The world over cyber crime has taken deep root and the use of cyberspace by sophisticated cyber criminals has assumed serious proportion today. Criminals and terrorists associated with drug trafficking, terrorist outfits are employing Internet for anti social, anti national and criminal activities with impunity.

Terrorist groups are deftly using Internet for passing on information with regard to executing various terrorist acts having serious negative impact on human life. The cyber-terrorists have even acquired the capability to penetrate computer systems using “logic bombs” (coded devices that can be remotely detonated), electro magnetic pulses and high-emission radio frequency guns, which blow a devastating electronic wind through a computer system. The hackers have gone to the extent of distributing free hacking software -- Rootkit, for instance -- to enable an intruder to get root access to a network and then control as though they were the system’s administrators.

Many instances of cyber crime involve techno-trespass and unauthorized access to the computer system and data or programmes stored in computers. This access could be without authorization or exceeding the authorization given to an individual. The unauthorized access may lead to theft, alteration or destruction of data, tampering with computer programmes or other software, damage to computers or computer systems including damage to data stored on storage devices, such as hard disks, floppy disks, CD-ROMs, etc. This would, in turn, lead to serious financial loss to the organisation. Thus computer crime today has emerged as a challenge for criminal justice system and law enforcement.

Studies have shown that computer criminals are generally computer professionals or computer-literate persons and are not history sheeters and mostly without previous criminal record. Studies also show that the threat is mostly from employees or from those with access to the system, such as maintenance personnel, hardware and software vendors, etc. however, external threats via remote access have shown an increasing trend.

Broadly speaking, computer-related crimes may be categorized into two major categories:

1) Where the computer is a target of the crime.
2) Where computer is an instrument of the crime.

I. Computer as target of the Crime
In the first category of computer crimes, computer is the target of the crime. Some of
the crimes, which would fall under this category are:

a. Sabotage of computer systems or computer networks;
b. Sabotage of operating systems and programmes;
c. Theft of data/information (this is the fastest growing computer-related crime);
d. Theft of intellectual property, such as computer software;
e. Theft of marketing information; and
f. Blackmail based on information gained from computerized files, such as medical information, personal history, sexual preferences, financial data, etc.

II. Computer as an Instrument facilitating crime
In the second category of computer-related crimes, computer is used as an instrument facilitating crime. Most vivid example of computers being used as an instrument of Cyber crime has been the recent attack on parliament where computer and internet was used in a variety of ways to perpetrate the crime. The terrorist and criminals are using Internet methods such as e-mail, to flash encrypted messages around the globe. Frauds related to electronic banking or electronic commerce are other typical examples. In these crimes, computer programmes are manipulated to facilitate the crimes namely,

a. Fraudulent use of Automated Teller Machine (ATM) cards and accounts;
b. Credit card frauds;
c. Frauds involving electronic finds transfers;
d. Telecommunication Frauds; and
e. Frauds relating to Electronic Commerce and Electronic Data Interchange.

Theft of Intellectual Property Rights is also part of cyber space burglars. In USA alone, the Fortune 1000 companies suffer a loss of about 300 billion dollars annually on this account. Their targets are computer software, semiconductor, and pharmaceutical units. The conventional law dealing with these crimes are proving to be of Stone Age incapable of dealing with crime of lightening speed imparted by high technology.

Cybercrime and Indian Scenario
Although, Internet penetration in India is just 1%, the problem of Cybercrime has assumed serious proportion and appreciating the risk it poses to the Information Technology sector, the Information Technology Act, 2000 has delineated various kinds of offences and prescribed punishment for the commission of such offences.

The Act recognizes a number of computer crimes. Briefly these are destruction, alteration knowingly or intentionally of any computer source, documentation, computer system or computer network. It prescribes punishment of imprisonment of 3 years or fine of Rs2 Lakhs or both. Any misrepresentation to the certifying authorities or the controller for obtaining any licenses or digital signature certificate invites imprisonment of upto two years or fine of Rs.1 lakh or both. Similarly breach of confidentiality will invite imprisonment of 2 years or fine of Rs.1 lakh or both. The
Act contains a provision quite similar to the provision in most other statutes relating to offences committed by companies and their officers.

The provision of Act will apply to contravention committed outside the country by any person irrespective of his nationality. Similarly in case of offence committed outside India, if the act constituting involves a computer, computer system or computer network located in India, it would fall under the purview of this law. The Act contains provisions relating to power to search etc. In fact, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorized by the Central Government may enter any public place and search and arrest without warrant any person found who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act. The clause gives powers to the state to arrest a person even on suspicion and supposed to have deterrent effect on the commission of cybercrimes.

Some of the offences and punishment dealt under the Information Technology Act, 2000 are described below:

I. Damage to Computer, Computer system and Computer network: If any person without permission of the owner or any other person who is in charge 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 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, 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.  

II. 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.

Explanation. For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.  

III. Hacking with computer system.
(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack:
(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.  

(Section 43 of the IT Act, 2000)

(Section 65 of the IT Act, 2000)

(Section 66 of the IT Act, 2000)
IV. Publishing of information which is obscene in electronic form.

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 five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees. *(Section 67 of the IT Act, 2000)*

The enactment of the Information Act, 2000 has also led to amendments in the Reserve Bank of India Act, 1934, the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Indian Telegraph Act, 1885, the Bankers' Books Evidence act, 1891 and the General Clauses Act, 1857. These amendments have accorded electronic records and electronic signatures the same treatment as to the paper records and signatures for the purpose of complying with statutory writing, signature, evidentiary and record keeping. These Acts have been harmonized with the Information Technology Act, 2000.

**Indian Penal Code, 1860**

A number of amendments have been made to sections 29, 167, 172, 192, 463, 464 and the like. The key amendment relates to the widening of term document to include electronic records. Section 464 now recognizes the concept of digital signature.

**Indian Evidence Act, 1872**

The key provisions that are sought to be made in Indian Evidence Act relate to widening of the scope of term ‘document’ to include electronic record. Most importantly, section 65B recognises admissibility of computer outputs in the media, paper, optical or magnetic form. There are detailed provisions relating to admissibility of computer output as evidence. New section 73A prescribes procedures for verification of digital signatures. New Section 85A and 85B create presumption as regards electronic contracts, electronic records and digital signatures, digital signature certificates and electronic messages.

**Grey Areas in countering Cybercrime**

Although countries world over are highly concerned about combating cyber-crime. Nevertheless several problems exist. The first, and the most difficult, is to identify the culprit. As the Net can be accessed from any part of the globe, the field is wide open for hackers. Even if the identity of the hacker is established after following the electronic trail, it would be highly problematic to decide under which country's law he/she can be prosecuted.
If the country that suffered damage wants to prosecute a culprit of foreign nationality, there has to be an extradition treaty with the country where the hacker is resident. Besides, the legal framework for proceeding with prosecution is still not certain. In spite of the extradition treaty, if a law allegedly broken in a country has no equivalent in the culprit’s native country, there can be no prosecution.

In developing countries including India, the problem is further compounded because of the lack of training of cops on subjects such as computer forensics to investigate into cyber crimes or of the adjudicating officers. This will adversely affect the fight against cybercrime. Unless the police is able to retrieve data from a computer, they would not be able to deal with the cyber crimes in right earnest.

The Indian Information Technology Act also prescribes low penalty for hackers. The maximum penalty for hackers is only Rs 3 lakh, which is very low, compared to the damages they cause. Ideally the penalty should be over and above the damages caused. The Indian Act also does not have any specific mention of frauds related to misuse of credit card numbers. Since computer crime has international dimensions, the international cooperation is a pre-requisite to prevent computer crimes. Although international concern was expressed in UN Manual on the prevention and control of computer related crimes, but it lacks the teeth.

There is also an absence of bilateral treaties/international legislature to deal with cross-border cyber crimes leaves organisations vulnerable to threats of attacks from other countries. In fact, an international agreement on dealing with cyber crime is urgently needed to address the problem in holistic manner. In this light, the idea to declare Cybercrime a crime against humanity on the lines of "piracy" and "hijacking" should be seriously pondered over.

Distance between criminals and authorities has become enormous as the cybercrime has acquired international dimensions. The criminals can move on a high way at the speed of light on which there are no traffic signals, no constables, without international border with no custom or immigration authorities to call the criminal to halt.

As the world basks in its achievements in the field of Communications and Information Technology, it has become highly imperative to check the menace of Cybercrime.

(Atul Kumar, an Attorney at law, is with Corporate Law Group, New Delhi. Reach him at atulkumar@clgindia.com and kratul@rediffmail.com.)

Source: http://www.inomy.com/ 01/03/2002