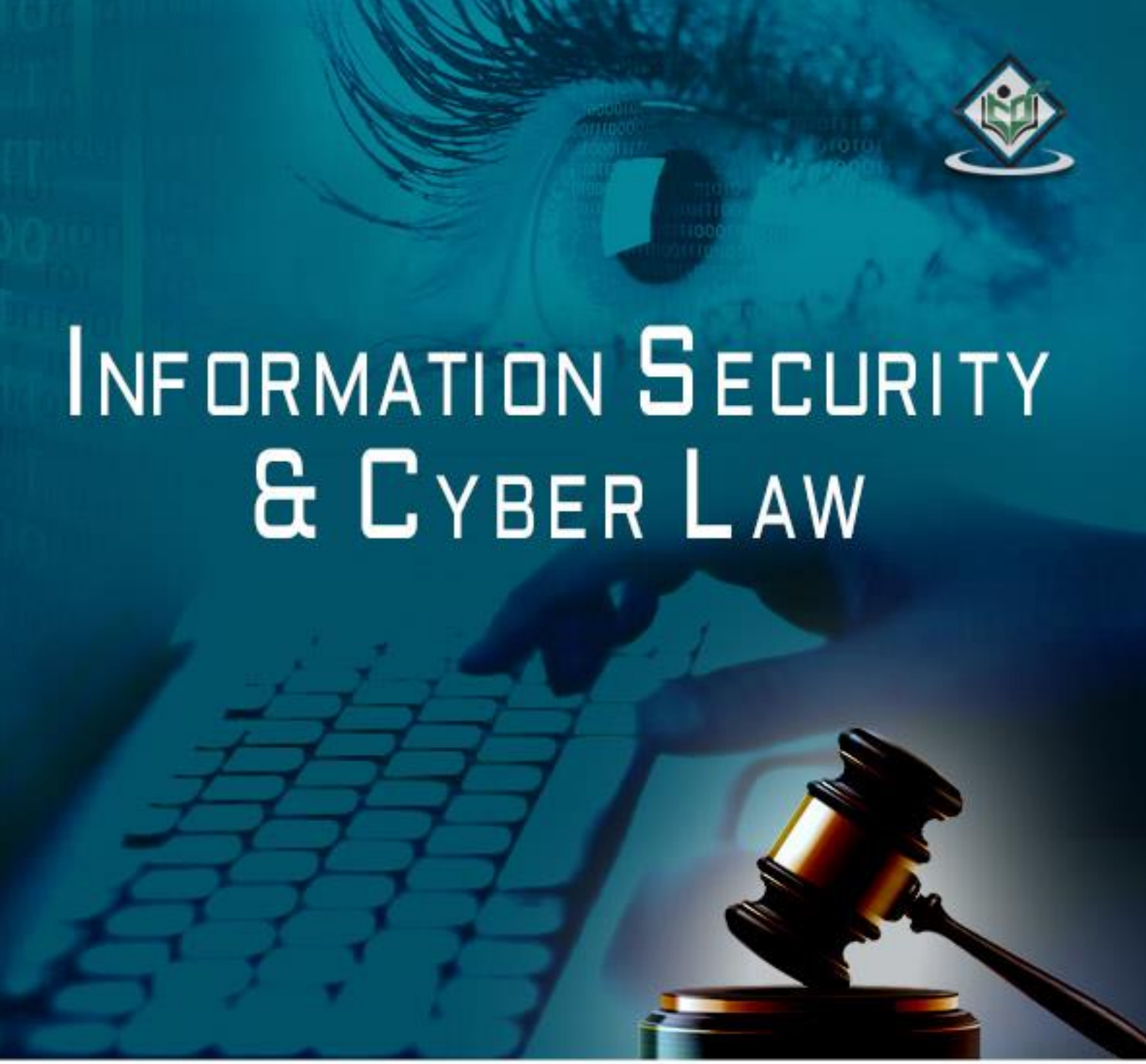


Information Security & Cyber Law

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

About the Tutorial i

Audience i

Prerequisites i

Copyright and Disclaimer i

Table of Contents ii

1. INTRODUCTION 1

Cyberspace 1

Cybersecurity 1

Cybersecurity Policy 1

Cyber Crime 2

Nature of Threat 2

Enabling People 3

Information Technology Act 4

Mission and Vision of Cybersecurity Program 4

2. OBJECTIVES 6

Emerging Trends of Cyber Law 6

Create Awareness 6

Areas of Development 7

International Network on Cybersecurity 8

3. INTELLECTUAL PROPERTY RIGHTS 9

Types of Intellectual Property Rights 9

Advantages of Intellectual Property Rights 10

Intellectual Property Rights in India 10

Intellectual Property in Cyber Space 11

4. STRATEGIES FOR CYBER SECURITY 12

Strategy 1: Creating a Secure Cyber Ecosystem 12

Comparision of Attacks 13

Case Study 14

Types of Attacks 16

Strategy 2: Creating an Assurance Framework 17

Strategy 3: Encouraging Open Standards 18

Strategy 4: Strengthening the Regulatory Framework 18

Strategy 5: Creating Mechanisms for IT Security 19

Strategy 6: Securing E-Governance Services 20

Strategy 7: Protecting Critical Information Infrastructure 20

5. POLICIES TO MITIGATE CYBER RISK 22

Promotion of R&D in Cybersecurity 22

Reducing Supply Chain Risks 24

Mitigate Risks through Human Resource Development 24

Creating Cybersecurity Awareness 25

Information sharing 25

Implementing a Cybersecurity Framework 26

6. NETWORK SECURITY 29

Types of Network Security Devices 29

Firewalls 29

Antivirus 30

Content Filtering 30

Intrusion Detection Systems 31

7. I.T. ACT 32

Salient Features of I.T. Act **32**

Scheme of I.T. Act **32**

Application of the I.T. Act **33**

Amendments Brought in the I.T. Act **33**

Intermediary Liability **34**

Highlights of the Amended Act **34**

8. SIGNATURES 35

Digital Signature **35**

Electronic Signature **35**

Digital Signature to Electronic Signature **35**

9. OFFENCE AND PENALTIES 37

Offences **37**

Compounding of Offences **42**

10. SUMMARY 44

11. FAQ 45

1. 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,

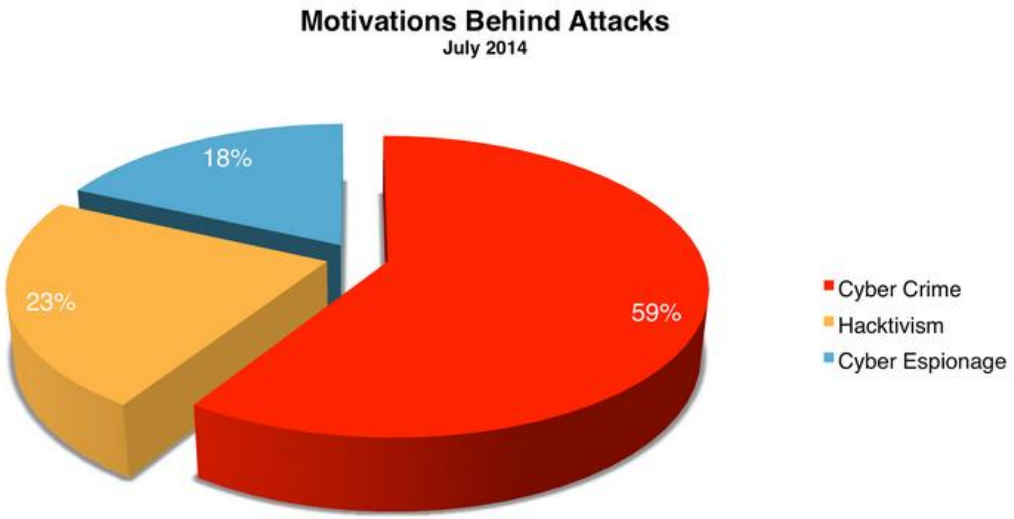
businesses, national infrastructures, and governments alike. The effects of these threats transmit significant risk for the following:

- 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. 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.

3. INTELLECTUAL PROPERTY RIGHTS

Intellectual property rights are the legal rights that cover the privileges given to individuals who are the owners and inventors of a work, and have created something with their intellectual creativity. Individuals related to areas such as literature, music, invention, etc., can be granted such rights, which can then be used in the business practices by them.

The creator/inventor gets exclusive rights against any misuse or use of work without his/her prior information. However, the rights are granted for a limited period of time to maintain equilibrium.

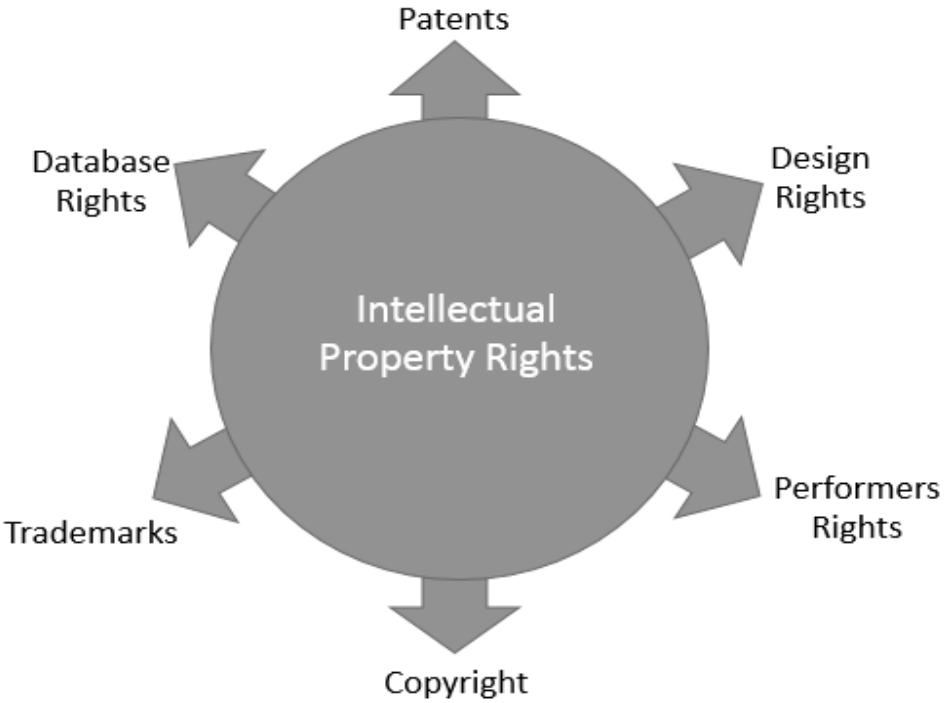
The following list of activities which are covered by the intellectual property rights are laid down by the World Intellectual Property Organization (WIPO):

- Industrial designs
- Scientific discoveries
- Protection against unfair competition
- Literary, artistic, and scientific works
- Inventions in all fields of human endeavor
- Performances of performing artists, phonograms, and broadcasts
- Trademarks, service marks, commercial names, and designations
- All other rights resulting from intellectual activity in the industrial, scientific, literary, or artistic fields

Types of Intellectual Property Rights

Intellectual Property Rights can be further classified into the following categories:

- Copyright
- Patent
- Trademark
- Trade Secrets, etc.



Advantages of Intellectual Property Rights

Intellectual property rights are advantageous in the following ways:

- Provides exclusive rights to the creators or inventors.
- Encourages individuals to distribute and share information and data instead of keeping it confidential.
- Provides legal defense and offers the creators the incentive of their work.
- Helps in social and financial development.

Intellectual Property Rights in India

To protect the intellectual property rights in the Indian territory, India has defined the formation of constitutional, administrative and jurisdictive outline whether they imply the copyright, patent, trademark, industrial designs, or any other parts of the intellectual property rights.

Back in the year 1999, the government passed an important legislation based on international practices to safeguard the intellectual property rights. Let us have a glimpse of the same:

- The **Patents** (Amendment) Act, 1999, facilitates the establishment of the mail box system for filing patents. It offers exclusive marketing rights for a time period of five years.

- The **Trade Marks** Bill, 1999, replaced the Trade and Merchandise Marks Act, 1958.
- The **Copyright** (Amendment) Act, 1999, was signed by the President of India.
- The ***sui generis*** legislation was approved and named as the Geographical Indications of Goods (Registration and Protection) Bill, 1999.
- The **Industrial Designs** Bill, 1999, replaced the Designs Act, 1911.
- The **Patents (Second Amendment)** Bill, 1999, for further amending the Patents Act of 1970 in compliance with the TRIPS.

Intellectual Property in Cyber Space

Every new invention in the field of technology experiences a variety of threats. Internet is one such threat, which has captured the physical marketplace and have converted it into a virtual marketplace.

To safeguard the business interest, it is vital to create an effective property management and protection mechanism keeping in mind the considerable amount of business and commerce taking place in the Cyber Space.

Today it is critical for every business to develop an effective and collaborative IP management mechanism and protection strategy. The ever-looming threats in the cybernetic world can thus be monitored and confined.

Various approaches and legislations have been designed by the law-makers to up the ante in delivering a secure configuration against such cyber-threats. However it is the duty of the intellectual property right (IPR) owner to invalidate and reduce such *mala fide* acts of criminals by taking proactive measures.

4. STRATEGIES FOR CYBER SECURITY

To design and implement a secure cyberspace, some stringent strategies have been put in place. This chapter explains the major strategies employed to ensure cybersecurity, which include the following:

- Creating a Secure Cyber Ecosystem
- Creating an Assurance Framework
- Encouraging Open Standards
- Strengthening the Regulatory Framework
- Creating Mechanisms for IT Security
- Securing E-governance Services
- Protecting Critical Information Infrastructure

Strategy 1: Creating a Secure Cyber Ecosystem

The cyber ecosystem involves a wide range of varied entities like devices (communication technologies and computers), individuals, governments, private organizations, etc., which interact with each other for numerous reasons.

This strategy explores the idea of having a strong and robust cyber-ecosystem where the cyber-devices can work with each other in the future to prevent cyber-attacks, reduce their effectiveness, or find solutions to recover from a cyber-attack.

Such a cyber-ecosystem would have the ability built into its cyber devices to permit secured ways of action to be organized within and among groups of devices. This cyber-ecosystem can be supervised by present monitoring techniques where software products are used to detect and report security weaknesses.

A strong cyber-ecosystem has three symbiotic structures - **Automation**, **Interoperability**, and **Authentication**.

- **Automation:** It eases the implementation of advanced security measures, enhances the swiftness, and optimizes the decision-making processes.
- **Interoperability:** It toughens the collaborative actions, improves awareness, and accelerates the learning procedure. There are three types of interoperability:
    - Semantic (i.e., shared lexicon based on common understanding)

- Technical
- Policy – Important in assimilating different contributors into an inclusive cyber-defense structure.

- **Authentication:** It improves the identification and verification technologies that work in order to provide:
  - Security
  - Affordability
  - Ease of use and administration
  - Scalability
  - Interoperability

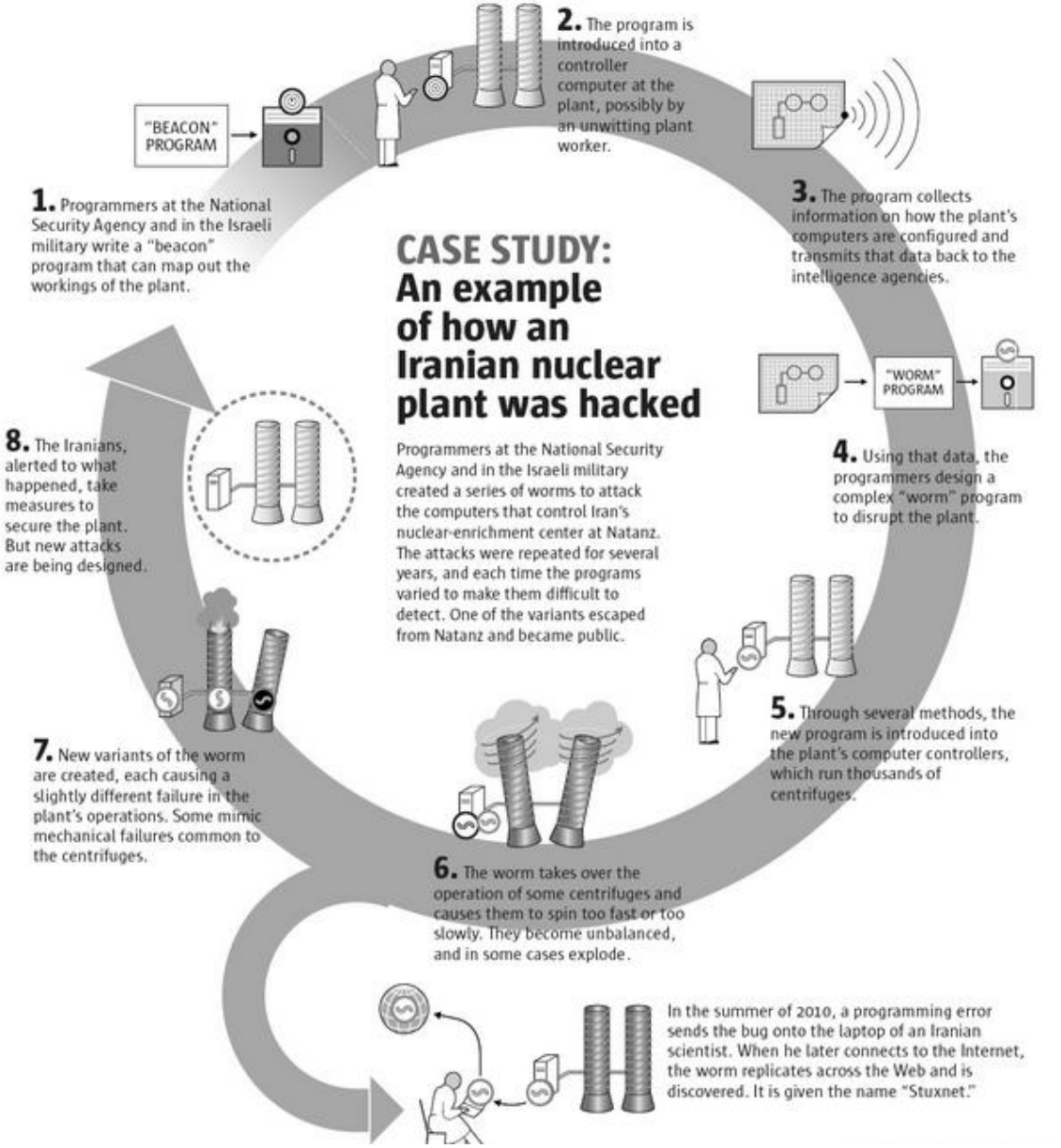
Comparison of Attacks

The following table shows the *Comparison of Attack Categories against Desired Cyber Ecosystem Capabilities*:

	Categories of Cyber Attack							
Desired Cyber Ecosystem Capabilities	Attrition	Malware	Hacking	Social Tactics	Improper Usage (Insider)	Physical Action; Loss or Theft	Multiple Component	Other
Automation	x	x	x	x	x	x	x	x
Authentication	x	x	x	x		x	x	x
Interoperability	x	x	x	x			x	
Automated Defense Identification, Selection, and Assessment	x	x	x	x	x	x	x	x
Build Security In	x	x	x	x		x	x	x
Business Rules-Based Behavior Monitoring	x	x	x	x	x	x	x	x
General Awareness and Education	x	x	x	x	x	x	x	x
Moving Target	x	x	x	x			x	x
Privacy	x	x	x	x	x	x	x	x
Risk-Based Data Management	x	x	x	x	x	x	x	x
Situational Awareness	x	x	x	x	x	x	x	x
Tailored Trustworthy Spaces	x	x	x	x			x	x

Case Study

The following diagram was prepared by ***Guilbert Gates for The New York Times***, which shows how an Iranian plant was hacked through the internet.



Explanation: A program was designed to automatically run the Iranian nuclear plant. Unfortunately, a worker who was unaware of the threats introduced the program into the controller. The program collected all the data related to the plant and sent the information to the intelligence agencies who then developed and inserted a worm into the plant. Using the worm, the plant was controlled by miscreants which led to the generation of more worms and as a result, the plant failed completely.

Types of Attacks

The following table describes the attack categories:

Attack Category	Description of Attack
Attrition	Methods used to damage networks and systems. It includes the following: • distributed denial of service attacks • impair or deny access to a service or application • resource depletion attacks
Malware	Any malicious software used to interrupt normal computer operation and harm information assets without the owner's consent. Any execution from a removable device can enhance the threat of a malware.
Hacking	An attempt to intentionally exploit weaknesses to get unethical access, usually conducted remotely. It may include: • data-leakage attacks • injection attacks and abuse of functionality • spoofing • time-state attacks • buffer and data structure attacks • resource manipulation • stolen credentials usage • backdoors • dictionary attacks on passwords • exploitation of authentication
Social Tactics	Using social tactics such as deception and manipulation to acquire access to data, systems or controls. It includes: • pre-texting (forged surveys) • inciting phishing • retrieving of information through conversation
Improper Usage (Insider Threat)	Misuse of rights to data and controls by an individual in an organization that would violate the organization's policies. It includes: • installation of unauthorized software • removal of sensitive data

Physical Action/Loss or Theft of Equipment	Human-Driven attacks such as: • stolen identity tokens and credit cards • fiddling with or replacing card readers and point of sale terminals • interfering with sensors • theft of a computing device used by the organization, such as a laptop
Multiple Component	Single attach techniques which contains several advanced attack techniques and components.
Other	Attacks such as: • supply chain attacks • network investigation

Strategy 2: Creating an Assurance Framework

The objective of this strategy is to design an outline in compliance with the global security standards through traditional products, processes, people, and technology.

To cater to the national security requirements, a national framework known as the **Cybersecurity Assurance Framework** was developed. It accommodates critical infrastructure organizations and the governments through "Enabling and Endorsing" actions.

Enabling actions are performed by government entities that are autonomous bodies free from commercial interests. The publication of "National Security Policy Compliance Requirements" and IT security guidelines and documents to enable IT security implementation and compliance are done by these authorities.

Endorsing actions are involved in profitable services after meeting the obligatory qualification standards and they include the following:

- ISO 27001/BS 7799 ISMS certification, IS system audits etc., which are essentially the compliance certifications.
- 'Common Criteria' standard ISO 15408 and Crypto module verification standards, which are the IT Security product evaluation and certification.
- Services to assist consumers in implementation of IT security such as IT security manpower training.

Trusted Company Certification

Indian IT/ITES/BPOs need to comply with the international standards and best practices on security and privacy with the development of the outsourcing market. ISO 9000, CMM, Six Sigma, Total Quality Management, ISO 27001 etc., are some of the certifications.

Existing models such as SEI CMM levels are exclusively meant for software development processes and do not address security issues. Therefore, several efforts are made to create a model based on self-certification concept and on the lines of Software Capability Maturity Model (SW-CMM) of CMU, USA.

The structure that has been produced through such association between industry and government, comprises of the following:

- standards
- guidelines
- practices

These parameters help the owners and operators of critical infrastructure to manage cybersecurity-related risks.

Strategy 3: Encouraging Open Standards

Standards play a significant role in defining how we approach information security related issues across geographical regions and societies. Open standards are encouraged to:

- Enhance the efficiency of key processes,
- Enable systems incorporations,
- Provide a medium for users to measure new products or services,
- Organize the approach to arrange new technologies or business models,
- Interpret complex environments, and
- Endorse economic growth.

Standards such as ISO 27001[3] encourage the implementation of a standard organization structure, where customers can understand processes, and reduce the costs of auditing.

Strategy 4: Strengthening the Regulatory Framework

The objective of this strategy is to create a secure cyberspace ecosystem and strengthen the regulatory framework. A 24X7 mechanism has been envisioned to deal with cyber threats through National Critical Information Infrastructure

Protection Centre (NCIIPC). The Computer Emergency Response Team (CERT-In) has been designated to act as a nodal agency for crisis management.

Some highlights of this strategy are as follows:

- Promotion of research and development in cybersecurity.
- Developing human resource through education and training programs.
- Encouraging all organizations, whether public or private, to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cybersecurity initiatives.
- Indian Armed Forces are in the process of establishing a cyber-command as a part of strengthening the cybersecurity of defense network and installations.
- Effective implementation of public-private partnership is in pipeline that will go a long way in creating solutions to the ever-changing threat landscape.

Strategy 5: Creating Mechanisms for IT Security

Some basic mechanisms that are in place for ensuring IT security are: link-oriented security measures, end-to-end security measures, association-oriented measures, and data encryption. These methods differ in their internal application features and also in the attributes of the security they provide. Let us discuss them in brief.

Link-Oriented Measures

It delivers security while transferring data between two nodes, irrespective of the eventual source and destination of the data.

End-to-End Measures

It is a medium for transporting Protocol Data Units (PDUs) in a protected manner from source to destination in such a way that disruption of any of their communication links does not violate security.

Association-Oriented Measures

Association-oriented measures are a modified set of end-to-end measures that protect every association individually.

Data Encryption

It defines some general features of conventional ciphers and the recently developed class of public-key ciphers. It encodes information in a way that only the authorized personnel can decrypt them.

Strategy 6: Securing E-Governance Services

Electronic governance (e-governance) is the most treasured instrument with the government to provide public services in an accountable manner. Unfortunately, in the current scenario, there is no devoted legal structure for e-governance in India.

Similarly, there is no law for obligatory e-delivery of public services in India. And nothing is more hazardous and troublesome than executing e-governance projects without sufficient cybersecurity. Hence, securing the e-governance services has become a crucial task, especially when the nation is making daily transactions through cards.

Fortunately, the Reserve Bank of India has implemented security and risk mitigation measures for card transactions in India enforceable from 1st October, 2013. It has put the responsibility of ensuring secured card transactions upon banks rather than on customers.

"E-government" or electronic government refers to the use of Information and Communication Technologies (ICTs) by government bodies for the following:

- Efficient delivery of public services
- Refining internal efficiency
- Easy information exchange among citizens, organizations, and government bodies
- Re-structuring of administrative processes.

Strategy 7: Protecting Critical Information Infrastructure

Critical information infrastructure is the backbone of a country's national and economic security. It includes power plants, highways, bridges, chemical plants, networks, as well as the buildings where millions of people work every day. These can be secured with stringent collaboration plans and disciplined implementations.

Safeguarding critical infrastructure against developing cyber-threats needs a structured approach. It is required that the government aggressively collaborates with public and private sectors on a regular basis to prevent, respond to, and coordinate mitigation efforts against attempted disruptions and adverse impacts to the nation's critical infrastructure.

It is in demand that the government works with business owners and operators to reinforce their services and groups by sharing cyber and other threat information.

A common platform should be shared with the users to submit comments and ideas, which can be worked together to build a tougher foundation for securing and protecting critical infrastructures.

The government of USA has passed an executive order "Improving Critical Infrastructure Cybersecurity" in 2013 that prioritizes the management of cybersecurity risk involved in the delivery of critical infrastructure services. This Framework provides a common classification and mechanism for organizations to:

- Define their existing cybersecurity bearing,
- Define their objectives for cybersecurity,
- Categorize and prioritize chances for development within the framework of a constant process, and
- Communicate with all the investors about cybersecurity.

5. POLICIES TO MITIGATE CYBER RISK

This chapter takes you through the various policies laid to minimize cyber risk. It is only with well-defined policies that the threats generated in the cyberspace can be reduced.

Promotion of R&D in Cybersecurity

Due to the ever-increasing dependence on the Internet, the biggest challenge we face today is the security of information from miscreants. Therefore, it is essential to promote research and development in cybersecurity so that we can come up with robust solutions to mitigate cyber risks.

Cybersecurity Research

Cybersecurity Research is the area that is concerned with preparing solutions to deal with cyber criminals. With increasing amount of internet attacks, advanced persistent threats and phishing, lots of research and technological developments are required in the future.

Cybersecurity Research – Indian Perspective

In the recent years, India has witnessed an enormous growth in cyber technologies. Hence it calls for an investment in the research and development activities of cybersecurity. India has also seen many successful research outcomes that were translated into businesses, through the advent of local cybersecurity companies.

Threat Intelligence

Research work to mitigate cyber-threats is already being commenced in India. There is a proactive response mechanism in place to deal with cyber threats. Research and Development activities are already underway at various research organizations in India to fight threats in cyberspace.

Next Generation Firewall

Multi-identity based expertise such as Next Generation Firewall that offers security intelligence to enterprises and enable them to apply best suited security controls at the network perimeter are also being worked on.

Secured Protocol and Algorithms

Research in protocols and algorithms is a significant phase for the consolidation of cybersecurity at a technical level. It defines the rules for information sharing and processing over cyberspace. In India, protocol and algorithm level research includes:

- Secure Routing Protocols
- Efficient Authentication Protocols
- Enhanced Routing Protocol for Wireless Networks
- Secure Transmission Control Protocol
- Attack Simulation Algorithm, etc.

Authentication Techniques

Authentication techniques such as Key Management, Two Factor Authentication, and Automated key Management provide the ability to encrypt and decrypt without a centralized key management system and file protection. There is continuous research happening to strengthen these authentication techniques.

BYOD, Cloud and Mobile Security

With the adoption of varied types of mobile devices, the research on the security and privacy related tasks on mobile devices has increased. Mobile security testing, Cloud Security, and BYOD (Bring Your Own Device) risk mitigation are some of the areas where a lot of research is being done.

Cyber Forensics

Cyber Forensics is the application of analysis techniques to collect and recover data from a system or a digital storage media. Some of the specific areas where research is being done in India are:

- Disk Forensics
- Network Forensics
- Mobile Device Forensics
- Memory Forensics
- Multimedia Forensics
- Internet Forensics

Reducing Supply Chain Risks

Formally, supply chain risk can be defined as:

> *Any risk that an opponent may damage, write some malicious function to it, deconstruct the design, installation, procedure, or maintenance of a supply item or a system so that the entire function can be degraded.*

Supply Chain Issues

Supply chain is a global issue and there is a requirement to find out the interdependencies among the customers and suppliers. In today's scenario it is important to know: *What are the SCRM problems?* and *How to address the problems?*

An effective SCRM (Supply Chain Risk Management) approach requires a strong public-private partnership. Government should have strong authorities to handle supply chain issues. Even private sectors can play a key role in a number of areas.

We cannot provide a one-size-fits-all resolution for managing supply chain risks. Depending on the product and the sector, the costs for reducing risks will weigh differently. Public Private Partnerships should be encouraged to resolve risks associated with supply chain management.

Mitigate Risks through Human Resource Development

Cybersecurity policies of an organization can be effective, provided all its employees understand their value and exhibit a strong commitment towards implementing them. Human resource directors can play a key role in keeping organizations safe in cyberspace by applying the following few points.

Taking Ownership of the Security Risk Posed by Employees

As most of the employees do not take the risk factor seriously, hackers find it easy to target organizations. In this regard, HR plays a key role in educating employees about the impact their attitudes and behavior have on the organization's security.

Ensuring that Security Measures are Practical and Ethical

Policies of a company must be in sync with the way employees think and behave. For example, saving passwords on systems is a threat, however continuous monitoring can prevent it. The HR team is best placed to advise whether policies are likely to work and whether they are appropriate.

Identifying Employees who may Present a Particular Risk

It also happens that cyber-criminals take the help of insiders in a company to hack their network. Therefore it is essential to identify employees who may present a particular risk and have stringent HR policies for them.

Creating Cybersecurity Awareness

Cybersecurity in India is still in its evolution stage. This is the best time to create awareness on issues related to cyber security. It would be easy to create awareness from the grass-root level like schools where users can be made aware how Internet works and what are its potential threats.

Every cyber café, home/personal computers, and office computers should be protected through firewalls. Users should be instructed through their service providers or gateways not to breach unauthorized networks. The threats should be described in bold and the impacts should be highlighted.

Subjects on cybersecurity awareness should be introduced in schools and colleges to make it an ongoing process.

The government must formulate strong laws to enforce cybersecurity and create sufficient awareness by broadcasting the same through television/radio/internet advertisements.

Information sharing

United States proposed a law called **Cybersecurity Information Sharing Act of 2014** (**CISA**) to improve cybersecurity in the country through enhanced sharing of information about cybersecurity threats. Such laws are required in every country to share threat information among citizens.

Cybersecurity Breaches Need a Mandatory Reporting Mechanism

The recent malware named **Uroburos/Snake** is an example of growing cyber-espionage and cyber-warfare. Stealing of sensitive information is the new trend. However, it is unfortunate that the telecom companies/internet service providers (ISPs) are not sharing information pertaining to cyber-attacks against their networks. As a result, a robust cybersecurity strategy to counter cyber-attacks cannot be formulated.

This problem can be addressed by formulating a good cybersecurity law that can establish a regulatory regime for obligatory cybersecurity breach notifications on the part of telecom companies/ISPs.

Infrastructures such as automated power grids, thermal plants, satellites, etc., are vulnerable to diverse forms of cyber-attacks and hence a breach notification program would alert the agencies to work on them.

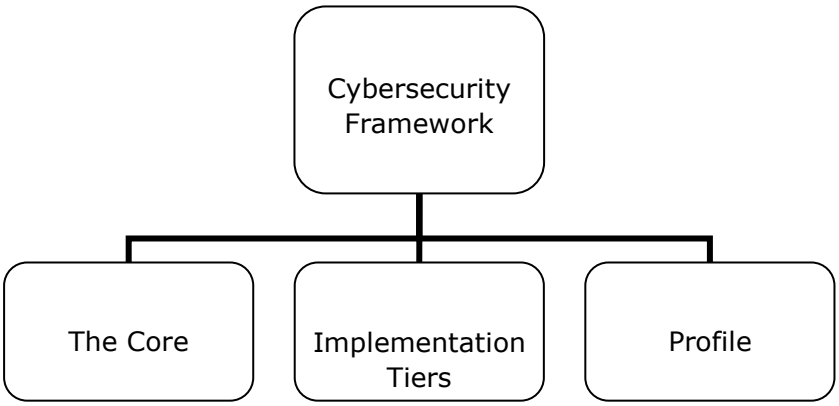
Implementing a Cybersecurity Framework

Despite the fact that companies are spending on cybersecurity initiatives, data breaches continue to occur. According to *The Wall Street Journal*, "Global cybersecurity spending by critical infrastructure industries was expected to hit $46 billion in 2013, up 10% from a year earlier according to Allied Business Intelligence Inc." This calls for the effective implementation of the cybersecurity framework.

Components of Cybersecurity Framework

The Framework comprises of three main components:

- The Core,
- Implementation Tiers, and
- Framework Profiles.



Components of Cybersecurity Framework

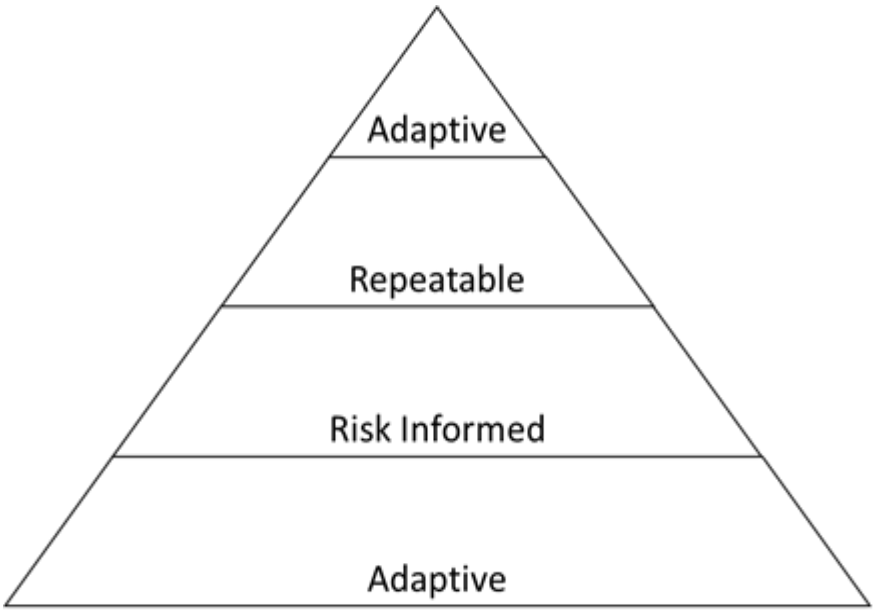
The Framework Core

The Framework Core is a set of cybersecurity activities and applicable references that having five simultaneous and constant functions—Identify, Protect, Detect, Respond, and Recover. The framework core has methods to ensure the following:

- Develop and implement procedures to protect the most critical intellectual property and assets.
- Have resources in place to identify any cybersecurity breach.
- Recover from a breach, if and when one occurs.

The Implementation Tiers

The Framework Implementation Tiers define the level of sophistication and consistency an organization employs in applying its cybersecurity practices. It has the following four levels.



Framework Implementation Tier levels

Tier 1 (Partial): In this level, the organization's cyber-risk management profiles are not defined. There is a partial consciousness of the organization's cybersecurity risk at the organization level. Organization-wide methodology to managing cybersecurity risk has not been recognized.

Tier 2 (Risk Informed): In this level, organizations establish a cyber-risk management policy that is directly approved by the senior management. The senior management makes efforts to establish risk management objectives related to cybersecurity and implements them.

Tier 3 (Repeatable): In this level, the organization runs with formal cybersecurity measures, which are regularly updated based on requirement. The organization recognizes its dependencies and partners. It also receives information from them, which helps in taking risk-based management decisions.

Tier 4 (Adaptive): In this level, the organization adapts its cybersecurity practices "in real-time" derived from previous and current cybersecurity activities. Through a process of incessant development in combining advanced cybersecurity technologies, real-time collaboration with partners, and continuous monitoring of activities on their systems, the organization's cybersecurity practices can quickly respond to sophisticated threats.

The Framework Profile

The Framework Profile is a tool that provides organizations a platform for storing information concerning their cybersecurity program. A profile allows organizations to clearly express the goals of their cybersecurity program.

Where do You Start with Implementing the Framework?

The senior management including the directors should first get acquainted with the Framework. After which, the directors should have a detailed discussion with the management about the organization's Implementation Tiers.

Educating the managers and staff on the Framework will ensure that everyone understands its importance. This is an important step towards the successful implementation of a vigorous cybersecurity program. The information about existing Framework Implementations may help organizations with their own approaches.

6. NETWORK SECURITY

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Types of Network Security Devices

Active Devices

These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

Passive Devices

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

Preventative Devices

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

Unified Threat Management (UTM)

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

Firewalls

A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.

Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.

Most personal computers use software-based firewalls to secure data from threats from the internet. Many routers that pass data between networks contain

firewall components and conversely, many firewalls can perform basic routing functions.

Firewalls are commonly used in private networks or *intranets* to prevent unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

An ideal firewall configuration consists of both hardware and software based devices. A firewall also helps in providing remote access to a private network through secure authentication certificates and logins.

Hardware and Software Firewalls

Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For larger networks – e.g., for business purpose – business networking firewall solutions are available.

Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.

Antivirus

An antivirus is a tool that is used to detect and remove malicious software. It was originally designed to detect and remove viruses from computers.

Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, keyloggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

Content Filtering

Content filtering devices screen unpleasant and offensive emails or webpages. These are used as a part of firewalls in corporations as well as in personal computers. These devices generate the message "Access Denied" when someone tries to access any unauthorized web page or email.

Content is usually screened for pornographic content and also for violence- or hate-oriented content. Organizations also exclude shopping and job related contents.

Content filtering can be divided into the following categories:

- Web filtering
- Screening of Web sites or pages
- E-mail filtering

- Screening of e-mail for spam
- Other objectionable content

Intrusion Detection Systems

Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are the appliances that monitor malicious activities in a network, log information about such activities, take steps to stop them, and finally report them.

Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage. Intrusion detection systems can also perform the following actions:

- Correct Cyclic Redundancy Check (CRC) errors
- Prevent TCP sequencing issues
- Clean up unwanted transport and network layer options

7. I.T. ACT

As discussed in the first chapter, the Government of India enacted the Information Technology (I.T.) Act with some major objectives to deliver and facilitate lawful electronic, digital, and online transactions, and mitigate cyber-crimes.

Salient Features of I.T. Act

The salient features of the I.T. Act are as follows:

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- It defines in a new section that *cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public*.
- It provides for the constitution of the Cyber Regulations Advisory Committee.
- It is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.
- It adds a provision to Section 81, which states that the provisions of the Act shall have overriding effect. The provision states that *nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957*.

Scheme of I.T. Act

The following points define the scheme of the I.T. Act:

- The I.T. Act contains **13 chapters** and **90 sections**.
- The last four sections namely sections 91 to 94 in the I.T. Act 2000 deals with the amendments to the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934 were deleted.

- It commences with Preliminary aspect in Chapter 1, which deals with the short, title, extent, commencement and application of the Act in Section 1. Section 2 provides Definition.
- Chapter 2 deals with the authentication of electronic records, digital signatures, electronic signatures, etc.
- Chapter 11 deals with offences and penalties. A series of offences have been provided along with punishment in this part of The Act.
- Thereafter the provisions about due diligence, role of intermediaries and some miscellaneous provisions are been stated.
- The Act is embedded with two schedules. The First Schedule deals with Documents or Transactions to which the Act shall not apply. The Second Schedule deals with electronic signature or electronic authentication technique and procedure. The Third and Fourth Schedule are omitted.

Application of the I.T. Act

As per the sub clause (4) of Section 1, *nothing in this Act shall apply to documents or transactions specified in First Schedule*. Following are the documents or transactions to which the Act shall not apply:

- **Negotiable Instrument** (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
- A **power-of-attorney** as defined in section 1A of the Powers-of-Attorney Act, 1882;
- A **trust** as defined in section 3 of the Indian Trusts Act, 1882;
- A **will** as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;
- Any **contract** for the sale or conveyance of immovable property or any interest in such property;
- Any such class of documents or transactions as may be notified by the Central Government.

Amendments Brought in the I.T. Act

The I.T. Act has brought amendment in four statutes vide section 91-94. These changes have been provided in schedule 1-4.

- The first schedule contains the amendments in the Penal Code. *It has widened the scope of the term "document" to bring within its ambit electronic documents.*

- The second schedule deals with amendments to the India Evidence Act. *It pertains to the inclusion of electronic document in the definition of evidence.*
- The third schedule amends the Banker's Books Evidence Act. *This amendment brings about change in the definition of "Banker's-book". It includes printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device. Similar change has been brought about in the expression "Certified-copy" to include such printouts within its purview.*
- The fourth schedule amends the Reserve Bank of India Act. *It pertains to the regulation of fund transfer through electronic means between the banks or between the banks and other financial institution.*

Intermediary Liability

Intermediary, dealing with any specific electronic records, is a person who on behalf of another person accepts, stores or transmits that record or provides any service with respect to that record.

According to the above mentioned definition, it includes the following:

- Telecom service providers
- Network service providers
- Internet service providers
- Web-hosting service providers
- Search engines
- Online payment sites
- Online auction sites
- Online market places and cyber cafes

Highlights of the Amended Act

The newly amended act came with following highlights:

- It stresses on privacy issues and highlights information security.
- It elaborates Digital Signature.
- It clarifies rational security practices for corporate.
- It focuses on the role of Intermediaries.
- New faces of Cyber Crime were added.

8. SIGNATURES

Digital Signature

A digital signature is a technique to validate the legitimacy of a digital message or a document. A valid digital signature provides the surety to the recipient that the message was generated by a known sender, such that the sender cannot deny having sent the message. Digital signatures are mostly used for software distribution, financial transactions, and in other cases where there is a risk of forgery.

Electronic Signature

An electronic signature or e-signature, indicates either that a person who demands to have created a message is the one who created it.

A signature can be defined as a schematic script related with a person. A signature on a document is a sign that the person accepts the purposes recorded in the document. In many engineering companies digital seals are also required for another layer of authentication and security. Digital seals and signatures are same as handwritten signatures and stamped seals.

Digital Signature to Electronic Signature

Digital Signature was the term defined in the old I.T. Act, 2000. **Electronic Signature** is the term defined by the amended act (I.T. Act, 2008). The concept of Electronic Signature is broader than Digital Signature. Section 3 of the Act delivers for the verification of Electronic Records by affixing Digital Signature.

As per the amendment, verification of electronic record by electronic signature or electronic authentication technique shall be considered reliable.

According to the **United Nations Commission on International Trade Law (UNCITRAL)**, electronic authentication and signature methods may be classified into the following categories:

- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
- Those bases on the physical features of the user, i.e., biometrics.
- Those based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.

- Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).

According to the UNCITRAL MODEL LAW on Electronic Signatures, the following technologies are presently in use:

- Digital Signature within a public key infrastructure (PKI)
- Biometric Device
- PINs
- Passwords
- Scanned handwritten signature
- Signature by Digital Pen
- Clickable "OK" or "I Accept" or "I Agree" click boxes

9. OFFENCE AND PENALTIES

The faster world-wide connectivity has developed numerous online crimes and these increased offences led to the need of laws for protection. In order to keep in stride with the changing generation, the Indian Parliament passed the Information Technology Act 2000 that has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The law defines the offenses in a detailed manner along with the penalties for each category of offence.

Offences

Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.

Cyber-crime usually includes the following:

- Unauthorized access of the computers
- Data diddling
- Virus/worms attack
- Theft of computer system
- Hacking
- Denial of attacks
- Logic bombs
- Trojan attacks
- Internet time theft
- Web jacking
- Email bombing
- Salami attacks
- Physically damaging computer system.

The offences included in the I.T. Act 2000 are as follows:

- Tampering with the computer source documents.
- Hacking with computer system.

- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Example

Offences Under The It Act 2000:
Section 65. Tampering with computer source documents:
Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation: For the purpose of this section “computer source code” means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Object: The object of the section is to protect the “intellectual property” invested in the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law

Essential ingredients of the section:

knowingly or intentionally concealing

knowingly or intentionally destroying

knowingly or intentionally altering

knowingly or intentionally causing others to conceal

knowingly or intentionally causing another to destroy

knowingly or intentionally causing another to alter.

This section extends towards the Copyright Act and helps the companies to protect their source code of their programs.
Penalties: Section 65 is tried by any magistrate.
This is cognizable and non-bailable offence.
Penalties: Imprisonment up to 3 years and / or
Fine: Two lakh rupees.

The following table shows the offence and penalties against all the mentioned sections of the I.T. Act:

Section	Offence	Punishment	Bailability and Congizability
Section 65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC.
Section 66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC
Section 66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC
Section 66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
Section 66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC

Section 66-D	Cheating by Personation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
Section 66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
Section 66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions
Section 67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
Section 67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment up to 5 ears and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
Section 67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non Bailable, Cognizable and triable by Court of JMFC

Section 67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
Section 68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
Section 69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
Section 69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
Section 69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cybersecurity	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
Section 70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine	Offence is Non-Bailable, Cognizable.

Section 70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable
Section 71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
Section 72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
Section 72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.	Offence is Cognizable, Bailable
Section 73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
Section 74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.

Compounding of Offences

As per Section 77-A of the I. T. Act, *any Court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under the Act.*

No offence shall be compounded if:

- *The accused is, by reason of his previous conviction, is liable to either enhanced punishment or to the punishment of different kind; OR*

- *Offence affects the socio economic conditions of the country; OR*
- *Offence has been committed against a child below the age of 18 years; OR*
- *Offence has been committed against a woman.*

The person alleged of an offence under this Act may file an application for compounding in the Court. The offence will then be pending for trial and the provisions of Sections 265-B and 265-C of Cr. P.C. shall apply.

10. SUMMARY

Cyber Laws are the sole savior to combat cyber-crime. It is only through stringent laws that unbreakable security could be provided to the nation's information. The I.T. Act of India came up as a special act to tackle the problem of Cyber Crime. The Act was sharpened by the Amendment Act of 2008.

Cyber Crime is committed every now and then, but is still hardly reported. The cases of cyber-crime that reaches to the Court of Law are therefore very few. There are practical difficulties in collecting, storing and appreciating Digital Evidence. Thus the Act has miles to go before it can be truly effective.

In this tutorial, we have tried to cover all the current and major topics related to Cyber Laws and IT Security. We would like to quote the words of a noted cyber law expert and Supreme Court advocate Mr Pavan Duggal to conclude this tutorial.

> *While the lawmakers have to be complemented for their admirable work removing various deficiencies in the Indian Cyberlaw and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyberlaw a cyber-crime friendly legislation; - a legislation that goes extremely soft on cyber criminals, with a soft heart; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment accorded to them under the existing law; ….. a legislation which makes a majority of cybercrimes stipulated under the IT Act as bailable offences; a legislation that is likely to pave way for India to become the potential cyber-crime capital of the world.*

11. FAQ

1. What is Cybercrime?

Cybercrime refers to all the activities done with criminal intent in cyberspace. Because of the anonymous nature of the internet, miscreants engage in a variety of criminal activities. The field of cybercrime is just emerging and new forms of criminal activities in cyberspace are coming to the forefront with each passing day.

2. Do we have an exhaustive definition of Cybercrime?

No, unfortunately we don't have an exhaustive definition of cybercrime. However, any online activity which basically offends human sensibilities can be regarded as a cybercrime.

3. What are the various categories of Cybercrimes?

Cybercrimes can be basically divided into three major categories:

- Cybercrimes against persons,
- Cybercrimes against property, and
- Cybercrimes against Government.

4. Tell us more about Cybercrimes against persons.

Cybercrimes committed against persons include various crimes like transmission of child pornography, harassment using e-mails and cyber-stalking. Posting and distributing obscene material is one of the most important Cybercrimes known today.

5. Is Cyber harassment also a Cybercrime?

Cyber harassment is a distinct cybercrime. Various kinds of harassment does occur in cyberspace. Harassment can be sexual, racial, religious, or other. Cyber harassment as a crime also brings us to another related area of violation of privacy of netizens. Violation of privacy of online citizens is a Cybercrime of a grave nature.

6. What are Cybercrimes against property?

Cybercrimes against all forms of property include unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information.

7. Is hacking a Cybercrime?

Hacking is amongst the gravest Cybercrimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer system without your knowledge and has tampered with precious confidential data.

The bitter truth is that no computer system in the world is hacking proof. It is unanimously agreed that any system, however secure it might look, can be hacked. The recent denial of service attacks seen over the popular commercial sites like E-bay, Yahoo, and Amazon are a new category of Cybercrimes which are slowly emerging as being extremely dangerous.

Using one's own programming abilities to gain unauthorized access to a computer or network is a very serious crime. Similarly, the creation and dissemination of harmful computer programs which do irreparable damage to computer systems is another kind of Cybercrime.

8. What is Cybercrime against Government?

Cyber Terrorism is one distinct example of cybercrime against government. The growth of Internet has shown that the medium of cyberspace is being used by individuals and groups to threaten the governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual hacks into a government or military maintained website.

9. Is there any comprehensive law on Cybercrime today?

As of now, we don’t have any comprehensive laws on cybercrime anywhere in the world. This is the reason that the investigating agencies like FBI are finding the Cyberspace to be an extremely difficult terrain. Cybercrimes fall into that grey area of Internet law which is neither fully nor partially covered by the existing laws. However, countries are taking crucial measures to establish stringent laws on cybercrime.

10. Is there any recent case which demonstrates the importance of having a cyber law on cybercrime within the national jurisdictions of countries?

The most recent case of the virus "I love you" demonstrates the need for having cyber laws concerning cybercrimes in different national jurisdictions. At the time of the web publication of this feature, Reuters has reported that "The Philippines has yet to arrest the suspected creator of the 'Love Bug' computer virus because it lacks laws that deal with computer crime, a senior police officer said". The fact of the matter is that there are no laws relating to cybercrime in the Philippines.

11. What is Vishing?

Vishing is the criminal practice of using social influence over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain

access to sensitive information such as credit card details from the public. The term is a combination of "Voice" and phishing.

12. What is Mail Fraud?

Mail fraud is an offense under United States federal law, which includes any scheme that attempts to unlawfully obtain money or valuables in which the postal system is used at any point in the commission of a criminal offense.

13. What is ID Spoofing?

It is the practice of using the telephone network to display a number on the recipient's Caller ID display which is not that of the actual originating station.

14. What is Cyber espionage?

It is the act or practice of obtaining secrets from individuals, competitors, rivals, groups, governments, and enemies for military, political, or economic advantage using illegal exploitation methods on the internet.

15. What is the meaning of Sabotage?

Sabotage literally means willful damage to any machinery or materials or disruption of work. In the context of cyberspace, it is a threat to the existence of computers and satellites used by military activities.

16. Name the democratic country in which The Cyber Defamation law was first introduced.

South Korea is the first democratic country in which this law was introduced first.

17. What are Bots?

Bots are one of the most sophisticated types of crime-ware facing the internet today. Bots earn their unique name by performing a wide variety of automated tasks on behalf of the cyber criminals. They play a part in "denial of service" attack in internet.

18. What are Trojans and Spyware?

Trojans and spyware are the tools a cyber-criminal might use to obtain unauthorized access and steal information from a victim as part of an attack.

19. What are Phishing and Pharming?

Phishing and Pharming are the most common ways to perform identity theft which is a form of cyber-crime in which criminals use the internet to steal personal information from others.

20. Mention some tips to prevent cyber-crimes.

- Read the latest ways hackers create phishing scams to gain access to your personal information.
- Install a firewall on your computer to keep unwanted threats and attacks to a minimum.
- Use caution while opening emails and clicking links. You should tread carefully while downloading content from unverified sources.
- Create strong passwords for any websites where personal information is stored.