CHAPTER IV
INFORMATION TECHNOLOGY ACT AND ITS APPLICATIONS

INTRODUCTION

New information technology and communication systems have made dramatic changes in the way we live and the means to transact our daily business. Businessmen are increasingly using computers to create, transmit and store information in electronic form instead of traditional paper documents. It is cheaper, easier to store and retrieve and speedier to communicate. Although people are aware of the advantages of the electronic form of business provides, they are also reluctant to conduct business or conclude and transaction in the electronic form due to lack of appropriate legal framework. Electronic commerce eliminates need for paper based transactions. The two principal hurdles which stand in the way of facilitating information technology applications in various fields and electronic governance, are the requirements of storing, accessing, writing and signature for legal recognition. At present many legal provisions assume the existence of paper based records and documents which should bear signatures. The Law of Evidence is traditionally based upon paper-based records and oral testimony. Hence, to facilitate information technology applications, the need for legal changes has become an urgent necessity.

This chapter covers the overall details of Information Technology Act and its Applications in the field of education system and in the day to day work within the organization.
The majority of cyber related incidents are the result of error or negligence, and therefore this chapter also tries to evaluate cyber crime awareness to educate the students of how to be aware of threats and to have a secure internet usage.

The Government of India realized the need for introducing a new law and for making suitable amendments to the existing laws to facilitate information technology applications and give legal recognition to electronic records and digital signatures. The legal recognition to electronic records and digital signatures in turn will facilitate the conclusion of contracts and the creation of legal rights and obligations through the electronic communication like Internet. This gave birth to the Information Technology Bill, 1999.

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for information technology applications and e-commerce in India and would have a major impact businesses and the new economy in India. An Information Technology Act provides legal recognition for the transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "Electronic Commerce", which involve the use of alternatives to paper based methods of communication and storage of information.

The Information Technology Act, 2000 also aims to provide the legal framework under which legal sanctity is accorded to all electronic records and
other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal Code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes.

THE INFORMATION TECHNOLOGY ACT AND IT’S OBJECTIVES

The Information Technology Act is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.
Objectives of the Information Technology Act are:

i) To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as “electronic commerce” in place of paper based methods of communication;

ii) To give legal recognition to Digital signatures for authentication of any information or matter which requires authentication under any law.

iii) To facilitate electronic filing of documents with Government departments.

iv) To facilitate electronic storage of data.

v) To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions.

vi) To give legal recognition for keeping of books of accounts by banker’s in electronic form.

vii) To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker’s Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

**CYBER CRIME**

Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth
to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

The Cyber crime can be categorize in two ways:

a) The Computer as a Target : using a computer to attack other computers.
   e.g. Hacking, Virus/Worm attacks, DOS attack etc.

b) The computer as a weapon : using a computer to commit real world crimes.
   e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

INFORMATION TECHNOLOGY ACT AND BUSINESS SCHOOLS

The information technology is being widely used all the areas of life. The increasing demand for management education, change in nature of business and industry within the newly created borderless market environment, and the revolution in information technology provide an opportunity to change the curricula and delivery system of management education so as to provide prospective managers an edge to successfully face the challenge in globally competitive setting. Therefore, management education and IT has to develop a mutually supportive relationship for achieving excellence.

India is using multi-technologies in imparting management education. At the one end, some premier institutions are having access to all facilities in terms of educational technology such as multimedia system, LAN, WAN, and World Wide Web on the other hand a large number of business school are still
depending only on stereotyped lecture method in imparting knowledge. Therefore the existence of technology gap provides an opportunity to use IT supported education technologies for better delivery of education, easier access to a number of knowledge sources, sharing through networks and quality distance learning in management education.

It is of major concern that the staff and students while using the information technology facilities might not be aware of the laws related to information technology. Hence it is a crucial issue that the users of information technology must be aware of the information technology act and the penalties for abiding these rules.

The following Table No. 4.1 shows the various types of crimes and the penalties implemented in Information Technology Act.

<table>
<thead>
<tr>
<th>Sr.No.</th>
<th>Types of Offences / Crime</th>
<th>Penalty</th>
<th>Precautions to be taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Damage to Computer and Computer Systems</td>
<td>Imprisonment upto one year and/or fine upto one lakh rupees.</td>
<td>Don’t allow unauthorized person to enter or use the computer systems.</td>
</tr>
<tr>
<td>2.</td>
<td>Destroy or alter any information residing in the computer resource or web site</td>
<td>Imprisonment upto 3 years and/or fine upto two lakh rupees.</td>
<td>Check for the systems and web sites with fixed time interval.</td>
</tr>
<tr>
<td></td>
<td>Information Technology Offences and Penalties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Hacking with computer system / deleting or altering the information stored in computer system</td>
<td>Imprisonment upto 3 years and/or fine of Rs.2 lakhs.</td>
<td>Don’t disclose the passwords of the computer systems with unauthorized persons.</td>
</tr>
<tr>
<td>4.</td>
<td>Sending offensive messages through electronic mail or electronic message</td>
<td>Punishment with imprisonment which may extend upto 3 years.</td>
<td>Secure your e-mail IDs and passwords.</td>
</tr>
<tr>
<td>5.</td>
<td>Cyber Terrorism – intent to threaten the unity, integrity, security of India</td>
<td>Punishment with imprisonment which may extend to imprisonment of life.</td>
<td>Don’t share passwords of your personal computers with colleagues and outsiders, which may send the false messages and news through your computer system.</td>
</tr>
<tr>
<td>6.</td>
<td>Publishing or transmitting obscene material in electronic form.</td>
<td>Imprisonment for a term which may extend to 5 years and fine of Rs. 5 lakh.</td>
<td>Don’t allow unauthorized person to enter or use the computer systems.</td>
</tr>
<tr>
<td>7.</td>
<td>Disclosure of information in Breach of Lawful Contract – Publishing wrong Digital Signature Certificate</td>
<td>Imprisonment upto 2 years and/or fine of Rs. One lakh rupees.</td>
<td>Check the transactions regularly to and verify them regularly.</td>
</tr>
</tbody>
</table>


**INFORMATION TECHNOLOGY OFFENCES AND PENALTIES**

The Information Technology Act provides the explanation on various information technology offences and the respective penalties and compensations. Some of the major offences and the penalties are as follows:

1) **Damage To Computer And Computer Systems - Penalty and Compensation :**

The Information Technology Act provides the facility of penalty to any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network -
(a) access 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 authorized 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,

(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.
(j) 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.

The overall net effect of IT Act, 2000 has come into operation. The information in the electronic format has been granted legal validity and sanction, digital signatures have been defined and made legal. It is now possible to retain information in an electronic format. Electronic contract has been recognized to be legal and binding. Some types of cyber crimes have been defined and made punishable offences like hacking, damage to computer source code, publishing of information which is obscene in the electronic form, breach of confidentiality and privacy and publishing digital signature certificate false in certain particulars and for fraudulent purpose.

2) Intentionally Tampering With The Computer Source Code Documents - Penalty and Compensation:

“Computer Source Code” means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

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.
3) **Hacking with Computer System - Penalty and Compensation:**

‘Hacking’ is a term used to describe the act of destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility, or affecting it injuriously in spite of knowing that such action is likely to cause wrongful loss or damage to the public or that person.

The Information Technology Act provides that a person who commits hacking shall be punished with a fine upto Rs.2 lakhs or with imprisonment upto 3 years, or with both.

4) **Sending Offensive Messages Through Communication Service, etc. - Penalty and Compensation:**

"Electronic Mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

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

5) **Identity Theft - Penalty and Compensation:**

    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 5 years or liable to fine which may extend to one lakh rupees or both.

6) **Violation of Privacy - Penalty and Compensation:**

    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.

(a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) “capture”, with respect to an image, means to videotape, photograph, film or record by any means;

(c) “private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) “publishes” means reproduction in the printed or electronic form and making it available for public.

7) **Cyber Terrorism - Penalty and Compensation:**
Whoever,

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to
the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life’.

8) Publishing of information which is obscene in electronic form - Penalty and Compensation :

Information Technology Act has provision for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to five years and with fine which may extend to Rs.1 lakh on first conviction. In the event of second or subsequent conviction the imprisonment would be for a term which may extend to ten years and fine which may extend to Rs. 2 lakhs.

9) Publishing or Transmitting Obscene Material in Electronic Form - Penalty and Compensation :

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.

10) Publishing or Transmitting of Material Containing Sexually Explicit Act, etc. in Electronic Form - Penalty and Compensation:

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.

11) Misrepresentation - Penalty and Compensation:

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, 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.

There is a punishment for breach of confidentiality and privacy of electronic records, books, information, etc. by a person who has access to them without the consent of the person to whom they belong with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both.
If anybody 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, then it is considered as breach of confidentiality and privacy, hence the 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.

12) Disclosure of Information in Breach of Lawful Contract - Penalty and Compensation:

Any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both. The Act provides punishment for publishing a Digital Signature Certificate false in material particulars or otherwise making it available to any other person with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both.

CONCLUDING REMARKS

Until recently, many information technology (IT) professionals lacked awareness of and interest in the cyber crime phenomenon. In many cases, law
enforcement officers have lacked the tools needed to tackle the problem; old laws didn’t quite fit the crimes being committed, new laws hadn’t quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance.

India needs total international cooperation with specialised agencies of different countries. Police has to ensure that they have seized exactly what was there at the scene of crime, is the same that has been analysed and the report presented in court is based on this evidence. It has to maintain the chain of custody. The threat is not from the intelligence of criminals but from our ignorance and the will to fight it. The law is stricter now on producing evidence especially where electronic documents are concerned.

The computer is the target and the tool for the perpetration of crime. It is used for the communication of the criminal activity such as the injection of a virus/worm which can crash entire networks.

The Information Technology Act, specifies the acts which have been made punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T., certain omissions and commissions of criminals while using computers have not been included, several offences having bearing on cyber-arena are also registered under the appropriate sections of the IPC.

Cyber Crimes are a new class of crimes to India rapidly expanding due to extensive use of internet. Getting the right lead and making the right interpretation are very important in solving a cyber crime.
It is of crucial importance that all the staff and students of business schools should have proper knowledge of Information Technology Act so that they can take care of themselves while using the facilities of information technology in their routine work.

REFERENCES

Books:

Article:
“Cyber Law & Information Technology”, Talwant Singh, Addl. Distt. & Sessions Judge, Delhi

Internet Sites:
1. www.legalserviceindia.com/cyber/itact.html

###