Journal of Social Welfare and Management
Volume 2 Number 2, April - June 2010

Computer crimes and preventive measures in cyber law

Shiva Kanaujia Sukula
K. K. Mittal

ABSTRACT

The article deals with the concept and rising of computer crimes in India. It provides certain key points to distinguish and differentiate the Cyber Crime with the conventional Crime. It highlights how Cyber Crime takes place? Further discusses the E-mail related crimes and Computer Fraud. It discusses in detail about the provisions in Cyber Law in context with Computer Related Offences such as Penalty and Compensation for damage to computer, computer system, etc.; Compensation for failure to protect data; Tampering with Computer Source Documents and some others. It highlights and suggests for Prevention of Cyber Crime. While highlighting the efforts made by government, various offices for help with an example of Pune are given. The article concludes with an urge to fight cyber crime.

Key words: computer crimes, cyber crimes, cyber law.

INTRODUCTION

There are various illegal activities like e-mail espionage, credit card fraud, spams, software piracy and so on, for which the computer is being used. Criminal activities in the cyberspace are on the rise. Computer crime, cyber crime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. Additionally, the terms computer crime or cyber crime are restricted to describing criminal activity in which the computer or network is a necessary part of the crime.

DEFINITION

Computer crime or cyber crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.

DIFFERENTIATING THE CYBER CRIME WITH THE CONVENTIONAL CRIME

A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences. Cyber crime is the latest and perhaps the most complicated problem in the cyber world. The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual

Author's Affiliation*Asstt. Librarian, Central Library, Ch. Charan Singh University, Meerut. U.P. ** Head, Dept. of Institute of Legal Studies, Ch. Charan Singh University, Meerut. U.P.

Reprint's requests: Shiva Kanaujia Sukula, Author's Affiliation*Asstt. Librarian, Central Library, Ch. Charan Singh University, Meerut. U.P., E-mail: shivajrf@rediffmail.com

(Received on 11.08.10, accepted on 15.09.2010)

property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system. There is apparently no distinction between cyber and conventional crime. However on a deep introspection we may say that there exists a fine line of demarcation between the conventional and cyber crime, which is appreciable. The demarcation lies in the involvement of the medium in cases of cyber crime. The *sine qua non* for cyber crime is that there should be an involvement, at any stage, of the virtual cyber medium.(1)

For example, Ritu Kohli Case, being India's first case of cyber stalking, was indeed an important revelation into the mind of the Indian cyber stalker.A young Indian girl being cyber stalked by a former colleague of her husband, Ritu Kohli's case took the imagination of India by storm. The case which got cracked however predated the passing of the Indian Cyberlaw and hence it was just registered as minor offences under the Indian Penal Code.(2)

HOW CYBER CRIME TAKES PLACE

Various methods and techniques are applied while committing cyber crime. Some of them are given as following:

A. Unauthorized access to computer systems or networks / Hacking.

B. Theft of information which was contained in electronic form.

C. Email bombing

D. Data diddling

E. Salami attacks

F. Denial of Service attack

G. Virus / worm attacks

H. Logic bombs

I. Trojan attacks

J. Internet time thefts

K. Web jacking

E-MAIL RELATED CRIMES

Email is the world's most preferred form of communication. Like any other form of communication, email is also misused by criminal elements. The factors such as ease of access and use speed and relative anonymity of email has made it a powerful tool for criminals.(3) Some of the major email related crimes are:

A. Email spoofing

B. Sending malicious codes through email

C. Email bombing

D. Sending threatening emails

E. Defamatory emails

F. Email frauds

E-mail and Short Message Service (SMS) messages are seen as casual communication including many things that would never be put in a letter. But unlike spoken communication, there is no intonation and accenting, so the message can be more easily distorted or interpreted as offensive.

COMPUTER FRAUD

Computer fraud is any dishonest misrepresentation of fact intended to induce another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

1. Altering computer input in an unauthorized way. This requires little technical expertise and is not an uncommon form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;

2. Altering, destroying, suppressing, or stealing output, usually to conceal

unauthorized transactions: this is difficult to detect;

3. Altering or deleting stored data; or

4. Altering or misusing existing system tools or software packages, or altering or writing code for fraudulent purposes. This requires real programming skills and is not common.

5. Manipulating banking systems to make unauthorized identity theft with reference to ATM fraud.

PROVISIONS IN CYBER LAW

Various provisions are given in ITAA 2008. which are as following[4, 5, 6]:

Section No 43 deals with: Penalty and Compensation for damage to computer, computer system, etc.

Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008)

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 or computer resource (ITAA2008)

(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 thereunder,

(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,

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means (Inserted vide ITAA-2008)

(g) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, (Inserted vide ITAA 2008)

(h) he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. (Change vide ITAA 2008)

Section 43 A

Compensation for failure to protect data (Inserted vide ITAA 2006)

Where a body corporate, possessing, dealing or 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, not exceeding five crore rupees, to the person so affected. (Change vide ITAA 2008)

Offences

(i). Section 65 deals with: **Tampering with Computer Source Documents**

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

(ii). Section 66 deals with: **Computer Related Offences** (Substituted vide ITAA 2008)

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Explanation: For the purpose of this section,-

a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;

b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

(iii). Section 66 A deals with: **Punishment for sending offensive messages through communication service, etc.**(Introduced vide ITAA 2008)

Any person who sends, by means of a computer resource or a communication device,-

a) any information that is grossly offensive or has menacing character; or

b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008)

shall be punishable with imprisonment for a term which may extend to two three years and with fine.

(iv). Section 66 B deals with: **Punishment for dishonestly receiving stolen computer resource or communication device (Inserted Vide ITA 2008)**

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

(v) Section 66C deals with: **Punishment for identity theft. (Inserted Vide ITA 2008)**

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

(vi) Section 66D deals with: **Punishment for cheating by personation by using computer resource** (Inserted Vide ITA 2008)

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

(vii). Section 66E deals with: **Punishment for violation of privacy. (Inserted Vide ITA 2008)**

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three

years or with fine not exceeding two lakh rupees, or with both

Punishment for publishing or transmitting obscene material in electronic form (Amended vide ITAA 2008)

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or 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 two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

(i). Section 67 A deals with: Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form (Inserted vide ITAA 2008)

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or

(ii) which is kept or used bona fide for religious purposes.

***(ii). Section 67 B deals with* Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.**

Whoever,-

(a) Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) Creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) Facilitates abusing children online or

(e) Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) Which is kept or used for bonafide heritage or religious purposes

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

Breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

(i). Section 76 deals with: Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

PREVENTION OF CYBER CRIME

A. Prevention is always better than cure. It is always better to take certain precaution while operating the net. For online security precaution, prevention, protection, preservation and perseverance should be practised. A person should keep in mind the following things-

B. To prevent cyber stalking, a person should avoid disclosing any information pertaining to self.

C. None should send any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.

D. Always use latest and up date anti virus software to guard against virus attacks and keep back up volumes.

E. Any person should never send the credit card details to any site that is not secured, to guard against frauds.

F. The children should be watched regularly about their Internet and computer use.

G. 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.

AN EXAMPLE OF PUNE

The number of people coming forward with cyber crime complaints is on a significant rise. "In a year after the cyber cell of Pune police was started in July 2003 only nine complaints of cyber crime were received. There was a manifold rise as in the year 2008; Pune cyber crime Cell has received 2007 cyber crime complaints. The "Cop Tech" forum is an initiative of Pune police, NASSCOM and Data Security Council of India (DSCI) to increase sharing of ideas and knowledge on cyber security, for making Pune a cyber safe city. Police signed a memorandum of understanding (MoU) with NASSCOM, while launching the "Cop Tech" forum. This was the first MoU of its kind in the country.[11]

VARIOUS OFFICES FOR HELP

Cyber Police Station Mumbai BKC Police. Station Building Bandra Kurla Complex, Opp. I.C.I.C.I. Bank, Bandra E, Mumbai, Maharashtra - 400051 Tel:022 - 26504481, 26504882, 26504483 It comes under Kherwadi. Division,	**Cyber Cell Mumbai** Cyber Crime Investigation cell, Annex III, 1st floor, Office of the Commissioner of Police, D.N. Road, Mumbai - 400001 Email: officer@cybercellmumbai.com Tel: +91 - 022 - 24691233 http://www.cybercellmumbai.com/
Cyber Cell Bangalore Cyber Crime Police Station C.O.D Headquarters, Carlton House, # 1, Palace Road, Bangalore - 560 001 Tel.Nos. +91- 080-2201026 /+91- 080-2943050 Fax : +91 - 080- 2387611 e-mail : ccps@kar.nic.in **http://www.cyberpolicebangalore.nic.in/**	**CBI Cyber Cell** Supdt. of Police, Cyber Crime Investigation Cell Central Bureau of Investigation, 5th Floor, Block No. 3, CGO Complex, Lodhi Road, New Delhi - 3, Phone: 4362203, 4392424 : EMail: cbiccic@bol.net.in : Web: http://cbi.nic.in/
Cyber Cell Pune Assistant Commissioner of Police Cyber Crime Investigation Cell Police Commissioner Office of Pune 2, Sadhu Vaswani Road,Camp, Pune 411001 Contact Details: +91-20-26127277 +91-20-26165396 +91-20-26128105 (Fax) E-Mail: punepolice@vsnl.com	**Delhi Police** **http://delhipolice.nic.in/**

CONCLUSION

To fight cyber crime there needs to be a tightening of international digital legislation and of cross-border law enforcement co-ordination. But there is need to be a more creative and inventive response from the organisations under threat. Piecemeal, reactive security solutions are giving way to strategically deployed multi-threat security systems. Instead of having to install, manage and maintain disparate devices, organisations can consolidate their security capabilities into a commonly managed appliance. These measures combined, in addition to greater user education are the best safeguard against the deviousness and pure innovation of cyber-criminal activities.

REFERENCES

1 http://www.legalserviceindia.com/lawyers/delhi.htm.

2. Ritu Kohli vs. State of Maharashtra. 2003; 756 MH 843.

3. http://cybercrime.planetindia.net/email_crimes.htm
4. http://cybercrime.planetindia.net/it-act-2008.htm
5. http://cybercrime.planetindia.net/publication.htm
6. IT Act (Amendment) Act 2008, Google Docs. http://www.google.com/salient_features_of_the_IT_amendment_Act_2008. Pdf+information+technology+amendment+act+2008&hl=en&gl=in
7. http://www.cybercellmumbai.com/
8. http://www.cyberpolicebangalore.nic.in/
9. http://cbi.nic.in/
10. http://delhipolice.nic.in/
11. http://punekar.in/site/2009/07/01/cyber-crime-cases-are-on-the-rise-in-pune/