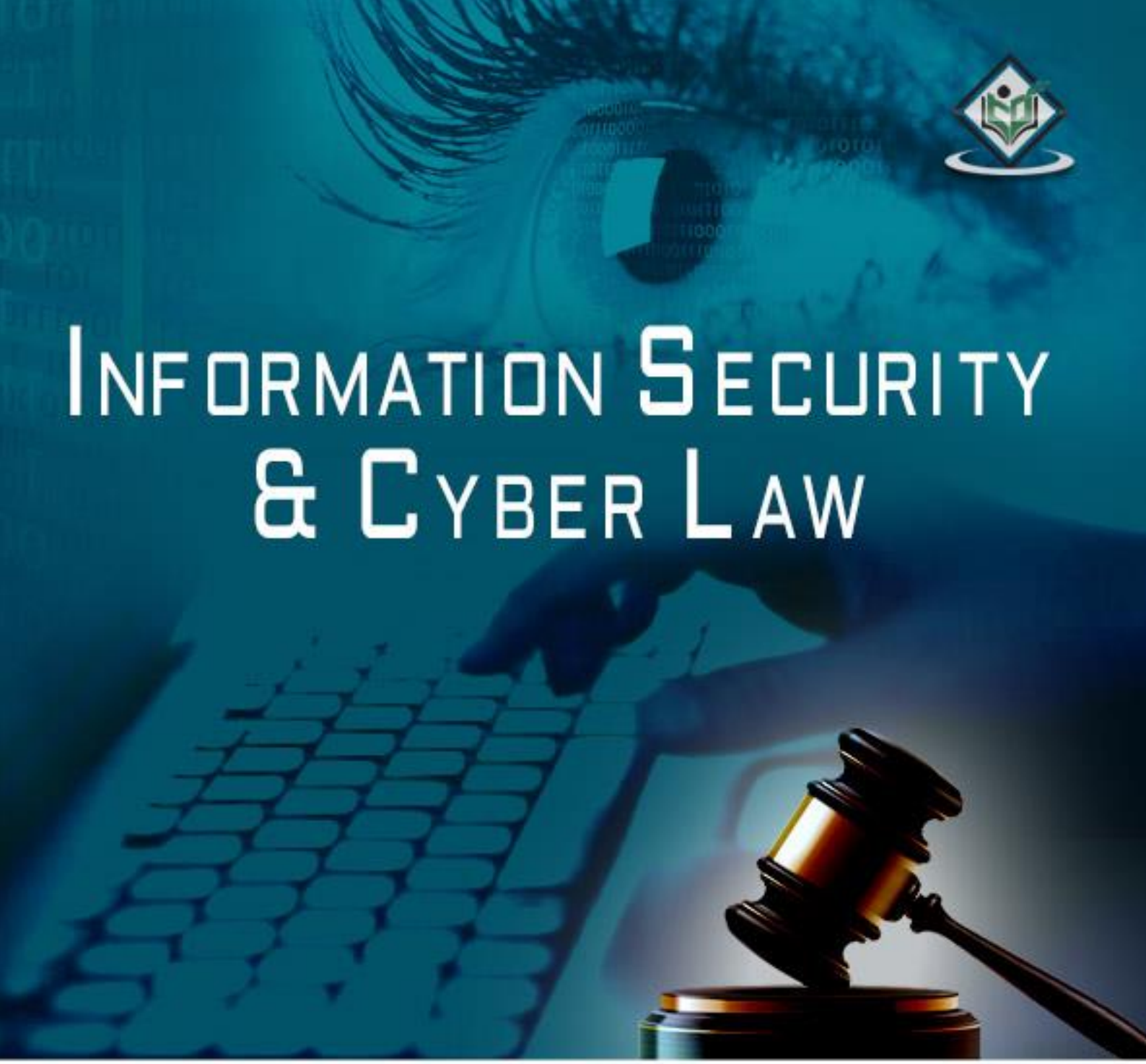


Information Security & Cyber Law

tutorialspoint

SIMPLYEASYLEARNING

www.tutorialspoint.com

https://www.facebook.com/tutorialspointindia

https://twitter.com/tutorialspoint

About the Tutorial

The Internet has now become all-encompassing; it touches the lives of every human being. We cannot undermine the benefits of Internet, however its anonymous nature allows miscreants to indulge in various cybercrimes.

This is a brief tutorial that explains the cyber laws that are in place to keep cybercrimes in check. In addition to cyber laws, it elaborates various IT Security measures that can be used to protect sensitive data against potential cyber threats.

Audience

Anyone using a computer system and Internet to communicate with the world can use this tutorial to gain knowledge on cyber laws and IT security.

Prerequisites

You should have a basic knowledge of Internet and its adverse effects.

Copyright and Disclaimer

Table of Contents

1. Information Security and Cyber Law – Introduction

Cyberspace

Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks.

With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

Cybersecurity

Cybersecurity denotes the technologies and procedures intended to safeguard computers, networks, and data from unlawful admittance, weaknesses, and attacks transported through the Internet by cyber delinquents.

ISO 27001 (ISO27001) is the international Cybersecurity Standard that delivers a model for creating, applying, functioning, monitoring, reviewing, preserving, and improving an Information Security Management System.

The Ministry of Communication and Information Technology under the government of India provides a strategy outline called the National Cybersecurity Policy. The purpose of this government body is to protect the public and private infrastructure from cyber-attacks.

Cybersecurity Policy

The cybersecurity policy is a developing mission that caters to the entire field of Information and Communication Technology (ICT) users and providers. It includes:

- Home users
- Small, medium, and large Enterprises
- Government and non-government entities

It serves as an authority framework that defines and guides the activities associated with the security of cyberspace. It allows all sectors and organizations in designing suitable cybersecurity policies to meet their requirements. The policy provides an outline to effectively protect information, information systems and networks.

It gives an understanding into the Government's approach and strategy for security of cyber space in the country. It also sketches some pointers to allow collaborative working across the public and private sectors to safeguard information and information systems. Therefore, the aim of this policy is to create a cybersecurity framework, which leads to detailed actions and programs to increase the security carriage of cyberspace.

Cyber Crime

The **Information Technology Act 2000** or any legislation in the Country does not describe or mention the term **Cyber Crime**. It can be globally considered as the gloomier face of technology. The only difference between a traditional crime and a cyber-crime is that the cyber-crime involves in a crime related to computers. Let us see the following example to understand it better:

Traditional Theft: A thief breaks into Ram's house and **steals** an object kept in the house.

Hacking: A Cyber Criminal/Hacker sitting in his own house, through his computer, hacks the computer of Ram and **steals** the data saved in Ram's computer without physically touching the computer or entering in Ram's house.

The I.T. Act, 2000 defines the terms –

- access in computer network in **section 2(a)**
- computer in **section 2(i)**
- computer network in **section (2j)**
- data in **section 2(0)**
- information in **section 2(v)**.

To understand the concept of Cyber Crime, you should know these laws. The object of offence or target in a cyber-crime are either the computer or the data stored in the computer.

Nature of Threat

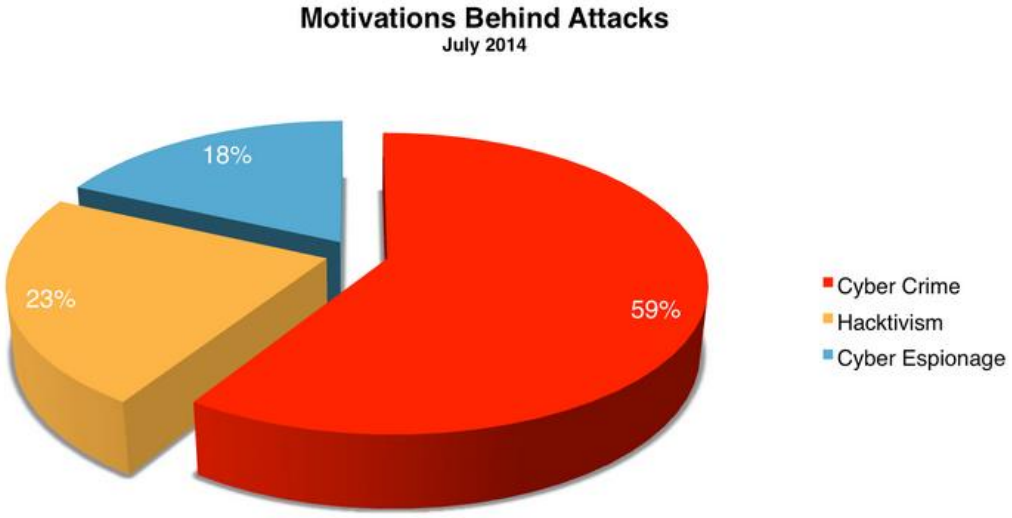
Among the most serious challenges of the 21st century are the prevailing and possible threats in the sphere of cybersecurity. Threats originate from all kinds of sources, and mark themselves in disruptive activities that target individuals, businesses, national infrastructures, and governments alike. The effects of these threats transmit significant risk for the following:

- public safety
- security of nations
- stability of the globally linked international community

Malicious use of information technology can easily be concealed. It is difficult to determine the origin or the identity of the criminal. Even the motivation for the disruption is not an easy task to find out. Criminals of these activities can only be worked out from the target, the effect, or other circumstantial evidence. Threat actors can operate with considerable freedom from virtually anywhere. The motives for disruption can be anything such as:

- simply demonstrating technical prowess
- theft of money or information
- extension of state conflict, etc.

Criminals, terrorists, and sometimes the State themselves act as the source of these threats. Criminals and hackers use different kinds of malicious tools and approaches. With the criminal activities taking new shapes every day, the possibility for harmful actions propagates.



Enabling People

The lack of information security awareness among users, who could be a simple school going kid, a system administrator, a developer, or even a CEO of a company, leads to a variety of cyber vulnerabilities. The awareness policy classifies the following actions and initiatives for the purpose of user awareness, education, and training:

- A complete awareness program to be promoted on a national level.
- A comprehensive training program that can cater to the needs of the national information security (Programs on IT security in schools, colleges, and universities).
- Enhance the effectiveness of the prevailing information security training programs. Plan domain-specific training programs (e.g., Law Enforcement, Judiciary, E-Governance, etc.)

- Endorse private-sector support for professional information security certifications.

Information Technology Act

The Government of India enacted The Information Technology Act with some major objectives which are as follows:

- To deliver lawful recognition for transactions through electronic data interchange (EDI) and other means of electronic communication, commonly referred to as **electronic commerce** or E-Commerce. The aim was to use replacements of 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.

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000. The I. T. Act got the President's assent on June 9, 2000 and it was made effective from October 17, 2000. By adopting this Cyber Legislation, India became the 12th nation in the world to adopt a Cyber Law regime.

Mission and Vision of Cybersecurity Program

Mission

The following mission caters to cybersecurity:

- To safeguard information and information infrastructure in cyberspace.
- To build capabilities to prevent and respond to cyber threats.
- To reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

Vision

To build a secure and resilient cyberspace for citizens, businesses, and Government.

2. Information Security and Cyber Law – Objectives

The recent Edward Snowden revelations on the US surveillance program PRISM have demonstrated how a legal entity network and computer system outside a particular jurisdiction is subject to surveillance without the knowledge of such legal entities. Cyber cases related to interception and snooping are increasing at an alarming rate. To curb such crimes, cyber laws are being amended quite regularly.

Emerging Trends of Cyber Law

Reports reveal that upcoming years will experience more cyber-attacks. So organizations are advised to strengthen their data supply chains with better inspection methods.

Some of the emerging trends of cyber law are listed below:

- Stringent regulatory rules are put in place by many countries to prevent unauthorized access to networks. Such acts are declared as penal offences.
- Stakeholders of the mobile companies will call upon the governments of the world to reinforce cyber-legal systems and administrations to regulate the emerging mobile threats and crimes.
- The growing awareness on privacy is another upcoming trend. Google's chief internet expert Vint Cerf has stated that *privacy may actually be an anomaly*.
- **Cloud computing** is another major growing trend. With more advancements in the technology, huge volumes of data will flow into the cloud which is not completely immune to cyber-crimes.
- The growth of **Bitcoins** and other virtual currency is yet another trend to watch out for. Bitcoin crimes are likely to multiply in the near future.
- The arrival and acceptance of data analytics, which is another major trend to be followed, requires that appropriate attention is given to issues concerning **Big Data**.

Create Awareness

While the U.S. government has declared October as the National Cybersecurity Awareness month, India is following the trend to implement some stringent awareness scheme for the general public.

The general public is partially aware of the crimes related to **virus transfer**. However, they are unaware of the bigger picture of the threats that could affect their cyber-lives. There is a

huge lack of knowledge on e-commerce and online banking cyber-crimes among most of the internet users.

Be vigilant and follow the tips given below while you participate in online activities:

- Filter the visibility of personal information in social sites.
- Do not keep the "remember password" button active for any email address and passwords
- Make sure your online banking platform is secure.
- Keep a watchful eye while shopping online.
- Do not save passwords on mobile devices.
- Secure the login details for mobile devices and computers, etc.

Areas of Development

The "Cyberlaw Trends in India 2013" and "Cyber law Developments in India in 2014" are two prominent and trustworthy cyber-law related research works provided by Perry4Law Organization (P4LO) for the years 2013 and 2014.

There are some grave cyber law related issues that deserve immediate consideration by the government of India. The issues were put forward by the Indian cyber law roundup of 2014 provided by P4LO and Cyber Crimes Investigation Centre of India (CCICI). Following are some major issues:

- A better cyber law and effective cyber-crimes prevention strategy
- Cyber-crimes investigation training requirements
- Formulation of dedicated encryption laws
- Legal adoption of cloud computing
- Formulation and implementation of e-mail policy
- Legal issues of online payments
- Legality of online gambling and online pharmacies
- Legality of Bitcoins
- Framework for blocking websites
- Regulation of mobile applications

With the formation of cyber-law compulsions, the obligation of banks for cyber-thefts and cyber-crimes would considerably increase in the near future. Indian banks would require to keep a dedicated team of cyber law experts or seek help of external experts in this regard.

The transactions of cyber-insurance should be increased by the Indian insurance sector as a consequence of the increasing cyber-attacks and cyber-crimes.

International Network on Cybersecurity

To create an international network on cybersecurity, a conference was held in March 2014 in New Delhi, India.

The objectives set in the International Conference on Cyberlaw & Cybercrime are as follows:

- To recognize the developing trends in Cyberlaw and the legislation impacting cyberspace in the current situation.
- To generate better awareness to battle the latest kinds of cybercrimes impacting all investors in the digital and mobile network.
- To recognize the areas for stakeholders of digital and mobile network where Cyberlaw needs to be further evolved.
- To work in the direction of creating an international network of cybercrimes. Legal authorities could then be a significant voice in the further expansion of cyber-crimes and cyber law legislations throughout the globe.