Subject Name: Information Security & Cyber Laws

Subject Code: MCA – 501(N)

Subject Topic: Information Security, IT Act 2000

Himanshu Shukla

Assistant Professor

Department of Computer Application

UIET, CSJM University, Kanpur

Information Security

Information Security

Information security a set of practices intended to keep data secure from unauthorized access or alterations, both when it's being stored and when it's being transmitted from one machine or physical location to another. You might sometimes see it referred to as *data security.* As knowledge has become one of the 21st century's most important assets, efforts to keep information secure have correspondingly become increasingly important.

Information security principles

The basic components of information security are classified as CIA which stands *Confidentiality, Integrity,* and *availability.*

- **Confidentiality** is the element of the most immediately comes to mind when you think of information security. Data is confidential when only those people who are authorized to access it can do so; to ensure confidentiality, you need to be able to identify who is trying to access data and block attempts by those without authorization. Passwords, encryption, authentication, and defence against cyber-attacks are all techniques designed to ensure confidentiality.

•

Integrity means maintaining data in its correct state and preventing it from being improperly modified, either by accident or maliciously. Many of the techniques that ensure confidentiality will also protect data integrity—after all, a hacker can't change data they can't access—but there are other tools that help provide a defense of integrity in depth: checksums can help you verify data integrity, for instance, and version control software and frequent backups can help you restore data to a correct state if need be. Integrity also covers the concept of non-repudiation: you must be able to *prove* that you've maintained the integrity of your data, especially in legal contexts

Availability is the mirror image of confidentiality: while you need to make sure that your data can't be accessed by unauthorized users, you also need to ensure that it *can* be accessed by those who have the proper permissions. Ensuring data availability means matching network and computing resources to the volume of data access you expect and implementing a good backup policy for disaster recovery purposes.
In an ideal world, your data should always be kept confidential, in its correct state, and available; in practice, of course, you often need to make choices about which information security principles to emphasize, and that requires assessing your data.

Need of Information Security

- **Securing the functionality of the organization:** The Authorized members and decision maker in organizations must set policy and operates their organization in compliance with the complex, shifting legislation, efficient and capable applications.

- **Providing the safe operation of applications:** The organization is under immense pressure to acquire and operates integrated, efficient and capable applications. The modern organization needs to create an environment that safeguards application using the organizations IT systems, particularly those application that serves as important elements of the infrastructure of the organization.

- **Securing the database use by the organization:**

Data in the organization can be in two forms are either in rest or in motion, the motion of data signifies that data is currently used or processed by the system. The values of the data motivated the attackers to seal or corrupts the data. This is essential for the integrity and the values of the organization's data. Information security ensures the protection of both data in motion as well as data in rest.

- **Providing Safeguard technology for organizations:**

The organization must add intrastate services based on the size and scope of the organization. Organizational growth could lead to the need for public key infrastructure, PKI an integrated system of the software, encryption methodologies. The information security mechanism used by large organizations is complex in comparison to a small organization. The small organization generally prefers symmetric key encryption of data.

Cyberspace

Cyberspace is describing the non-physical channel created by computer systems. Online systems, for example, create a cyberspace within which people can communicate with one another (via e-mail), do research, or simply window shop. Like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery. Unlike real space, though, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse.

Some programs, particularly computer games, are designed to create a special cyberspace, one that resembles physical reality . In its extreme form, called virtual reality, users are presented with visual, auditory, and even tactile feedback that makes cyberspace feel real.

Netizens

The term **netizen** is defined with two words Internet and citizen, as in a "citizen of the net" or "net citizen. It describes a person actively involved in online communities or the Internet in general.

The term commonly also implies an interest and active engagement in improving the Internet, making it an intellectual and a social resource, or its surrounding political structures, especially in regard to open access, net neutrality and free speech

Netizens are not just anyone who comes on-line, and they are especially not people who come on-line for isolated gain or profit. They are not people who come to the Net thinking it is a service. Rather they are people who understand it takes effort and action on each and everyone's part to make the Net a regenerative and vibrant community and resource. Netizens are people who decide to devote time and effort into making the Net, this new part of our world, a better place.

Information Technology Act, 2000

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, 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 Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

The Information Technology Act, 2000 or ITA, 2000 or IT Act, was notified on October 17, 2000. It is the law that deals with cybercrime and electronic commerce in India. In this article, we will look at the objectives and features of the Information Technology Act, 2000.

In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the model law on electronic commerce (e-commerce) to bring uniformity in the law in different countries.

Further, the General Assembly of the United Nations recommended that all countries must consider this model law before making changes to their own laws. India became the 12th country to enable cyber law after it passed the Information Technology Act, 2000.

While the first draft was created by the Ministry of Commerce, Government of India as the E-Commerce Act, 1998, it was redrafted as the 'Information Technology Bill, 1999', and passed in May 2000.

Objectives and Scope of Information Technology Act 2000

The Information Technology Act, 2000 provides legal recognition to the transaction done via an electronic exchange of data and other electronic means of communication or electronic commerce transactions.

- Grant legal recognition to all transactions done via an electronic exchange of data or other electronic means of communication or e-commerce, in place of the earlier paper-based method of communication.
- Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication
- Facilitate the electronic filing of documents with Government agencies and also departments
- Facilitate the electronic storage of data
- Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions
- Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

Features of the Information Technology Act 2000

1. All electronic contracts made through secure electronic channels are legally valid.
2. Legal recognition for digital signatures.
3. Security measures for electronic records and also digital signatures are in place
4. A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized
5. Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer.
6. An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court
7. Digital Signatures will use an asymmetric cryptosystem and also a hash function
8. Provision for the appointment of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Controller to act as a repository of all digital signatures.
9. The Act applies to offenses or contraventions committed outside India
10. Senior police officers and other officers can enter any public place and search and arrest without warrant

References:

- www.indiacode.nic.in
- www.tutorialspoint.com
- www.geeksforgeeks.org
- “Information Technology Law and Practice”, Vakul Sharma
- www.google.com