Cyber Crime

Crime is an act or omission, which is prohibited by the law particularly criminal. Cyber-Crime is the latest and perhaps the most specialized and dynamic field in cyber-laws. "Cyber crimes can be plainly define as " Crimes directed at a computer or computer system" But the complex nature of cyber crimes cannot be sufficiently expressed in such simple and limited term"[1].The Organization for Economic Co-operation and Development (OECD) recommended the working definition of cyber crime "computer related crime is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and the transmission of data."[2]In 2001, The Council of Europe Convention31 defines cybercrime in Articles 2-10 in four different categories: 1) offences against the confidentiality, integrity and availability of computer data and systems; 2) computer- related offences; 3) contentrelated offence; 4) offences related to infringements of copyright and related rights[3].One of the greatest lacunae of this field is the absence of a set of comprehensive law anywhere in the world. Further the growth ratio of internet and cyber-law is not proportional Too. The era of nuclear warfare conceived the idea of a system which could even survive the devastation of nuclear weapons. "A post-apocalypse command grid" was the original idea for Internet -'Bruce Sterling' has stated. The idea of 'internet' was conceived in the early 60's while a code for its regulation was mooted in late 90's. This clearly brings about the reason for the complication of cyber-crime.

Cyber offences fall under the Indian Penal Code.

(i) Sending threatening messages by email Section 503 IPC
(ii) Sending defamatory messages by email Section 499 IPC
(iii) Forgery of electronic records Section 463 IPC
(iv) Bogus websites, cyber frauds Section 420 IPC
(v) Email spoofing Section 463 IPC
(vi) Web-jacking Section 383 IPC
(vii) E-Mail Abuse Section 500 IPC
(viii) Online sale of Drugs NDPS Act

[1]Cybercrime: Talat Fatima, (2011) Eastern Book Company, Lucknow. Page 89.
[2]The Criminal Aspect in Cyber Law in The Indian Cyber Law, Suresh T. Vishwanathan, (2001) Bharat Law House, Jaipur Page 7.
[3]http://www.conventions.coe.int.Treaty

(ix) Online sale of Arms Arms Act

(x) Pornographic Section 292 IPC

India has enacted the first I.T.Act, 2000 based on the UNCIRAL model recommended by the general assembly of the united nations by a resolution dated 30th.jan.1997 .The preamble to this Act gives a very clean picture in this regard.

Chapter XI of this Act deals with offences/crimes along with certain other provisions scattered in this Acts .The various offences which are provided under this chapter are - Tampering with Computer source documents

S.65; Hacking with Computer systems

S.67; Access to protected system

S.70; Misrepresentation

S.71; Breach of Confidentiality and Privacy

S.72; Fraud

S.74; Further Chapter IX u/p of S.43 restricts the damage to Computer, computer system, etc.

Commission of Cyber-Crime may be broadly divided against three basic groups -

1.Individual

a). person&

b). property of an individual

2. Organization

a. Government

b. Firm, Company, Group of Individuals.

3. Society at large

The following are the crimes, which can be committed against the followings group Against Individuals -

i. Harassment via e-mails.

ii. Cyber-stalking.

iii. Dissemination of obscene material.

iv. Defamation.

v. Hacking/cracking.

vi. Indecent exposure.

Individual Property: -

i. Computer vandalism.

ii. Transmitting virus.

iii. Netrespass.

iv. Unauthorized control over computer system.

v. Hacking /cracking.

Against Organization: -

i. Hacking & Cracking.

ii. Possession of unauthorized information.

iii. Cyber terrorism against the government organization.

iv. Distribution of pirated software etc.

Against Society at large.

i. Pornography (basically child pornography).

ii. Polluting the youth through indecent exposure.

iii. Trafficking.

Cyber crime and cyber terrorism

There is not exhaustive definition of cyber crime, but we can say that it includes activities which offend human sensibilities. And on the other hand when we talk about the cyber terrorism , we will see that it is premeditated or politically motive attack against information , computer system , programs, data's which result in violence against property , government as well as people at large. We have so many example like red fort case, e- mail threats in tajmahal case and supreme court e-mail threat case.

The difference between the two however is with regard to the motive and the intention of the perpetrator.

While a cyber crime can be described simply as an unlawful act wherein the computer is either a tool or a target or both, cyber terrorism deserves a more detailed definition. One can define cyber terrorism as a premeditated use of disruptive activities or the threat thereof, in

cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.[4]

Measures To Curb The Crime

Though by passage of time and improvement in technology to provide easier and user friendly methods to the consumer for make up their daily activities, it has lead to harsh world of security threats at the same time by agencies like hackers, crackers etc. various Information technology methods have been introduced to curb such destructive activities to achieve the main objects of the technology to provide some sense of security to the users. Few basic prominent measures used to curb cyber crimes are as follows:

A) Encryption: This is considered as an important tool for protecting data in transit. Plain text (readable) can be converted to cipher text (coded language) by this method and the recipient of the data can decrypt it by converting it into plain text again by using private key. This way except for the recipient whose possessor of private key to decrypt the data, no one can gain access to the sensitive information.

Not only the information in transit but also the information stored on computer can be protected by using Conventional cryptography method. Usual problem lies during the distribution of keys as anyone if overhears it or intercept it can make the whole object of encryption to standstill. Public key encryptograpy was one solution to this where the public key could be known to the whole world but the private key was only known to receiver, its very difficult to derive private key from public key.

B) Syncronised Passwords: These passwords are schemes used to change the password at user's and host token. The password on synchronized card changes every 30-60 seconds which only makes it valid for one time log-on session. Other useful methods introduced are signature, voice, fingerprint identification or retinal and biometric recognition etc. to impute passwords and pass phrases

C) Firewalls: It creates wall between the system and possible intruders to protect the classified documents from being leaked or accessed. It would only let the data to flow in computer which is recognized and verified by one's system. It only permits access to the system to ones already registered with the computer.

[4] Article on legalserviceindia.com-" Cyber Crimes and General Principles"

D) Digital Signature: Are created by using means of cryptography by applying algorithms. This has its prominent use in the business of banking where customer's signature is identified by using this method before banks enter into huge transactions.[5]

Nature of offences and penalties :

The objective of the act is mainly to facilitate e-commerce and not specifically to govern cyber crimes, the act , however, defines certain offences and penalties that deal with acts and commissions coming under the purview of the term cyber crimes. Chapter XI deals with the offences and chapter IX deals with penalties and adjudication. Chapter IX focuses on the following features:

1) Regulating conduct in its unique way;
2) Civil regulation to be employed by premises rather than criminal;
3) The process of adjudication is entrusted to adjudicating officers rather then regular civil courts;
4) Such adjudicating officer are required to know the law and IT or must have judicial experience;
5) Adjudicating officers are vested with the powers of civil courts;
6) The proceeding to be conducted by such adjudicating officers are to be construed as judicial proceeding;
7) The quantum of compensation to be calculated at market rate for loss or suffering.

- Penalty for damage of computer, computer system , network: Section 43 of the act stipulates a liability to pay damages in the form of compensation not exceeding Rs. One crore to the persons so affected where any person without permission of the owner or any other person, who is in-charge of a computer, computer system or computer network, does any of the following acts:-
    1. Accesses or secures to such computer, computer system or computer network;
    2. Downloads, copies or extracts any data, computer data base or information from such computer system or computer network including information or data held or stored in any removable storage medium.

3. Introduces causes to be introduces any computer containment or computer virus into any computer, computer system or network
4. Damages or causes to be damaged any computer , computer system or computer network , data base or any other programme residing in such computer , computer system, network.
5. Disrupts and causes disruption of any computer, computer system or computer network.

- Penalty for failure of return, information, etc section 44 of the act prescribes certain legal information and states that if nay person who is required under this act or any rule or regulation made there runder to furnish returns, maintain books, accounts, etc. the said provisions are:
    1. Furnish any document , return or export to the controller of the certifying authority fails to furnish the same, he shall be liable to penalty not exceeding one lakh and fifty thousand rupees for each such failure.
    2. File any return or furnish any information , books, or other documents within the time specified therefore in the regulation fails to file return or furnish the same within the time specified therefore in the regulation, he shall be liable to a penalty not exceeding 5000 rupees for every day during which such failure continues.
- Residuary penalty: section 45 of the act provides that whoever contravenes any rules or regulations much under act , for the contravention of which no penalty has been separately provided , shall be liable to pay compensation not exceeding 25000 rupees to the person affected by such contravention or a penalty not exceeding 25000 rupees.[6]

According to the provision contained In section 46 and 47 of the act , only an adjudicating officer appointed under act can adjudicate on these penalties or compensation on the basis of the following factors taken into consideration:

a) The amount of unfair advantage , as and when quantified made as 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.

- **Offences relating to tempering with computer sources documents**: chapter XI of the act defines certain offences and prescribes certain punishments for such offences. Section 65 defines the offences of tempering with the computer sources documents in the following words:

> Section 65: tampering with computer sources documents : whoever knowingly or intentionally conceals, destroys, or alters or intentionally or knowingly causes another to conceal ,destroy or alter any computer sources code used for a computer, computer programme , computer system or computer network, when the computer code is required to be kept or maintained by the time being in force shall be punishable with imprisonment upto 3 yrs, or with fine which may be extended upto 2 lakh rupees. or both.

For the purpose of explanation of this section , the word "computer source code" means the listing of program, computer commands, design and layout and programme analysis of computer resources in any form.

- **Offence of hacking:** section 66 defines the offence of hacking with the computer system. Under provision of this section, whoever with intent to cause or knowingly that he is likely to cause wrongful loss of damage to the public or any person destroys or alters any information residing in a computer resources or diminishes its value or utility or affects it injuriously by any means, commits hacking and whoever commits hacking shall be punishable with imprisonment up to 3yrs with fine, which may be extended upto rupees or with both.
- **Offence of obscene publication in electronic form:** section 67 of the act makes the publication of information which is obscene in electronic form an offence. According to this provisions, whoever publishes or transmits or causes to be published in the electronic form, any material which is luscious or appeal to the prurient interest or its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances , to read , see, hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to 5 yrs and with fine which may extend to 1 lakh rupees and in the event of a second or susquentconvicton with imprisonment of either description

for a term which may extend to 10 yrs and also with fine which may extend to 2 lakh rupees. The section covers the cyber crimes such as child pornography existing in the cyberspace.

- **Offences of non-** compliance of instruction from controller: .

How Can We Prevent Computer Crime?

a. By Educating Everyone.

For example, users and systems operators; people who hold personal data and the people about whom it is held; people who create intellectual property and those who buy it; and the criminals. **We must educate people to:**

1.Understand how technology can be used to help or hurt others.

2. Think about what it would be like to be the victim of a computer hacker or computer pirate.

b. By Practicing Safe Computing.

1. Always ask: Who has or may have access to my log-in address?

2. Remember: People such as computer hackers and pirates who hurt others through computer technology are not "**cool.**" They are breaking the law.

CONCLUSION

Crucial aspect of problem faced in combating crime is that, most of the countries lack enforcement agencies to combat crime relating to internet and bring some level of confidence in users. Present law lacks teeth to deter the terrorist groups for committing cyber crimes if you see the punishment provides by the Act it's almost ineffective, inefficient and only provides punishment of 3 years at the maximum. Harsher laws are required at this alarming situation to deal with criminals posing threat to security of funds, information, destruction of computer systems etc. Information Technology Act is applicable to all the persons irrespective of their nationalities (i.e. to non-citizens also) who commits offence under the Information Technology Act outside India, provided the act or conduct constituting the offence or contravention involves computer, computer systems, or computer networks located in India under Section 1 and Section 75 of the Information Technology Act, but this provision lacks practical value until and unless the person can be extradited to India. Therefore it's advised that we should have Extradition treaties among countries. To make such provisions workable.

Reference:

Book

1. Cyber crime- Law & policy perspectives, Dr. Mrs. K. SitaManikyam (2009) Hind Law House, Pune.

2 JogaRao, S.V., Law of Cyber Crimes,Wadhwa Publication, Nagpur 2004

3 Talat Fatima, Cyber Crimes, Eastern Book Company, Lucknow.2011

4 The Criminal Aspect in Cyber Law in The Indian Cyber Law, Suresh T. Vishwanathan, (2001) Bharat Law House, Jaipur

5 Rodney D. Ryder ,Guide to cyber Laws, Wadhwa Publication Nagpur, 2003

6 P .K. Singh , Laws on Cyber Crime, Book Enclave, Jaipur, 2007

7 Barkha U Rama Mohan , Cyber Law & Crime, Asia Law House, Hyderabad.2011

8 http://www.conventions.coe.int.Treaty.

9 http://www.legalindia.com/cyber-crimes-and-the-law