Cyber Crime: Practices and Policies for Its Prevention

Ajeet Singh Poonia
Department of Computer Science and Engineering
College of Engineering and Technology, Bikaner, India.
pooniaji@gmail.com

Dr. Awadesh Bhardwaj
Department of Management Studies
Malviya National Institute of Technology, Jaipur, India.
awbh2001@gmail.com

Dr. G. S. Dangayach
Department of Mechanical Engineering
Malviya National Institute of Technology, Jaipur, India.
dangayach@gmail.com

Abstract- Cyber civilization considers knowledge as an integral part of society and human systems. With the facilities of cyber civilization the evils of cyber civilization also need to be equally tackled through technological as well as social means. The phenomenal growth of computers and Internet services has engendered the problem of cyber crime proliferation on the account of investigation difficulties and lack of strong evidences further, existing laws and preventive measures are not effective to curb such crimes. So to cope up with the situation we have to modify the old policies and practices to meet our security needs. Also we can see that the crimes are coming in new forms embedded with new technologies, which is very difficult to investigate with the available resources. To stand with them we need a hi-tech technology enabled security system and investigators along with the awareness among the common man, as today’s crime have no defined boundaries.

Keywords- Cyber civilization, Cyber crime, cyber ethics, cyber world

I. INTRODUCTION

Cyber crime is different from Conventional crime (“a legal wrong that can be followed by criminal proceedings which may result into punishment.”(1)). Cyber crime is the latest and perhaps the most complicated problem in the cyber world. It is defined as “Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime” (2) A generalized definition of cyber crime may be “ unlawful acts wherein the computer is either a tool or target or both”(3) .Cybercrime is also substantially different from computer crime. It's like the difference between people who use computers for all they can be versus people who use computers as a tool like a typewriter. Cyber crime is hard to detect, thus giving the perpetrators plenty of time to flee the area in which the crime was committed, because of this fact the criminals can be in another country far away from the scene of the crime by the time it is detected. Computer is a major source for cyber crime. Cyber crime is any illegal activity arising from one or more Internet components. Cybercrime can include everything from non-delivery of goods or services and computer intrusions to
intellectual property rights abuses, economic espionage, online extortion, international money laundering, and a growing list of other Internet-facilitated offenses. Further, it is not easy to identify immediately about the crime method used, and to answer questions like where and when it was done.

II. WHAT’S DIFFERENT ABOUT CYBER CRIME?

Cyber crimes—harmful acts committed from or against a computer or network—differ from most terrestrial crimes. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.

Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their “virtual” counterparts. Web pages such as the ecommerce sites recently hit by widespread, distributed denial of service attacks may not be covered by outdated laws as protected forms of property.

A. Types of Cyber Crime

Cyber Crime comes in many forms and in many ways. Below mentioned are the different types of Cyber crime:

1) Communications in Furtherance of Criminal Conspiracies

Just as legitimate organizations use the information networks for record keeping and communication, so too are the activities of criminal organizations enhanced by the advent of information technology. There is evidence of information systems being used in drug trafficking, gambling, money laundering and weapons trade just to name a few.

2) Telecommunications Piracy

Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. This has produced the temptation to reproduce copyrighted material either for personal use or for sale at a lower price.

3) Electronic Money Laundering

For some time now electronic funds transfers have assisted in concealing and moving the proceeds of crime. Emerging technologies make it easier to hide the origin and destination of funds transfer. Thus money laundering comes to the living room.

4) Electronic Vandalism and Terrorism

All societies in which computers play a major role in everyday life are vulnerable to attack from people motivated by either curiosity or vindictiveness. These people can cause inconvenience at best and have the potential to inflict massive harm.

5) Sales and Investment Fraud

As electronic commerce or e-commerce as it is called becomes more and more popular, the application of digital technology to fraudulent crime will become that much greater.

6) Illegal Interception of Information

Developments in telecommunications as well as data transfer over the net have resulted in greater speed and capacity but also greater vulnerability. It is now easier than ever before for unauthorized people to gain access to sensitive information.

7) Cyber Pornography

Spread of Child pornography and sexually explicit material.

8) Information Piracy and Forgery

Digital technology permits perfect reproduction of the original documents, examples are birth certificates, passport, false identity, counterfeiting of currency, negotiable instruments etc.

9) Hacking

Information theft from computers hard disk, removal storage etc. Data theft, data destroy, stealing and altering information.
10) Internet time thefts

By stealing user name and password, criminals use for themselves and steal the internet time allotted to the purchaser.

11) Hate/Communal Crimes

As building a web page is not expensive and reaches to billions of people, criminals spread hate or communal information or rumours, by building a website and also recruits people for their operation through advertisement.

12) Altering Websites

The hacker deletes some pages of a website, uploads new pages with the similar name and controls the messages conveyed by the web site.

B. Penetration methods of Cyber crime

There are various methods through which the crime is penetrated into the computer, network, hardware, software or in your cell phone. They are:

1) Unauthorized access

Unauthorized access also known as cracking as opposed to hacking, means gaining access to a system without permission of the users or without proper authority. This is generally done either by fake identity, or by cracking access codes.

2) E-mail bombing

This means sending a large number of mails to the victim resulting in the victims mail account (in case of individual) or server (in case of corporations) crashing.

3) Data diddling

This kind of attack involves altering the raw data before it is processed by a system and re-altering it after processing.

4) Salami attack

This is generally used to commit financial crimes. Here the key is to make the alteration so small that in a single case it would go unnoticed. For example a bank employee deducts five rupees from every customers account. The individual customers are unlikely to notice this small change but the employee will make a significant earning.

5) Logic Bomb

This is an event dependent program. This implies that this program is created to do something only when a certain event occurs.

6) Virus/Worm attack

A virus is a program, which attaches itself to another file or a system and then circulates to other files and to other computers via a network. They usually affect computers by either altering or deleting data from it. Worms on the other hand do not interfere with data. They simply multiply until they fill all available space on the computer.

7) Trojan attack

A Trojan is a program, which appears to be something useful but under the disguise of a useful program causes some damage.

8) Denial of service attack

This involves flooding the computer resource with more requests than it can handle. This causes the resource to crash, thereby denying the authorized users the service.

9) Distributed denial of service

This is a denial of service attack in which the perpetrators are more than one in number and geographically displaced. It is very difficult to control such attacks.

10) E-mail spoofing

A spoofed email is one, which appears to originate from one source but actually originates from another.

11) Phishing

In a typical phishing scam, phishers send out emails which appear to come from a legitimate company, in an attempt to scam users into providing private information that will be used for identity theft. Phishers use a variety of sophisticated devices to steal information—including pop-up windows,
URL masks which simulate real Web addresses, and keystroke loggers that capture what you type, such as account names and passwords.

12) Pharming

It is an attempt to defraud Internet surfers by hijacking a Web site’s domain name, or URL, and redirecting users to an imposture Web site where fraudulent requests for information are made.

III. TOOLS AND TECHNIQUES USED IN CYBER CRIME

Unauthorized Access is the main tool used by Criminals. Following are the common techniques used for unauthorized access.

1. Port Scanner

A port scan is a method used by hackers to determine which ports are open or in use on a system or network. By using various tools a hacker can send data to TCP or UDP ports one at a time. Based on the response received the port scan utility can determine if that port is in use. Using this information the hacker can then focus their attack on the ports that are open and try to exploit any weaknesses to gain access.

2. Packet Sniffing

Packet sniffing is the act of capturing packets of data flowing across a computer network. The software or device used to do this is called a packet sniffer. Packet sniffing is to computer networks what wire tapping is to a telephone network. Packet sniffing has legitimate uses to monitor network performance or troubleshoot problems with network communications.

3. Password Cracking

All systems cache, passwords in memory during, login session. Therefore, if a hacker can gain access to all memory on the system, he can likely sift the memory for passwords. Likewise, hackers can frequently sift page files for passwords. To crack a password means to decrypt a password, or to bypass a protection scheme. Another form of password cracking attack is all possible combinations of letters, numbers and symbols are tried out one by one, till the password is found out.

4. Buffer Overflow

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user’s file, change data, or disclose confidential information. As the excess data “overflows” into other areas of the computer’s memory. This allows the hacker to insert executable code along with the input, thus enabling the hacker to break into the computer.

5. Keylogger

Keylogger is a software program or hardware device that is used to monitor and log each of the keys a user types into a computer keyboard. The user who installed the program or hardware device can then view all keys typed in by that user. Because these programs and hardware devices monitor the keys typed in a user can easily find user passwords and other information a user may not wish others to know about.

IV. CAUSE OF CYBER CRIME

1) Capacity to store data in comparatively small space

The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier.

2) Easy to access

The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not
due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

3) Complex

The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

4) Negligence

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

5) Loss of evidence

Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

6) Motivation

Intellectual challenge of mastering complex system was the motivation in the past for criminals, but presently criminals are driven by greed, lust, power, revenge, adventure. The desire to inflict loss or damage or revenge is the present motivation for criminals.

7) Opportunities

Growth of computing abilities in banking, stock exchange, air traffic control, telephones, electric power, health welfare institution and education, has though brought down the cost leading to revolutionary changes in commerce, communications, entertainment and education, and is providing more criminal opportunities owing to few vulnerabilities that exist in information technology.

8) Poor response from Law Enforcing Agencies

Many developing countries lack appropriate law to tackle the cyber crime attackers. Due to this the criminal are far from reach and easily get rid of punishments.

V. CYBER-CRIME INVESTIGATIONS

While most businesses lack the requisite in-house resources and technical know-how to carry out sophisticated cyber-crime investigations, nevertheless, there are some basic steps which they can take to assist the authorities in unravelling these offences. These are as follows:

1) Scope of Losses

The first step in any cyber-crime investigation should be to determine the extent of the loss incurred. Where the financial losses are negligible, but nevertheless distasteful, consideration should be given to other options open to management. This should be done prior to committing resources to any costly and timeconsuming investigation. For example, where an insider is involved, as the case of an unauthorized use, termination is a viable option.

2) Regulatory Directives

Where funds and financial records are involved, banks and other financial institutions are frequently required by governmental mandates to investigate and report their findings to the authorities. A failure to do so could expose the organization to civil and/or criminal sanctions; as well as civil litigation, in the event that customer financial accounts or records are involved.

3) Adverse Publicity

Cyber-crimes have become so pervasive in the corporate sector, as to almost constitute the norm. Nevertheless, their
public disclosure can result in damaging publicity for the corporate victim. Management should consider the necessary steps to minimize any potential damages ensuing from such disclosure(s). This is especially necessary where law requires such disclosures.

4) Prosecuting Cyber-Crime

While every state - and the federal government – have cyber-crime laws on the books, these frequently vary in terms of their scope and the sanctions they impose. While data crimes may result in tough sanctions under some state cyber-crime laws, they may result in little or no penal sanctions in other jurisdictions.

5) Occurrence of Crime

In those cases where a cyber-crime is not current - ‘stale’ is the term the authorities use to describe crimes that occurred months or years in the past, but were only recently discovered - investigating it for purposes of prosecution could prove difficult and bear little fruition. In addition, the evidence may have been destroyed or accidentally erased; witnesses may have left the area, the culprit may prove difficult to locate, etc. Further, the authorities are likely to show little or no interest in prosecuting an offence that is stale; since it will spark little or no interest by the public or the press.

VI. PRACTICES RECOMMENDED FOR CYBER CRIME PREVENTION

Prevention is always better than cure. It is always better to take certain precaution while operating the net.

- Firewalls: These are programs, which protect a user from unauthorized access attacks while on a network. They provide access to only known users, or people who the user permits.
- Frequent password changing: With the advent of multi-user systems, security has become dependent on passwords. Thus one should always keep passwords to sensitive data secure. Changing them frequently and keeping them sufficiently complex in the first place can do this.
- Safe surfing: Safe surfing involves keeping ones e-mail address private, not chatting on open systems, which do not have adequate protection methods, visiting secure sites. Accepting data from only known users, downloading carefully, and then from known sites also minimizes risk.
- Frequent virus checks: One should frequently check ones computer for viruses and worms. Also any external media such as floppy disks and CD ROMS should always be virus checked before running.
- Email filters: These are programs, which monitor the inflow of mails to the inbox and delete automatically any suspicious or useless mails thus reducing the chances of being bombed or spoofed.
- Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
- Always keep back up volumes so that one may not suffer data loss in case of virus contamination
- Never send your credit card number to any site that is not secured, to guard against frauds.
- Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
- It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
- Web site owners should watch traffic and check any irregularity on the site. Putting hostbased intrusion detection devices on servers may do this.
• Web servers running public sites must be physically separate protected from internal corporate network.

• Make Backups of Important Files and Folders to protect important files and records on your computer if your computer malfunctions or is destroyed by a successful attacker?

• Disconnect from internet when not in use.

• Habitually download security protection update patches & Keep your browser and operating system up to date.

• Change administrator’s password from the default password. If the wireless network does not have a default password, create one and use it to protect the network.

• Disable file sharing on computers.

• Turn off the network during extended periods of non-use, etc.

• Check your online account frequently and make sure all listed transactions are valid. Use a variety of passwords, not same for all of your account.

• Never respond to text messages from someone you don't know.

• Never let someone you don't know use your cell phone and avoid posting your cell phone number online.

• Open email attachment carefully

VII. POLICIES RECOMMENDED FOR CYBER CRIME PREVENTION

Other than the practices discussed above, some policies are also recommended for the code of cyber society, to be at safer side. These policies should be bring into practical part so that the practices are easier to implement. Policies recommended are:

• Integrated policies are required to ensure the effective benefits from the Information system. The basic challenge and issue in the development of a cyber society, is the lack of financial and trained human resources.

• A strong education system should be followed in the society to deliver education at every stage of the society with a special stress on Information Technology which should be secure and free from cyber crime and in reach to a common man.

• Promotion of Research & Development in ICTs area and also in Human Resource Development as a core part of the system.

• Up to date, common, and mutually supporting cyber laws should be there to fight with cyber crime and protection of intellectual property rights towards the creation of cyber crime free information society.

• Adoption of ICTs standards, regulation, and quality assurance to foster high quality and secure services and productions that keep competition in place for the benefits of the communities within each country.

• High levels of awareness among the each part of the society should be there in regard to information security and cyber crime and increased exchange of information on information security and cyber crime at the regional and national levels should be there.

• Effective mechanisms should be there for detection and prevention of cyber crime and improving protection against, detection of, and responses to, cyber crime, at the lower level itself.

• Conduct national user awareness campaigns for the general user, including children and young people, educational institutions, consumers, government officials and the private sector, using different media.

• Educate and involve the media professionals, and then encourage them to increase public awareness.
• Engage large private sector corporations and industry associations in the sponsorship of awareness programs.

• Stress should be laid on less developed countries on effective systems, for protection against, detection of and responses to, cyber crime.

• Promote and support the use of filtering, rating, parental control and related software, as well as measures for the establishment of safe environments for the use of the Internet by children.

• Law enforcement personnel must be trained and equipped to address high-tech crimes.

• Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.

• Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.

• Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a 24-hour basis.

• Prevention is better than cure. Awareness raising, education, and technical support to prevent e-crime is essential, but without discouraging the development of e-commerce.

VIII. CONCLUSION

With the information highway having entered our very homes, we are all at increasing risk of being affected by Cybercrime. Everything about our lives is in some manner affected by computers. Under the circumstances its high time we sat up and took notice of the events shaping our destinies on the information highway. Cybercrime is everyone’s problem. There is no doubt that the Internet offers criminals unparalleled opportunities. And its time we did something to protect ourselves. Information is the best form of protection. Concrete measures must be found in order to track electronics evidence, classify the material that needs to be search, and their preservation, so that systems are better protected from cyber intrusions. In addition, new rules and regulations must be developed by law enforcement agencies to address the various families of computer crime

REFERENCES


[3] Duggal Pawan


[12] Rolf H. Webera, Transparency and the governance of the Internet, Computer Law &
Cyber Crime: Practices and Policies for Its Prevention

[13] Ramifications of Cyber Crime and Suggestive Preventive Measures. Jivesh Govil, SJtuvdeesnht GMoevmilb, eSrt,uIdFeEntE M ember, IEEE and Jivika Govil Dept. of Electrical Engineering & Computer Science University of Michigan, Ann Arbor, Michigan, USA jivesh@umich.edu Jivika Govil Dept. of Information Tech. and Computer Science Apeejay College of Engineering, MD University Gurgaon, Haryana, India jivikag@email.com

[14] A Guide To Cyber-Crime Investigations ,August Bequai, Legal Editor, 7921~otws Branch Drive, Suite 133, Mcban, VA 22102, 1JSA.

[15] Cyber Crime Information System for Cyberethics Awareness A.B. Patki S. Lakshminarayanan S. Sivasubramanian S.S. Sarma (Authors are with Department of Information Technology, Government of India) <apatki@mit.gov.in> <sln@mit.gov.in> <siva@mit.gov.in> ssarma@mit.gov.in


[17] Internet crime Cyber Crime – A new breed of criminal? Kit Burden & Creole Palmer, Barlow Lyde & Gilbert