5 - (1)

Cybercrimes and Cyber security

1. Why Do We Need Cyber laws: The Indian Context.
2. The Indian IT Act.
3. Challenges to Indian Law and Cybercrime Scenario in India
4. Consequences of Not Addressing the Weakness in Information Technology Act.
5. Digital Signatures and the Indian IT Act.
6. Information Security Planning and Governance.
7. Information Security Policy Standards and Practices.
8. The information Security Blueprint.
9. Security education, Training and awareness program.
10. Continuing Strategies.

Why Do We Need Cyberlaws: The Indian Context

- Cyberlaw is a framework created to give legal recognition to all risks arising out of the usage of computers and computer networks.
- Under the preview of cyberlaw, there are several aspects, such as, *intellectual property*, *data protection and privacy*, *freedom of expression* and *crimes committed using computers*.
- The Indian Parliament passed its first cyberlaw, the ITA 2000, aimed at providing the legal infrastructure for E-Commerce in India. IT Act 2000
- ITA 2000 received the assent of the President of India and it has now become the law of the land in India.
- The Government of India felt the need to enact relevant cyberlaws to regulate Internet based computer related transactions in India.
- It manages all aspects, issues, legal consequences and conflict in the world of cyberspace, Internet or WWW.
- In the Preamble to the Indian ITA 2000, it is mentioned that it is an act 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*.
- The reasons for enactment of cyberlaws in India are summarized below:

5 (3)

1. Although India possesses a very well defined legal system, covering all possible situations and cases that have occurred or might take place in future, the country lacks in many aspects when it comes to newly developed Internet technology. It is essential to address this gap through a suitable law given the increasing use of Internet and other computer technologies in India.
2. There is a need to have some legal recognition to the Internet as it is one of the most dominating sources of carrying out business in today's world.
3. With the growth of the Internet, a new concept called *cyberterrorism* came into existence.

- Cyberterrorism includes the use of disruptive activities with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives in the world of cyberspace. It actually is about committing an old offense but in an innovative way.
- Keeping all these factors into consideration, Indian Parliament passed the Information Technology Bill on 17 May 2000, known as the ITA 2000.
- It talks about cyberlaws and forms the legal framework for electronic records and other activities done by electronic means.

The Indian IT Act

- As mentioned above, this Act was published in the year 2000 with the purpose of providing legal recognition for transactions carried out by means of electronic data interchange, commonly referred to as *electronic commerce*.
- Electronic communications 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.
- Another purpose of the Indian IT Act was to amend the Indian Penal Code (IPC), the Indian Evidence Act 1872, the Bankers' Books Evidence Act 1891, the Reserve Bank of India Act 1934 and matters connected therewith or incidental thereto.
- The Reserve Bank of India Act has got Section 58B about Penalties. Subsequently, the Indian IT Act underwent some important changes to accommodate the current cybercrime scenario; a summary of those changes is presented in Table 6.7 – note

Need of Information Security Policy

- aim of Information security Policy is to Protect the data & limit to Unauthorized access.

⇒ Establish a general approach to Information Security
⇒ Document Security measures & user access control policies.
⇒ Detect & minimize the misuse of data, networks, mobile devices & Computers.
⇒ Protect the reputation of the organization.
⇒ Protect Customers data such as Credit Card Numbers.
⇒ Provide effective mechanisms to responds to complaints.

Elements of Information Security Policy

Information Security Objectives

- Confidentiality
- Integrity
- Availability

Authority & access control

- Hierarchical Pattern
- Network Security Policy

Data Support & operation

- Data protection Regulation
- Data Backup
- movement of Data

Introduction to Indian Cyber law (IT law)

Cyber law is the law governing cyber space. Cyber space include Computer, S/W, H/W, networks etc, Internet, email, websites etc.

Law

1. That have been approved by government.
2. Which are in force over a certain Territory.
3. must be obeyed by all persons on that territory.

Section 66 - using password of another person

Section 66D - Cheating using computer resource

Section 66E - Publishing private Images of others

Section 66F - Act of Cyber Terrorism

Section 69 - Govt's power to Block websites

Section 43A - Data protection at corporate level

No of Cyber crime cases Reported in year 2016.

UP - 2700
Maharashtra - 2400
Karnataka - 1400
Rajasthan - 900

National Crime Record Bureau

Areas of Cyber law

1. Fraud
2. Copyright
3. Harassment
4. Stalking
5. Trade secrets
6. Freedom of speech

Objective & Scope of the Digital Personal Data protection Act 2023

On August 11, 2023 India enacted the Act

Introduced	→	Passed	→	Passed	→	Signed by President of India
Lok Sabha		Lok Sabha		Rajya Sabha		
Aug 03, 2023		Aug 07, 2023		Aug 09, 2023		Aug 11, 2023

Highlights of the Bill

- The Bill will apply to the processing of Digital Personal Data within India where such data is collected online, or collected offline and is Digitised. It will also apply to such processing outside india, if it is for offering goods or services in India.
- Personal data may be processed only for a lawful purpose upon consent of an Individual.
- Bill grants certain rights to individuals including the right to obtain information, seek correction & erasure

→ The Bill does not regulate risk of Harm arising from processing of personal Data.

→ The Bill does not grant the right to data portability and the right to forgotten to the data principal.

→ The Bill allow transfer of personal data outside India.

→ The members of the Data protection Board of India will be appointed for Two years and will be eligible for re-appointment

Penalties

ⓐ Rs 200 crore for non-fulfilment of obligations for children

ⓑ Rs 250 crore for failure to take security measures to prevent data breaches.

specially the changes to Section 66 and the corresponding punishments for cyber offenses.

- The scope and coverage of the Indian IT Act is briefly described in Section 27.4, Ref. #6, Books, Further Reading.
- The structure of the Indian ITA 2000 is provided in Table 6.6 for readers' immediate reference.
- The sections mentioned in bold italics are relevant in the discussion of cybercrime and information security.

ITA Sections are as follows:

1. Section 65: Tampering with computer source documents
2. Section 66: Computer-related offences
3. Section 67: Punishment for publishing or transmitting obscene material in electronic form
4. Section 71: Penalty for misrepresentation
5. Section 72: Penalty for breach of confidentiality and privacy
6. Section 73: Penalty for publishing Digital Signature Certificate false in certain particulars
7. Section 74: Publication for fraudulent purpose

Positive Aspects of the ITA 2000

The Indian ITA 2000, though heavily criticized for not being specific on cybercrimes, in our opinion, does have a few good points.

1. Prior to the enactment of the ITA 2000 even an E-Mail was not accepted under the prevailing statutes of India as an accepted legal form of communication and as evidence in a court of law. But the ITA 2000 changed this scenario by legal recognition of the electronic format. Indeed, the ITA 2000 is a step forward.
2. From the perspective of the corporate sector, companies are able to carry out E-Commerce using the legal infrastructure provided by the ITA 2000. Till the coming into effect of the Indian cyberlaw, the growth of E-Commerce was impeded in our country basically because there was no legal infrastructure to regulate commercial transactions online.

3. Corporate will now be able to use digital signatures to carry out their transactions online. These digital signatures have been given legal validity and sanction under the ITA 2000A.
4. In today's scenario, information is stored by the companies on their respective computer system, apart from maintaining a backup. Under the ITA 2000, it became possible for corporate to have a statutory remedy if anyone breaks into their computer systems or networks and causes damages or copies data. The remedy provided by the ITA 2000 is in the form of monetary damages, by the way of compensation, not exceeding `10,000,000.
5. ITA 2000 defined various cybercrimes. Prior to the coming into effect of the Indian Cyberlaw, the corporate were helpless as there was no legal redress for such issues. However, with the ITA 2000 instituted, the scenario changed altogether.

Weak Areas of the ITA 2000

As mentioned before, there are limitations too in the IT Act; those are mainly due to the following gray areas:

1. The ITA 2000 is likely to cause a conflict of jurisdiction.
2. E-Commerce is based on the system of domain names. The ITA 2000 does not even touch the issues relating to domain names.
3. The ITA 2000 does not deal with issues concerning the protection of Intellectual Property Rights (IPR).
4. As the cyberlaw is evolving, so are the new forms and manifestations of cybercrimes. The offenses defined in the ITA 2000 are by no means exhaustive.
5. The ITA 2000 has not tackled issues related to E-Commerce like privacy and content regulations.

Challenges to Indian Law and Cybercrime Scenario in India

The offenses covered under the Indian ITA 2000 include:

1. Tampering with the computer source code or computer source documents;
2. un-authorized access to computer ("hacking" is one such type of act);
3. publishing, transmitting or causing to be published any information in the electronic form which is lascivious or which appeals to the prurient interest;

4. failure to decrypt information if the same is necessary in the interest of the sovereignty or integrity of India, the security of the state, friendly relations with foreign state, public order or for preventing incitement to the commission of any cognizable offense;
5. securing access or attempting to secure access to a protected system;
6. misrepresentation while obtaining any license to act as a Certifying Authority (CA) or a digital signature certificate;
7. breach of confidentiality and privacy;
8. publication of digital signature certificates which are false in certain particulars;
9. publication of digital signature certificates for fraudulent purposes.

- There are legal drawbacks with regard to cybercrimes addressed in India – there is a need to improve the legal scenario.
- These drawbacks prevent cybercrimes from being addressed in India.
- **First**, the difficulties/ drawbacks with most Indians not to report cybercrimes to the law enforcement agencies because they fear it might invite a lot of harassment.
- **Second**, their awareness on cybercrime is relatively on the lower side.
- Another factor that contributes to the difficulty of cybercrime resolution is that the law enforcement agencies in the country are neither well equipped nor knowledgeable enough about cybercrime.
- There is a tremendous need for training the law enforcement agencies in India. Not all cities have cybercrime cells.
- Most investigating officers with the Police force may be well equipped to fight cybercrime we need dedicated, continuous and updated training of the law enforcement agencies.

Consequences of Not Addressing the Weakness in Information Technology Act

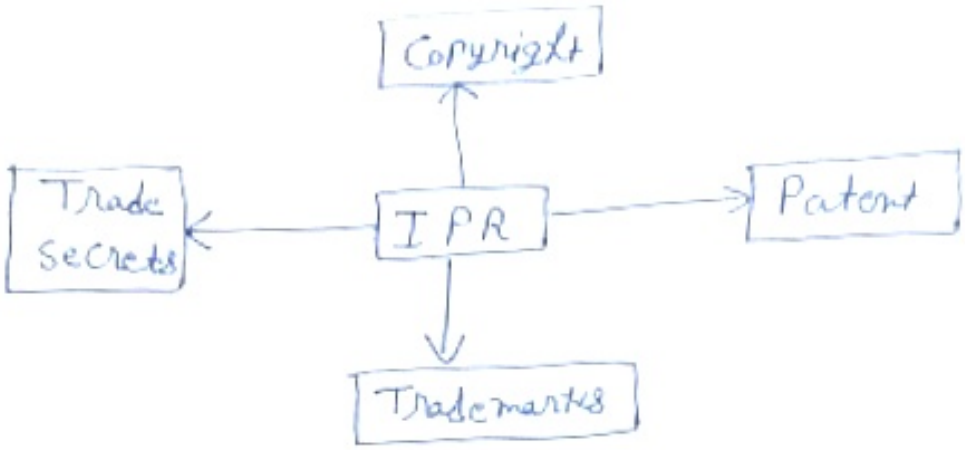
- In light of the discussion so far, we can see that there are many challenges in the Indian scenario for fight with cybercrime.
- Cyberlaws of the country are yet to reach the level of sufficiency and adequate security to serve as a strong platform to support India's E-Commerce industry for which they were meant. India has lagged behind in keeping pace with the world in this regard.
- The consequences of this are visible – India's outsourcing sector may get impacted.

Intellectual Property Rights (IPR)

IPR are the rights given to each & every person for creating of new thing according to their minds.

IPR usually give the creator a complete right over the use of his creation for a certain period of time.

IPR is the legal rights that cover the benefits given to individuals who are the owners are inventors of work.



Advantages of IPR

- IPR yields exclusive right to the creators or Inventors.
- It encourage individuals to distribute & share information & data instead of keeping it confidential.
- It provides legal defense & offers the creators the incentive of their work.
- It help in social & financial development
- It inspires people to create new thing without fear.

Indian Trademark Act – 1999
Copyright Act – 1957
Patent Act_1957
Design Act – 2000
IT Act – 2000

Copyright © → Books, Video, music, computer programs

Patent → Disclosure of the invention

Trademark → letter, logo, graphic, shape, sound ®

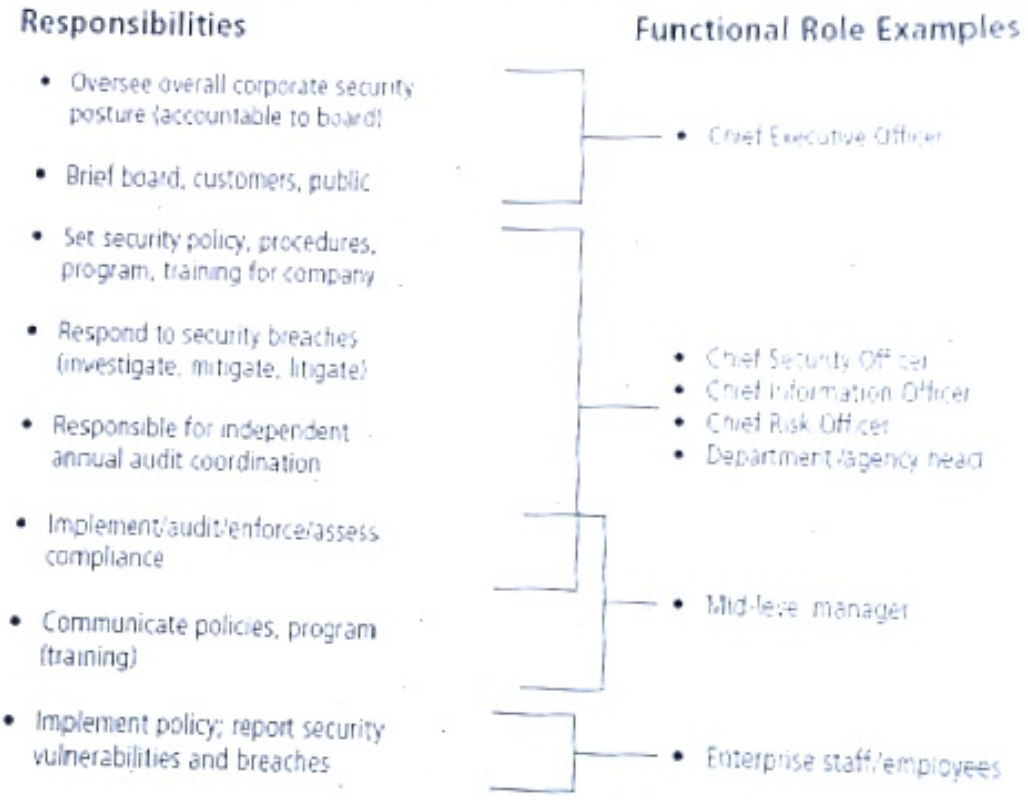
Trade secrets → formula of any product

objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly."

c **Information security governance:** The application of the principles of corporate governance to the information security function

According to the Information Technology Governance Institute (ITGI), information security governance includes all of the accountabilities and methods undertaken by the board of directors and executive management to provide:

- Strategic direction
- Establishment of objectives
- Measurement of progress toward those objectives
- Verification that risk management practices are appropriate
- Validation that the organization's assets are used properly



Information Security Governance roles and responsibilities

Information Security Policy, Standards, and Practices

- Management from all communities of interest, including general staff, information technology, and information security, must make policies the basis for all information security planning, design, and deployment.
- Policies direct how issues should be addressed and how technologies should be used.
- Policies do not specify the proper operation of equipment or software - this information should be placed in the standards, procedures, and practices of users' manuals and systems documentation.
- In addition, policy should never contradict law.
- Policy must be able to stand up in court, if challenged; and policy must be properly administered through documented acceptance. Otherwise, an organization leaves itself

Policy as the Foundation for Planning

a. **de facto standard :** A standard that has been widely adopted or accepted by a public group rather than a formal standards organization. Contrast with a de jure standard.

b. **de jure standard** : A standard that has been formally evaluated, approved, and ratified by a formal standards organization. Contrast with a de facto standard.

c. **Guidelines**: Within the context of information security, a set of recommended actions to assist an organizational stakeholder in complying with policy.

d. **Information security policy:** A set of rules that protects an organization's information assets.

e. **Policy**: A set of principles or courses of action from an organization's senior management intended to guide decisions, actions, and duties of constituents.

f. **Practices**: Within the context of information security, exemplary actions that an organization identifies as ideal and seeks to emulate. These actions are typically employed by other organizations.