cyber crimes

Our mouse can be just as dangerous as a bullet or a bomb
Rep. Lamar Smith (R- Texas)

Suryaa.R

B.Com LL. B (Hons), LL.M. (corporate Law),
ADVOCATE, HIGH COURT, CHENNAI, INDIA.

ABSTRACT: **Cyber-crimes are technology- b a s e d crimes. Cyber-crimes are a combination of the offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of a victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunications networks such as the internet. Computer crime refers to criminal activity involving a computer. The computer may be used in committing a crime or it may be the target. Net crime refers to criminal use of the internet. Cyber-crime may be defined as any illegal activity that uses a computer as its primary means of function. The term 'cybercrime' can refer to offences including criminal activity against data, infringement of content and copyright, fraud, unauthorised access, child pornography and cyber stalking**

I. INTRODUCTION

Business and societies have to depend upon the ecological revolution for their day-to-day activities. The stage has reached that earth's revolution would come to stand still if one is not exposed to this.

II. HISTORY OF CYBER CRIME[1]

The first recorded cyber crime took place in 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest from of a computer, has been around since 3500 B.C. In India, Japan and China, the era of modern computer, however, began with the analytical engine of Charles Babbage. The first spam email took place in 1976 when it was sent over the ARPANT. The first virus was installed on an apple computer in 1982 when a high school student, Rich skrenta developed the EIK cloner.

III. CYBER CRIME

Cyber-crimes are technology- b a s e d crimes. Cyber crimes are a combination of the offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of a victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunications networks such as the internet. Computer crime refers to criminal activity involving a computer. The computer may be used in committing a crime or it may be the target. Net crime refers to criminal use of the internet. Cyber crime may be defined as any illegal activity that uses a computer as its primary means of function. The term 'cyber crime' can refer to offences including criminal activity against data, infringement of content and copyright, fraud , unauthorised access, child pornography and cyber stalking. The computer or internet is used as a means to do such crimes. These are organized and white- c o l l a r crimes. Cyber criminals are technocrats who understand, interpret and misuse of information technology. Crime is facilitated by or involves the use of electronic communications or information systems or electronic device. Most of the criminals opt this kind of crime because it can be committed from anywhere and what is needed is only a laptop or even a borrowed system

IV. CLASSIFICATION OF CYBER CRIMES[2]

- Against persons.
- Against Business and Non-business organizations.
- Against the government.

Based on the nature of attacks they can be further classified into:

Malware:

Malware is software that takes control of other's computer to pass on or spread a bug that corrupts the system.

Cyber Pornography:

This is an act of publishing and printing pornographic material and the use the internet to transmit it.

Salami Attack:

This refers to financial crimes involving the technology by fraudulently gaining access to an information system of others.

Hacking:

A hacker is an unauthorized user who attempts to or gains access to an information system of others. I t is an invasion

[1] Short Essay on Cyber Crime, by Piyush Jain

in to the privacy of data.

Phishing:

Phishing is trying to fool people to parting with their money by requesting customers to enter their username, password or other personal information to access their account for some reason. They directed to a fraudulent replica of the original institution's website.

Vishing:

Vishing is the practice of using social engineering and social networks to gain access to private. personal and financial Information from the public for the purpose of financial reward.

Bot networks:

In this the spamsters and other perpetrators of cyber crimes remotely take control of computers without the users realizing it. Such affected computers known as zombies.

Packet Sniffing:

In this the hacker intercepts the transmission between two computers and all the hacker needs is the IP address from one of the computers and to gain an access to the data. The data is not stolen Instead the sniffers copy the hex and translate it into original data.

Tempest attacks:

Data that passes though circuitry and mechanical devices produce electro-magnetic emanation. This allows hackers to monitor and put data from network cables.

Buffer overflow:

Buffers are created to hold a finite amount of data and when it overflows, it goes into adjacent buffers that would cause the data to be overwritten. In this the extra data can contain instructions that trigger specific actions.

Cyber Stalking:

Cyber stalking is essentially using the Internet to repeatedly harass another person. Such information can leave one vulnerable to this.

Bacteria or Rabbit Programs:

They reproduce themselves exponentially and take up all the processor capacity, memory, or disk space.

E-mail spoofing and E-mail bombing:

A spoofed email is one that appears to originate from one source but actually has been sent from another source. In this case, the goal of the attacker is to interrupt the victim's e-mail service

Trojan and Rats:

These are programs that appear to be doing what the user wants while they are actually doing something else such as deleting files or formatting disks. RATs are remote access. Trojans provide a backdoor into the system.

Data Diddling:

In this the information is changed from the way it should be entered by a person typing in the data, a virus that changes data This is one of the simplest methods of committing a computer-related crime

V. INSTANCES OF CYBER CRIME[3]

Email account hacking:

Emails are increasingly being used for, business communication, online transactions and social interaction. Most email account holders do not take basic precautions to protect their email account passwords. The victim's email account password is stolen and the account is then misused for sending out malicious code (virus, worm, Trojan etc) to people in the victim's address book. The recipients of these viruses believe that the email is coming from a known person and run the attachments. This infects their computers with the malicious code. The suspect would install key loggers in public computers (such as cyber cafes, airport lounges etc) or the computers of the victim.

Email scam:

Emails are fast emerging as one of the most common methods of communication. At the same time criminals are also using emails extensively for their illicit activities. In the first step, the suspect convinces the victim that the victim is going to get a lot of money (by way of winning a lottery or from a corrupt African bureaucrat who wants to transfer his ill-gotten gains out of his home country). In order to convince the victim, the suspect sends emails (some having official looking documents as attachments). Once the victim believes this story, the suspect asks for a small fee to cover legal expenses or courier charges. If the victim pays up the money, the suspect stops all contact. The suspect creates email accounts in fictitious names and sends out millions of fraudulent emails using powerful spam software.

Source code theft:

Source code is the programming instructions that are compiled into the executable files that are sold by software development companies. The suspect (usually an employee of the victim) steals the source code and sells it to a business rival of the victim. If the suspect is an employee of the victim, he would usually have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage device

Software piracy:

Many people do not consider software piracy to be theft. There is a common perception amongst normal computer users to not consider software as "property". This has led to software piracy. The software pirate sells the pirated software in physical media (usually CD ROMs) through a close network of dealers. The suspect uses high speed CD duplication equipment

[3] KPMG INTERNATIONAL Issues Monitor "Cyber Crime – A Growing Challenge for Governments July 2011", Volume Eight

to create multiple copies of the pirated software. This software is sold through a network of computer hardware and software vendors

Web defacement:

Website defacement is usually the substitution of the original home page of a website with another page. Religious and government sites are regularly targeted by hackers. The homepage of a website is replaced with a pornographic or defamatory page. In case of Government websites, this is most commonly done on symbolic days (e.g., the Independence Day of the country). The defacer may exploit the vulnerabilities of the operating system or applications used to host the website. This will allow him to hack into the web server and change the home page and other pages. Alternatively, he may launch a brute force or dictionary attack to obtain the administrator passwords and He can then connect to the web server and change the Web Pages.

Use of Internet and Computers by terrorists:

Many terrorists are using virtual as well as physical storage media for hiding information and records of their illicit business. The suspects carry laptops wherein information relating to their activities is stored in encrypted and password protected form. They also create email accounts using fictitious details. In many cases, one email account is shared by many people. E.g., one terrorist composes an email and saves it in the draft folder. Another terrorist logs into the same account from another city / country and reads the saved email. He then composes his reply and saves it in the draft folder. The emails are not actually sent. This makes email tracking and tracing almost impossible. The terrorists purchase small storage devices with large data storage capacities. They also purchase and use encryption software. The terrorists may also use free or paid accounts with online storage providers.

VI. EFFECTS OF COMPUTER CRIME

Economic impact:

Today 's consumer has become increasingly dependent on computers, networks, and the information these are used to store and preserve, the risk of being subjected to cyber-crime is high. Trading of stocks, bank transactions, purchases are made using credit card via online. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy.

Impact on consumer:

Cyber-attackers intrude into other's cyber space and try and break the logic of that space, the customer visiting the concerned space will be frustrated and discouraged to use the said site on a long-term basis. The site in question is termed as the fraudulent but the criminal mastermind in the hidden attack is not recognized as the root cause. This makes the customer lose confidence in the said space

VII. MEASURES FOR CYBER SECURITY[4]

Intrusion Detection and Prevention System (IDPS)

Intrusion detection is the process of monitoring the events occurring in a computer system or network Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. IDPS are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators IDPS record information of observed events and notify security administrators about observed events, and reports

Agent Based Distributed Intrusion Detection System (ABDIDS)

Agent Based Distributed Intrusion Detection System is a defensive mechanism to protect systems and networks from abuse. ABDIDS is a fully distributed system made by set of nodes with three types of agents Monitoring Registry Agents (MoRA), Monitoring Agents (MoA) and managing agents (MA). It provides

(a) Early warning
(b) Detecting and isolating

GPRS (Global Positioning and Remote Sensing) Security Architecture

GPRS is a set of security mechanisms, It mainly aims at two goals namely: To protect the network against unauthorized access, and to protect the privacy of users. For betterment, some defensive mechanisms to protect our computer system and network information from attacks and abuses are installation of intrusion detection and prevention system (IDPS), Agent Based Distributed Intrusion Detection System (ABDIDS), GPRS security architecture, use of anti-virus software, firewalls, etc.

VIII. CASES OF CYBER CRIMES IN INDIA[5]

Pune Citibank Mphasis call centre fraud

US $ 3,50,000 from City bank accounts of four US customers were dishonestly transferred to bogus accounts in Pune, through internet. The call center employees of a call center gained the confidence of the its customers and obtained their user's information like pin etc. the information obtained were used to transfer money fraudulently from their accounts.

[4] Janhavi J Deshmukh and Surbhi R Chaudhari, Dept. of Computer Science & Engineering, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, India.

[5] Rohas Nagpal," Cyber Crime & Digital Evidence –Indian Perspective", "Real world cybercrime cases"

Parliament attack case

The terrorists who attacked the parliament on December 13,2001 hacked into the networking system of the parliament and used the information gained (including that of government of India's emblem and ID's.

The bank NSP case

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "Indian bar associations" and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

IX. CONCLUSION

Computers add a new dimension to criminal law, presenting many issues for law enforcement. At the forefront of law enforcement concerns is the necessity to secure adequate training to combat these crimes. The policy and legal issues are equally challenging. It has become a necessity to enact legislation that protects and safeguards the developing technology. The speed with which the technology develops makes this an important concern. Issues of jurisdiction and enforcement power present special problems to the World Wide Web. When countries adopt different standards of judiciary and judiciary powers this becomes a problem. As technology develops, the law needs to respond to these new developments to deter those who would abuse and misuse the new technology.

The capacity of human mind is indecipherable. So, protecting cyber space from cyber crime is difficult. However, it is possible to check them to reduce the interpret of cyber crimes. But the problem is that most cases related to cyber crime remains unreported due to lack of awareness.

"It is widely known that the victims of internet crimes are often reluctant to report an offence to authorities. In some cases, the individual or organization may not even be aware a crime has been committed. Even though facilities for reporting incidents of cyber crime have improved in recent years many victims remain reluctant due essentially to embarrassment."

Norton cybercrime report 2011 revealed 431 million adults in 24 countries had been victims of cyber crime and are escalating at an alarming rate and the financial cost of global crime is $388 billion. Cyber crimes are considered to be a global epidemic.

X. ACKNOWLEDGEMENT:

It is pleasant duty for me to make acknowledgement for the guidance that I have received from my family members, peers and esteemed friends. I am indebted to my family members for their unconditional love and moral support throughout the duration of this research.

References:

[1] Hemraj Saini, Yerra Shankar Rao, T.C.Panda, "Cyber-Crimes and their Impacts: A Review", International Journal of Engineering Research and Applications(IJERA) ISSN: 2248-9622 , Vol. 2, Issue 2,Mar-Apr 2012,

[2] Karen Scarfone, Peter Mell "Guide to Intrusion Detection and Prevention Systems (IDPS)", National Institute of Standards and Technology Special Publication 800-94 Natl. Inst. Stand. Technol. Spec. Publ. (February 2007)

[3] Computer Crime - Conclusion - Criminal, Technology, Law, and Enforcement - JRank Articles

[4] Anju P Rajan Mathew, A. AJilaylwin, Shaileshwari M U"Cyber security solutions for DLMS meters using GSM/GPRS technology"