04 Introduction to Security Policies and Cyber Laws

OBJECTIVES

- Need for information security policy
- ISO Information security standards
- Various security policies and their review process
- Indian cyber law
- Objective and scope of the IT Act, 2000
- Intellectual property issues
- Intellectual-property-related legislation in India
- The Patent Law
- The copyright law
- The semiconductor law
- Software License

An information security policy is the documentation of organizational-level decisions on safeguarding information. While taking these decisions, managers face difficulty in making choices for resource allocation, competing objectives, and organization strategy related to safeguarding both technical and information resources and guiding employee behavior.

While designing an information security policy, it is ideal to understand that information is an asset and property of an organization. As such, information reaches beyond the territories of Information Technology (IT) and is present in all the areas of an organization. For effective results, an information security policy should be a part of the organization's asset management program and be organization wide.

There are various forms, styles, and kinds of security policies as there are different organizations, businesses, agencies, and universities. Apart from the various forms, each organization has a particular culture or mental model on the basis of which a policy should look and approve the document. The important aspect to be noted here is that each organization requires an information security policy.

The chapter begins with the need for security policies. Then it discusses about the International Standard Organization (ISO) information security standards. Further, you learn about various security policies and their review process. Apart from the security policies, the chapter also discusses about the Indian cyber law and the objective or scope of the IT Act, 2000. Next, it introduces you to the intellectual property issues and the Intellectual Property Related (IPR) legislation in India. Finally, the chapter explains the various laws such as patent, copyright, semiconductor, and software license.

4.1 Need for an Information Security Policy

From the software professional's perspective, the overall objective of an information security policy is to protect the integrity, confidentiality, and availability of information. It is true from the security perspective; however, not the organization objective. It is known that information is an asset and the property of an organization. As an asset, the management of an organization is expected to ensure that the appropriate levels of controls are in place to protect this resource.

An information security policy should be part of any organization's overall asset security policy. This policy is not defined to meet the security needs or audit requirements; it is a business process that allows management with the processes required to perform the fiduciary responsibility. The management of an organization is charged with a trust to ensure that adequate controls are in place to safeguard the asset of an enterprise. The security policies, standards, and procedures define a security program.

The information security professionals of an organization are responsible to implement security policies that depict the business and mission requirements of an organization.

Let's now discuss the information security standards defined by ISO.

4.2 Information Security Standards – ISO

It is known that security plays an important role in safeguarding the assets of an organization. As no single formula can guarantee 100% security, there is a requirement for a set of standards to ensure that the appropriate level of security is achieved, resources are utilized efficiently, and the best security practices are implemented. This section discusses the various standards and regulations available for information security.

The ISO, established in 1947, is a non-governmental international body that collaborates with the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU). ISO has laid the following security standards:

- **ISO/IEC 27002:2005 (Code of practice for information security management)**: Refers to a code of practice for information security management which sets as a common basis and practical guideline for developing enterprise-level security standards and effective management practices.

  This standard specifies guidelines and best practices recommendations for the following ten security domains:

  - Security policy
  - Organization for information security
  - Asset management
  - Human resource security
  - Physical and environmental security
  - Communications and operations management
  - Access control
  - Information systems acquisition, development, and maintenance
  - Information security incident management
  - Business continuity management and compliance

- **ISO/IEC 27001:2005 (information security management system – requirements)**: Specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System (ISMS) within an organization. This standard allows an organization to select the adequate and proportionate security control to secure information assets. This standard is applicable for all types of organizations, including business enterprises, government agencies, etc.

  This standard defines a cyclic model known as "Plan-Do-Check-Act" (PDCA) model with the objective of establishing, implementing, monitoring, and improving the effectiveness of an enterprise's ISMS. The phases of the PDCA cycle are as follows:

  - The Plan phase to establish the ISMS
  - The Do phase to implement and operate the ISMS

- The Check phase to monitor and review the ISMS
- The Act phase to maintain and improve the ISMS

❒ **ISO/IEC 15408 (evaluation criteria for IT security)**: Consists of three parts: ISO/IEC 15408-1:2005 (introduction and general model), ISO/IEC 15408-2:2005 (security functional requirements), and ISO/IEC 15408-3:2005 (security assurance requirements). This standard helps an organization in evaluating, validating, and certifying the security assurance of a technology product against various factors such as security functional requirements specified in the standard.

❒ **ISO/IEC 1335 (IT Security Management)**: Consists of a series of guidelines for technical security control measures such as:

- The ISO/IEC 13335-1:2004 standard defines the concepts and models for information and communication technology security management
- The ISO/IEC TR 13335-3:1998 standard defines the techniques for the management of IT security
- The ISO/IEC TR 13335-4:2000 standard covers the selection of safeguards
- The ISO/IEC TR 13335-5:2001 covers management guidance on network security

4.3 Introducing Various Security Policies and Their Review Process

It has been discussed earlier that many organizations are required to develop and maintain specific security policies and procedures. Apart from designing a security policy, its review process is also essential to ensure that the policy is appropriate or adequate. Let's begin with a discussion on the following types of security policies and then focus on the review process:

❒ The World Wide Web (WWW) policy

❒ The e-mail security policy

❒ The corporate policy

This section also presents yet another sample security policy.

■ WWW Policy

The Internet is a network of networks providing various services such as sending e-mails, transferring files, login from remote systems, and WWW. The WWW is the universe of the

Internet-accessible information. While browsing the Internet, there are various risks, some of which are as follows:

- The software provided to the employees for business use can be used for any for-profit outside business activity or potentially embarrasses the company
- The software or documents downloaded over the WWW can contain virus
- The users of an organization while browsing the Internet can access sites containing offensive materials

To avoid such risks, the organization needs to define the WWW policy. Some examples of WWW policy are as follows:

- No offensive or harassing material may be made available through company websites
- No personal commercial advertising should be made available through company websites
- The personal material on or accessible from the website should be minimal
- No company confidential material should be made available
- Users of an organization should not be permitted to install or run Web servers

E-mail Security Policy

E-mails can be used not only to improve the communication between employees, but also to transmit proprietary information, harass other users, engage in illegal activities, and serve as evidence against the company in legal actions. E-mail is actually the electronic version of a postcard and requires special policy considerations from archiving to content guidelines. Therefore, the organizations should take various points into consideration while writing e-mail policies.

Generally, while creating an e-mail policy, the general rules and guidelines that users need to follow should appear first in the e-mail policy document. An organization can include the following "Ten Commandments of E-mail" while developing an e-mail policy:

1. You will [may be replaced may be complicated by readers] demonstrate the same respect thy gives to verbal communications.
2. You will check thy spelling, thy grammar, and read thine own message thrice before thou send it.

3. You will not forward any chain letter.
4. You will not transmit unsolicited mass e-mail (spam) unto anyone.
5. You will not send messages that are hateful, harassing, or threatening unto fellow users.
6. You will not send any message that supports illegal or unethical activities.
7. You will remember thine e-mail is the electronic equivalent of a post card and will not be used to transmit sensitive information.
8. You will not use thine email broadcasting facilities except for making appropriate announcements.
9. You will keep thy personal email use to a minimum.
10. You will keep thy policies and procedures sacred and help administrators protect them from abusers.

■ Corporate Policy

Corporate policy is the formal declaration of the principles and procedures according to which a company will operate. These principles or guidelines are laid down by the board of directors of a company or the senior management policy committee. A corporate policy comprises:

- Company's mission statement
- Company's objectives
- Principles on the basis of which strategic decisions are made

A corporate policy also lays down the factors for measuring performance and ensuring accountability at all levels of an organization. It is also known as company policy, which is defined after an analysis of all internal and external factors, affecting an organization's objectives, operations, and plans.

■ Sample Security Policy

Let's now look at the sample security policy. The template of the sample security policy is as follows:

1. Information security policy
   a. Purpose

b. Aims and commitments

c. Responsibilities

d. Councils

e. Heads of departments

f. Users and external parties

2. Risk assessment and the classification of information

a. Risk assessment of information held

b. Personal data

3. Protection of information systems and assets

4. Protection of confidential information

a. Storage

b. Access

c. Remote access

d. Copying

e. Disposal

f. Use of portable devices or media

g. Exchange of information and use of e-mail

h. Cryptographic controls

i. System planning and acceptance

j. Backup

k. Further information

l. Hard copies

i. Protective marking

ii. Storage

iii. Removal

iv. Transmission

v. Disposal

j. Enforcement

k. Compliance

l. Other relevant university policies or guidance

m. Contacts for further information

n. Sample risk assessment

o. Scope, criteria, and organization

   i. Scope

   ii. Criteria

5. Risk identification and analysis

   a. Assets

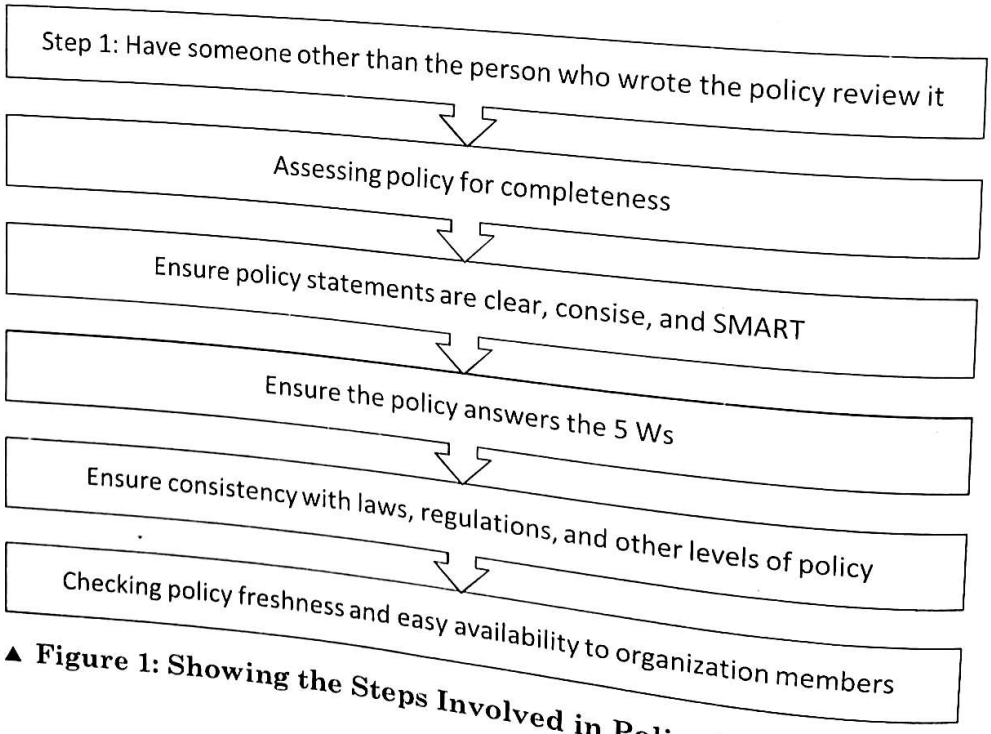
   b. Threats and risks

6. Appendix 1: Sample risk assessment

7. Glossary

■ Policy Review Process

Each policy created should be reviewed appropriately to ensure successful policy development. Figure 1 shows the six important steps to be performed while evaluating information
security policy:



▲ **Figure 1: Showing the Steps Involved in Policy Review Process**

Let's discuss each of these steps in detail.

- **Step 1:** Having someone other than the person who wrote the policy review it: Generally, people tend to identify their own errors in a small percentage of time. Therefore, someone other than the person who created the policy should review and assess for mistakes. The policy reviewer should be aware about the organization fundamentals of information security and detail oriented for best results. Moreover, the person should be technically sound to review the policy for technical accuracy.

  The security policy should have an owner who has approved management responsibility for the development, review, and evaluation of the policy. Instead of the policy owner, the other person or team should be assigned the task to improvise the policy.

- **Step 2:** Assessing policy for completeness: The second step is divided into the following sub steps:

  - Assessing policy framework for completeness: Checks or examines the existence of standards and procedures supporting the policy set
  - Assessing policy elements for completeness: Checks or examines if the policy is not flawed due the lack of an element

- **Step 3:** Ensuring that policy statement is clear, concise, and SMART: SMART stands for specific, measurable, achievable, realistic, and time-bound. In this step, the policy reviewer ensures that the policy is clear, and simple language is used to ensure that it can be easily understood by everyone.

- **Step 4:** Ensuring that policy answers the 5 Ws: In this step, the reviewer checks whether the appropriate function is defined for the correct person in place. The reviewer also ensures when the actions will be accomplished. In other words, the policy should clearly explain the purpose, background, or policy statement.

- **Step 5:** Ensuring consistency with laws, regulations, and other levels of policy: In this step, the reviewer ensures that the policy is consistent with various laws and regulations; otherwise, the organization will face lawsuits. Also, the policy should ensure consistency with the laws and regulations of each country. During policy assessment, the policies are checked for consistency with lower and higher levels. Any discrepancy found should be resolved.

- **Step 6:** Checking policy freshness and easy availability to organization members: In this step, a policy is examined for provisions to keep it updated. This is important because an outdated policy can result into damage than good.

4.4 Introduction to Indian Cyber Law

Before indulging in any hacking activity, an ethical hacker must be familiar with the penalties of hacking a system. Prior to hacking a system, the ethical hacker must get a signed legal document from the target organization. Ethical hackers should know when and where to use their hacking skills and understand the consequences of misusing these skills.

Cybercrimes involve criminal activities, such as fraud, theft, forgery, and defamation, which are subject to the Indian Penal Code (IPC). In cybercrimes, a computer can be either used as a tool or a target object or both. In India, the unlawful use of computers has given birth to a new age of cybercrimes that are addressed by the IT Act, 2000. A separate set of laws, known as cyber laws or Internet laws, has been designed to regulate cybercrimes.

The two categories of cyber laws are as follows:

- **Computer as a target:** Specifies that a computer is used as a tool to attack other computers, such as virus and worm attacks
- **Computer as a weapon:** Specifies that a computer is used as a weapon to commit crimes, such as credit card frauds, cyber terrorism, and pornography

The IT Act, 2000 consists of 94 sections that are grouped into 13 chapters. It also includes four schedules. This Act was later amended in 2008, and it now includes 124 sections and 14 chapters. The amendments made in 2008 have replaced Schedules I and II and deleted Schedules III and IV.

The IT Act, 2000 addresses issues such as legal recognition of electronic records, legal recognition of digital signatures, secure electronic record, secure digital signature, and license to issue digital signature certificates. The IT Act, 2000 amended in 2008 has brought several additional new sections in it on offences such as cyber terrorism and data protection.

Need for Cyber Laws

With the growth of the Internet, various new systems have also developed, such as electronic commerce (for example, online marketing or online shopping) and electronic learning. Since these systems involve money transactions, there was an urgent need for some legal system to prevent frauds. This in turn led to the formulation of cyber laws.

Jurisprudence of Cyber Law

IT Act, 2000 is the primary source of cyber laws in India. It came into force on October 17, 2000. The Act was primarily brought up to provide legal recognition to electronic commerce and facilitate filing of electronic records with the Government. The Act also penalizes persons involved in cybercrimes and issues strict punishments (imprisonment terms up to 10 years and compensation up to 1 crore). A number of rules, regulations, orders, and acts were passed subsequently to complement the IT Act, 2000. They are as under:

- An executive order was passed on September 12, 2002. It contained instructions related to the provisions of the Act with regard to protected systems and application for the issuance of a Digital Signature Certificate. The IT (Removal of Difficulties) Order, 2002 was passed on September 19, 2002 in which minor errors in the Act were rectified.
- In 2002, the Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002 was passed, which amended the IT Act to introduce the concept of electronic cheques and truncated cheques. IT (Use of Electronic Records and Digital Signatures) Rules, 2004 was brought up in 2004 to provide the necessary legal framework for filing of documents with the Government issue of licenses by the Government and facilitated payment and receipt of fees to the Government bodies. Same day, the IT (Certifying Authorities) Rules, 2000 was enforced. It contained rules related to the eligibility, appointment, and working of Certifying Authorities (CAs). It also laid down the technical standards, procedures, and security methods to be used by a CA. The rules were subsequently amended in 2003, 2004 and 2006. IT (Certifying Authority) Regulations, 2001 was enforced on July 9, 2001. The regulations further added to the technical standards and procedures to be followed by a CA. It contained the following two important guidelines for CAs:
  - Guidelines for the submission of application for a license to operate as a CA under the IT Act. These guidelines were issued on July 9, 2001.

- Guidelines for the submission of certificates and certification revocation lists to the Controller of CAs for publishing in the National Repository of Digital Certificates. These guidelines were issued on December 16, 2002.

The Cyber Regulations Appellate Tribunal (CRAT) (Procedure) Rules, 2000 was also enforced on October 17, 2000. These rules provide for the appointment and working of the CRAT. The primary role of CRAT is to hear appeals against orders of the Adjudicating Officers. The CRAT (salary, allowances, and other terms and conditions of service of Presiding Officer) Rules, 2003 lay down the salary, allowances, and other terms for the Presiding Officer of the CRAT. IT (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provide some additional powers to the CRAT.

The IT (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 were passed on March 17, 2003. These rules lay down the qualifications required for the recruitment of Adjudicating Officers. The chief responsibility of the Adjudicating Officers under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation, etc. These rules also lay down the manner and mode of inquiry and adjudication by these officers.

There were neither Adjudicating Officers nor any CRAT for almost two years even after the implementation of the IT Act. A public interest litigation was filed by the students of the Asian School of Cyber Laws in the Bombay High Court for the appointment of Adjudicating Officers and establishing CRAT. On October 9, 2002, the Bombay High Court ordered for the recruitment of Adjudicating Officers and constitution of CRAT. The court directed the Central Government to announce an appoint so as to make the public aware. Following this, the Central Government passed an order on March 23, 2003, which appointed the Secretary of Department of Information Technology of each State or Union Territories of India as the adjudicating officer for that State or Union Territory. The IT (Security Procedure) Rules, 2004were enforced on October 29, 2004. They deal with secure digital signatures and secure electronic records. Also relevant are the IT (Other Standards) Rules, 2003. An order related to blocking of websites was passed on February 27, 2003. This authorized the Computer Emergency Response Team (CERT-IND) to instruct the Department of Telecommunications (DoT) to block a particular website.

Several cybercrimes come under the ambit of the IPC such as forgery of electronic records, cyber frauds, destroying electronic evidence, etc. The IPC requires digital

evidences as per the Indian Evidence Act for penalization purpose. The evidences must be proved in court. In cases where bank records are used as evidence, the provisions of the Bankers' Book Evidence Act (as amended by the IT Act) become relevant. There is also Reserve Bank of India Act (amended by the IT Act), which may become relevant in select cases. The Code of Criminal Procedure and the IT Act play an important role in the investigation and adjudication of cybercrimes in India. Let's now learn about objective and scope of the IT Act 2000.

4.5 Objective and Scope of the IT Act, 2000

The IT Act, 2000 consists of 94 sections that are grouped into 13 chapters. There are four schedules included in this IT Act. This Act was later amended in 2008, and now it includes 124 sections and 14 chapters. The amendments made in 2008 have replaced Schedules I and II and deleted Schedules III and IV. The IT Act, 2000 addresses issues, such as legal recognition of electronic records, legal recognition of digital signatures, secure electronic record, secure digital signature, and license to issue digital signature certificates. The IT Act, 2000 amended in 2008 has brought several additional new sections in it regarding offences, such as cyber terrorism and data protection.

India is the 12th country in the world to adopt cyber laws. The IT Act of India was legislated on May 17, 2000. The Act aims at the regulation of the use of IT. It aims mainly to legalize and regulate the system of electronic data interchange, electronic communication, and electronic commerce. This Act extends to the whole of India and also applies to any offence or contravention thereunder committed outside India by any person. The Act covers use of all the computer systems and networks located in India. Let us have a look on the main features of this Act:

- Chapter 1 of the Act deals with important definitions of the terms used in the regulation. It sets the scope of meaning of key terms of which the Act comprises.
- Chapter 2 covers regulations regarding digital signature. It provides legal recognition to digital signature.
- Chapter 3 deals with electronic governance. It legalizes the use of electronic records in government organizations and establishments.

- Chapter 4 involves attribution, acknowledgment, and dispatch of electronic records and their certifying authority.
- Chapter 5 comprises secure electronic records and secure digital signatures. It establishes the rules and regulations related to the electronic gazettes.
- Chapter 6 covers regulation of certifying authorities.
- Chapter 7 deals with digital signature and details its certification with the duties of subscribers.
- Chapter 8 involves duties of subscribers.
- Chapter 9 comprises penalties and adjudication by the cyber regulations appellate Tribunal. It covers penalty for damaging a computer or computer system.
- Chapter 10 details about the establishment of the CRAT to secure justice in such cases.
- Section 85 of the Act specifies the corporate social responsibility of a business. As per the Act, the directors and managers of a corporation are responsible to uphold the corporate responsibility with pursuance of law and IT ethics. Any violation of IT ethics or this law that is conducted with the knowledge of these authorities holds them responsible for not stopping it.

The Act contributes significantly in empowering organizations to fight against cybercrimes. It also protects the rights of consumers in carrying on with electronic business.

4.6 Intellectual Property Issues

Intellectual property refers to intangible property that has been created by individuals and corporates for their personal benefit or usage such as copyright, trade mark, patent, and digital data. It is created through human intelligence and mental efforts. It is therefore unethical to copy or steal the creativity and efforts of someone else. The technology that contributes to the creation and security of documents over the computer is the same that contributes in copying it easily. The dissemination of this copied document is also very quick and easy.

India is one of the signatories of the agreement that established the World Trade Organization (WTO). WTO came into force on January 1, 1995. The WTO Agreement consists of an agreement on Trade-Related Aspects of Intellectual Property Rights

(TRIPS). TRIPS prescribes the minimum standards to be adopted by the member countries within a stipulated timeframe regarding the following seven areas of intellectual property:

i. Copyright and related rights
ii. Trademarks
iii. Geographical indications
iv. Industrial designs
v. Patents
vi. Layout designs (Topographies) of integrated circuits
vii. Protection of undisclosed information

Let's now learn about intellectual-property-related legislation in India.

4.7 Overview of Intellectual-Property-Related Legislation in India

Intellectual property rights refer to the rights given to a person or an organization for their intellectual activity, i.e., creations of mind. This intellectual activity may be in the field of industry, science, literature, or any other artistic field. According to the Centre for Intellectual Property Rights, there are four major categories of Intellectual Property Rights in India, namely, Copyright, Patent, Trade Mark, and Design Protection.

Computer software come under the ambit of Copyright law and are protected by the Indian Copyright Act, 1957. The Indian Copyright Act was amended in 1994. These amendments came into effect from May 10, 1995. The main features of the Indian Copyright
Act are as follows:

- The Act specifies clearly the rights of a copyright holder
- The Act deals with the rentals of software
- The Act clearly states the rights of a user to make backup copies

Since software copyright violation can be carried out very easily by simply copying the software and since it is difficult in most cases to distinguish between an original software and a duplicate software, it had become utmost necessary to implement the Copyright Act. Some of the key features of the Act are as follows:

- Copying and distributing of copyrighted software without proper authorization is illegal according to section 14 of the Act
- The violator of the Act is liable to be tried under civil as well as criminal law
- A violator may be subjected to civil and criminal action for injunction, actual damages (which includes the profits, if any, made by the violator), or statutory damages per infringement
- The Act provides for strict punishment and/or heavy fines for any violation of software copyright
- According to Section 63 B, jail term of minimum 7 days can be given for a software copyright violation, which can be extended up to 3 years

■ Rationale behind Intellectual Property

To understand the rationale behind intellectual property, we must revisit the concept of *property* and the justification behind the protection of tangible property. In a capitalist society, such justification comes from two angles – labor and personality.

The justification from labor angle was put forward by Locke. According to Locke, a person creates property for himself and the State when he takes from the State what nature has provided as a common resource and mixes his labor with it. The State must encourage such people by rewarding them so that they remain innovative and perform better. Similar is the case with intellectual property. It involves both – innovation and value creation.

The society must encourage people to strive to be innovative and come up with creative solutions to generate wealth and welfare. Locke's idea of occurrence of commons in abundance in the primitive stage corresponds to the idea of intellectual property in modern day. This is public domain.

Another analogy can be drawn between tangible and intangible intellectual properties. All kinds of labor do not enjoy the same stature in society. Very good examples of this are slave labor and labor done by a housewife. The work done by slaves has never been counted as property generators. Similarly, even though the housewives are engaged whole day in some or the other activity of the household, their labor is not recognized as an economic activity. In the same way, the traditional knowledge and folklore do not get recognized as creation of knowledge, skill, or idea in the field of intellectual property.

The justification for IP from the *personality* angle is based on the belief that property represents the personality of a person. Hegel was the main advocate of this view who believed that property is the embodiment of one's personality. Property is a personal and private thing and needs to be protected. The same holds true for intellectual property also. However, this justification may apply differently to different subject matters. For example, the creations of mind in the field of creativity like art, music, or literature may reflect the personality of the creator, but software development, engineering designs, etc. do not support this justification. However, the personality justification has found place in the moral rights under the Copyright Act. These moral rights relate to preserving the integrity of the work against any change which has the potential of damaging either the reputation of the author or the message of his work.

Thus, none of the angles has been able to justify Intellectual Property Rights completely. Some intellectual properties derive their justification from the labor angle while others derive justification from the personality angle. Both the angles must be considered together for serving the entire gamut of intellectual property.

Underlying Premises of IP

IP is primarily the mental activity to produce some monetary benefits, and it is based on certain premises. You have the rights to own intellectual properly if you are generating any kind of wealth/welfare through your creative solutions. The IPRs are based on the following three premises:

1. Creative activities culminating in IP can be increased by proper encouragement and adequate economic incentives.
2. The creators of intellectual property should be rewarded in a just manner by giving appropriate economic benefit. This economic benefit can be ensured by granting them monopoly rights over their creation for a limited period of time.
3. The intellectual property regime ensures just economic rewards to creators of wealth and at the same time safeguards the interests of other entrepreneurs and the society at large.

Balancing the Rights of the Owner of the IP and the Society

Similar to any other right granted to us by our constitution, intellectual property rights are also not absolute but are limited by the rights of fellow citizens and the rights of the

society. These rights are strongly guided by the considerations that the state has to provide an equal access to opportunities to all its citizens while protecting the intellectual property rights of individuals. Thus, it becomes the responsibility of the state to harmonize conflicting claims and maintain a balance.

IPRs are essentially negative rights that they stop others from copying or counterfeiting the intellectual property of an individual or organization. For example, in case of patents, if an invention is patented by a person for a certain time period and another person, working independently, makes the same invention, the person is expected to get a license from the first person to use his invention during that time period. But in cases of other IPRs like Copyright or Trademark, this absolute right can be made somewhat lenient to safeguard the rights of others.

The state seeks to safeguard the rights of other individuals by adopting mechanisms like limiting the period of IPRs and making preservation of life, environment, peace, and morality important factors in the grant of IPRs. The licenses can also be revoked in cases of abuse of IPR.

■ Enforcement of IPRS

While in most contracts, the rights and obligations of the contracting parties are clearly laid down, any disputes that may arise in connection with the contract can be resolved on the basis of the provisions in the contract itself. IPRs are different from these contracts in that they are aimed at excluding others from doing certain things as regards the IP even without the existence of a formal contract between them and the owner of the right. The purpose of IPRs will be served only when they can be implemented with speed and within reasonable cost.

The national laws provide the legal framework for dealing with the IPR violations. In addition to this, TRIPS agreement also provides certain guidelines to the member countries of WTO. These guidelines are related to the IPR enforcement and must be included in the IPR-related national laws. The TRIPS agreement also lays down certain conditions to be fulfilled for effective enforcement of IPRs. These conditions are as follows:

- The procedure of IPR enforcement should be fair and equitable
- It should be simple and not complicated

4.8

- It should be speedy
- The parties involved should enjoy the right to:
  - Be heard
  - Produce evidence
  - Get a written decision
  - Judicial review, etc.

The remedy granted by the court of law can be injunctive or a compensatory relief or the court may require the defendant to deposit the infringed material for destruction. This make the purpose of IPR enforcement quite clear to prevent infringements of property rights of people while safeguarding legitimate trade at the same time.

IP and Constitution of India

The Constitution of India mentions Patents, Inventions and Designs, Copyright, Trade Marks, and Merchandise under entry 49 of the Union list of matters, falling within the Union Government, for the purpose of legislation. There is no specific mention of intellectual property in the Constitution. Property, in the constitution, generally means tangible property. However, IP as a form of property can be put under Article 300A, which deals with property that can be entitled to a legal right.

It has been observed by experts that there may be situations where the Intellectual Property Right of a person, especially the Copyright, clashes with the fundamental right to freedom of speech and expression granted to all the citizens by the Constitution of India. The courts have always tried to safeguard the fundamental rights of the citizens, especially the freedom of speech and expression. Any other right that poses a threat to the freedom of speech and expression of people is likely to face challenges.

Let's now learn about patent.

4.8 Patent

A Patent is a monopoly right granted by the State to an inventor for a limited period of time in exchange for the public disclosure of the invention. The monopoly rights mean the right to make, use, license, or sell an invention to the exclusion of others. Once the term of patent expires, the invention comes into the public domain. In India, all patents are granted for period of 20 years.

The system of granting patents serves many purposes. If the invention is commercially utilized, the patent ensures just reward to the inventor in terms of money and recognition, thus paying the inventor for investing his time and effort, knowledge and skills, and money and other resources. For the society, the commercial exploitation of an invention means newer and better products, higher productivity, and more efficient means of production. The main objective of granting patents is to accelerate the technological and industrial development.

A patent system promotes technological innovation and its spread. This directly and indirectly affects the society, leading to better utilization of resources, development, growth, and prosperity. Thus, the number of patents filed and granted nationally and internationally is a good indicator of the growth of science and technology in a country.

Patents are granted by the State and hence have territorial applicability. It is valid only in the country that has granted the patent. There is no mechanism to obtain a global patent. A person is required to apply separately in all the countries where he/she may want his/her invention to be protected.

However, there exists a unified procedure for filing of patent applications in more than one country at the same time. This has been made possible by the Patent Cooperation Treaty (PCT) of the World Intellectual Property Organization (WIPO). Under this treaty, the applicant can file an application for patenting his/her invention in any one of the countries which is a member of the PCT. The application thus filed is called an International Application. This establishes a filing date, also called priority date, in all the other member countries. After this, the applicant has to follow the procedure for seeking patent in each country of his/her choice individually. This is because granting of patents is the prerogative of every state and there is no such thing as an international patent. There were 123 members of PCT as on October 15, 2003. India joined the PCT on December 7, 1998.

■ The Patent System

The practice of granting monopolies by patent is not a new concept and can be traced back to over 600 years. The term **patent** has originally come from the term *Letters Patent*. It was a grant given by the King or the Queen to individuals, mainly for inventions. This grant used to be certain rights or privileges which were presented in the form of an open document carrying the King's or the Queen's seal at the bottom.

In India, the patenting system is governed by Indian Patents Act, 1970. The Act was later amended by Patents (Amendment) Act, 1999 and Patents (Amendment) Act, 2002. The amendments came into force on May 2, 2003.

Patentable Invention

According to the Indian Patent Act, a patentable invention is defined as follows:

"A new product or process involving an inventive step and capable of industrial application."

Thus, an invention must fulfill the following three requirements for being considered as a patentable invention:

- **The invention must be 'new'**: Something that is already present and known is not patentable. An invention is considered new if it does not form a part of the already available knowledge on the date of filing the application. If the invention is disclosed, in any way, before filing the application for patent, it is disqualified from being 'new'. For example, an English inventor was denied grant of a patent for inventing an improved design of a ball point pen because he had mistakenly published the details of his invention even before filing the application for patent.
- **The invention must involve an 'inventive step'**: 'Inventive step' means that the invention must not be obvious or follow directly from something which is already known. An example of an inventive step could be rolling of metals without affecting their original characteristics but adding on other characteristics like increasing toughness, etc.
- **The invention must have 'industrial application'**: To be patentable, the invention has to be capable of industrial application. Industry here refers to any practical and useful activity which is not related to creative and aesthetic activity. It may or may not be related to the use of machineries and manufacturing.

Nonpatentable Invention

A patent that cannot be patented by an individual or an organization is termed as nonpatentable. There are a number of categories that are nonpatentable. Anything can be patented only if it is a fresh invention, and it causes no harm to the living beings in the world and follows the law.

The categories which cannot be patented under IPA are as follows:

- An invention, which is detrimental to public order, morality, environment, or health; for example, the invention of a new type of gambling machine.
- An invention related to atomic energy. In India, atomic energy is not a public domain. It is the sole responsibility of the Central Government. An invention which is against the laws of nature. A discovery of a scientific principle or the formulation of an abstract theory is not patentable on the grounds that it is not an invention.
- The discovery of a living thing or *non-living* substances or objects occurring in nature because it is not an invention.
- A substance obtained by a mere admixture of certain components or a process of producing such a mixture does not qualify as an inventive step and hence cannot be patented
- Arrangement or re-arrangement or duplication of known devices, where each functions independent of one another in a known way without changing the end results also does not qualify as an inventive step and hence is non-patentable.
- Traditional knowledge is non-patentable because they are not new and form a part of the prior knowledge or state of the art. A mathematical or business method or a computer programme or algorithms are not patentable as they follow logically from a known premise.

The following items also do not qualify as inventions as defined by the Indian Patents Act and are therefore not patentable:

- A method related to agriculture or horticulture
- Any process related to the medicinal, surgical, curative, prophylactic, diagnostic, therapeutic, or other treatment of human beings and animals
- Plants and animals in whole or part, excluding micro-organisms
- Seeds and biological processes for the production of plants and animals

The following two categories belong to other forms of intellectual property and hence are not subject matters of patents:

- A literary, dramatic, musical, or artistic work, including cinematographic work and television productions. This is covered by Copyright Act.

- Layout designs of integrated circuits. These are covered separately by the SICLD Act.

There are certain substances which do not come under patenting, but the process of manufacturing those substances can be patented. Some examples are as follows:

- Substances which could be used as food or medicine or drug.
- Substances which are prepared or produced by chemical processes such as biochemical, biotechnological, and microbiological processes. However, if the substance itself is used as a medicine or drug, it can be patented.

Computer programmes and microorganisms are two such areas where patent protection is increasingly sought. In India, computer programmes are protected under the Copyright Act, 1957.

Dr. Ananda Chakraborty was granted a patent in 1980 by the US Supreme Court. Hegenetically engineered bacterium, which could degrade oil spills. The bacterium did not exist naturally. This satisfied the criteria of novelty, non-obviousness, and industrial application which were necessary for an invention to be patentable. This was the first time in the history that a living entity was given the status of a product. In the modern days, biotechnology and genetics are emerging as major fields of research. Employment of living entities like microorganisms, viruses, genetic elements like DNA, RNA, enzymes, plant cell lines, animals, etc. has become inevitable and common in developing newer technologies in these areas. Since these are indispensable for the advancement of science and technology and possess huge potential for creating wealth and profits, it is imperative to grant intellectual property protection to them. However, the patent protection involving living entities do face serious ethical and legal issues. This can be understood from the fact that the USA has not been able to grant patent protection to the creation of the animal clone Dolly, the cloned sheep.

A point to remember in this context is that there exists a very thin line of distinction between 'discovery' and 'invention' in a number of cases in biotechnology. Thus, even though a discovery may relate to living entity, it may qualify as an invention. The definition of 'discovery' and 'invention' therefore needs to be reviewed so that the distinction between them is easy and unambiguous.

■ Procedure for Obtaining Patent

The application for getting a patent for an invention may be made by a person who is the true and first inventor of the invention (or his/her assignee) or by the legal representative of a deceased person, provided that he/she was entitled to file such an application by the deceased person before his/her death.

If the inventor is an employee in an organization, the inventions made by him/her during his/her employment would be patentable in his/her name. The ownership of the patent would, however, depend on the contract between the employee and his/her employer. In R&D organizations, normally, the ownership rights are retained by the employer while the patent is in the employee's name.

Let's now learn about copyright.

4.9 Copyright

Copyright is a form of protection provided to the authors of "original works of authorship." This is given in the fields of literature, dramatics, music, art, etc. This protection is applicable to published as well as unpublished works. In India, the Copyright protection is governed by the Indian Copyright Act, 1976. The Section 106of the Copyright Act, 1976 gives the following exclusive rights to the authors:

- To make copies of the work or to phonorecord it.
- To prepare derivative works based upon the original work.
- To distribute copies or phonorecords of the work to the public either by sale or rent or lease or lending, etc.
- To perform the work in public if the work is in the field of literature, music, dramatics, choreography, pantomimes, motion pictures, or any other audio visual work.
- To display the work publicly if the work is in the field of literature, music, dramatics, choreography, pantomimes, motion pictures or any other audiovisual work.
- If the work is related to sound recordings, he/she has a right to perform the work publicly by means of a digital audio transmission.
- In addition to these, authors of works of visual art may also have the rights of attribution and integrity according to section 106A of the Copyright Act, 1976.

- It is illegal for anyone to infringe any of the rights provided by the copyright.
- Act to the owner of copyright. These rights, however, are not unlimited in scope.

Some of the limitations defined by the Sections from 107 to 121 of the Copyright Act, 1976 are:

1. Doctrine of fair use is applied
2. Limited use of copyrighted work is permitted on the payment of specified royalties and compliance with statutory conditions

The Section 14 of the Copyright Act defines "copyright" as the exclusive right to do or authorize the doing of any of the following:

1. To reproduce a computer programme in any material form; including the storing of it on any medium by electronic means.

   Illustration 1

   Tanmay has the exclusive right to reproduce the School Management software on CD, DVD, and other storage media.

   Illustration 2

   Tanmay has the exclusive right to upload the School Management software onto his website.

2. To issue copies of the computer programme to the public.

   Illustration 1

   Tanmay has the exclusive right to provide the School Management software along with computer magazines so that the general public can use the software.

   Illustration 2

   Tanmay has the exclusive right to upload the School Management software onto his website so that people around the world can download it.

3. To performthe computer programme in public or communicate it to the public.

   Illustration 1

   Tanmay has the exclusive right to give a public demonstration of the workings of the School Management software.

4. To make any cinematograph film or sound recording in respect of the computer programme.

Illustration 1

Tanmay has the exclusive right to make a promotional film depicting the working of the School Management software.

Illustration 2

Tanmay has the exclusive right to make a promotional sound recording depicting the working of the School Management software.

5. To make any translation of the computer programme.

Illustration 1

Currently, the School Management software has all the menu commands and help files in English. Tanmay has the exclusive right to make a version of the School Management software that has the menu commands and help files in Hindi.

6. To make any adaptation of the work.
7. To do, in relation to a translation or an adaptation of the computer programme, any of the acts specified above.
8. To sell, give on hire, offer for sale, or offer for hire any copy of the computer programme.

Illustration 1

Tanmay has the exclusive right to offer the School Management software for sale.

Illustration 2

Tanmay has the exclusive right to act as an Application Service Provider for the School Management software; e.g., a user will be charged a small fee per month for using the School Management software.

Who can claim copyright?

In case works of authorship, the copyright is the property of the author who has created the work. Thus, the author or those who derive their rights through the author can claim copyright.

If the work was done by a hired person, the employer is considered the author and the copyright for the work goes to the employer. 'Work made for hire' has been defined by the Section 101 of the Copyright Act as:

1. a work prepared by an employee within the scope of his or her employment or
2. a work specially ordered or commissioned for use as:
   - a contribution to a collective work
   - a part of a motion picture or other audio-visual work
   - a translation
   - a supplementary work
   - a compilation
   - an instructional text
   - a test
   - answer material for a test
   - an atlas

if it is agreed between the parties in a written agreement that the work shall be considered as a work made for hire.

In case of a joint work, unless there is a contrary agreement, all the authors are the co-owners of the copyright. This is, however, not the case with collective works like publication of periodicals where each author contributes separately. The copyright for each contribution rests with the individual contributor.

Two general principles for copyright are as follows:

- Transfer of a work to a person does not by itself transfer the copyright with it
- Minors may claim copyright, but the laws of the state may regulate the business dealings involving copyrights owned by the minors

Copyright protects "original works of authorship" that are produced in a tangible form of expression. The work thus produced may be communicated with the help of a machine or device.

What Works are Protected?

Copyrightable works include the following categories:

1. Literary works
2. Musical works, including any accompanying words
3. Dramatic works, including any accompanying music
4. Pantomimes and choreographic works
5. Pictorial, graphic, and sculptural works
6. Motion pictures and other audiovisual works
7. Sound recordings
8. Architectural works

These categories need to be viewed broadly. For example, computer programs and most "compilations" may be registered as "literary works"; maps and architectural plans may be registered as "pictorial, graphic, and sculptural works."

What is not protected by copyright?

Several categories of material are generally not eligible for copyright protection. Some of these are:

- ❒ Works that have not been fixed in a tangible form of expression
- ❒ Titles, names, short phrases, and slogans; familiar symbols or designs; mere variations of typographic ornamentation, lettering, or coloring; mere listing of ingredients or contents
- ❒ Ideas, procedures, methods, systems, processes, concepts, principles, discoveries, or devices
- ❒ Works that consist of information that is a common property and that contains no original authorship; for example, standard calendars, height and weight charts, tape measures, etc.

How to secure a copyright?

Copyright is secured automatically upon creation.

Copyright is secured automatically when a work is created. A work is considered as "created" when it is fixed in a copy or a phonorecord for the first time.

"Copies" are defined as material objects from which a work can be read or visually perceived either directly or with the help of a machine or device, such as books, manuscripts, sheet music, film, videotape, or microfilm.

"Phonorecords" are material objects which contain fixations of sounds such as cassette tapes, CDs, or vinyl disks.

Thus, for example, a song (the "work") can be fixed in sheet music ("copies") or in phonograph disks ("phonorecords"),or both. If a work is prepared over a period of time, the part of the work that is fixed on a particular date constitutes the created work as of that date.

The Copyright Act, 1976 defines publication as follows:

- "Publication" is the distribution of copies or phonorecords of a work to the public by sale or other transfer of ownership, or by rental, lease, or lending. The offering to distribute copies or phonorecords to a group of persons for the purposes of further distribution, public performance, or public display constitutes publication. A public performance or display of a work does not by itself constitute a publication.
- Publication is no longer necessary for acquiring copyright as it was under Copyright Act,1909.

Copyright Registration

Copyright registration is a legal formality intended to make a public record of the basic facts of a particular copyright. However, registration is not a condition of copyright protection. Even though registration is not a requirement for protection, the copyright law provides several inducements or advantages to encourage copyright owners to make registration.

Some of the advantages are as follows:

- Registration establishes a public record of the copyright claim.
- Before an infringement suit may be filed in court, registration is necessary.
- If made before or within five years of publication, registration will establish prima facie evidence in the court of the validity of the copyright and of the facts stated in the certificate.
- If registration is made within three months after publication of the work or prior to an infringement of the work, statutory damages and attorney's fees will be available to the copyright owner in court actions. Otherwise, only an award of actual damages and profits is available to the copyright owner.

- Registration allows the owner of the copyright to record the registration with the U. S. Customs Service for protection against the importation of infringing copies. For additional information, visit the U. S. Customs and Border Protection website at www.cbp.gov/xp/cgov/import.
- Registration may be made at any time within the life of the copyright. Unlike the law before 1978, when a work has been registered in unpublished form, it is not necessary to make another registration when the work becomes published, although the copyright owner may register the published edition, if desired.

Let's now learn about law related to semiconductor layout and design.

4.10 Law Related to Semiconductor Layout and Design

The layoutdesign of a semiconductor integrated circuit refers to a layout of transistors and other circuitry elements which are connected through lead wires.

The Intellectual Property Rights in the field of SemiConductor Integrated Circuit Layout Design are protected by the Semiconductor Integrated Circuits Layout-Design (SICLD) Act, 2000. It provides the routes and mechanisms for the protection to all SemiConductor Integrated Circuit Layout Designs IPR applications which are filed in the registry in India. The SICLD Act is being brought up in stages. The Act was first implemented on September 4, 2000. The rules under the Act were published on December 11, 2001. Sections 3 and 5 of the Act were implemented on October 1, 2004.

The main features of the SICLD Act, 2000 are as follows:

- The Act is applicable to the whole of India.
- The layout design of the integrated circuit chips are to be registered with the SICLD Registry for availing IPR protection.
- The Act lists the layoutdesigns of integrated circuits which can be registered it.
- It defines the duration for which the registration of layoutdesigns is valid.
- It lists the IPR rights which the registration provides to the person/organization.
- It specifies how the infringement of layoutdesigns occurs.
- It lays down the procedures for the assignment and transmission of the registered layoutdesigns.
- The Act provides the use of registered layout designs by the registered users. It provides that an Appellate Board can be used as a forum of redressal.
- It specifies how the royalties are to be handled.

- It provides the steps to be taken in cases of national emergency or extreme public urgency.
- It specifies penalty in cases of:
  - infringement of layout design
  - falsely representing a layout design as registered
  - improperly describing a place of business
  - falsification of entries in the register
  - forfeiture of goods
  - offences by companies
- The Act contains certain guidelines for agents.
- Lastly, the Act also provides for reciprocity with other recognized countries.

The SICLD Registry maintains a register of all the layout designs (which are registered with it) with the name, address, and other details of the proprietor. People are allowed to have a look at the registry after making the required payment.

The steps involved in the registration of a layout design with the Registry are as follows:

- The creator of the layout design needs to fill an application form and submit it at the SICLD Registry.
- The application may be accepted or rejected or accepted partially requiring certain modifications.
- The accepted applications are advertised within 14 days of acceptance and a 3 months wait period is given for filing of oppositions.
- In case opposition is filed in the 3 months wait period, a counter statement to the opposition can be filed within 2 months from the date of receipt of notice of opposition. A copy of the counter statement is also sent to the opposing party.
- The Registrar may take hearing with the parties and has the discretion to grant or reject the application of registration on the basis of conclusions of the hearing.
- Aggrieved party can appeal to the Appellate Board or in its absence to the Civil Court for relief on any ruling of the Registrar.

4.11 Software License

A software license is a contract law governing the use or redistribution of software. Software licenses are generally categorized into proprietary license and free-and-open source. A major difference between them is the terms defined for the distribution of the

software for the end users. Generally, a software license grants an end user the permission to use one or more copies of software. Apart from providing rights and imposing restrictions on the use of software, software licenses typically contain provisions allocating liability and responsibility between the parties that enter into the license agreement.

Summary

The chapter has helped to explore the need for the security policies. It has provided a brief discussion on the ISO information security standards. Further, various security policies and their review process are discussed.

Apart from the security policies, the chapter also focused on the Indian cyber law and the objective or scope of the IT Act, 2000. Next, you were introduced to the intellectual property issues and the IPR legislation in India. Also, various laws such as patent, copyright, semiconductor, and software license were explained toward the end of the chapter.

Exercises

■ Multiple Choice Questions

Q1. Which of the following ISO standards sets as a common basis and practical guideline for developing enterprise-level security standards and effective management practices?

a. ISO/IEC 27002:2005 (Code of Practice for Information Security Management)

b. ISO/IEC 27001:2005 (Information Security Management System – Requirements)

c. ISO/IEC 15408 (Evaluation Criteria for IT Security)

d. ISO/IEC 1335 (IT Security Management)

Ans. The correct option is a.

Q2. Under which of the following steps the existence of standards and procedures supporting the policy set is checked?

a. Have someone other than the person who wrote the policy review it

b. Assessing policy for completeness

c. Ensure that policy statements are

d. Ensure that the policy answers