Module 5 (9 Hours)	**Cyber Security:** Fundamentals of Security, terminologies, CIA Triad, computer security policies,types of cyber crime,cuber security initiatives in India, Cyber laws.

Fundamentals of Security

In the context of cybersecurity and information technology, security refers to a broad range of procedures and ideas intended to shield assets such as networks, systems, and data from different types of attacks and weaknesses. The following are some essential ideas and security tenets:

1. Confidentiality: This guarantees that information is only available to those with the necessary authorizations. Secure communication routes, access controls, and encryption are frequently used to accomplish this.

2. Integrity: Integrity guarantees the accuracy and reliability of data. It entails guarding against unwanted changes to data and confirming its accuracy with techniques like digital signatures and checksums.

3. Availability: The ability to obtain information and services when required. Redundancy, backup systems, and proactive monitoring are used to do this in order to minimise and avoid downtime.

4. Authentication: This process confirms that entities, systems, or users seeking to access resources are who they say they are. Passwords, fingerprints, and multi-factor authentication (MFA) are common techniques.

5. Authorization: An authenticated user or system's access to certain resources or actions is determined by authorization. Common authorization systems include role-based access control (RBAC) and access control lists.

6. Encryption: Data is encrypted and then transformed into a secure format that can only be unlocked with the right decryption key. Safeguarding data when it's in transit and at rest is imperative.

7. Firewalls: These network security tools filter and regulate data coming into and going out of a network. They can be set up according to specified rules to either permit or prohibit traffic.

8. Intrusion Detection and Prevention Systems (IDS/IPS): While IPS can actively block or prevent suspicious behaviour, IDS watches network traffic for indications of it. They support the process of locating and handling security incidents.

9. Vulnerability management: Preventing security breaches in a proactive manner involves locating and fixing software and system vulnerabilities. Patch management and routine scanning are crucial elements.

10. Security Policies: An organization's security practices are governed by a set of security policies and procedures that specify permissible use, incident response, and other crucial security criteria.

11. Security Awareness Training: A major security risk is human error. Employees who get regular training and awareness programmes are better able to identify security issues and take appropriate action.

12. Incident Response Plan: It's critical to have a clear plan in place for handling security-related problems. It provides instructions on what to do in the event of a breach or security incident, reducing damage and recovery time.

13. Security Risk Assessment: By identifying and prioritising security threats, periodic risk assessments help organisations deploy resources more wisely.

14. Physical Security: An organization's physical assets, such as servers and data centres, are safeguarded by physical security measures like access controls, surveillance, and environmental controls.

15. corporate Continuity and Disaster Recovery: To guarantee uninterrupted availability, plans for carrying on with corporate activities in the event of natural or man-made disasters are crucial.

16. Compliance: Organisations are required to abide by regulatory obligations in several industries. Since breaking these rules can have negative financial and legal repercussions, complying with them is essential to security.

17. Security Monitoring and Logging: To identify and look into security problems, it is essential to keep a close eye on systems and networks and to log every occurrence in great detail.

18. The Least Privilege Principle states that systems and users should only be given the minimal amount of access necessary to complete their jobs. This lessens the possible harm caused by a security breech.

19. Zero Trust Security Model: Even for entities that are part of the network, trust is never taken for granted and is constantly confirmed under a Zero Trust model. This strategy lessens the risk of network breaches and insider attacks.

20. Security Updates and Patch Management: To fix known vulnerabilities, it's essential to keep software and systems updated with security patches.

Building a strong and effective security posture is based on these security foundations. The cybersecurity landscape is constantly changing, and organisations need to continuously adapt and evolve their security processes to remain ahead of growing threats.

CIA Triad

A key idea in information security, the CIA Triad stands for three essential values that must be upheld and balanced in order to guarantee the security of data and systems. What the CIA Triad is not:

1. Confidentiality: This refers to the idea that only authorised people, procedures, or systems should have access to certain information. It entails shielding private information from exposure, disclosure, or unwanted access. Data classification, access controls, and encryption are some ways to achieve confidentiality.

2. Integrity: Integrity is concerned with preserving the precision, dependability, and credibility of data and systems. It guarantees that unauthorised parties cannot tamper with or alter data. Organisations utilise methods like digital signatures, checksums, and access controls to prevent unauthorised modifications in order to maintain integrity.

3. Availability: Availability guarantees that information and services are continuously and uninterruptedly available when needed. It entails guarding against and lessening disturbances including denial-of-service assaults, hardware malfunctions, and network outages. Plans for disaster recovery, redundancy, and backups are frequently put into practice to ensure availability.

A fundamental framework for comprehending and putting information security measures into practice is provided by the CIA Triad. Establishing a balance between these three concepts can help organisations develop a strong security posture.

• Balancing Act: Striking a balance between these three ideas might be difficult in real life. Strict access controls, for instance, may unintentionally affect availability while enhancing confidentiality. Finding the ideal balance depends on an organization's risk tolerance and unique needs.

• Security Guidelines: The CIA Triad is typically taken into consideration while creating security rules and procedures. They specify how data should be managed to preserve availability, secrecy, and integrity.

• Trade-offs: There may be occasions when security precautions need trade-offs. For instance, enhancing security to safeguard privacy could result in less usability or greater complexity. For organisations to effectively accomplish their security goals, these trade-offs must be evaluated and managed.

• Evolution: Although the CIA Triad is a fundamental idea, the security environment is always changing. Additional tactics or principles may be needed to counter new dangers and difficulties. For example, the old CIA Triad may need to be supplemented with principles like accountability, non-repudiation, and authenticity.

To sum up, the CIA Triad provides a basic framework for considering and executing information security. It offers a clear method for comprehending the main goals of protecting data and

systems inside a company and is necessary for efficiently planning, carrying out, and overseeing security actions.

Computer Security Policies

The best practices, regulations, and recommendations for maintaining the security and integrity of computer systems and data inside an organisation are found in computer security policies, which are crucial documents. The foundation for overseeing and preserving information security is defined in part by these policies. Typical forms of computer security policy include the following:

1. Acceptable Use Policy (AUP): An AUP describes the permissible and forbidden uses for staff members of a company's networks, computers, and internet access. Typically, it deals with matters like using corporate resources for personal gain, having access to improper content, and using social media.

2. Password Policy: This policy establishes guidelines for the creation and maintenance of passwords, including standards for their length, complexity, expiration, and regularity of changes. Its goal is to stop illegal access brought on by shoddy or stolen passwords.

3. Access Control Policy: Policies for giving, rescinding, and controlling user access to different systems and resources are outlined in access control policies. Access request procedures, role-based access control, and the least privilege principle are frequently included in this policy.

4. Data Classification and Handling Policy: This policy specifies the proper security measures for each type of data and divides it into groups according to sensitivity. It guarantees that more protection is given to sensitive data.

5. Incident Response Policy: In the event of a security incident or breach, an incident response policy describes the actions and protocols that must be taken. It facilitates excellent damage reduction and recovery from security incidents.

6. Network Security Policy: This policy outlines the guidelines and recommended procedures for safeguarding the network infrastructure of a company. It might provide instructions for setting up firewalls, segmenting networks, and granting remote access.

7. Remote Access Policy: Policies for remote access to an organization's network and systems outline the conditions and security precautions that must be followed by authorised staff members and employees. It addresses topics including safe authentication and the use of VPNs.

8. Bring Your Own Device (BYOD) Policy: A BYOD policy describes the guidelines for connecting personal devices to the corporate network, including security precautions and data protection standards, as more employees utilise their own devices for work.

9. Software and Patch Management Policy: To keep systems safe and current, this policy controls the installation and upgrading of software and patches.

10. Physical Security Policy: The goal of physical security policy is to protect an organization's physical assets, like server rooms and data centres. They deal with things like environmental controls, surveillance, and access restrictions.

11. User Training and Awareness Policy: To assist staff in identifying and successfully addressing security issues, this policy promotes continuous security training and awareness initiatives.

12. Vendor and Third-Party Security Policy: This policy describes the security standards and expectations for partners that deal with outside vendors or third parties to safeguard the company's information and systems.

13. Data Retention and Destruction Policy: This policy lays forth standards for the amount of time that data should be kept on hand as well as safe disposal techniques for data that is no longer required.

14. Encryption Policy: To safeguard data while it's in transit and at rest, an encryption policy establishes the circumstances and methods for using encryption.

15. Compliance Policy: This document describes how an organisation plans to adhere to applicable laws, rules, and industry standards as well as the procedures for doing so.

To keep the organization's information security efficient and in line with its objectives and mandates, computer security policies should be routinely reviewed, updated, and shared with all staff members.

TYPES OF CYBER CRIME

The term "cybercrime" describes illegal activity involving computers, networks, and digital technology. These crimes can include those with financial motivations as well as those with malicious intent, theft of private data, or interference with vital systems. These are a few prevalent categories of cybercrime:

1. Hacking: To obtain control, steal information, or interfere with operations, hackers gain unauthorised access to computer systems or networks. Hackers can breach security by using a variety of methods or by taking advantage of flaws.

2. Malware: A broad category of software intended to harm, interfere with, or obtain unauthorised access to computer systems is referred to as malware, short for malicious software. This group includes ransomware, spyware, Trojan horses, worms, and viruses.

3. Phishing: Phishing is a kind of social engineering assault in which online fraudsters utilise phoney emails, texts, or websites to deceive people into disclosing private information, such credit card numbers or passwords.

4. Identity Theft: To perpetrate fraud, open false accounts, or impersonate victims for financial gain, cybercriminals steal personal and financial information.

5. Distributed Denial of Service (DDoS) Attacks: DDoS attacks include flooding a target network or server with so much traffic that it becomes unreachable. Attackers plan these attacks using botnets or other tools.

6. Cyber Extortion: If a ransom is not paid, thieves will either encrypt data, start DDoS attacks, or leak confidential information. Attacks using ransomware are a frequent kind of cyber-extortion.

7. Data Breaches: These occur when private information is exposed to unauthorised parties, frequently leading to the theft of financial and personal data. These hacking incidents may be the consequence of inadvertent or intentional hacking.

8. Internet Scams and Fraud: This category covers a broad range of internet scams in which perpetrators trick victims into parting with money or commodities, including advance fee fraud, lottery scams, and online auction scams.

9. Cyberbullying and Online Harassment: Cyberbullying is the practice of harassing, threatening, or intimidating others online, usually via social media or online chats.

10. Child exploitation is the term for the production, ownership, and dissemination of obscene material featuring children, frequently via the internet. This kind of cybercrime is actively opposed by law enforcement.

11. Insider Threats: These are situations in which employees of a company abuse their access rights in order to steal information, compromise systems, or conduct fraudulent activities.

12. Industrial Espionage: To obtain a financial advantage or a competitive edge, cybercriminals use industrial espionage to steal trade secrets, intellectual property, and private information from enterprises.

13. Cyber Warfare: For political, economic, or geopolitical objectives, nation-states and state-sponsored organisations wage cyberwar on the vital infrastructure, governmental institutions, and military systems of other nations.

14. Cryptojacking: Cryptojacking is the illegal mining of cryptocurrencies without the knowledge or agreement of an individual or organisation using their computational resources.

15. Carding: Carding is a type of credit card fraud in which unapproved online or offline cash withdrawals or purchases are made using credit card information that has been stolen.

16. SIM Card Swapping: To intercept calls, texts, and two-factor authentication codes, criminals use social engineering strategies to persuade cell providers to switch a victim's phone number to a new SIM card.

It is noteworthy that cybercrime is a dynamic and diverse domain, with novel forms of cyberthreats and attacks appearing on a frequent basis. In order to reduce the dangers connected to various kinds of cybercrime, user awareness and cybersecurity measures are essential.

CYBER SECURITY INITIATIVES IN INDIA

India has worked hard to improve cybersecurity through a number of industry and government-level programmes and organisations. Among India's major cybersecurity initiatives are:

1. National Cyber Security Policy (NCSP): Created by the Indian government in 2013, the NCSP offers a thorough framework for defending sensitive data and vital infrastructure against online attacks. It provides tactics for bolstering the legal system, advancing cybersecurity research and development, and improving cybersecurity.

2. Indian Computer Emergency Response Team (CERT-In): CERT-In is the national organisation in charge of handling cybersecurity issues and providing mitigation. In order to handle cyber risks and vulnerabilities, it offers both proactive and reactive support.

3. National Critical Information Infrastructure Protection Centre (NCIIPC): NCIIPC works to defend government agencies, financial institutions, transportation networks, and other vital information infrastructure against cyberattacks. It collaborates with many industries to improve cybersecurity.

4. Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre): This programme attempts to assist individuals and groups in cleaning malware-infected equipment and defending against online threats by offering free tools and antivirus solutions.

5. Indian Cyber Crime Coordination Centre (I4C): I4C was founded to facilitate information sharing between law enforcement agencies, coordinate investigations into cybercrimes, and improve the capacity to effectively combat cybercrimes.

6. Digital India Initiative: This programme promotes the usage of digital services and technology. It encourages the adoption of safe and secure online conduct, such as protecting personal information and transactions.

7. Cyber Surakshit Bharat: Through training and awareness campaigns, this initiative—which was started in association with the Data Security Council of India (DSCI)—aims to improve cybersecurity knowledge and capabilities across a range of industries.

8. Information Sharing and Analysis Centres (ISACs): To increase cybersecurity resilience, a number of ISACs have been established to promote information sharing and cooperation among stakeholders in particular industries, such as banking, telecommunications, and power.

9. National Digital Crime Resource and Training Centre (NDCRTC): NDCRTC was founded to offer cybersecurity and digital forensics resources, research, and training.

10. Cybersecurity Awareness and Capacity Building Programmes: To inform people and organisations about the best practices for cybersecurity, a number of public and private organisations in India run awareness campaigns and capacity-building initiatives.

11. Industry Collaboration: To improve cybersecurity, the Indian government works with industry associations and the private sector. This covers collaboration with IT firms and public-private partnerships.

Cybersecurity research and development: The establishment of cybersecurity research centres and the provision of financing for research projects are examples of initiatives that foster innovation in the field.

These programmes seek to improve India's cybersecurity framework, safeguard vital resources, and increase public, corporate, and governmental understanding of the value of cybersecurity. Given the growth of India's digital economy and the need to guard against cyberthreats and vulnerabilities, cybersecurity is still a top priority.

CYBER LAWS

Cyber laws are legal rules and regulations that regulate activities and issues linked to the use of the internet, computer systems, data, and digital technology. They are often referred to as cybersecurity laws or internet laws. These laws cover a wide range of topics related to cyberspace, such as cybercrimes, data protection, intellectual property, and online privacy. Here are some typical classifications and illustrations of cyber laws:

1. Privacy and Data Protection Laws:

• GDPR, or the General Data Protection Regulation: The GDPR gives data subjects rights over their data and governs how personal data is collected, processed, and stored within the European Union.

• California Consumer Privacy Act (CCPA): This US law gives Californians control over their personal information and places restrictions on how companies can use and disclose that information.

2. Cybercrime laws include the Computer Fraud and Abuse Act (CFAA), which covers data theft, unauthorised access to computer systems, and other cybercrimes in the US.

• Information Technology Act, 2000 (India): Among other things, the Act covers data protection, electronic signatures, and cybercrimes.

3. Intellectual Property Laws:

• The Digital Millennium Copyright Act (DMCA): This law, which is applicable in the United States, safeguards copyrights in digital environments and gives copyright holders a way to ask for the removal of information that violates their rights.

• World Intellectual Property Organisation (WIPO) Treaties: Global guidelines for the protection of intellectual property online are established by international treaties such as the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.

4. Electronic Transactions and E-Signature Laws: In the US, the Uniform Electronic Transactions Act (UETA) establishes the legal foundation for electronic records and signatures.

• eIDAS law: This European Union law creates a legal foundation for trust services and electronic identification for online transactions.

5. Cybersecurity Laws: • The National Institute of Standards and Technology (NIST) Cybersecurity Framework: Although not legally binding, it offers recommendations for improving cybersecurity procedures across a range of institutions.

• Cybersecurity Information Sharing Acts (CISA): US CISA legislation promote the exchange of cybersecurity threat data between public and private sector organisations.

6. Laws Against Online Harassment and Cyberbullying: Provisions against online harassment, cyberbullying, and stalking are found in a number of nations' legal frameworks, such as those in the United States, the United Kingdom, and India.

7. Digital Consumer Protection legislation: Various nations have enacted legislation to shield their citizens from online fraud, false advertising, and scams.

8. Regulation of Telecommunications and the Internet: These laws control the availability of internet services and cover topics like net neutrality, data retention, and authorised interceptions.

9. National and International Cybersecurity Strategies: To address cybersecurity issues at the national level, governments create national cybersecurity strategies. International collaboration in the fight against cybercrime is facilitated by organisations and accords such as the Budapest Convention on Cybercrime.

10. Cross-Border Data movement Laws: Certain nations' data protection laws prohibit the movement of personal information across borders unless a number of requirements or security measures are satisfied.

These rules are essential for upholding the integrity and security of the digital environment, safeguarding people's and organisations' rights and privacy, and defining acceptable conduct and activities online. However, because national borders are not respected by the internet, the enforcement and harmonization of cyber laws across different jurisdictions remain complex and evolving challenges.