done without his or her consent. Often

The legitimacy and purpose of these cameras cannot be verified thereby not knowing whether they are complying with the rules and regulation or plain simply spying on us. The Norwegian Data protection agency has in their 2003 annual report unveiled several cases where surveillance cameras have been misused or setup without permission. Other data protecting agencies around the world report a similar frustration regarding unlawful use of these devices.

In an effort to fight terrorism the United State government t has come up with several mechanisms such as the Government Surveillance via passenger profiling (CAPPSII) program. This is a controversial passenger profiling and surveillance system that required passengers to give their birth date, home phone number and home address before boarding a U.S flight. Under CAPPS II, travel authorities would check these and other personal details against the

information collected in government t and commercials database, then tag the passenger with a color-coded score indicating the level of security risk that the individual appear to p0ose. Each airline passenger will be classified with a color code such as a green, yellow or red risk level. Passenger classified as green will be subject to only normal checks, while yellow will get extra screening and red wont.

1.3.2 Credit cards

The preferred means of payment these days in many industrialized countries are credit cards and one might ask how widespread is their use? The Central Bank of Norway's annual report on payment system for 2002 shows that total purchase of goods and services with the use of Norwegian payment cards in 1993 was 118.8 million transactions amounting to 57.8 billion NOK. In 2002 this figure rose to 516.5 transactions and an outstanding 201.9 billion NOK. A similar trend is shown on almost all of the industrialized countries annual statistical reports. For example, every time we use a payment card at a grocery store, restaurant, bar, bookstore and any other purchase we make, our names are correlated with our purchases and entered into giant databases.

1.3.3 Internet

The Internet has enriched people with information and given them the opportunity to do business and shopping online. It offers a variety of services

that are in most cases essential to individuals and the ease at which those connectivity and usage has exploded within the last decade. The Norwegian statistical gathered agency SSB has in their 2002 yearbook indicated that the number of Internet subscribers increased from 381342 in 1998 to 1235 596 in 2001. Different government statistical bureaus around the world also report a huge increase in the number of people that are online. Concerns over consumers privacy has been raised by many since Internet Service Providers (ISPs) and Web sites now collect and sell data about on-line users at unparallel rates. There are a multitude of data gathered tools available for everyone and these are being used to monitor the activities of unsuspecting Internet users what's alarming is that often, these tools covertly collect the information without the user's knowledge.

1.3.4 Mobile phones

Subscriptions to mobile phones have also enjoyed a tremendous increase over the last 10 years. Out of a population of 4 million in Norway, there were 3911011 mobile subscribers in 2002 compared to 371 403 in 1993. This is not unique for Norway, but rather a worldwide phenomenon. Also Nigeria. One of the latest services of offered by mobile phones is Location Based Services (LBS), which in its basic form will give individual information about their location. Examples of such services are friend-finder and Buddy which are

currently offered by some network operators such as Telia in Sweden and Notcom in Norway.

People who signup for this service have the opportunity of locating their friends or loved ones as long as they are registered in their list. Location Based services doesn't only give away the location of individuals but gives a pattern on what services individuals interested in. the ability to gathered and pass on personal information about consumers has been a key selling point for interactive media. Marketers have been told they will be able to gain access to everything from what movie preferences a household has to what it had for dinner last night. With that data, they plan to send marketing messengers based on personal likes and dislikes. This increase the quantity and value of personal information in the marketplace thus creating a conflict between those who feel they have a right to profit from such information and those who feil they have a right to privacy.

1.4 Emerging Technologies of Radio Frequency Identification (RFID)

REID is an item-tagging technology which is already in use in the supply chain to track assets like containers and trailers. REID tags are tiny computer chips connected to miniature antennae that can be affixed to physical objects. In the most commonly touted applications of RFID, the microchip contains an Electronic product Code (EPC) with sufficient capacity to provide unique identifiers for all produced worldwide. These tags are so small which makes them ideal to place them into clothing, purses, shopping bags, suitcases and

more. The Electronic product Code potentially enables every object on earth to have own unique ID that can be linked to its purchaser or owner at the point of sale or transfer. The tags can be read from a distance and are not restricted to line of sight. While there are beneficial uses of REID, it could be deployed in away that threaten individual's privacy.

Just as the ability to freely use, store and communicate data is critical for any nation; it is equally essential for the effectiveness operation of an organization of virtually any size anywhere in the world. As individuals, whether we like it or not, we are all totally reliant on data storage systems to lives in the manner to which we have become accustomed.

Inevitably, there will be a portion of the population who seek to take advantage of this proliferation of, and dependence upon, computer technology. They work to identify and exploit any weakness that are discovered in computer systems new or old, and to use this knowledge to further their own financial, criminal or political aims.

Most communication devices are now computers and virtually all computers are communication devices, in one form or another. This simple statement has profound implication for data security, confidentiality, accessibility, assurance, integrity and of course for the science of computer forensics.

It is important to realize just how reliant we are upon computer and how vulnerable the vast majority of us are to computer-related crime. Any organization's system is only as strong as its weakest point. Any element of the system, including the human element that allows it to be compromised could potentially make an organized the victim of a computer-related crime. It is therefore vital that these vulnerable points are understood and appropriate preventive measures taken access to all data? It's often impossible to put a financial value on a company's customer database, financial records, product designs or source code. If this information fall into the wrong hands it could, and frequently does, spell disaster for a business. What would you do if employee be3gings to leak critical information to a competitor? The employee may be interested in joining them and will certainly stand out among the other applicants if he is able to bring information to give them a competitive advantage. If this scenario seems implausible, consider that in Africa especially in Nigeria, we have got several unrecorded cases frequently in recent years.

Are existing information security systems adequate to detect such events? Even if they are capable of doing so, alert the management of the organization or the Nigeria society constantly with the requirements of a tribunal or in a Court of Law. It is easy to overlook the more blatant threats. Companies spend a fortune on expensive security equipment but freely allow employees to leave the

building with DVDs backup taps, telephones or PDAs in their briefcases or bags. The only way to ensure complete protection is by establishing a strict usage police. This should specify exactly who has access to what and individuals must then be monitored to make sure it is being adhered to. It may however be that a policy this tight actually detrimental to the efficient running of the business.

Traditional defenses for data, both and in out of an organization, were based upon the concept of a secure system perimeter. Today, with the advent of mobile communication, home working and widely distributed data storage, this concept has become less relevant. New principles therefore need to be adopted. Whatever the strategy, the policy should be documented, distributed to the relevant people and it should then also be maintained.

1.5 Pornography and other inappropriate Internet use

The possession of pornographic material is not in itself an offence. However, if it is found on company systems it suggests that company time and resources have been used to collect it. Usually, this material has been downloaded from the Internet, which means that company IT resources have been for illegitimate purpose.

Over many years, the frequency of downloaded pornography occurring on corporate machines we have received for commercial data purposes, as opposed

to those disks and media received for computer investigation has diminished. As little as five years ago we noted that the majority of disks received contained some pornography. These disks came from all levels within an organization, form board level downwards. Recently however, this trend has received, so that today minorities of disks received for commercial data recovery contain pornography. It is strongly suspected, that its as a result of the greater awareness that this type of material can be identified and tracked by the organization internal IT control system. The po8int here is that when formulating a corporate acceptable usage policy, be realistic as what people may do and draw guidelines accordingly.

Inappropriate use is not restricted to pornography – some employees may be habitually on-line visiting football sites or Internet chat rooms, for example. While some activities may be viewed more favorably than others, all carry a cost measurable in bandwidth and time that could otherwise be spent working.

It is vital that the company has a clear, up to date, written policy that states:

(i)What constitutes appropriate use of the internet?

(ii)What system will be used to monitor staff Internet Usage?

(iii)What procedures are in place to deal with those that break the rules?

Recent interest in Corporate Governance also brings this aspect of the control of this element of the company resources into a sharper focus.

1.6 Types of Crimes

1.6 .1 Hacking

In the world of computers, a hacker is someone who devises an ingenious method of solving a computer problem. But in recent years this term has hijacked by the media and Hollywood to describe someone who breaks into supposedly secure computer systems to steal information, destroy data or assume control. Typically young highly intelligent but lacking in social graces, these hackers often do not think of themselves as doing anything wrong. Instead they often try to justify their own actions by accusing their targets of being oppressors in a society where information should be free. Hackers appeal to the public imagination and have acquired their own strange sort of glamour.

Computer systems are by their nature highly complex. They are more likely to expose any security holes as a result of human error than by any serious design flaws so usually; hacking is less likely to involve inventing ingenious program to fool the victims' computer system, that snooping for passwords or attempting to gain access by various social engineering methods.

The people who have the greatest opportunity to exploit or hack a system are those who operate, manage or otherwise have legitimate access to it. Companies are therefore many times more likely to be hacked by someone's they already

know, employ or to whom they give free access to their systems. Most often it's not the highly complex system exploit that is used to gain access to a system. Although this can happen, it is the simple expedient of obtaining a user name and password that accompanies a system. This is obvious but frequently ignored lessons.

1.6.2 Password

Passwords are one element in the armory of tools employed to keep information from hackers and other unwanted visitors out of a system. The correct use of passwords, their importance and their vulnerabilities must be clearly understood by all members of an organization. In many organizations this is part of the standard staff induction training programme. Contractors, temporary staff and home workers must also be remembered when formulati8ng a password policy.

Education about social engineering scams should also be considered. When conducting security reviews, a few obvious problems occur with monotonous regularly such as: Employees displaying their password on post-notes, Passwords written down in diaries, notes books, and so on. We also have same password used for all users of a system. For example, all administrator passwords identical for all staff, administration passwords widely known to all, and administrator log on used for all purposes.

No passwords on administration accounts are seen as inconvenient and irritating. This relaxed attitude is widespread and the cause of many security problems.

Thanks to the widespread destruction caused by the rapid propagation of malicious software such as Melissa and the Love Bug and the subsequent publicity on computer virus. They often use the term to refer to just about any piece of malicious software but there clear definitions as to what constitutes a virus.

1.6.3 Virus

A is a piece of programming code that replicates itself by infecting other programs. In addition, it causes an unexpected and usually unwelcome event know as its payload. A virus cab be transmitted as an attachment to an email (this is how Melissa and Love Bug spread so quickly), as a download form the Internet or can be present on a floppy disk, CD or flash drive. Some viruses start havoc a soon as their code is executed. Others lay dormant until circumstances cause them to be triggered. They rang from the playful; and mildly annoying (such as a Happy Birthday Ludwig displayed on screen on the anniversary of Beethoven's birthday) to the extremely destructive, which can erase data, stop the operating system from functioning properly and even bring down entire networks.

A worm is code that does not infect other programs and usually does not carry a payload. Often its presence only becomes apparent when areas of the system suffer due to the strain placed on system resources causing other tasks to show or be stopped.

A Trojan horse is a malicious computer program contained inside apparently innocuous programming or data. Disguised like this, it can take control of a system and do whatever damage it is designed to do. One notorious example of a Trojan horse was disguised as a virus-killer program. The name comes from Homer's Iliad where the Greeks presented the Trojans w9ith a large wooden horse as a gift. Their warrior was hiding inside and during the night, they emerged and overran Troy. Unlike a virus, a Trojan does not create copies of itself. It is p[particularly effective at circumventing computer security measures, because hostile code can be placed on the inside of an established security perimeter.

A logic Bomb is code introduced surreptitiously and is designed to execute (or explode) under circumstances such as the lapse of a certain amount of time or the failure of a user to respond to a certain event.

This software is usually 8introduced introduce unintentionally, by opening an email or loading a file that is infected. A policy on accepted email attachments, procedures for loading data from media external to the company and up-to-date ant-virus software from a reputable vendor is often sufficient to protect against the worst of these incidents.

1.6.4 Software piracy

Software piracy is still commonly practiced and widespread. It can be difficult for an organization to assess the true financial impact of this types of theft, since nothing tangible is removed. The issue of software piracy has been well published recently by the music industry and the financial impact of the downloading of music in the form of MP3s is beginning to be understood. Software piracy can affect anyone who produces goods capable of being stored in an electronic format. If this information becomes freely available on the Internet, it becomes extremely difficult, if not impossible, to contain the situation. The victim might be the company itself (if it produces its own software) and /or a third party vendor.

1.6.5 Electronic Founds Transfer

E- Commerce is a fact of life. Online banking is now core to the way the banks do business. Indeed many of the high street banks have disposed of many of their physical high street properties to the point where they are reliant on online

banking themselves. As with many aspects of security, user confidence is critical to the take up rate and continued use of the services.

There have been many reported instances where online transaction systems have provided weakness, which have be exploited by fraudsters. The same could be said of course for traditional banking systems, probably since their inception. The often received less media attention. It is also true that organizations prefer to keep any such strictly under wraps, fearing that customers and investors would lose faith in their ability to run a secure operation. Whilst understandable, this is a short-sighted approach because it means that the culprits are never caught and are therefore free to prey on other organizations.

It is tempting fact to say any system is 100% secure, as without doubt some systems are more secured and better implemented than others. User education is important in preventing this type of fraud. Understanding what information they should and should not be expected to provide is also crucial.

1.6.6 Scams

Most scams revolve around get rich quick schemes or offering expensive items at rock-bottom prices Human nature being as it is, these scams take in many people, and will probably continue to do so. The attraction for the perpetrations of fraud using computer systems with access to email and the Internet is the

huge potential audience. Whilst the scams themselves are often nothing new most of them have been operating for years through other media – there is considerably more money to the made online.

Chain letters, please from Nigerian citizens offering millions for laundering money, bogus charities, bogus charity appeals, auction sites offering goods for sale that don't exist or don't belong to the seller ….. all appeal peoples greed or naivety – both of which seem to be plentiful supply.

1.6.7 Impersonation

It is easy to adopt another person's identity on a computer system. Most commercial e-mail services are fairly insecure and are not good at verifying that a specific sender or recipient of an email is who they say they are. As we have already seen, people are careless about keeping their passwords secure and this situation is made who's by the ability of some browsers and operating systems to remember passwords. The idea here is to save the user from having to type them each time require accesses. But all they need to do is step away from their machine and someone else could log on and assume their identity.

It is possible for anyone to create an e-mail account and send e-mails relatively anonymously. Frequently the only requirement for creating a new account is to

supply an e-mail address that is unique. It is possible to use this account to impersonate others. More technically complex methods exist to achieve this, and are widely used. The best advice is, when the sender's identity is in doubt, check.

1.7 Framework Supporting Crime Technology

When vogon first started investigating computer crime, a typical scenario would be a business running a stand-alone PC with a single hard disk. As time went on and client/server systems became increasingly popular, our investigations would sometimes revolve around a small network.

Today, the trend is towards highly distributed data storage, which posses its own problems. In simple terms, this means that different parts of the same data storage system can be located on entirely separate computers. These may be on a different computer in a different building or in a different country. Jurisdiction issues play an important part in this type of cross border investigation. The Internet as a global network is unconcerned and largely unaffected by regional jurisdiction, it is ever changing and hugely complex. It offers hugely rich and dynamic resources to the user. It is also an ideal place for criminals to operate. On the Internet, an individual so inclined can enjoy a broad virtual anonymity.

Technological and social developments relating to the use of mobile devices create new opportunities of the criminal and threats to an organization. Such devices includes, telephone PDAs, removable storage devices, and the complete range of electronic data storage devices including cameras, MP3 players, etc.

Investigating contemporary computer systems is a complex business requiring a fundamental understanding of sophisticated technologies and employing appropriate techniques to safeguard the evidence capture. At each stage of an investigation care must be taken to ensure that not only is the technology understood but also, all work is carried out strictly in accordance with recognized forensic principles.

People

It is a statement of fact that the people who know the most about a system are also in the best position to abuse it. Often IT staffs are included in the suspect and if the finger of blame is being pointed at them, they may not be too forthcoming about the finer details during an investigation. They are also in the best position to attempt to hide, destroy or otherwise obfuscate critical data containing evidence. Allegations or wrongdoings unsubstantial by facts also open the way fore industrial tribunals, claims of constructive dismissal, and can generate a huge amount of bad feeling and animosity if handled incautiously.

It takes experienced investigations with the ability to put the system together piece by piece to truly understand how it all fits. Who has knowledge of the entire system in your organization? It might be just one or two people. In a large system, or one developed by a third party, it may be that no individual understands any more than a investigation, and we strongly suggest that professional advice is taken before embarking on any internal investigation that may potentially involve civil or criminal action. Evidentially incautious or inappropriate action taken at the data capture stage of a case can destroy or invalidate the results even bef0ore starting the actual investigation.

Data

The key to any investigation is data. Without an accurate and reliable data, there is no evidence. Without evidence the perpetrator of a crime cannot be brought to justice.

Computer data is extremely fragile. Even switching on a computer has the potential to destroy or damage vital information such as log files, which an experienced investigator can use to understand what has occurred. There are many circumstances in the real world, as opposed to forensic textbooks, in which the collection and preservation of data is especially difficult. The following list is not exhaustive, but offers a representative selection of situations often encountered:

Data recoded across many disks or tapes, such as in RAID arrays and disk striping Data recorded across many different media. For example, the use of hierarchical storage management systems Data existing on many different servers in a distributed system or storage Area Network (SAN) Data in different geographical areas, such as a wide Area Network (WAN) spacing different continents Remote computing – virtual private Networks (VPN) Data stored in proprietary (that is, non-standard) formats data stored on damaged media data encryption – file/partition/disk encryption systems, data stored on a platter locked disk that is, a disk that will not provide data without a password being provided, data stored on complex tape systems (multistreamed/multiplexed tape backup systems).

Creating a Duplicate or Clone Disk

Laying an image down to a duplicate disk is a quick and simple solution and in some instances is often a sensible first step for those with limited technical equipment or capability. This allows the file system to be mounted and viewed on an investigators computer, some call this process disk clothing, Disk cloning lacks the advantages of some of the more sophisticated processing methods. There are no search facilities available and some files with the data stamps showing when they were last accessed will be changed as the investigator trawls through the data. An investigator also requires a comprehensive knowledge of

the operating system that any original data comes from. Some operating systems such as Netware, UNIX and pose their own special problems and require additional; expertise.

Disk Emulation

This method is similar to the disk duplication method and again does not offer search facilities. Because the disk is emulated rather than accessed via software, all the files are write protected and are therefore unchanged by an investigations.

This method is not widely used, as it requires specialist technology and techniques. In some circumstances this is an appropriate alternative method for computer investigation.

Electronic Disclosure

The principles of electronics disclosure, or electronic discovery, are the same for electronically held data as they are for traditional paper based systems. A simple explanation would be, for example, a US based organization involved in litigation of some sort. Both parties would have a duty to disclose a "copy, or a description by location or category of, all documents, data compilations, tangible things that are in possession, custody or control of the party and that the disclosing party may use to support its claims or defense". If all documentation

were held on paper the problem whilst formidable would be clear and understandable by all.

Electrically held information, for example in the form of a spreadsheet, would pose a different problem. A paper copy of a spreadsheet would reveal numbers, but not the meta-data associated with the numbers found in electronic format. Metadata is simply data about data, and in this example might include:

(i) What formula, if any, was to gene rate the result?

(ii)When the spreadsheet was created?

(iii)When the spreadsheet was last update?

(iv)Who owns the spreadsheet?

(v)Where was the spreadsheet stored?

(vi)Was it password protected?

(vii)What version of the application package used to create the spreadsheet?

Electronic Disclosure or Electronic Discovery, depending upon which side of the Atlantic you reside, is the process of disclosing a carefully defined sub-set of information to the opposite party, usually in a litigation situation. It needs to be complete as defined by the terms of reference, but care must also be taken not to disclose improper material. Disclosure of certain material may place an

organization in breach of data protection legislation, whether disclosure was inadvertent or otherwise.

In today's digital world most business store documents electronically and communicate via e-mail. As a result, 80% of court cases rely upon files and correspondence that never have been committed to paper, yet during disclosure, they are frequently printed out and the hard copies used as evidence. It is clear that there is a fundamental flaw with this approach. The situation becomes far more complex when considering the nature of a typical data storage strategy used by a large organization. Data used and accessed daily is most likely to be stored on local hard drives; server based hard drives, or perhaps a storage area network type storage solution.

This is fine as far as it goes, although it may still present a high level of technical complexity in terms of accurate disclosure if, for example, the contents of an email server are to be correctly disclosed.

In this example, disclosure may depending upon the circumstances, need to encompass.

- Current e-mails
- Deleted e-mails

- E-mail attachments
- Deleted e-mail attachments

It is not sufficient to book only at the data currently held on a system. To comply with typical disclosure requirements, consideration must also be given to the data held in a back up system.

At this point the backup strategy must be considered and examined in detail to determine what has been backed up, and how the disclosure requirements can met this is often far more complex than it first appear.

Some of the typical problems that may be encountered include:

- Lack of understanding of exactly what has been backed up
- Lack of understanding at the right level of the backup strategy
- Lack of comprehensive of the volume of data involved

Assuming that the above issues can be resolved, technical issues must also be considered when considering the implications of full and complete disclosure, and any statement that can be made in this respect. Some of the serious technical problems that organization regularly encounters include: Inability to restore backup media software formats, and Inability to restore backup hardware formats. Dynamic changes that have occurred within the organization's internal IT system which make straightforward restoration of data difficult Software

platforms of file systems longer supported due to system migration over as period of time.

1.8 Objectives of the study

The following are the objectives of the study:

(a) Identify computer security issues within the information technology industry especially its level of awareness within the Nigeria Domain.

(b) Provider support to ensure successful prosecutions.

(c) Deter potential offenders.

(d) Promote computer ethics and public awareness.

1.9 Significance of the study

The convenience associated with IT and the Internet is now being exploited to serve criminal purposes. Recently, a report indicated that Nigeria is losing losing about $80 million (₦11.2 billion) yearly to software piracy. The report was the findings of a study, conducted by Institute of Digital Communications (IDC), a market research and forecasting firm, based in South Africa, on behalf of Business Software Alliance of South Africa.

CHAPTETR TWO

LITERATURE REVIEW

2.1 Introduction

The abuse of the Internet continues to grow at an alarming rate. In 1998, 547 cases on computer intrusion were opened. Later, the number of similar cases increased to 1,154 in 1999. However, Federal Bureau of investigation (FBI), the United state' Chief Inspector stated at a recent Senate hearing in Abuja that the number of computer crimes between 2001 and 2006 has dou8ble that of 1999. The FBNI state that the main threat came form the "computer professionals, hackers and virus founders who are not satisfied with their life or the way lives so they hunt for more money".

According to the United State of America's official statistics, it was found that, of the ninety percent (90%) interviewed whose computer systems had undergone Internet attacks in 1999, seventy percent (70%) stated that penetration into their system was connected with embezzlement of confidential information or financial fraud. Financial losses form information embezzlement and financial fraud result in $68 million and $56 million respectively. Financial losses of the 273 interviewed resulted in more than 265 million dollars. In 1998, the loss form attacks such as "service refusal" was $77,000 and dramatically increases up to $116,000 in 1999.

The advanced speed of technology has made it easier for computer criminals to conceal information about their crime s. due to the complexity of the digital environment, evidence is collected and handled differently than it was in the past and often requires careful computer forensic investigation. Crimes committed by computer users may cause damage or alteration to the computer system.

Preventive or deterrent measures are difficult in the cyber world, partly because of the ability of attackers to remain anonymous. An unrestricted cyber-war offensive however, would almost certainly give a new clues as to their identify. Computer network designs should integrate notions of robustness and survivability while contingency plans of the continued implementation of critical roles and missions with far less connectivity are important.

However, according to Ibrahim Lukman of Federal University of Technology Minna in this presentation at the 2004 Nigerian Association of Computer Student (NACOSS) national convention at University of Ibadan, maintained that 3 out of 5 Laptops systems that entered Nigerian market are gotten form Credit cards which are fraudulently acquired via the internet. The EFCC report of May 2005 also confirmed Lukman's earlier contributions that the so called *yahoo boys* are fast getting into the computer crime.

Precisely on July 4, 2007 the same EFCC organized sensitization campaign on the serious effect of computer crime or cyber crime on the Nigerian economy by organizing a one-day works shop in Abuja for the 2007 Batch A National Youth Service corps members. During the work shop, the EFCC Representative Ibrahim Balarabe confirmed over 700 Nigerians are serving jail term in foreign countries including United State of America and some parts of U.K through the Federal Bureau of investigation (FBI) for their direct involvement in respect of cyber crime. But Ibrahim Lukman during his presentation also challenged EFCC man that the case of cyber crime should not be shifted to computer professionals alone but a collaborative offences or crimes. In Nigeria alone, over 1,700 cyber 9ffenders (professionals and students) are currently in the EFCC custody which is sending a wrong signal to the International community.

There is however, an easier way to get online, the online service via e-commerce. Companies such as CompuServe, prodigy and AOL offered access to their network "communities" once logged onto the serve, users could download software, post messenges to bulletin boards and find information on a wide variety of topics and waste amazing amounts of tine in chat rooms or holdings private conversations through instant messaging.

The big lure of these services was ease of use. They provide a disk that is usually installed the proper software automatically and configured users

computer settings, so users didn't have to know anything about much of anything to get "connected" in their early days, the services were excruciatingly expensive by modern standards, in the 1980s, it cost US$25 an hour to connect to CompuServe. Went to unlimited usage plans that cost less than U*S$20 a month. The online services were not, in their early days, ISPs. Rather, they were private wide area networks (WANs) in which members interacted with each other but not with the "outside world" of the Internet, they were similar to BBSs on steroids. Later the services provided e-mail gateways so that their members could exchange e-mail with others outside the private network. They also added access to the World Web. Today, most online services are also ISPs. Even though ease of use associated with regular Internet providers has increased dramatically, many "Net newbie's" still find the online services easier use. This ease of use attracts criminals (along with legitimate users) who are not particularly technically proficient.

Another benefit of the online services that attracts criminals is the anonymity they offer. Generally, if you set up an account with a regular ISP, you're assigned to user account name and e-mail address based on that name. it's possible to get ISP to change your account name, but it's a lot of trouble and can't be done too frequently. Services such as AOL allow users to create secondary "screen names" that they can change whenever they want, making it easier for a criminal to change identities and cover his or her tracks.

The 2002/2003 British crime Survey showed eighteen percent (18%) of households with internet access said their home computer had been affected by a virus. This had increased to twenty seven (27%) between 2003 and 2004. one-third said the virus had damaged their computer. The biennial Department of Trade and business had a computer security incident in the 2006. However, the fear of experts around globe now is that, the problems associated with Computer crime may become almost uncontrollable when Nigerians get seriously involved. These statistics may underestimate the real situation as many organizations or individuals may be unaware that the security of their computer has been compromised. There are various reasons for the increase, outlined below.

2.2 Increasing financial motivation for computer crime

Information security experts suggest that the motives behind computer crime have changed. Traditionally it was motivated by desire for peer recognition and to demonstrate technical skills. However, it is now increasingly financially motivated. The growth of ecommerce, with forty-five percent (45%) of internet users participating in some form and the dependence of many aspects of financial life on computers has motivated this shift. Evidence can be found in the occurrence of extortion attempts and thefts of credit card details. More people are producing mail ware (collections of e-mails) to make money.

2.3 Crime and commercialization of the Internet

By 1991 e-mail users had began to consider the possibility that their Internet communications would be intercepted. Philip Zimmerman released an encryption program called pretty Good privacy (PGP) that could be used to protect sensitive messages. PGP was also used by criminals to hide evidence of their crimes form police. The first cyber bank, called First Virtual, came online in 1994, opening up vast new opportunities for hackers. Also that year, researchers began work on the "next generation" of the Internet protocol, called IPv6. The primary purpose of the new IPv4's 32-bit address space but another concern addressed by the new protocol version was to be IP security.

In 1995 the U.S Secrete Service and the Drug Enforcement Agency (DEA) obtained an internet wiretap to help build a case against suspects who were accused of producing and selling illegal cell phone cloning equipment. In 1996, Congress became concerned about the amount of pornography that was being exchanged over the Internet and passed the Communications Decency Act (CDA), whihich was later declared unconstitutional. Meanwhile, a cracker was able to shut down the public Access Networks Corporation in New York in 2005 using a hack attack that was described in a New York Journal of 2006. A cancel-bot (a virus) that was launched in world have "cracked down" on behaviors such as unauthorized access that were not covered by criminal status.

We seem to have all the most important elements for reducing the incidence of computer crime, we have laws (with teeth"); we have the tools; we even have the widespread awareness that is sometimes the most difficult component of a crime prevention effort. Why, then, is computer crime not only going away, but steadily increasing?

An important reason for the increase in computer Crime is the whirlwind pace at which new technologies are being developed to make our computing experience more productive, easier, faster and more fun. However, convenience and performance often come with a price and that price is security.

Cyber criminals love new technologies, including:

- Broadband
- Wireless
- Mobile computing and remote access
- Sophisticated Web technologies such as Java, ActiveX and so on
- Fance e-mail programs that support Hypertext Markup Language (HTML)
- E-commerce and online banking
- Instant messaging
- New operating systems

Cyber criminals also love standardization. If everyone uses the same operating system, or the same Web browser, or the same e-mail client, ir if all vendors adhere to the same specifications, the potential attacker has much less to learn and a much larger playing field. These new technologies and the standardization of computer and networking technologies are so dear to the heart of the cyber criminal.

2.4 Why Cyber criminals love Broadband

Broadband technologies such as XDSL, cable modern, and satellite Internet services have made Internet users' lives easier but they have also made it easier for hackers to invade those users' computers and networks. Because individual computers attached to broadband networks such as cable modern or DSL, behave more like computers attached to a network than like individual computers that use telephone lines to dial into the internet, it is easier to exploit the technology to gain unauthorized access. As a consequence, broadband users need to be much more security conscious than dialup Internet users.

2.5 The problem with 24/7 connectivity

A network is vulnerable to an attack from outside only when it is connected to an outside network. When most users and companies were connecting to the Internet with analog modern or dialup ISDN connections, their vulnerability to attack was limited because the system was available to outsiders only during a

session. When you finished doing what you wanted to do on Net, you disconnected and you system disappeared form the Internet. Additionally, most ISPs use Dynamic Host configuration protocol (DHCP) to assign IP addresses to dialup users. This means that your Internet-connected computer gets a new IP address each time you hang up and reconnect. DSL and cable are refereed to as always-on technologies. You don't have to dial up as connection each time you want to get onto the Internet; instead, you stay connected 24 hours a day, seven days a week. This makes it quicker and easier for you to access Internet resources. It also makes easier for you to run a server, allowing other authorized users to remotely access shared files on your system.

Because you IP address generally stay the same, since you don't disconnected, these unauthorized clients can find your server more easily form one communication session to the next. Powering the computers down breaks the connection (and "shuts the door to potential hackers). However, today's computers are made to run continuously (and except for some peripherals such as the monitors, generally run better and last longer when they do) so many technically savvy users never turn their systems off.

The problem with 24/7 technologies is that they make it easier for unauthorized folks to access the system too. The exposure is much greater with people who are "always open for business", given a hacker more time to mount a brute force

attack to guess the password or figure out which TCP/UDP ports might be open and vulnerable. Furthermore, because the IP address stays the same, it's easier for these hackers to return to the system next time they want to do a little virtual breaking and entering.

2.6 The problem with High-Speed Connectivity

Another advantage of broadband is the increased connectivity speed. Unlike an analog modern that's limited to 56Kbps (and practically speaking, less that due to federal regulations and the line considerations) DSL and cable companies offer high-speed downloads and often higher upload speeds as well. These means improved performance on your en, but if your service offers a high upload speed, it also means an intruder will be able to snatch your files more quickly. Luckily, in terms of security if not usability, most broadband services are asymmetric. That means that uploads and download speeds are not created equal; typically for consumer accounts, the upstream transfer rate is limited to 128Kbps by cable companies and anywhere form 128Kbps to 764Kbps by DSL providers. Even with these limitations, however, upstream speed is generally at least twice that of an analog modem- a boon to hackers downloading data from your computer to their own.

2.7 Low-Cost, 24/7 High-speed connectivity

The problems linked to high-speed 24/7 connectivity and high-speed data rates associated with consumer broadband technologies also exist with traditional

24.7 high-speed business solutions such as T-I. However, because most T-I lines are connected to companies that employ IT professionals, it is more likely that security measures are in place to offset the security risk.

The problem with cable and DSL is that these technologies have brought high-speed, always-on access to home and small office users who cant afford the high cost of T-I. These less sophisticated users are also less likely to be aware of the security risk or to have the technical expertise or budge to implement the proper level of security. Most small officers and a growing number of home users run network Address translation (NAT) software of some type to share Internet access with multiple PCs on a small LAN. This provides a small measure of security to the systems on the local network because NAT assigns private IP addresses to the NAT client computers. These addresses are not visible on the Internet. However, the NAT host computer that is directly connected to the Internet is exposed.

2.9 A World without Wires?

As at August 2001, Bank of America projections anticipate that there will be 400 million wireless uses by 2003, according to Eric W. Pfeiffer of Interlamination Data corporation reports that over 15 million subscribes already have wireless access to the Internet through personal Digital Assistants (PDA) and smart phones.

CHAPTER THREE

STATISTICS IN COMPUTER CRIME

3.1 Introduction

The statistics available are reports of the findings of a study, conducted by Institute of Digital Communications (IDC), a market research and forecasting firm, based in South Africa, on behalf of Business Software Alliance of South Africa. As it is now, cybercrime is an image nightmare for Nigeria. When you come across phrases like "Nigerian scam", the assumption that crosses your mind is that all (or conservatively, most) scam emails originate from Nigeria, or Nigerians.

In 2004, the federal government established a cybercrime working group, the Nigeria Cyber Working Group (NCWG), with the purpose of aiding Nigeria's demystification of the hydra-headed monster. The NCWG is an Inter-Agency body made up of all key law enforcement, security, intelligence and ICT agencies of government, plus major private organizations in the ICT sector. Some of these agencies include the Economic and Financial Crimes Commission (EFCC), Nigeria Police Force (NPF), the National Security Adviser (NSA), the Nigerian Communications Commission (NCC), Department of State Services (DSS), National Intelligence Agency

(NIA),Nigeria Computer Society(NCS), Nigeria Internet Group(NIG), Internet Services Providers' Association of Nigeria (ISPAN); National Information Technology Development Agency (NITDA), and Individual citizens representing public interest. The working group has two chairpersons and one coordinator. The duties of the Working Group include: Engaging in public enlightenment programs, 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. In addition, the working group was tasked with the responsibility of working with global cyber crime enforcement agencies in the USA, the UK and other countries, who are at fore-front of fighting cyber crime.

The Internet Crime Complaint Center (IC3) began operation on May 8, 2000 as the Internet Fraud Complaint Center. In December 2003, the Internet Fraud Complaint Center (IFCC) was renamed the Internet Crime Complaint Center (IC3) to better reflect the broad character of such criminal matters having a cyber (Internet) nexus. IC3 established a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI) to serve as a vehicle to receive, develop, and refer criminal complaints

regarding the rapidly expanding arena of cyber crime. IC3 was intended and continues to emphasize serving the broader law enforcement community, including federal, state and local agencies, which employ key participants in the growing number of Cyber Crime Task Forces. Since its inception, IC3 has received complaints across a wide variety of cyber crime matters, including online fraud (in its many forms), intellectual property rights (IPR) matters, computer intrusions (hacking), economic espionage (theft of trade secrets), child pornography, international money laundering, identity theft, and a growing list of additional criminal matters.

IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, and local level, IC3 provides a central referral mechanism for complaints involving Internet related crimes. Significant and supplemental to partnering with law enforcement and regulatory agencies, it will remain a priority objective of IC3 to establish effective alliances with industry. Such alliances will enable IC3 to leverage both intelligence and subject matter expert resources, pivotal in identifying and crafting an aggressive, proactive approach to combating cyber crime. In 2007, the IC3 saw an increase in

several additional crimes that were exclusively related to the Internet these included but are not limited to pet scams, check cashing scams, online dating fraud, phishing, spoofing, and spam. Each of these types of complaints has increased in prevalence over the past year.

Overall, the "IC3 2007 Internet Crime Report" is the seventh annual compilation of information on complaints received and referred by IC3 to law enforcement or regulatory agencies for action. This report provides an examination of key characteristics of 1) complaints, 2) perpetrators, 3) complainants, 4) interaction between perpetrators and complainants, 5) common Internet scams observed throughout the year and 6) success stories involving complaints referred by IC3. The results in this report are intended to enhance our general knowledge about the scope and prevalence of Internet crime in the United States. This report does not represent all victims of Internet crime or fraud because it is derived solely from information provided by the people who filed a complaint with IC3.

3.2 General IC3 Filing Information

Internet crime complaints are primarily submitted to IC3 online at www.ic3.gov. Complainants without Internet access can submit information via telephone. After a complaint is filed with IC3, the information is reviewed, categorized, and referred to the appropriate law enforcement or regulatory agency.

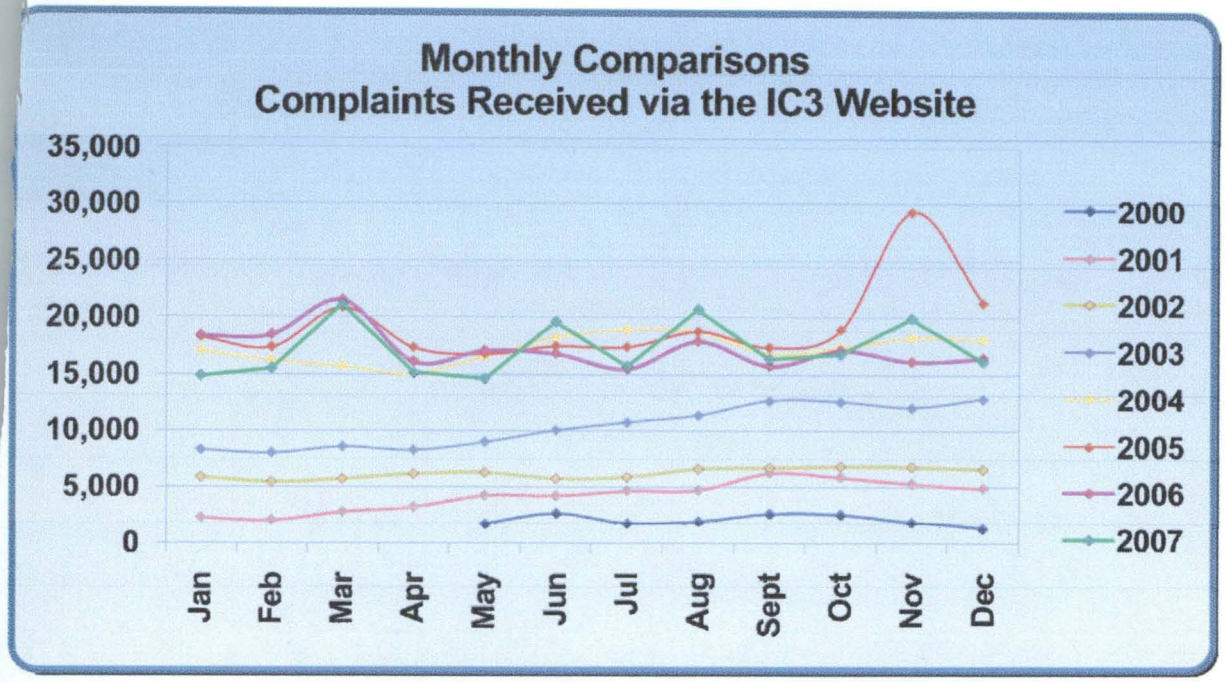

Fig.3.2 Number of complaints filed per month in2007

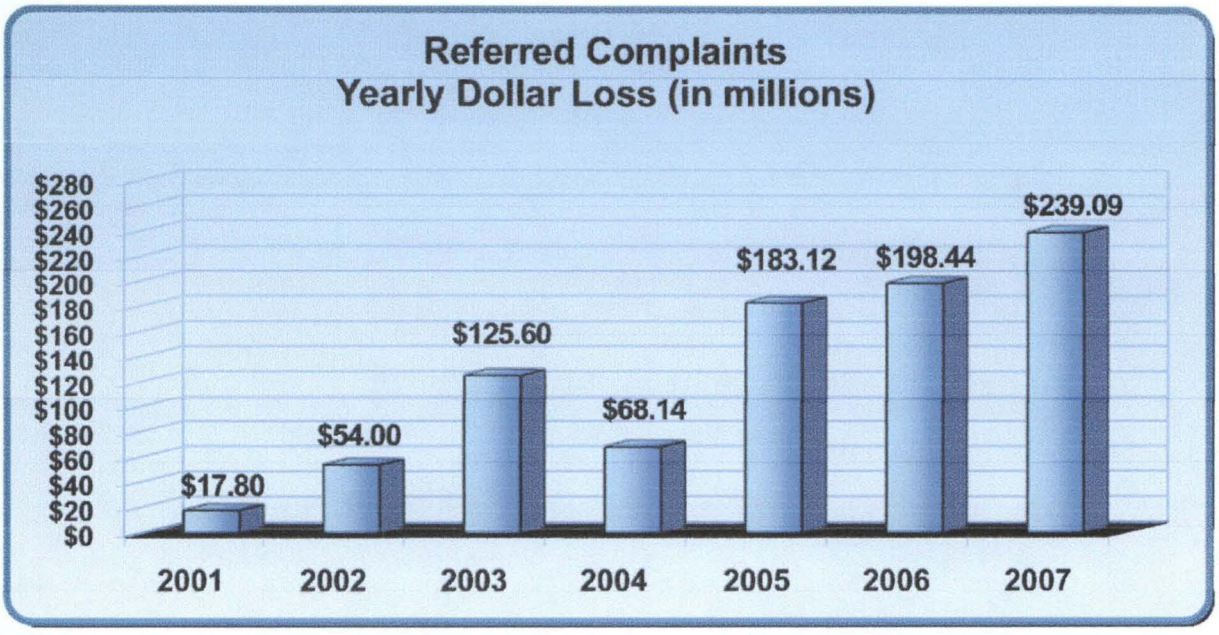

Fig.3.3 Yearly loss in dollar

The number of referred complaints has increased slightly from 86,279 in 2006 to 90,008 in 2007 (see Fig.3. 4). The 116,876 complaints that were not directly referred to law enforcement are accessible to law enforcement, used in trend analysis, and also help provide a basis for future outreach events and

educational awareness programs. Typically, these complaints do not represent dollar loss but provide a picture of the types of scams that are emerging via the Internet. These complaints in large part are comprised of fraud involving reshipping, counterfeit checks, phishing, etc.

During 2007, there were 219,553 complaints processed on behalf of the complainants. This total includes various crime types, such as auction fraud, non-delivery, and credit/debit card fraud, other criminal complaints as well as non-fraudulent complaints, such as computer intrusions, spam, and child pornography.

The results contained in this report were based on information that was provided to IC3 through the complaint forms submitted online at www.ic3.gov or www.ifccfbi.gov by complainants; however, the data represents a sub-sample comprised of those complaints referred to law enforcement. While IC3's primary mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime, those complaints involving more traditional methods of contact (e.g., telephone and mail) were also referred. Using information provided by the complainants, it is estimated that over 90% of all complaints were related to the Internet or online service. Criminal complaints were referred to law enforcement and/or regulatory agencies based on the residence of the subject(s) and victims(s). In 2007, there were 1 Memorandums of Understanding (MOUs) from non-NW3C member agencies added to the IC3

database system and an additional 12 NW3C member agencies added to the database.2007 Internet Crime Report.

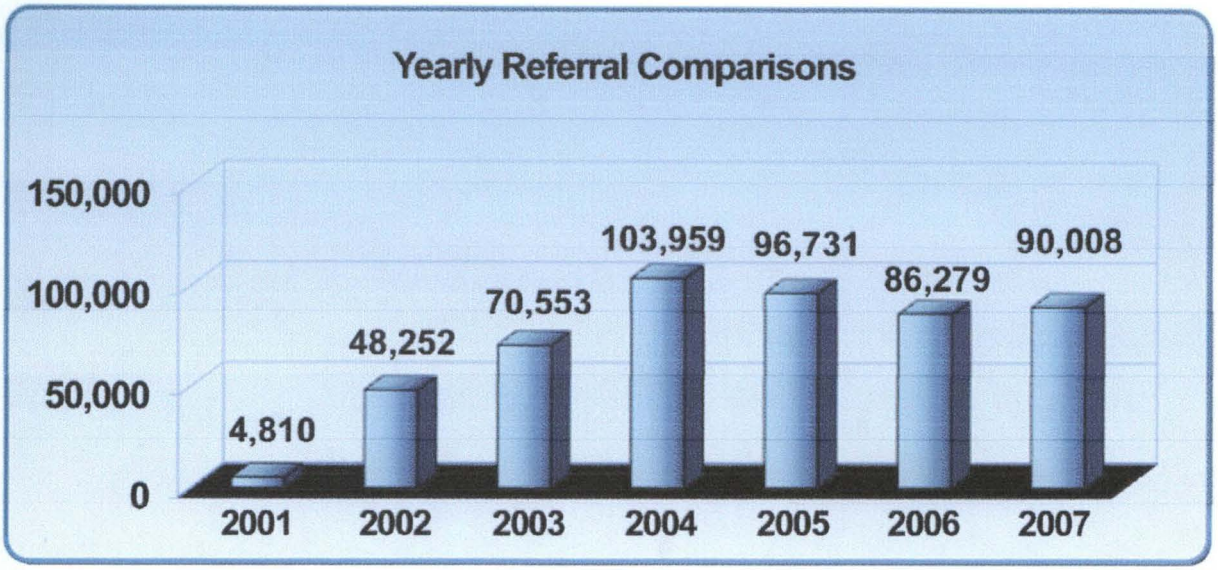

Fig.3.4 yearly referral comparisons

During 2007, Internet auction fraud was by far the most reported offense, comprising 35.7% of referred crime complaints. This represents a 20.5% decrease from the 2006 levels of auction fraud reported to IC3. In addition, during 2007, the non-delivery of merchandise and/or payment represented 24.9% of complaints (up 31.1% from 2006). Confidence fraud made up an additional 6.7% of complaints (see Fig. 3.5). Credit and debit card fraud, check fraud, and computer fraud complaints represented 17.6% of all referred complaints. Other complaint categories such as identity theft, financial institutions fraud, threats, and Nigerian letter fraud complaints together represented less than 8.3% of all complaints.

Statistics contained within a complaint category must be viewed as a snapshot which may produce a misleading picture due to the perception of consumers and how they characterize their particular victimization within a broad range of complaint categories. It is important to realize IC3 has actively sought support from many key Internet E-Commerce stake holders. As part of these efforts, many of these companies, such as eBay, have provided their customers with links to the IC3 website. As a direct result, an increase in referrals depicted as auction fraud has emerged.

Through its relationships with law enforcement and regulatory agencies, IC3 continues to refer specific fraud types to the agencies with jurisdiction over the matter. Complaints received by IC3 included confidence fraud, investment fraud, business fraud, and other unspecified frauds. Identity theft complaints are referred to the Federal Trade Commission (FTC) and also are being addressed by other agencies. Nigerian letter fraud or 419 scams are referred to the United States Secret Service (USSS) in addition to other agencies. Compared to 2006, there were slightly higher reporting levels of all complaint types, except for auction fraud and investment fraud, in 2007. For a more detailed explanation of complaint categories used by IC3, refer to Appendix I at the end of this report.

A key area of interest regarding Internet fraud is the average monetary loss incurred by complainants contacting IC3. Such information is valuable because it provides a foundation for estimating average Internet fraud losses in the general population. To present information on average losses, two forms of

averages are offered: the mean and the median. The mean represents a form of averaging familiar to the general public: the total dollar amount divided by the total number of complaints. Because the mean can be sensitive to a small number of extremely high or extremely low loss complaints, the median also is provided. The median represents the 50th percentile, or midpoint, of all loss amounts for all referred complaints. The median is less susceptible to extreme cases, whether the loss is high or low.

Of the 90,008 fraudulent referrals processed by IC3 during 2007, 72,226 involved a victim who reported a monetary loss. Other complainants who did not file a loss may have reported the incident prior to victimization (e.g., received a fraudulent business investment offer online or in the mail), or may have already recovered money from the incident prior to filing (e.g., zero liability in the case of credit/debit card fraud). Other referrals that do not have a dollar loss such as child pornography are sent to the National Center for Missing and Exploited Children, terrorist tips are sent to PACU and threats which are referred to state and local law enforcement.

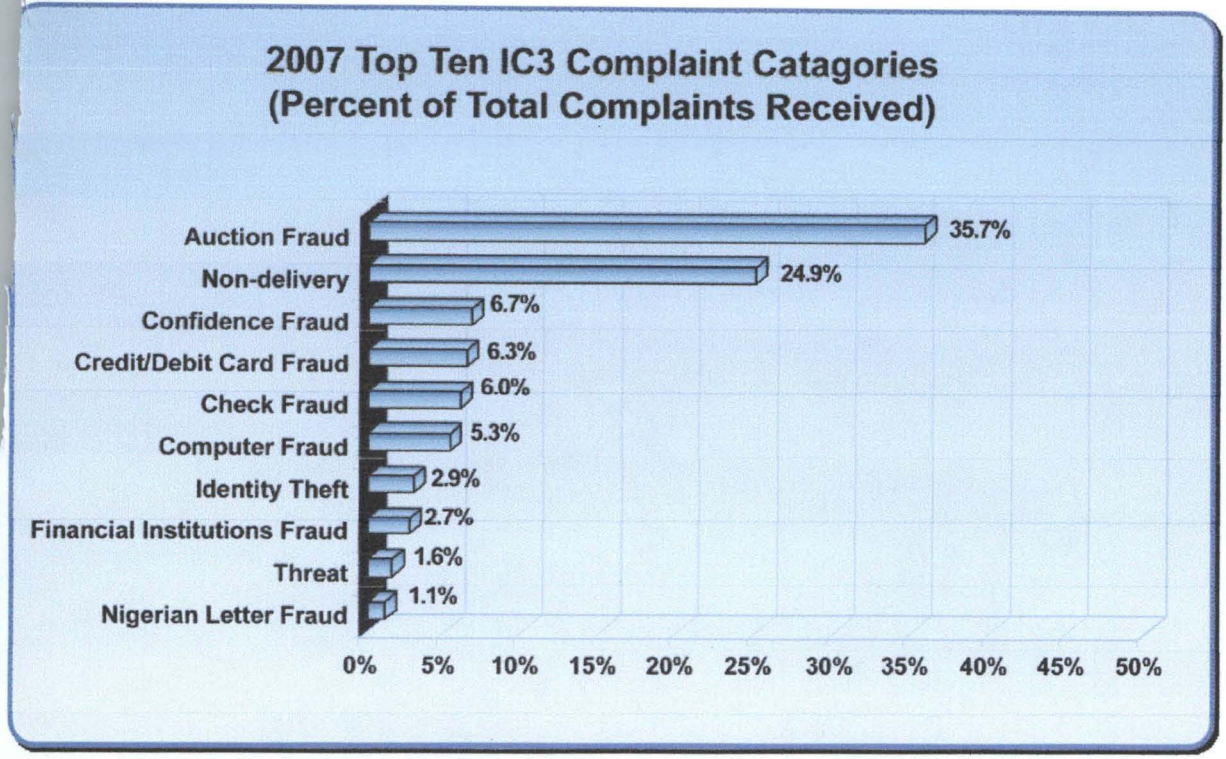

Fig.3.5Complaint Characteristics

A key area of interest regarding Internet fraud is the average monetary loss incurred by complainants contacting IC3. Such information is valuable because it provides a foundation for estimating average Internet fraud losses in the general population. To present information on average losses, two forms of averages are offered: the mean and the median. The mean represents a form of averaging familiar to the general public: the total dollar amount divided by the total number of complaints. Because the mean can be sensitive to a small number of extremely high or extremely low loss complaints, the median also is provided. The median represents the 50th percentile, or midpoint, of all loss amounts for all referred complaints.. The median is less susceptible to extreme cases, whether the loss is high or low.

For details (see Fig.3.6). A typical example is the fraud victims, with a median loss of $3,000.00 and Nigerian letter fraud (median loss of $1,922.99) were other high dollar loss categories. The lowest dollar loss was associated with credit/debit card fraud (median loss of $298.00).

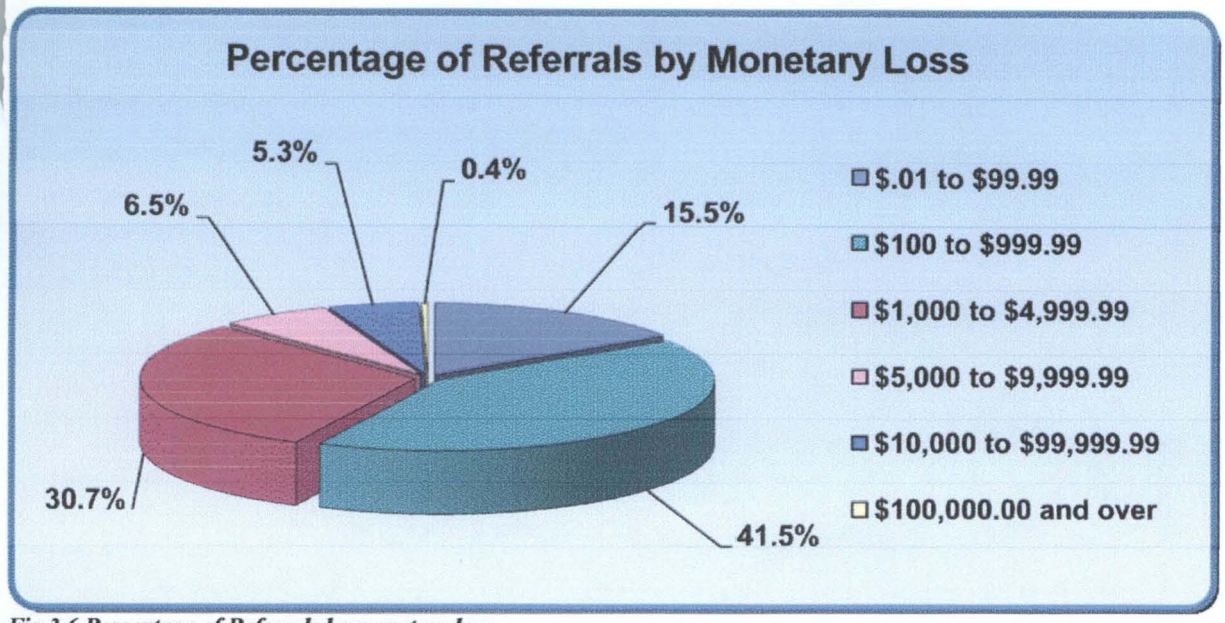

Fig.3.6 Percentage of Referrals by monetary loss

The highest dollar loss per incident was reported by Investment Fraud (median loss of $3,547.94). Check fraud victims, with a median loss of $3,000.00 and Nigerian letter fraud (median loss of $1,922.99) were other high dollar loss categories. The lowest dollar loss was associated with credit/debit card fraud (median loss of $298.00).

Amount Lost by Selected Fraud Type for Individuals Reporting Monetary Loss

Complaint Type	% of Reported Total Loss	Of those who reported a loss the Average (median) $ Loss per Complaint
ıvestment Fraud	6.1%	$3,547.94
Check Fraud	9.9%	$3,000.00
Nigerian Letter Fraud	6.4%	$1,922.99
Confidence Fraud	12.6%	$1,200.00
Auction Fraud	22.4%	$483.95
Non-delivery (merchandise and payment)	17.8%	$466.00
Credit/Debit Card Fraud	4.6%	$298.00

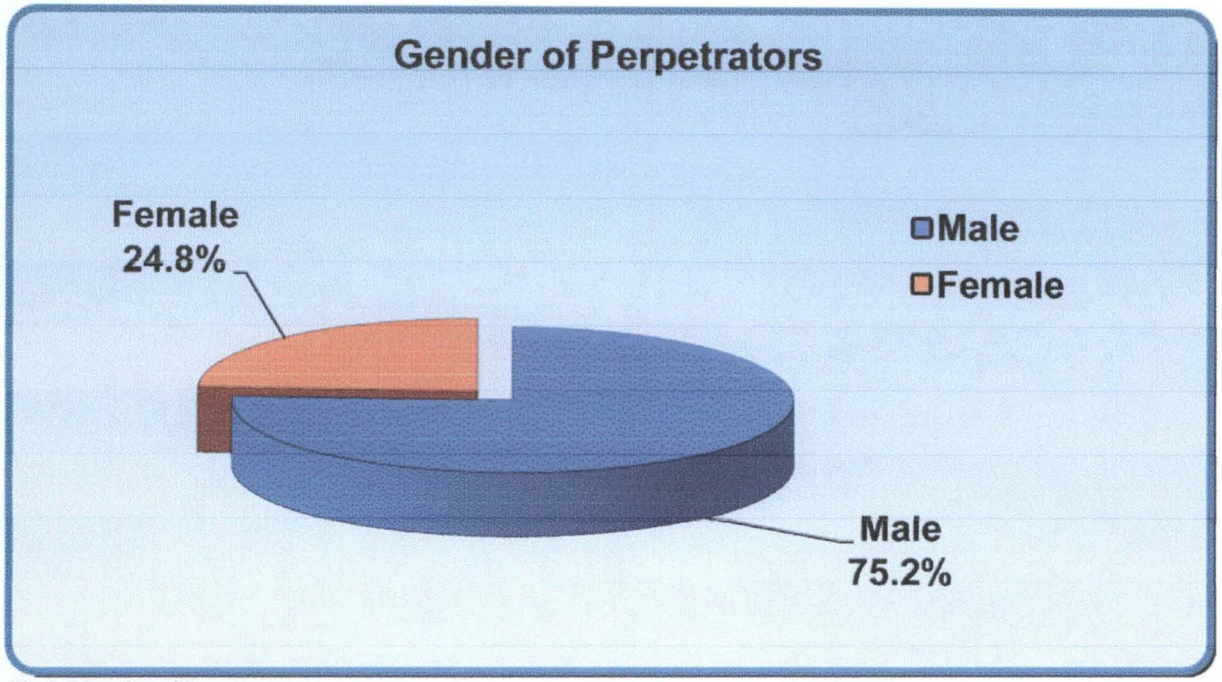

Fig.3.7Gender of Perpetrators

Equally important to presenting the prevalence and monetary impact of Internet fraud is providing insight into the demographics of fraud perpetrators. In those cases with a reported location, over 75% of the perpetrators were male and over half resided in one of the following states: California, Florida, New York, Texas, Illinois, Pennsylvania, and Georgia (see Fig.3.7). These locations are

among the most populous in the country. Perpetrators also have been identified as residing in United Kingdom, Nigeria, Canada, Romania, and Italy (see Map 3.1). Interstate and international boundaries are irrelevant to Internet criminals. Jurisdictional issues can impede investigations due to issues with multiple victims, multiple states/countries, and varying dollar loss thresholds used for initiating investigations.

Map 3.1

Top Ten Countries by Count (Perpetrators)

1. United States 63.2%

2. United Kingdom 15.3%

3. Nigeria 5.7%

4. Canada 5.6%

5. Romania 1.5%

6. Italy 1.3%

7. Spain 0.9%

8. South Africa 0.9%

9. Russia 0.8%

10. Ghana 0.7%

Source: IC3 Report for the year 2007

CHAPTER FOUR

Program Overviews

4.1 Introduction

This section seek to analyze the front-end programming (visual Basic 6.0) and the Back-end database (Microsoft Access) used to demonstrate a typical intrusion method called **"SQL INJECTION".** Data access pages to view, update, or analyze the database's data from the Internet or an internet. Stored data once in one table, but view it form multiple location. When you update the data, it automatically updates everywhere it appears.

4.2 SQL Injection:

SQL Injection is one of the many application and web attack mechanisms used by hackers to steal data from organizations. It is perhaps one of the most common application layer attack techniques used today. It is the type of attack that takes advantage of improper coding of your web applications that allows hacker to inject SQL commands into say a login form to allow them to gain access to the data held within your database. In essence, SQL injection arises because the field available for user input (sallow) SQL statement to pass through and query the database directly.

Web applications allow legitimate website visitors to submit and retrieved data to/from a database over the Internet using their preferred web browser. Databases are central to modern websites – they store data needed for websites

to deliver specific content to visitors and render information to customers, suppliers, employees and a host of stakeholders. User credentials, financial and payment information, company statistics may all be resident within a dataset and accessed by legitimate users through off the shelf and custom web applications. Web applications and database allow you to regularly run your business. SQL Injection is the hacking technique which attempts to pass SQL commands (statements) through web applications for execution by the backend database. If not sanitized properly, web applications may result in SQL injection attacks that allow hackers to view information from the database and /or even wipe it out. Such features as login pages, support and product request forms, feedback forms, search pages shopping carts and the general delivery of dynamic content, shape modern websites and provide businesses with the means necessary to communicate with prospect and customers. These website features are all examples of web applications which may be either purchased off-the shelf or developed as bespoke programs. These website features are all susceptible to SQL Injection attacks which arise because the fields available for user input allow SQL statements to pass through and query the database directly.

Take a simple login page where a legitimate user would enter his username and password combination to enter a secure area to view his personal details or upload his comments in a forum. When the legitimate user submits his details an SQL query is generated from these details and submitted to the databases for

verification. If valid, the user is allowed access. In other words, the web application that controls the login page will communicate with the database through a series of planned commands so as to verify the username and password combination. On verification the legitimate user is granted appropriate access.

Through SQL Injection, the hacker may input specifically crafted SQL commands with the intent of bypassing the login from barrier and assign what lies behind it. This is only possible if the inputs are not properly sanitized (i.e invulnerabilities provide the means for a hacker to communicate directly to the database).

The technologies vulnerable to this attack are dynamic script language including ASP, ASP, NET, PHP, JSP, and CGI. All an attacker needs is, to perform an SQL Injection hacking attack to a web browser, knowledge of SQL queries and creative guess work to important table and field names. The sheer simplicity of SQL Injection has fuelled its popularity.

In SQL Injection, the hacker uses SQL queries and creativity to get to the database of sensitive corporate data through the application. SQL or Structure Query Language is the computer language that allows you to store, manipulate, and retrieved data stored in a relational database (or a collection of tables which

organize and structure data). SQL is in fact, the only way that a web application (and users) can interact with the database.

Examples of relational database include **Oracle, Microsoft Access, MS SQL Server, MySQL,** and **Filemaker Pro**. All of which use SQL as their basic building blocks.

SQL commands include SELECT, INTENRET, DELETE and DROP TABLE

DROP TABLE is as ominous as it sounds and in fact will eliminate the table with a particular name.

In the legitimate scenario of the login page example above, the SQL commands planned of web application may look like the following.

SELECT count (*) a

FRM users list table

WHERE username= FIELD_ USERNAME AND password = FIELD _ PASSWORD"

In plain English, this SQL command (from the application) instructs the database to match the username and password input by the legitimate user to the combination it has already stored. Each type of application is hard coded with specific SQL queries that it will execute when performing its legitimate

functions and communicating with the database. If any input field of the web application is not properly sanitized, a hacker may inject additional SQL commands that broaden the range of SQL commands the web application will execute, this going beyond the original intended design and function. A hacker will thus have a clear channel of communication (or, in layman terms, a tunnel) to the database irrespective of all the intrusion detection system and network security equipment installed before the physical database server.

CHAPTER FIVE

CONCLUSION AND RECOMMNEDATIONS

5.1Summary

The IC3 report has outlined many of the current trends and patterns in Internet crime. The data indicates that fraud is increasing; however, reported complaints remained relatively level with 206,884 complaints in 2007, down from 207,492 complaints in 2006, 231,493 complaints in 2005, and 207,449 complaints in 2004. This total includes many different fraud types, non-fraudulent complaints, as well as complaints of other types of crime. Yet, research indicates that only one in seven incidents of fraud ever make their way to the attention of enforcement or regulatory agencies. The total dollar loss from all referred cases of fraud was $239.09 million in 2007 up from $198.44 million in 2006.

Internet auction fraud again was the most reported offense followed by non-delivered merchandise/payment and confidence fraud. Among those individuals who reported a dollar loss from the fraud, the highest median dollar losses were found among investment fraud victims ($3,547), check fraud victims ($3,000), and Nigerian letter fraud victims ($1,922). Male complainants reported greater losses than female complainants, which may be a function of both online purchasing differences by gender and the type of fraud. Comparing data from the 2006 and the 2007 reports, e-mail and web pages were still the two primary mechanisms by which the fraudulent contact took place.

Although this report can provide a snapshot of the prevalence and impact of Internet fraud, care must be taken to avoid drawing conclusions about the "typical" victim or perpetrator of these types of crimes. Anyone who utilizes the Internet is susceptible, and IC3 has received complaints from both males and females ranging in age from ten to one hundred years old. Complainants can be found in all fifty states, in dozens of countries worldwide, and have been affected by everything from work-at-home schemes to identity theft.

5.2 Conclusion

It is true that many e-crimes of the future will be traditional crimes simply perpetrated via or facilitated through the use of ICT. However, as indicated above, there are characteristics of electronic crime, such as anonymity, speed the ease with which one can participate in unlawful behavior and the potential for large scale victimizations that will present new and unique challenges. The ability to move quickly to preserve data and to get around encryption will also require new response.

Computer Crime (E-Crime) is truly a global issue and there will be an unprecedented need for international coordination and cooperation. An example of innovative response in this area is a recently announced initiative in relation to dealing with cross-border Internet fraud and improving consumer confidence in e-commerce. A response to computer crime will involve much stronger

partnerships with the private sector and other law enforcement and related agencies (s8uch as defense and intelligence) and a major thrust of addressing the issue must be one of prevention, otherwise policing will simply be overwhelming. It will also be important to understand the nature of the problem and to address the significant underreporting of the phenomenon.

New skills, technologies and investigative techniques will be required to detect, prevent and respond to electronic crime. This is not just about a realignment of existing effort. This new business will be characterized by new forms of crime, a far broader scope and scale of offending and victimization, and challenging technical and legal complexities. Innovative response such as the creation of cyber cops' 'cyber courts' and 'cyber judges' may eventually be required to overcome the significant jurisdictional issues.

It is clear that much more needs to be done to enhance our capacity to respond to incidents of computer crime, both nationally and internationally. Managing the response to and the investigation of such crime will indeed be complex and challenging. The police commissioner's Conference E-crime Strategy provides a valuable framework and set of guiding principles to fashion a range of new response.

Finally, Computer crime cost businesses millions of pounds every year. Companies continue to be ruined by malicious attacks, often from totally

unexpected quarters. Your company's data is its lifeblood. You need to be aware of the potential problems and have contingency plans in place to guard against attack.

5.3 Recommendation

"Essentially, cybercrime is information and intelligence- based activity. You cannot fight cybercrime with ignorance, strong directives or boastful talk". The first effort should be at user awareness of computer security among homes as well as businesses. In a study, respondents rated computer security as a high priority but over half admitted to little or no knowledge of safe practices. Although seventy five percent (75%) had a firewall, eighty-six percent (86%) did not follow recommendations to update their security software.

Understand as much as possible about how Internet auctions work, what your obligations are as a buyer, and what the seller's obligations are before you bid.

Find out what actions the website takes if a problem occurs and consider insuring the transaction and shipment.

Do not allow the seller or buyer to convince you to ignore the rules of a legitimate Internet auction website or exit the auction website to complete a transaction.

Do not invest in anything based upon appearances. Just because an individual or company has a flashy website doesn't mean it is legitimate. Web sites can be

created in just a few days. After a short period of taking money, a site can vanish without a trace.

Do not invest in anything about which you are not absolutely sure. Do your homework on the investment to ensure that it is legitimate.

Thoroughly investigate the individual or company to ensure that they are legitimate.

Don't give out your credit card or ATM number(s) online unless the website is both secure and reputable. Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. This icon is not a guarantee of a secure site, but may provide you some assurance.

Before using a site, check out the security software it uses to make sure that your information will be protected.

Make sure you are purchasing merchandise from a reputable/legitimate source.

Once again investigate the person or company before purchasing any products.

REFERENCES

Annual CSI/FBI computer crime and security survey (2002-2006): Computer Security Institute, and Federal Bureau of Investigation Computer Intrusion Squad.

Australian computer crime and security survey (2002-2006): AusCERT, AHTCC and Australian police agencies.

EFCC Journal on International Conference on Computer Crime (2007)

Fraud and technology crimes: findings from the 2002/03 British crime Survey and 2003 Offending, Crime and Justice Survey Jonathan Allen, Sarah Forest, Michael Levi, Hannah Roy, Michael Sutton, Debbie Wilson. Home Office, 2005.

Internet Crime Complaint Center annual reports(2005): Federal Bureau of Investigation and National White Collar Crime Center.

Cyber crime against businesses Rantana R Rantala(2004): Bureau of Justice Statistics technical report.

Information Security Branches Survey(2006): An Federal Bureau of Investigation (FBI) Journal vol. 06 page 803.

Clive Carmichael-Jones(2006):Investigating Computer Crime in the 21st Century.

Appendix 1
Complainant/Perpetrator Statistics, by State Complainants by State

Rank	State	Percent	Rank	State	Percent
1	California	14.4	27	South Carolina	1.2
2	Florida	7.2	28	Louisiana	1.1
3	Texas	7.2	29	Connecticut	1.0
4	New York	5.7	30	Kentucky	1.0
5	Pennsylvania	3.6	31	Utah	1.0
6	Illinois	3.5	32	Oklahoma	0.9
7	Ohio	3.1	33	Kansas	0.8
8	Washington	3.1	34	Arkansas	0.8
9	New Jersey	3.1	35	Iowa	0.7
10	Virginia	2.9	36	New Mexico	0.6
11	Michigan	2.8	37	Idaho	0.5
12	Arizona	2.8	38	Mississippi	0.5
13	Georgia	2.6	39	West Virginia	0.5
14	Maryland	2.6	40	New Hampshire	0.5
15	North Carolina	2.6	41	Hawaii	0.5
16	Colorado	2.5	42	Nebraska	0.4
17	Indiana	2.0	43	Maine	0.4
18	Massachusetts	2.0	44	Montana	0.3
19	Missouri	1.9	45	Rhode Island	0.3
20	Tennessee	1.8	46	District of Columbia	0.3
21	Oregon	1.7	47	Delaware	0.3
22	Wisconsin	1.6	48	Vermont	0.2
23	Minnesota	1.6	49	Wyoming	0.2
24	Alaska	1.4	50	South Dakota	0.2
25	Alabama	1.2	51	North Dakota	0.1
26	Nevada	1.2			

Complainant/Perpetrator Statistics, by State Perpetrators by State

Rank	State	Percent	Rank	State	Percent
1	California	15.8	27	Connecticut	1.0
2	Florida	10.1	28	Kentucky	1.0
3	New York	9.9	29	South Carolina	0.9
4	Texas	7.0	30	Oklahoma	0.8
5	Illinois	3.6	31	District of Columbia	0.8
6	Pennsylvania	3.5	32	Louisiana	0.7
7	Georgia	3.1	33	Kansas	0.7
8	Ohio	2.8	34	Maine	0.5
9	Washington	2.8	35	Iowa	0.5
10	New Jersey	2.8	36	Nebraska	0.5
11	Michigan	2.5	37	Arkansas	0.5
12	Arizona	2.4	38	Delaware	0.5
13	Nevada	2.3	39	New Hampshire	0.4
14	North Carolina	2.0	40	Rhode Island	0.4
15	Virginia	1.9	41	New Mexico	0.4
16	Indiana	1.7	42	Mississippi	0.4
17	Colorado	1.7	43	idaho	0.3
18	Maryland	1.7	44	West Virginia	0.3
19	Massachusetts	1.6	45	Montana	0.3
20	Missouri	1.5	46	Hawaii	0.3
21	Tennessee	1.4	47	Alaska	0.3
22	Utah	1.3	48	Wyoming	0.2
23	Wisconsin	1.2	49	Vermont	0.2
24	Minnesota	1.2	50	South Dakota	0.2
25	Alabama	1.2	51	North Dakota	0.1
26	Oregon	1.1			

Complainant/Perpetrator Statistics, by State Complainants per 100,000 people

Rank	State	Per 1,000	Rank	State	Per 1,000
1	Alaska	356.41	27	Connecticut	53.48
2	Colorado	90.65	28	Minnesota	53.35
3	Washington	86.76	29	New York	52.74
4	Maryland	83.39	30	Pennsylvania	52.23
5	Nevada	81.90	31	Tennessee	51.11
6	Oregon	79.41	32	Kansas	51.08
7	Arizona	78.58	33	North Carolina	51.04
8	District of Columbia	78.19	34	Delaware	50.88
9	Florida	71.18	35	Rhode Island	50.58
10	California	70.87	36	West Virginia	50.39
11	Virginia	68.33	37	Wisconsin	49.81
12	Utah	66.46	38	Michigan	49.71
13	New Hampshire	65.66	39	Georgia	49.36
14	Wyoming	65.03	40	Illinois	48.35
15	New Jersey	63.94	41	Arkansas	47.76
16	Idaho	63.23	42	South Carolina	47.55
17	Hawaii	63.11	43	Alabama	46.50
18	Ohio	62.24	44	Louisiana	45.91
19	Montana	59.51	45	Nebraska	44.01
20	Vermont	58.02	46	Oklahoma	43.04
21	Missouri	57.60	47	Kentucky	42.86
22	Maine	56.10	48	Iowa	42.76
23	Indiana	55.33	49	South Dakota	37.30
24	Massachusetts	54.25	50	North Dakota	35.17
25	Texas	54.04	51	Mississippi	32.10
26	New Mexico	53.56			

Complainant/Perpetrator Statistics, by State Perpetrators per 100,000 people

Rank	State	Per 1,000	Rank	State	Per 1,000
1	District of Columbia	99.10	27	Massachusetts	19.66
2	Nevada	65.45	28	Missouri	19.24
3	Delaware	41.98	29	Indiana	19.05
4	Florida	40.73	30	Alabama	18.99
5	New York	38.06	31	Hawaii	18.86
6	Utah	36.40	32	Virginia	18.45
7	Washington	31.96	33	Kansas	18.19
8	California	31.87	34	Michigan	18.12
9	Alaska	28.53	35	Ohio	18.09
10	Rhode Island	28.45	36	Tennessee	17.25
11	Arizona	27.99	37	Kentucky	17.23
12	Maine	27.63	38	Minnesota	16.95
13	Colorado	25.84	39	North Carolina	16.54
14	Montana	25.16	40	South Carolina	15.79
15	Georgia	24.25	41	Oklahoma	15.79
16	New Jersey	23.44	42	Idaho	15.67
17	Vermont	22.86	43	Wisconsin	15.37
18	Maryland	21.64	44	North Dakota	15.16
19	Texas	21.53	45	New Mexico	14.67
20	Oregon	21.43	46	South Dakota	13.56
21	Pennsylvania	20.94	47	Arkansas	11.92
22	New Hampshire	20.90	48	West Virginia	11.92
23	Wyoming	20.85	49	Louisiana	11.67
24	Illinois	20.70	50	Iowa	11.58
25	Connecticut	20.39	51	Mississippi	8.77
26	Nebraska	20.17			

Journal on International Conference on Internet Crimes (2006):

The Home Office, Fraud and Technology Crimes(2006): Findings from the British Crime Survey 2003/04, the 2004 offending crime and Justice Survey and administrative sources.

Unpublished presentation Cyber crime issues in Nigeria by Nuhu Ribadu(2006): (EFCC former Chairman), Nigeria.

Internet crime report(2007): Prepared by The National White Collar Crime Center Bureau of Justice assistance, Federal Bureau of Investigation, USA.

www.parliament.uk/parliamnetary_offices/post/pubs2006.cfm.

www.e-crimecongress.org

E-crime watch survey results CSO magazine(2005): US Secret Service and CERT Coordination Center.