Lecture-14

Cyber Crime and Cyber Contraventions

Introduction

The concept of cyber crime is not new in the knowledge society of 21st century. The kind of offences committed in India remained more or less same since 1860. However, with the coming of new Information and Communication Technologies and the internet and their growing misuse side by side, scenario has totally changed. On the one hand new technologies have facilitated the commission of old crimes by the bad elements and at the same time new crimes have originated commonly called as cyber crimes. It is important to note that cyber crimes are very easy to commit with very little sources but damage caused could be very huge. Because of internet bad elements are getting better networked and hence facilitating cyber crime.

United Nations has foreseen this problem way back in 2000 and gave warning signals that "in some countries, problems have arisen from the use of new information and communication technologies for trafficking in women and children and for purposes of all forms of economic and sexual exploitation." Criminals under pseudo identities enter the internet "chat-rooms" and exploit helpless women, girls, children and even men.

Jurist Lalitha Sridhar rightly pointed out that "our understanding of the virtual world is woefully slim; and of cyber crimes, even less. But, as law enforces are finding out, their effect on the real world is devastating." Therefore, the effect of cyber crimes committed through virtual world on the real world is devastating.

Historically, the first recorded cyber crime took place in the year 1820, when Joseph Merrie Jacquaid, a textile manufacturer in France produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabric. This resulted in a fear amongst jacquaid's employees that their traditional employment and livelihood were being threatened. They committed act of sabotage to discourage Jacquaid from further use of new technology.

In fact the term "Cyber Crime" is frequently used in 21st century knowledge society and is created by combination of two words cyber and crime. The term cyber denotes the cyber space i.e. virtual space and it means the informational space modeled through computer, in which various objects or symbol images of information exist. Therefore it is the place where the computer programs work and data is processed.

However, the term crime refers to a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has punishment under law. We can say that crime is a legal wrong that can be followed by criminal proceedings which may be result into punishments.

Thus simple definition of cyber crime is any unlawfull act where computer is either toll or target or both. However, some other definitions are:

"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"

Another name of cyber crime is computer crime and important definitions of computer are:

"Computer crime is an intentional act associated in any way with computers where a computer has suffered or could have suffered a loss, and a perpetrator made or could have made again."

"any illegal or unauthorised activity involving computers can be treated as computer crime. The crime can be against an individual or an organization. It can even be against the nation endangering or threatening to endanger its integrity and security."

Basically cyber crimes are aimed at stealing the computer, damaging information, or stealing information. Computer crime is not necessarily technical in origin. Most criminals act against computers does not directly involve technology. In fact, 72 percent of the computers crimes reported to the FBI in 2003 involved simple hardware theft.

The use of a computer to carry out any conventional criminal act, such as fraud, is called cyber crime and is a growing menace. Cyber crime is growing so rapidly, in fact, that the federal government has created a handful of agencies to deal with computer related crimes. According to an estimate, instances of internet fraud increased in 2002 as compared to 2001.

Classification of Cyber Crimes:

Whether an old crime is committed on or through computer or a new crime is committed, cyber crimes are of following types;

i. Crimes "on" the internet
ii. Crimes "of" the internet
iii. New crimes used for commission of old crimes.

Crimes on the internet: These are the old crimes which are committed on or through the new medium of the internet. For example, cheating, fraud, misappropriation, defamation, threats, etc. committed on or through or with the help of the internet. The internet with its speed and global access has made these crimes much easier, efficient, risk-free, cheap and profitable to commit.

Crimes of the internet: These are new crimes committed with the help of internet itself, such as hacking, planting viruses and IPR thefts.

New crimes used for commission of old crimes: for example, where hacking is committed to carry out cyber frauds.

Based on the victim of cyber crime

Further depending upon the victim of cyber crime, it may be broadly classified under three heads:

i. Against individual.
ii. Against organisations.
iii. Against society at large.

Based on nature (social or economic) of cyber crime

Another category of cyber crime is social and economic cyber crimes which includes following:

i. Social cyber crimes; and
ii. Economic cyber crimes

Social cyber crimes: In some countries problems have arisen by use of new ICTs e.g., trafficking in women and children for purposes of all forms of economic and sexual exploitation. Sometime criminals under pseudo identity enter the internet chat room and exploit helpless women and girls. Further, studies have shown that about 60% of websites are sexual in content and 20% of them solicited their visitors. Main social crimes are:

a. Trafficking
b. Cyber obscenity and pornography
c. Cyber terrorism
d. Cyber fraud
e. Cyber gambling

Economic cyber crimes: Economic offences affecting more than $ 1.2 trillion E-commerce industry worldwide includes following:

a. Credit card schemes
b. System corruption
c. Internet fraud
d. Dot com job scams
e. Corporate and political espionage
f. Mafia and drug peddlers
g. Multi-site gambling websites

Based on the Role of computers

Depending upon the role played by the computer in perpetrating crime, the computer may be involved as a victim of crime, or an instrument used to commit a crime or a repository of evidence related to the crime, i.e.,

a. Computer as a victim of crime
b. Computer as a tool of crime

c. Computer as a witness of crime

Computer as a victim of crime:

A computer or a computer network could be the target of an offence wherein the computer becomes the victim. In such cases, the computer's confidentiality, integrity, or accessibility is attacked. The information stored or the service provided by the victim is stolen or the victim is crippled and damaged. Such crimes involve disrupting the functioning of the computer, computer system or computer network; corrupting the operating system and programmes; theft or disturb data/information (e.g. marketing information), intellectual property violations and blackmailing by using personal information hacked from the computer systems. Examples of this form of computer crimes is the denial of service attacks on popular internet sites like yahoo, CNN etc. and the spread of the 'Melissa' and 'I Love You" viruses and their variants.

Computer as tool of crime:

Computer can be used as a tool or an active weapon for committing a crime, which includes fraud, IPR violations, and online transactions of illegal goods etc. computer can also be used as any other hi-tech equipment for committing traditional crimes. Such crimes include automated teller machine (ATM) frauds, credit cards frauds, frauds involving electronic fund transfer (EFT); embezzlement of funds from the banks; telecommunication frauds; counterfeiting and software piracy. These are also called assisted crimes. When computer is used as an active weapon for perpetuating the crime, it is also termed as 'information crime', as it could not be committed in absence of information technology.

Computer as a witness to crime:

A computer need not be only a victim or a tool; it could also be the witness to the offence. The examples of computer as a witness to crime are money laundering, illegal banking transactions, bulletin board system (BBS), storage of drug trafficking transaction record. Further a computer system may be used to detect information, which assists the criminal in commissioning the crime.

Based on nature, source and motive

Depending upon source, nature, motive and the impact, crimes can be of following types:

a. Computer Crimes
b. Computer related Crimes
c. Network Crimes

Computer Crimes: Computer misuse is a crime committed against a computer system or other digital media. It includes digital crimes such as computer hacking, illegal access, use of backdoors, viruses and other unauthorised intrusion or abuse.

Computer related crimes: Such crimes include computer pornography, theft of intellectual property and software copyright etc.

Network crimes: The computer network crime or the computer aided crimes are those where a computer or other digital media is used to facilitate crimes, such as blackmail, where the demand is sent via the internet and such crimes are committed against e-commerce suppliers.

Based on the criminal activities:

Depending upon the criminal activities, computer crimes are of following types:

a. Physical crimes
b. Data related crimes
c. Software related crimes

Physical crimes: The physical crimes are related to computer or its associated peripherals, hardware, software or the computer time.

Examples of such crimes are theft, breakage, destroying the data, output or media and inter-processing manipulations.

Data related crimes: In the data related crimes, unauthorised data or information in the digital form is entered in the computer systems or the data that should be entered is altered, suppressed or corrupted by the criminals so as to gain undue advantages. Computer fraud by input manipulation is the most common computer crime, which is easy to perpetrate and difficult to detect. The computer related crime should further be sub-classified into one of four main categories:

Data diddling

Data leakage

Data spying

Scavenging

Data diddling: data diddling is the most common form of computer crime, which is carried out by input manipulations. It involves changing the data, with malicious intentions, during or before feeding it into a computer and provides undue advantage to a specific party. It also includes adding fraudulent input data, altering the input data, omitting the desired input data, wrongly posting a transaction, making alterations or additions in the master file records, posting the transactions partially, destroying the output, and substituting the counterfeit output. Such types of changes can be affected by anyone associated with the

process of creating, recording, encoding, examining, checking, converting and transporting data that enters a computer.

Data leakage: it involves illegal copying the master file information of the computer for ransom, blackmailing or any other fraudulent purposes.

Data spying: it is important to note that for spying on the sensitive information of a person, his computer network is assessed from a remotely located computer, by using the legitimate password, or breaking the password. Such data is sold to others at a very high price.

Scavenging: It is method of obtaining or re-using the information, which might have been left after processing, in or around a computer system.

Software-related crimes: In such crimes, the system as well as the application software are affected or corrupted. As this is a very sophisticated form of crime and is much more dangerous so it is difficult to detect. Further it involves changing existing programmes in the computer system or inserting new programmes or routines and the computer programmers, analyst and other experts are involved in commissioning or making alteration in the software. The software-related crimes could be perpetrated by using various techniques like computer viruses, computer worms, Trojan horse, trap door, super zapping, wire-trapping, time bombs, logic bombs and salami bombs.

Prevention of cyber crimes

One should always take some preventive measures so as to protect himself from cyber attacks. The following point should be kept in mind while working on computers and internet:

- Exercise caution while sharing personal information such as your name, E-mail address etc. do not respond to E-mail messages that ask for your personal information.
- Do not visit unwanted gambling or related websites.
- Avoid sending any photographs to the strangers as these may be misused.
- Choose strong password so that these can not be easily decoded. It is always recommended to keep changing the password at regular intervals.
- Always keep on reviewing your credit card and bank statements regularly. If one gets the tip-off being stolen then timely action can be taken.
- Always keep on computer up-to-date. Install all necessary softwares at regular intervals as they are a great start towards keeping you safe.
- Install firewalls and antivirus software to keep guard of your softwares.
- Keep internal corporate web servers separate from web servers running public sites.
- Keep a watch on the sites that your children watch. Block the unwanted internet sites at regular intervals.

- It is better to use security programs that keep guard on cookies unguarded might prove fatal.
- Always keep backup of the data stored on your computer to safeguard against virus.

Cyber Crimes: Cyber offences and cyber contraventions under Information Technology Act, 2000:

Some jurists believe that cyber crime is a wider term and it includes both cyber offences and cyber contraventions (civil wrong). Under Information Technology Act, 2000 cyber offences are given in chapter XI (section 65-74) whereas cyber contraventions are mentioned under chapters IX (section 43-45)

Cyber contraventions under Information Technology Act, 2000

A cyber contravention refers to a civil wrong under information technology Act, 2000. It is important to note that law of Tort provides remedies for civil wrong where affected person can compel the wrongdoer to pay damages by way of compensations. However, for cyber contravention damages are provided under section 43-45 of Information Technology Act, 2000.

Penalty and compensation for damage to computer: (section 43)

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, —

(a) Accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any computer, computer system or computer network;

(f) Denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.—For the purposes of this section,—

(i) "computer contaminant" means any set of computer instructions that are designed— (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "Damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

Compensation for failure to protect data (section 43 A)

Where a body corporate, possessing, dealing r handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation: for the purpose of this section-

1. ‘Body corporate’ means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.
2. “Reasonable security practices and procedures” means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force.
3. “Sensitive personal data or information” means such personal information as may be prescribed by the Central Government in consultation with such professionals’ bodies or association as it may deem fit.

Penalty for failure to furnish information return, etc. (section 44)

If any person who is required under this Act or any rules or regulations made there under to—

(a) Furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(c) Maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Residuary penalty (section 45)

Whoever contravenes any rules or regulations made under this Act, for .the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Power to adjudicate (section 46)

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made there under the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

[1(A)] The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore.

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and—

(a) All proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;

(b) Shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.

(c) Shall be deemed to be a civil court for purposes of order XXI of the Civil Procedure Code, 1908.

Factors to be taken into account by the adjudicating officer (section 47)

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely:—

(a) The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(b) The amount of loss caused to any person as a result of the default; (c) the repetitive nature of the default.

(c) The repetitive nature of the default.