International Journal of Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-8)

Research Article | **August 2015**

Cyber Crime: Issues and Challenges

Kanika Jethwani*, Surbhi Gaur
IT Department, GGSIPU,
Delhi

Abstract—

Cyber Crime refers to the criminal act that deals with computers and networks. This crime is posing the challenges to existing national legal systems and it appears to be difficult to control and deal with these crimes within the existing frame of legal system. Specially, the problem of identity crises, jurisdiction and lack of legal recognition of acts makes it more difficult for legal systems to deal with the crime effectively. The location and trans-national character also makes it more difficult to deal with. This paper will discuss various aspects of Cyber crime including: defining the term, discrepancy among conventional and cyber crime, reasons for cyber crime, types of cyber crime, measures to prevent cyber crime and many more.

Keywords-- Cyber Crime, Hacking, Spoofing, Unauthorized Access, Virus, Worms

I. INTRODUCTION

With the growth in the usage of Internet, securing ones personal information is becoming more difficult. The hard fact is that one's personal details are becoming available at public databases due to interconnections among various people through internet. Due to these interconnections the information is widely available to people throughout the world. Hence, more number of people can easily access one's personal information. This access can be dangerous if one tries to access one's private or confidential information that a person would not like to share.

Though, internet technology has provided us with lot of luxuries and ease for our lives. It has made our lives easier in many ways. With all these luxuries, threats are also attached with it, which is a main disadvantage of this technology. One of the main threats of this technology is Cybercrimes.

Cybercrime is a criminal activity which is done using computers and internet. This can include anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrimes also include non monetary offences, such as network intrusions on other computes or dissemination of computer viruses and posting confidential information on the internet.

The growing list of cybercrimes includes crimes that have been made possible by computers, such as the dissemination of computer viruses and network intrusions and, as well as computer based variations of existing crimes, such as identity theft, stalking, bullying and terrorism. Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the internet to access and steal personal information from other users.

Two most common ways through which this is done is through phishing and pharming. Both these methods lure users to fake websites (that appear to be legitimate), where the users are asked to enter personal information such as credit card numbers, username and passwords, phone numbers, addresses, etc. that criminals can use to steal any one's identity.

Because cybercrimes covers such a broad scope of criminal activity, the examples above are only a few of the thousands of crimes that are considered Cybercrimes.

II. CYBERCRIME

Cybercrimes are defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".[1]

Cyber crime is the latest and the most complicated problem in the cyber world. "Cyber crime is said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime" [2]. "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]. The computer may be used as a tool in the following kinds of activity such as online gambling, pornography, financial crimes, intellectual property crime, sale of illegal articles, intellectual property crime, e-mail spoofing, cyber defamation, forgery, cyber stalking. The computer may become a target for unlawful acts in the following cases- theft of information contained in the electronic form, unauthorized access to computer/ computer system/ computer networks, data didling, web jacking , Trojan attacks, e-mail bombing, salami attacks, logic bombs, internet time thefts, theft of computer system, damaging the computer system phisically.

III. DISCREPANCY AMONG CONVENTIONAL AND CYBER CRIME

Cyber and conventional crime are not apparently distinct. However, on a deeper thought we may say that there exists a thin line of distinction between the conventional and cyber crime. The distinction lies in the involvement of the medium in cases of cyber crime. In cyber crime is basically a done through virtual cyber medium.

IV. REASONS FOR CYBER CRIME

Hart in his work "The Concept of Law" has said 'human beings are vulnerable so rule of law is required to protect them'. Applying this concept to the cyberspace we can say that computers are accessible, so rule of law is required to protect and safeguard them against cyber crime. The reasons for the accessibility of computers may be said to be:

A. Capacity to store data in comparatively small space

The computer has a unique characteristic that it can store large amount data in a very small space. Thus, large amount of information can be derived from this cyber space very easily.

B. Easy to access

The problem that is encountered while protecting a computer from unauthorised access is that, there occurs a gap not due to human error but due to the complex technology. For example if logic bomb are secretly implanted, then, key loggers can easily steal access codes, retina imagers, advanced voice recorders; etc. that can fool biometric systems and bypass firewalls.

C. Complex

The brain of a computer is operating system and this operating system is in turn composed of millions of complex codes. Human mind is deceptive and there is a possibility that it can lapse at any stage. The cyber criminals take advantage of this and can access the computer system.

D. Negligence

Negligence is very closely and directly connected with human control. So there is a probability that while protecting the computer system, there might be any negligence that in turn provides a cyber criminal to penetrate and gain access and control over the computer system.

E. Loss of evidence

Loss of evidence is a very obvious and common because all the data are frequently destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

V. TYPES OF CYBER CRIMES

Given below are the types of cybercrime:

A. Hacking

A hacker is an unauthorized user who attempts to or gains an access to an information system. Hacking is a crime even if there is no visible damage to the system, since it is an intrusion
in to the privacy of someone's data.

There are classes of Hackers.

1) *White Hat Hackers* - They believe that information sharing is good, and that its their responsibility to share their expertise by facilitating access to information.
2) *Black Hat Hackers* - They cause damage after intrusion. They may steal or modify information or insert viruses or worms which may damage the system. They are also called 'crackers'.
3) *Grey Hat Hackers* - Occasionally violates hacker ethics. Hackers will hack into networks, stand-alone computers and software. Network hackers try to gain unauthorized access to private networks for curiosity, challenge and distributing information. Crackers perform unauthorized intrusion with damage like stealing or changing of information or inserting viruses or worms.

B. Cyber Stalking

This involves use of internet to harass someone. The behavior in this crime includes
false accusations, threats etc.This involves following a person's movements across the Internet by posting messages (sometimes threatening) on bulletin boards frequented by the victim, entering chat-rooms frequented by the victim, constantly sending emails to the victim etc.

C. Spamming

Spamming is sending of unsolicited bulk and commercial messages over the internet. Although irritating to most email users, it is not illegal unless it causes damage such as overloading network and disrupting service to subscribers or creates .negative impact on consumer's attitudes for Internet Service Provider.

D. Cyber Pornography
Women and children are victims of sexual exploitation through internet. Pedophiles use the internet to send photos of illegal child pornography to targeted children so as to attract children to such funs.

E. Phishing
It is a criminally fraudulent process of acquiring sensitive information such as username, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

F. Software Piracy
It is an illegal reproduction and distribution of software for business or personal use. This is considered to be a type of infringement of copy right and a violation of a license agreement. Since the unauthorized user is not a party to the license agreement it is difficult to find out remedies.

G. Corporate Espionage
It means theft of trade secrets through illegal means such as wire taps or illegal intrusions.

H. Money Laundering
It means moving of illegally acquired cash through financial and other systems so that it appears to be legally acquired. eg. Transport cash to a country having less stringent banking regulations and move it back by way of loans the interest of which can be deducted from his taxes.

I. Embezzlement
Unlawful misappropriation of money, property or any other thing of value that has been entrusted to the offender's care, custody or control is called embezzlement. This crime is done by misusing the Internet facilities.

J. Password Sniffers
Password sniffers are programs that monitor and record the name and password of network users as they log in, putting in danger the security at a site. Any person who installs the sniffer, can act as an authorized user and log in to access on restricted documents.

K. Spoofing
It is the act of disguising one computer to, electronically "look" like another computer, in order to gain access to a system that would be normally is restricted.

L. Credit Card Fraud
In U.S.A. half a billion dollars have been lost annually by consumers who have credit cards and calling card numbers. These are stolen from on-line databases.

M. Web Jacking
The term refers to forceful taking of control of a web site by cracking the password..This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). Like terrorism, `e-terrorism' is utilizes hacking to cause violence against people or property, or least, it causes enough harm to generate fear.

N. Cyber terrorism
The use of computer resources to intimidate or coerce government, the population or any segment, thereof in furtherance of political or social objectives is called cyber terrorism. Individuals and groups quite often try to exploit anonymous character of the internet to threaten governments and terrorize the citizens of the country.

O. IP Crimes
Software Piracy, Copyright Infringement, Trademarks Violations, Theft of Computer Source Code. Email Spoofing a spoofed email is one that appears to originate from one source but actually has been sent from another source.

P. Cyber Defamation
This occurs when defamation takes place with the help of computers and/or the Internet. E.g. a person publishes defamatory matter about another on a website.

Q. Unauthorised Access
Also known as Hacking, involves gaining access illegally to a computer system or network and in some cases making unauthorized use of this access. Hacking is also an act by which other forms of cyber-crime (e.g., fraud, terrorism) are committed. Theft of any information contained in electronic form such as that stored in hard disks of computers, removable storage media, etc.

R. Email Bombing
This refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

S. Salami Attacks

These attacks are often used in committing financial crime and are based on the idea that a change or a modification, so insignificant, would go completely unnoticed in a single case. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say 5 cents a month) from the account of every customer. This unauthorized debt is likely to go unnoticed by an account holder.

T. Denial of Service (DNS) Attack

This involves flooding a computer resource with more requests than it can handle, causing the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. Another type of a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack, where the perpetrators are many and are spread geographically.

U. Virus/worm

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. These show their affect usually on the data present on a computer, either by changing the data or by its deletion. Viruses, on the other hand, do not require the host to attach themselves to. They make run able copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

V. Logic Bombs

These are event dependent programs where programs kick into action only when a certain event (known as a trigger event) occurs. Some viruses may be termed logic bombs because they lie dormant throughout the year and become active only on a specific date.

X. Trojan Attacks

It is an unauthorized program which runs from inside, what seems to be an authorized. It in reality conceals what it is actually doing.

Y. Trapdoor

Trapdoors are a system entrance that goes through the security system. These act as hidden logins or can act as administrative user definitions, added by system developers for many reasons. It hence allows control by an unauthorized or unknown user on a computer system. These are basically implemented at servers or mainframe systems

Z. Time bomb

These are software attacks that are designed to occur at a predetermined time or date. Technically speaking, the time bomb does not spread. It affects only the system on which it has been loaded.

A.A. Data diddling

It is the changing of data before or during entry into the computer system. Examples are forging or counterfeiting documents used for data entry and exchanging valid disks and tapes with modified replacements

VI. MEASURES TO PREVENT CYBER CRIME

There is a famous saying-Prevention is always better than cure. It is always better to take certain preventive measures while working on internet. One should make it a habit of doing this. Sailesh Kumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell, ha given the 5P strategy for cyber security: Precaution, Prevention, Protection, Preservation and Perseverance. A cyber user should keep in mind the following things-

1. To prevent cyber stalking one should avoid disclosing any personal information.
2. Always avoid sending any pictures or videos online particularly to unknown people and online friends as there have been many incidents of misuse of the personal pictures, videos etc.
3. Always use latest and updated anti virus software to guard against virus attacks.
4. Always keep back up volumes to avoid loss of data in case of virus attacks.
5. Never send your credit card details such as card number to any unsecured, to guard against frauds.
6. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
7. 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.
8. Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
9. Use of firewalls may be beneficial.
10. Web servers running public sites must be physically separate protected from internal corporate network.

Adjudication of a Cyber Crime - On the directions of the Bombay High Court the Central Government has by a notification dated 25th March 2013 has decided that the Secretary to the Information Technology Department in each state by designation would be appointed as the AO for each state.

VII. CONCLUSIONS

It is impossible to completely eliminate cyber crime from the cyber space. It is quite possible to take preventive measures and keep a check on it. From the past, it is evident that no regulation has ever succeeded in eliminating crime completely from the world. The only possible step is to make people aware of cyber crime. We would conclude with a word of caution for the users that they should keep in mind that the provisions of the cyber law are not so rigorous that they may control the growth of the IT industry and prove to be detrimental.

REFERENCES

[1] Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
[2] Parthasarathi Pati,-"CYBER CRIME", www.naavi.org
[3] Nagpal R. – What is Cyber Crime?

