



Cyber Security Unit – V

Dr. R. A. ROSELINE M.Sc., M.Phil., Ph.D.,
Associate Professor and Head,
Post Graduate Department Of Computer Applications,
Government Arts College, Coimbatore – 18.



Contents

- **Information Security and Cyber Law:**
 - Introduction
 - Objectives
 - Intellectual Property Rights
 - Strategies for Cyber Security
 - Policies to Mitigate Cyber Risk
 - Network Security
 - IT Act
 - Signatures
 - Offence and Penalties
- 
- 



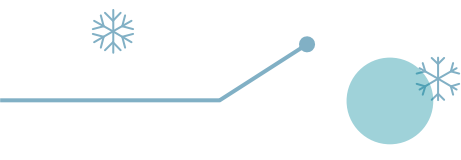
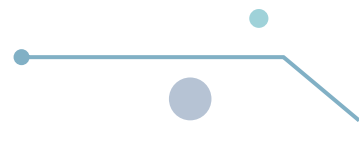
Introduction

1. Cyberspace
2. 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.





Cybersecurity

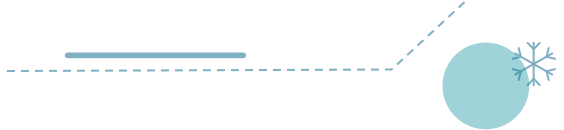
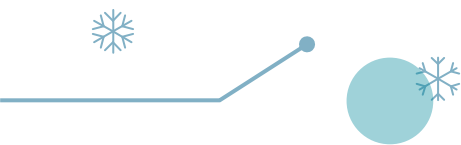
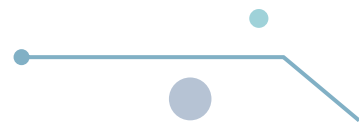
1. Cybersecurity denotes the technologies and procedures intended to safeguard computers, networks, and data from unlawful admittance, weaknesses, and attacks transported through the Internet by cyber delinquents.
 2. The Ministry of Communication and Information Technology under the government of India 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.
- 
- 



Cyber Crime

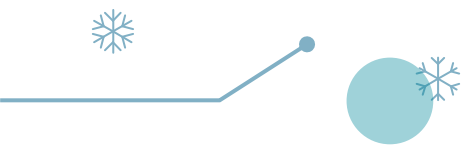
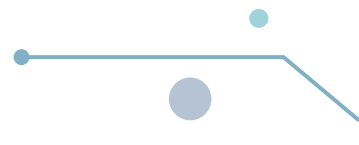
1. The Information Technology Act 2000 or any legislation in the Country does not describe or mention the term Cyber Crime.
2. It can be globally considered as the gloomier face of technology. The only difference between a traditional crime and a cyber-crime is that the cyber-crime involves in a crime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



- 
1. Traditional Theft: A thief breaks into Ram's house and steals an object kept in the house.
 2. 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.
- 
- 



Nature of Threat

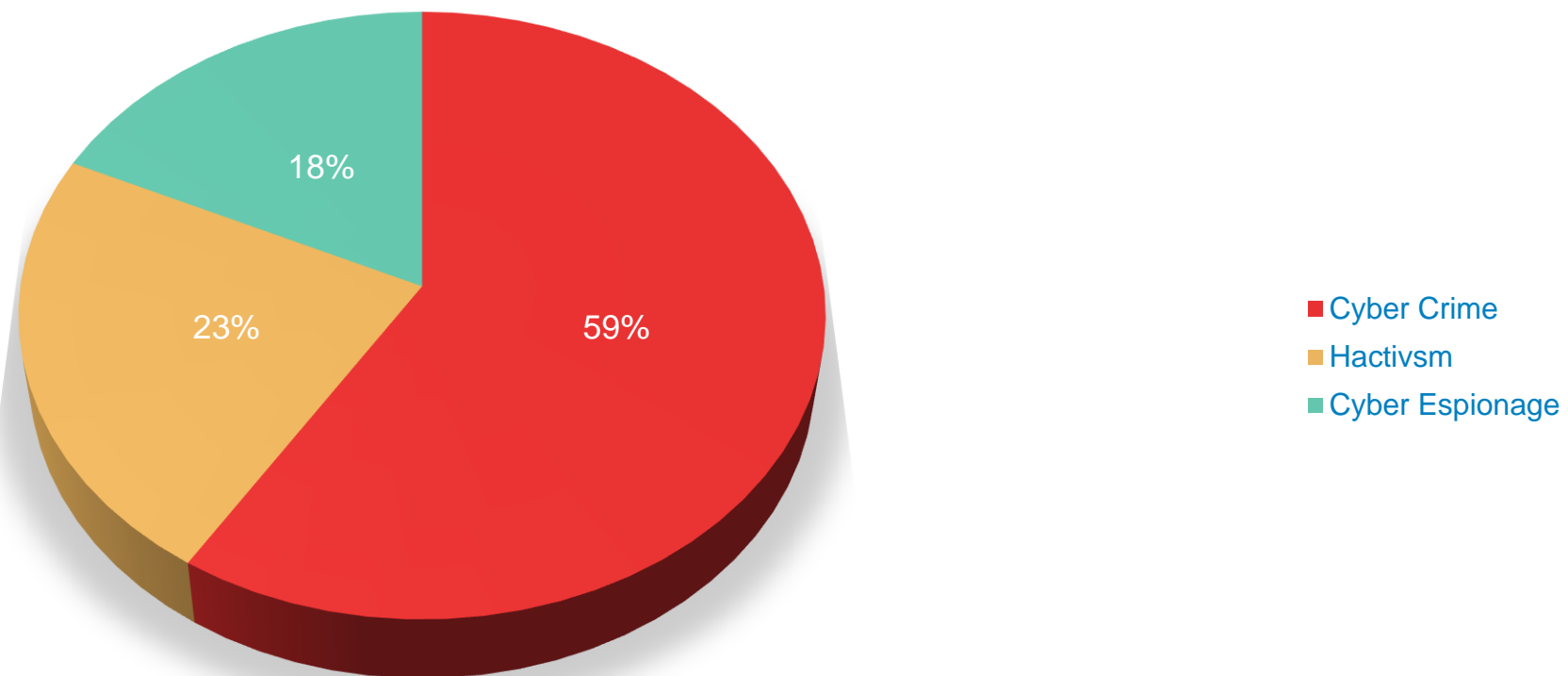
1. Threats originate from all kinds of sources, and mark themselves in disruptive activities that target individuals, businesses, national infrastructures, and governments alike. The effects of these threats transmit significant risk for the following:
 - i. public safety
 - ii. security of nations
 - iii. stability of the globally linked international community
- 
- 



1. 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:
 - i. simply demonstrating technical prowess
 - ii. theft of money or information
 - iii. extension of state conflict, etc.
2. 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.

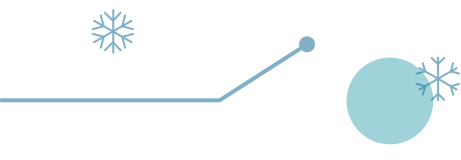
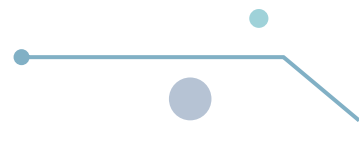



Motivations Behind Attacks July 2014

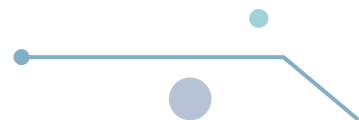




Information Technology Act

1. The Government of India enacted The Information Technology Act with some major objectives which are as follows:
 2. 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.
- 
- 

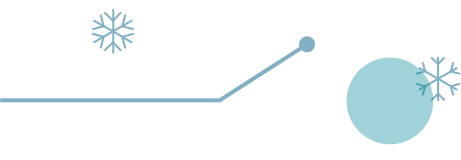
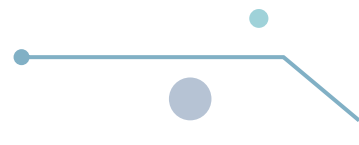
- 
1. To facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.





Mission and Vision of Cybersecurity

Program

1. Mission
 2. The following mission caters to cyber security:
 3. To safeguard information and information infrastructure in cyberspace.
 4. To build capabilities to prevent and respond to cyber threats.
 5. To reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.
- 
- 

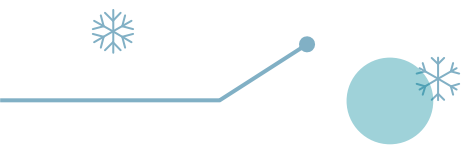
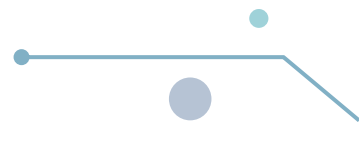




Vision

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



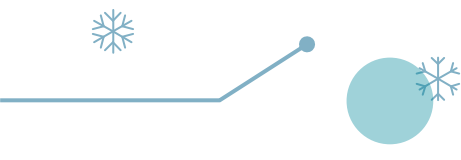
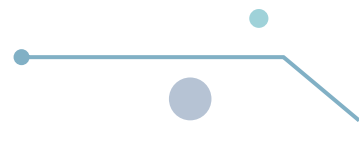
Objectives

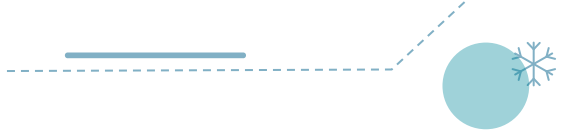
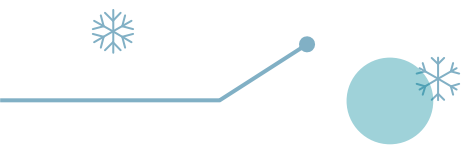
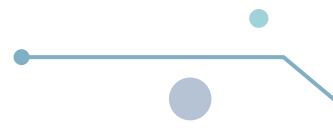
1. Emerging Trends of Cyber Law
 2. Reports reveal that upcoming years will experience more cyber-attacks. So organizations are advised to strengthen their data supply chains with better inspection methods. Some of the emerging trends of cyber law are listed below:
 3. Stringent regulatory rules are put in place by many countries to prevent unauthorized access to networks. Such acts are declared as penal offences.
 4. 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.
- 
- 

- 
1. 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*.
 2. **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.
 3. 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.
 4. 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**.
- 



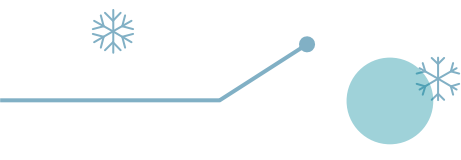
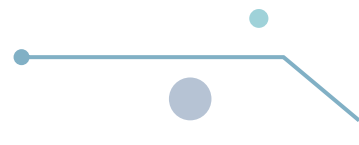
Create Awareness

1. 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.
 2. 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.
- 
- 

- 
1. 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:
 2. Filter the visibility of personal information in social sites. Do not keep the "remember password" button active for any email address and passwords
 3. Make sure your online banking platform is secure.
 4. Keep a watchful eye while shopping online.
 5. Do not save passwords on mobile devices.
 6. Secure the login details for mobile devices and computers, etc.
- 
- 









Areas of Development

1. The "Cyber law 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.
 2. 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).
- 
- 



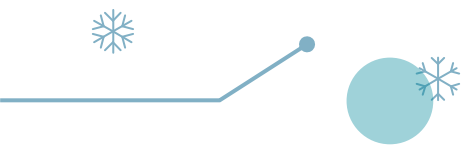
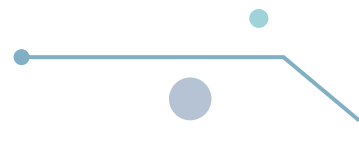
1. Following are some major issues:



- a. A better cyber law and effective cyber-crimes prevention strategy
 - b. Cyber-crimes investigation training requirements
 - c. Formulation of dedicated encryption laws
 - d. Legal adoption of cloud computing
 - e. Formulation and implementation of e-mail policy
 - f. Legal issues of online payments
 - g. Legality of online gambling and online pharmacies
 - h. Legality of Bitcoins
 - i. Framework for blocking websites
 - j. Regulation of mobile application
- 
- 
- 
- 

- 
- ❖ 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.
- 



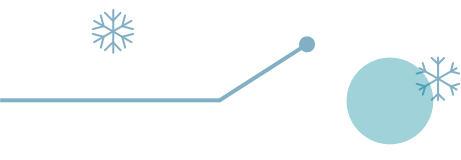
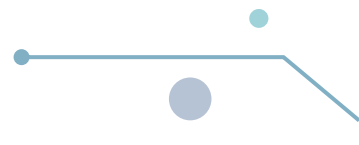
International Network on Cybersecurity


1. To create an international network on cyber security, a conference was held in March 2014 in New Delhi, India.
 2. The objectives set in the International Conference on Cyber law & Cybercrime are as follows:
 3. To recognize the developing trends in Cyber law and the legislation impacting cyberspace in the current situation.
- 
- 

- 
2. To generate better awareness to battle the latest kinds of cybercrimes impacting all investors in the digital and mobile network.
 3. To recognize the areas for stakeholders of digital and mobile network where
 4. Cyber law needs to be further evolved.
 5. 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 cybercrimes and cyber law legislations throughout the globe.
- 

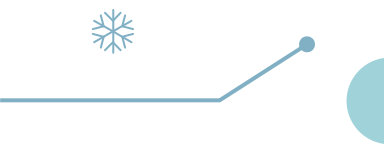
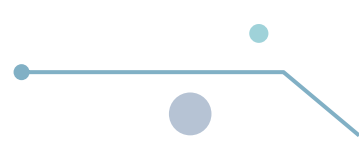


Intellectual Property Rights

1. 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.
 2. 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.
- 
- 

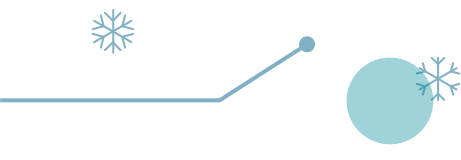
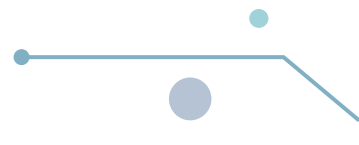


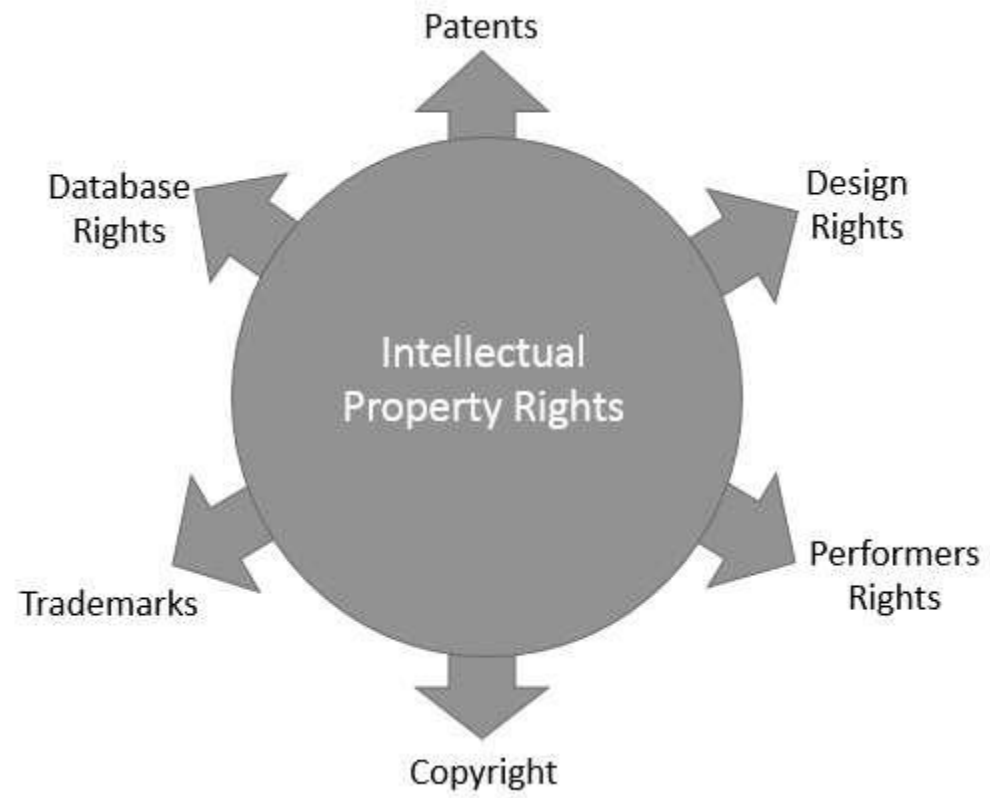
The following list of activities which are covered by the intellectual property rights are laid down by the World Intellectual Property Organization (WIPO):

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



Types of Intellectual Property Rights

1. Intellectual Property Rights can be further classified into the following categories:
 - i. Copyright
 - ii. Patent
 - iii. Trademark
 - iv. Trade Secrets, etc.
- 
- 



Advantages of Intellectual Property


1. Intellectual property rights are advantageous in the following ways:
2. Provides exclusive rights to the creators or inventors.
3. Encourages individuals to distribute and share information and data instead of keeping it confidential.
4. Provides legal defense and offers the creators the incentive of their work.
5. Helps in social and financial development.



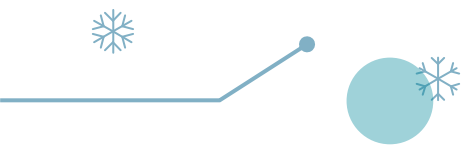
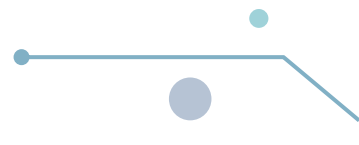
Intellectual Property Rights in India

1. To protect the intellectual property rights in the Indian territory, India has defined the formation of constitutional, administrative and jurisdictional 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

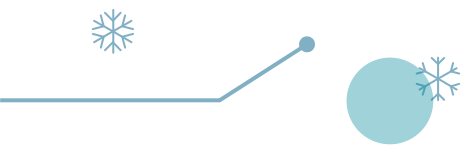
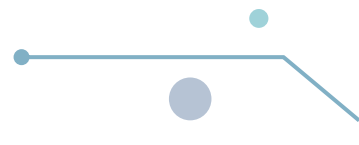
1. Every new invention in the field of technology experiences a variety of threats. Internet is one such threat, which has captured the physical marketplace and have converted it into a virtual marketplace.
2. To safeguard the business interest, it is vital to create an effective property management 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.*



Strategies for Cyber security


1. To design and implement a secure cyberspace, some stringent strategies have been put in place. the major strategies employed to ensure cyber security, which include the following:
 2. Creating a Secure Cyber Ecosystem
 3. Creating an Assurance Framework
 4. Encouraging Open Standards
 5. Strengthening the Regulatory Framework
 6. Creating Mechanisms for IT Security
 7. Securing E-governance Services
 8. Protecting Critical Information Infrastructure
- 
- 



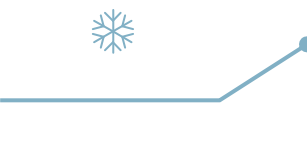
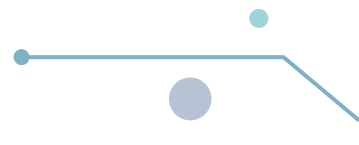
Strategy 1: Creating a Secure Cyber Ecosystem

1. 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.
2. This cyber ecosystem can be supervised by present monitoring techniques where software products are used to detect and report security weaknesses.



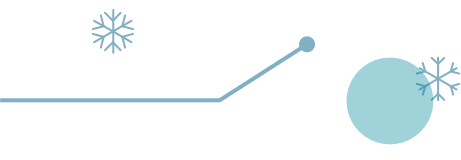
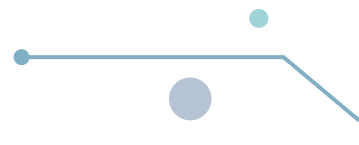


A strong cyber-ecosystem has three symbiotic structures - **Automation, Interoperability, and Authentication.**

- 1. Automation: It eases the implementation of advanced security measures,** enhances the swiftness, and optimizes the decision-making processes.
 - 2. 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
- 
- 



3. Authentication: It improves the identification and verification technologies that work in order to provide:

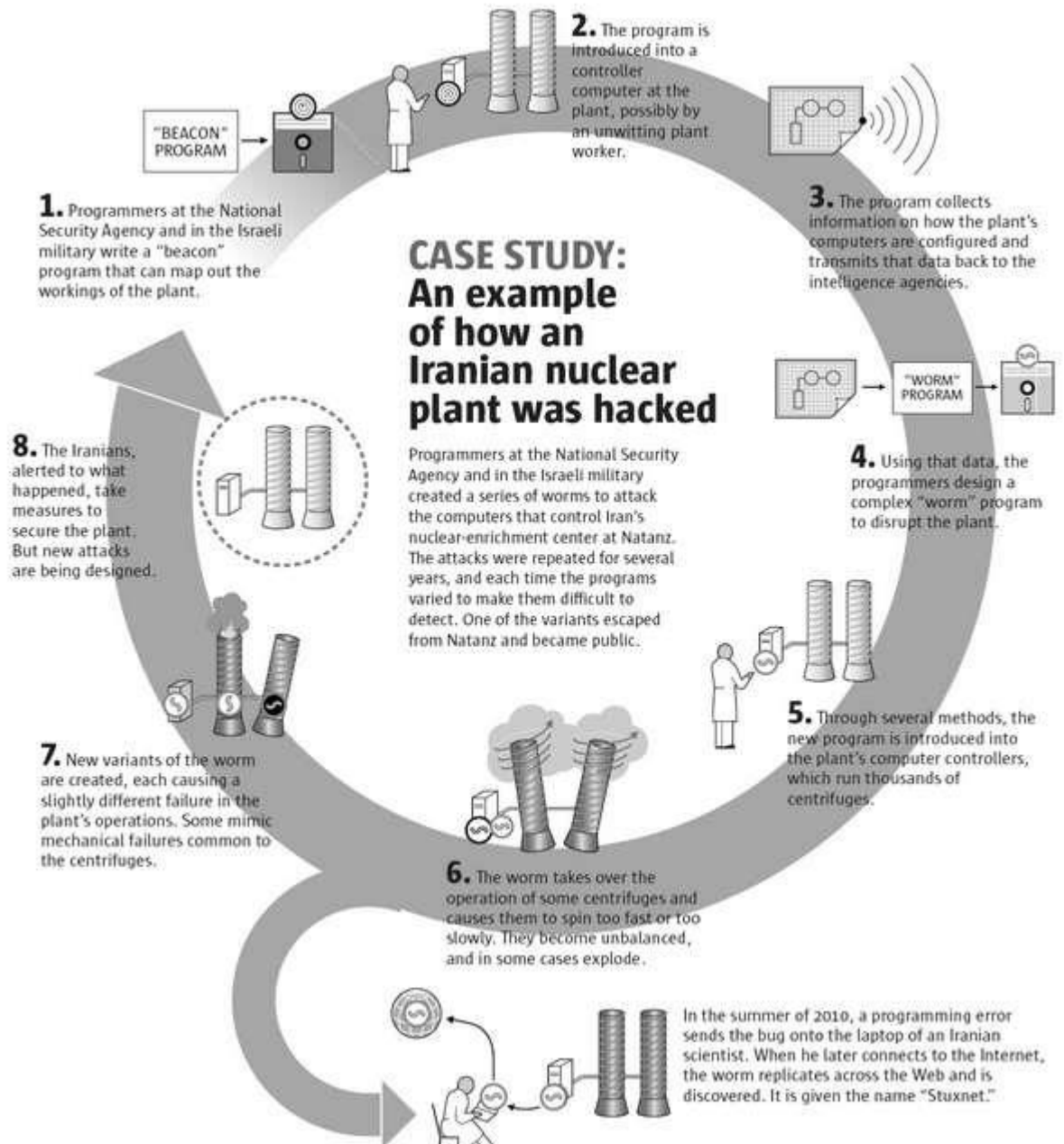
1. Security
 2. Affordability
 3. Ease of use and administration
 4. Scalability
 5. Interoperability
- 
- 




Comparison of Attacks


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

Desired Cyber Ecosystem Capabilities	Categories of Cyber Attack							
	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





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


1. The following table describes the attack categories:

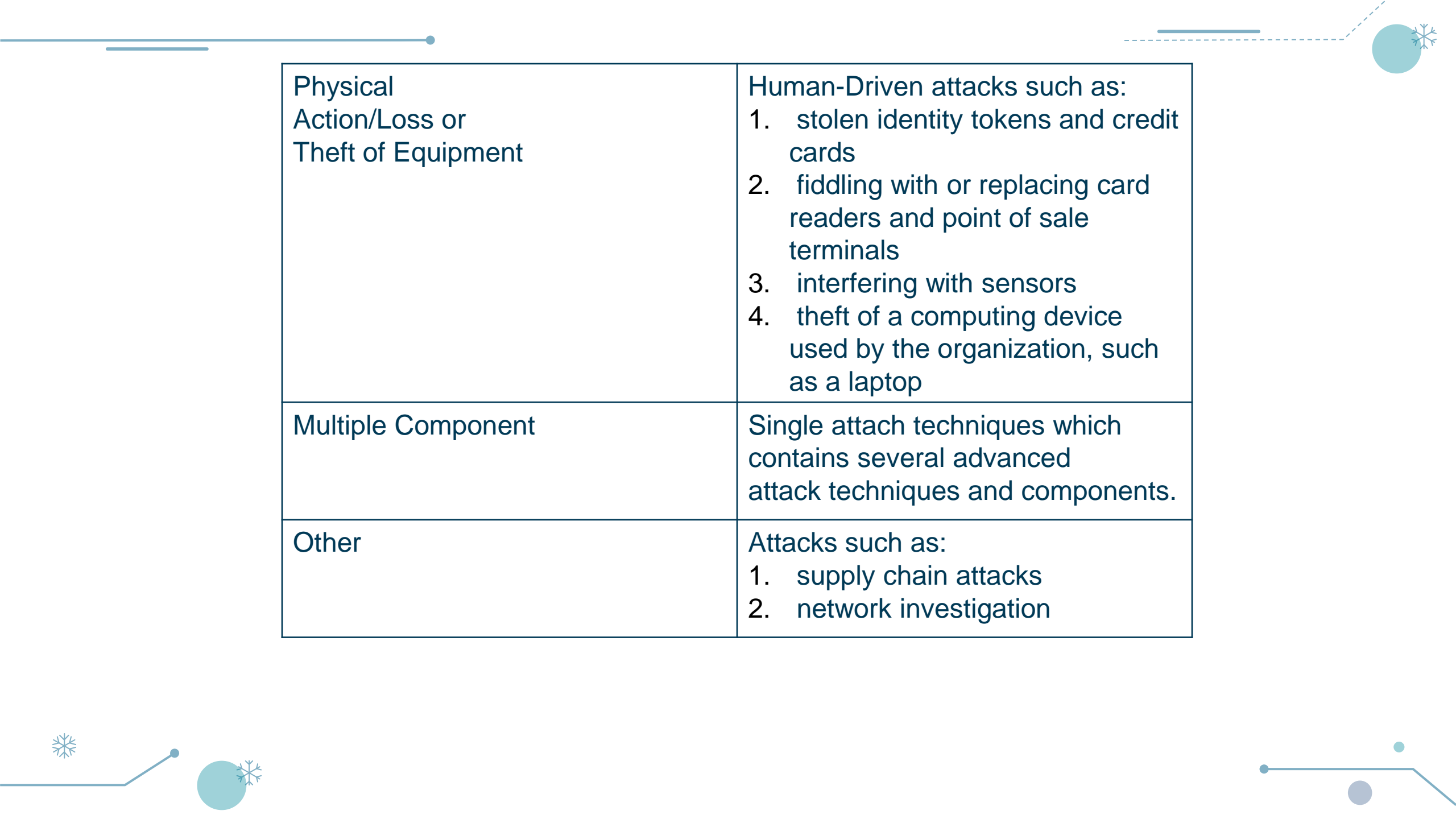
Attack Category	Description of Attack
Attrition	Methods used to damage networks and systems. It includes the following: <ol style="list-style-type: none">1. distributed denial of service attacks2. impair or deny access to a service or application3. resource depletion attacks

Malware	<p>Methods used to damage networks and systems. It includes the following:</p> <ol style="list-style-type: none">1. distributed denial of service attacks2. impair or deny access to a service or application3. resource depletion attacks
Hacking	<p>An attempt to intentionally exploit weaknesses to get unethical access, usually conducted remotely. It may include:</p> <ol style="list-style-type: none">1. data-leakage attacks2. injection attacks and abuse of functionality3. spoofing4. time-state attacks5. buffer and data structure attacks6. resource manipulation7. stolen credentials usage8. backdoors9. dictionary attacks on passwords10. exploitation of authentication



Social Tactics	Using social tactics such as deception and manipulation to acquire access to data, systems or controls. It includes: <ol style="list-style-type: none">1. pre-texting (forged surveys)2. inciting phishing3. 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: <ol style="list-style-type: none">1. installation of unauthorized software2. removal of sensitive data





Physical Action/Loss or Theft of Equipment	Human-Driven attacks such as: <ol style="list-style-type: none">1. stolen identity tokens and credit cards2. fiddling with or replacing card readers and point of sale terminals3. interfering with sensors4. theft of a computing device used by the organization, such as a laptop
Multiple Component	Single attack techniques which contains several advanced attack techniques and components.
Other	Attacks such as: <ol style="list-style-type: none">1. supply chain attacks2. network investigation



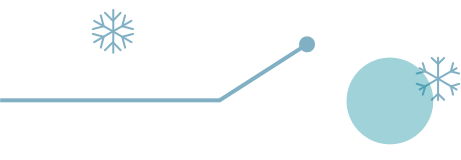
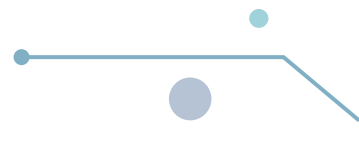
Strategy 2: Creating an Assurance Framework

1. The objective of this strategy is to design an outline in compliance with the global security standards through traditional products, processes, people, and technology.
2. 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

1. 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


1. Endorsing actions are involved in profitable services after meeting the obligatory qualification standards and they include the following:
 - a. ISO 27001/BS 7799 ISMS certification, IS system audits etc., which are essentially the compliance certifications.
 - b. 'Common Criteria' standard ISO 15408 and Crypto module verification standards, which are the IT Security product evaluation and certification.
 - c. Services to assist consumers in implementation of IT security such as IT security manpower training.



Trusted Company Certification

1. 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.






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

1. standards
2. guidelines
3. practices

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





Strategy 3: Encouraging Open Standards

1. Standards play a significant role in defining how we approach information security related issues across geographical regions and societies. Open standards are encouraged to:
 - a. Enhance the efficiency of key processes,
 - b. Enable systems incorporations,
 - c. Provide a medium for users to measure new products or services,
 - d. Organize the approach to arrange new technologies or business models,
 - e. Interpret complex environments, and
 - f. Endorse economic growth.
2. 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.



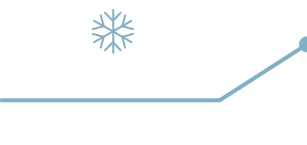
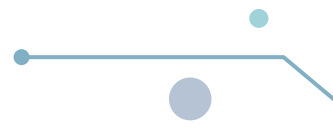
Strategy 4: Strengthening the

Regulatory Framework

1. 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).
2. 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 cyber security.
 - 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 cyber security initiatives.
 - Indian Armed Forces are in the process of establishing a cyber-command as a part of strengthening the cyber security 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
- 
- 



Strategy 5: Creating Mechanisms for IT Security

1. 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

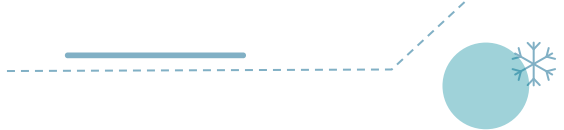




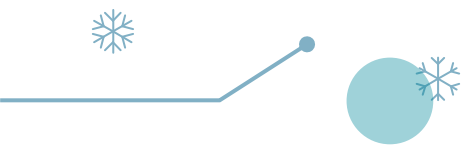
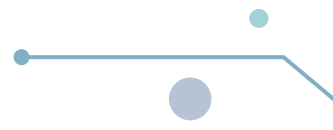
Strategy 6: Securing E-Governance

1. 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.





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



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

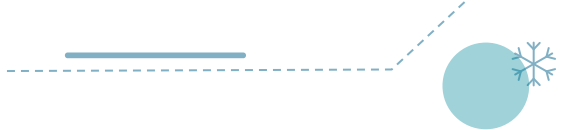


Strategy 7: Protecting Critical

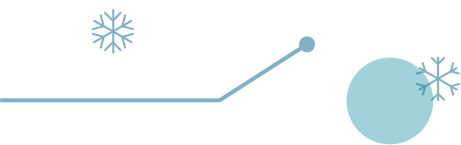
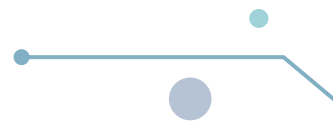
- ## Information Infrastructure
1. Critical information infrastructure is the backbone of a country's national and economic security. It includes power plants, highways, bridges, chemical plants, networks, as well as the buildings where millions of people work every day. These can be secured with stringent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



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

1. Define their existing cyber security bearing,
 2. Define their objectives for cyber security,
 3. Categorize and prioritize chances for development within the framework of a constant process, and
 4. Communicate with all the investors about cyber security.
- 
- 



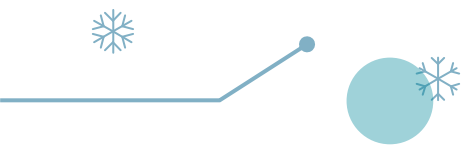
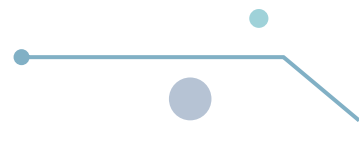
Policies to Mitigate Cyber Risk

1. Cybersecurity Research
2. 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.





Threat Intelligence

1. 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.
- 
- 



Secured Protocol and Algorithms

1. Research in protocols and algorithms is a significant phase for the consolidation of cyber security at a technical level. It defines the rules for information sharing and processing over cyberspace. In India, protocol and algorithm level research includes:
 - i. Secure Routing Protocols
 - ii. Efficient Authentication Protocols
 - iii. Enhanced Routing Protocol for Wireless Networks
 - iv. Secure Transmission Control Protocol
 - v. Attack Simulation Algorithm, etc.





Authentication Techniques

1. 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





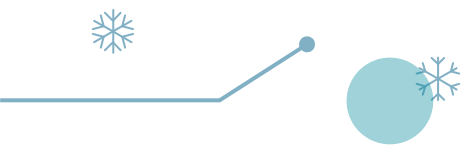
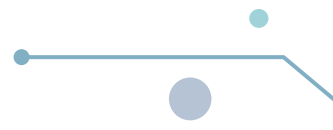
BYOD, Cloud and Mobile Security

1. 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

1. 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:
 1. Disk Forensics
 2. Network Forensics
 3. Mobile Device Forensics
 4. Memory Forensics
 5. Multimedia Forensics
 6. Internet Forensics
- 
- 



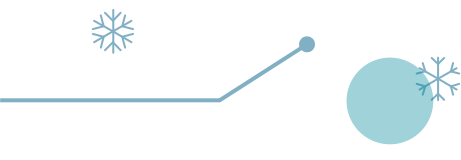
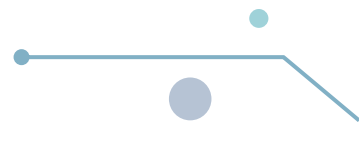
Reducing Supply Chain Risks

1. Formally, supply chain risk can be defined as:
2. 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

1. Supply chain is a global issue and there is a requirement to find out the interdependencies among the customers and suppliers.
 2. 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.
- 
- 

Mitigate Risks through Human Resource

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



1. Taking Ownership of the Security Risk

- Posed by Employees**
1. 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.





2. Ensuring that Security Measures are

- # Practical and Ethical
1. Policies of a company must be in sync with the way employees think and behave.
 2. 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.





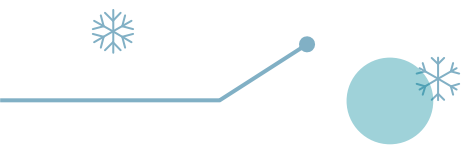
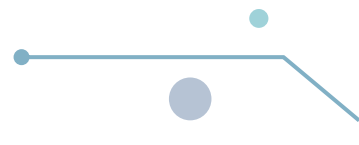
Identifying Employees who may Present

1. 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

1. 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.
 2. Subjects on cyber security awareness should be introduced in schools and colleges to make it an ongoing process.
 3. The government must formulate strong laws to enforce cyber security and create sufficient awareness by broadcasting the same through television/radio/internet advertisements.
- 
- 



Information sharing

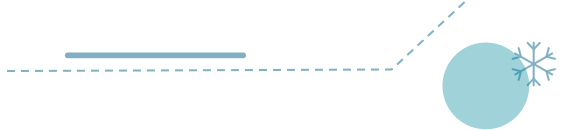
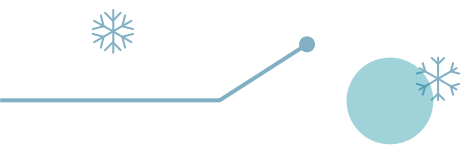
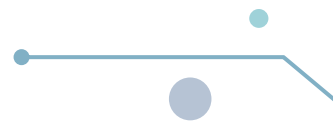
1. United States proposed a law called Cybersecurity Information Sharing Act of 2014 (CISA) to improve cyber security in the country through enhanced sharing of information about cyber security threats. Such laws are required in every country to share threat information among citizens.



Cybersecurity Breaches Need a

Mandatory Reporting Mechanism

1. The recent malware named Urdoures /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 cyber security strategy to counter cyber-attacks cannot be formulated.

- 
- This problem can be addressed by formulating a good cyber security law that can establish a regulatory regime for obligatory cyber security 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

1. According to The Wall Street Journal, "Global cyber security spending by critical infrastructure industries was expected to hit \$40 billion in 2013, up 10% from a year earlier according to Allied Business Intelligence Inc." This calls for the effective implementation of the cyber security framework.





Components of Cybersecurity

1. The Framework comprises of three main components:

Framework

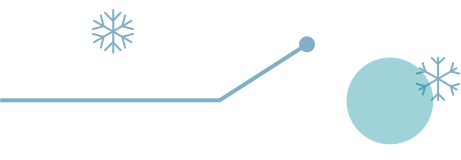
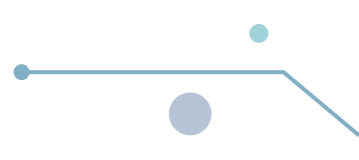
 - i. The Core,
 - ii. Implementation Tiers, and
 - iii. Framework Profiles.





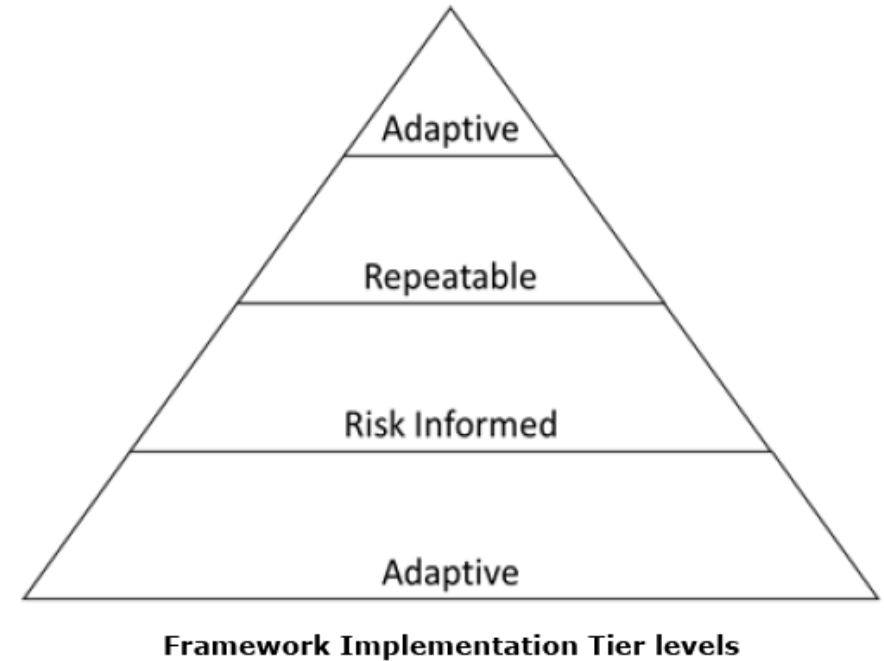
The Framework Core


The Framework Core is a set of cyber security 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 cyber security breach.
 - Recover from a breach, if and when one occurs.
- 
- 

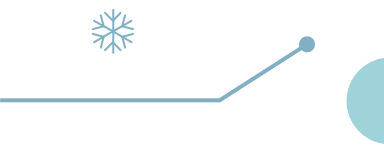
The Implementation Tiers

1. The Framework Implementation Tiers define the level of sophistication and consistency an organization employs in applying its cyber security practices.

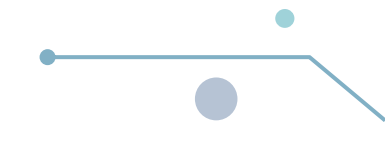





Tier 1 (Partial): In this level, the organization's **cyber-risk management profiles are not** defined. There is a partial consciousness of the organization's cyber security risk at the organization level. Organization-wide methodology to managing cyber security risk has not been recognized.



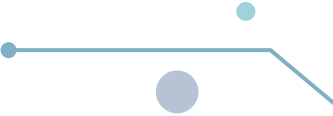

Tier 2 (Risk Informed): In this level, **organizations establish a cyber-risk management** policy that is directly approved by the senior management. The senior management makes efforts to establish risk management objectives related to cyber security and implements them





Tier 3 (Repeatable): In this level, the organization runs with formal cyber security 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 cyber security practices "in real-time" derived from previous and current cyber security activities. Through a process of incessant development in combining advanced cyber security technologies, real-time collaboration with partners, and continuous monitoring of activities on their systems, the organization's cyber security





The Framework Profile

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





Network Security

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



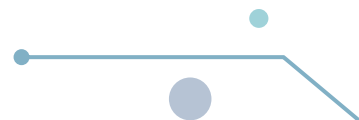
Types of Network Security Devices

1. Active Devices
 - 2. These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.
3. Passive Devices
 - 4. These devices identify and report on unwanted traffic, for example, intrusion detection appliances.
5. Preventative Devices
 - 6. These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.
7. Unified Threat Management (UTM)
 - 8. These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.



Firewalls

1. 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.





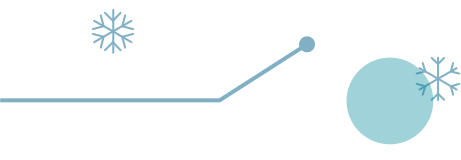
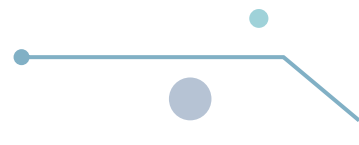
Hardware and Software Firewalls

1. 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.
2. Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.



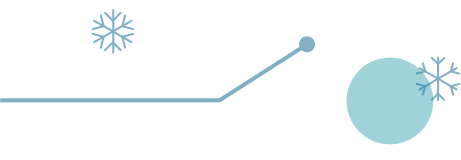
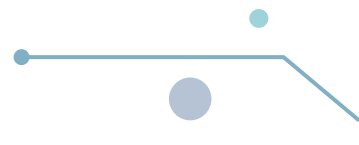


Antivirus

1. 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.
 2. Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, key loggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.
- 
- 

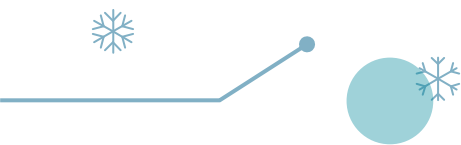
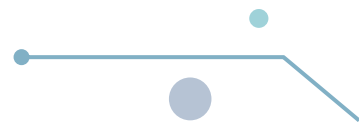


Content Filtering

1. Content filtering devices screen unpleasant and offensive emails or web pages. 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.
 2. 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:

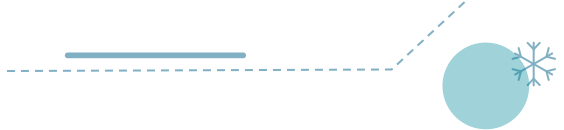
1. Web filtering
 2. Screening of Web sites or pages
 3. E-mail filtering
 4. Screening of e-mail for spam
 5. Other objectionable content
- 
- 



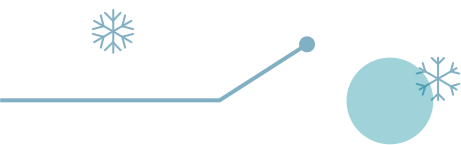
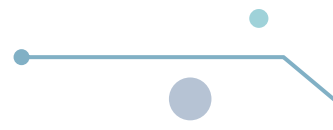
Intrusion Detection Systems

1. 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.



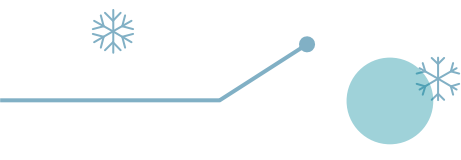
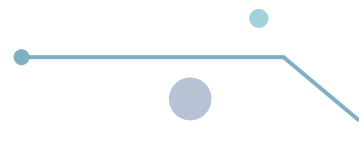


Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage. Intrusion detection systems can also perform the following actions:

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



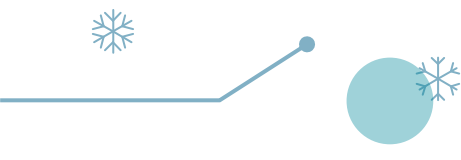
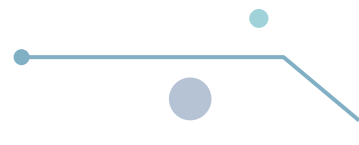
I.T. Act

1. Salient Features of I.T. Act
 2. The salient features of the I.T. Act are as follows:
 3. Digital signature has been replaced with electronic signature to make it a more technology neutral act.
 4. It elaborates on offenses, penalties, and breaches.
 5. It outlines the Justice Dispensation Systems for cyber-crimes.
 6. 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

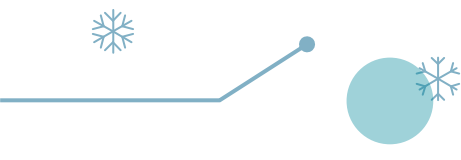
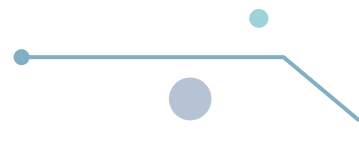
1. The following points define the scheme of the I.T. Act:
 2. I.T. Act 2000 deals with the amendments to the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934 were deleted.
 3. The Act is embedded with two schedules. The 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

1. Following are the documents or transactions to which the Act shall not apply:
2. Negotiable Instrument (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
3. A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
4. A trust as defined in section 3 of the Indian Trusts Act, 1882;
5. A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;
6. Any contract for the sale or conveyance of immovable property or any interest in such property;
7. Any such class of documents or transactions as may be notified by the Central Government.




Amendments Brought in the I.T. Act

1. The I.T. Act has brought amendment in four statutes vide section 91-94. These changes have been provided in schedule 1-4.
 2. 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.
 3. 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.*

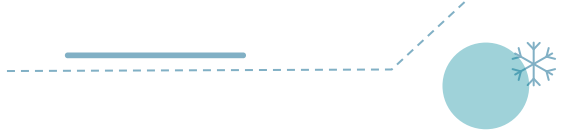
• The fourth schedule amends the Reserve Bank of India Act. *It pertains to the regulation of fund transfer through electronic means between the banks or between the banks and other financial institution.*



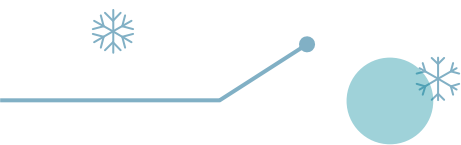
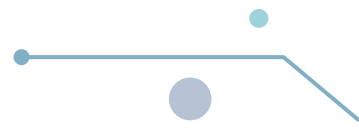


Intermediary Liability

1. 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.
- 
- 

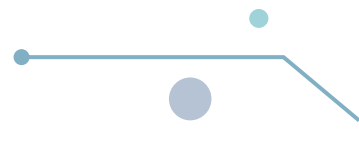


According to the above mentioned definition, it includes the following:

1. Telecom service providers
 2. Network service providers
 3. Internet service providers
 4. Web-hosting service providers
 5. Search engines
 6. Online payment sites
 7. Online auction sites
 8. Online market places and cyber cafes
- 
- 



Highlights of the Amended Act

1. The newly amended act came with following highlights:
 - a. It stresses on privacy issues and highlights information security.
 - b. It elaborates Digital Signature.
 - c. It clarifies rational security practices for corporate.
 - d. It focuses on the role of Intermediaries.
 - e. New faces of Cyber Crime were added.
- 
- 



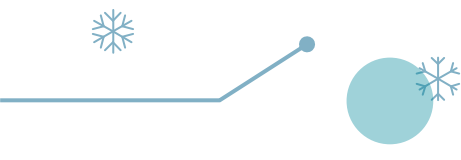
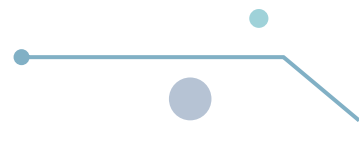
Signatures

1. Digital Signature
2. 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



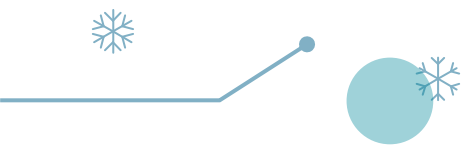
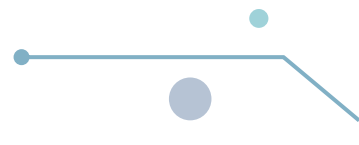


Electronic Signature

1. An electronic signature or e-signature, indicates either that a person who demands to have created a message is the one who created it.
 2. 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.
- 
- 





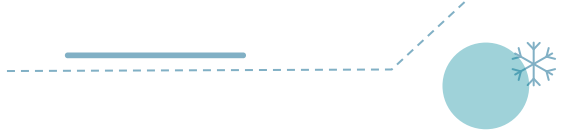
Digital Signature to Electronic Signature

1. 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.
- 
- 

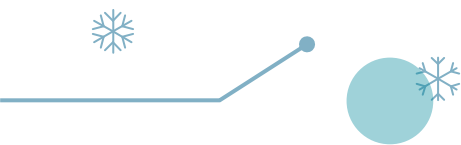
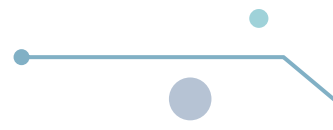


According to the **United Nations Commission on International Trade Law (UNCITRAL)**, **electronic authentication and signature methods may be classified into** the following categories:

- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
 - Those based 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
- 
- 



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

1. Digital Signature within a public key infrastructure (PKI)
 2. Biometric Device
 3. PINs
 4. Passwords
 5. Scanned handwritten signature
 6. Signature by Digital Pen
 7. Clickable "OK" or "I Accept" or "I Agree" click boxes
- 
- 



Offence and Penalties

1. 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.
 2. The law defines the offenses in a detailed manner along with the penalties for each category of offence.
- 
- 

Offences

1. 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.
2. Cyber-crime usually includes the following:
 - a. Unauthorized access of the computers
 - b. Data diddling
 - c. Virus/worms attack
 - d. Theft of computer system
 - e. Hacking
 - f. 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.

Compounding of Offences

1. 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:
 - i. 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.
- 