Cybersecurity Policy Documentation

UNIT 3

Topics in Unit 3

- Cybersecurity policy of Government of India
- Cybersecurity policies of an organization
- Reporting and Communication
- Importance of incident reporting
- Creating incident reports
- Communicating with stakeholders
- Legal and ethical considerations in reporting

National Cyber Security Policy -2013

- **Vision**
  - To build a secure and resilient cyberspace for citizens, businesses and Government
- **Mission**
  - To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

Objectives

- Create Secure Cyber Ecosystem:
  - Build trust in IT systems and online transactions
  - Boost IT adoption across all economic sectors
- Assurance Framework:
  - Design security policies
  - Promote compliance with global security standards
- Strengthen Regulatory Framework:
  - Ensure a secure cyberspace ecosystem

Objectives

- 24x7 Threat Mechanisms:
  - Gather strategic information on information and communication technology (ICT) threats
  - Develop response, resolution, and crisis management scenarios
- Protect Critical Infrastructure:
  - Operate a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC)
  - Mandate security practices for information resources
- Develop Indigenous Security Technologies:
  - Conduct research and pilot development
  - Deploy secure ICT products for national security

Objectives

- Improve ICT Product Security:
  - Establish testing and validation infrastructure
- Train Cybersecurity Professionals:
  - Create a workforce of 500,000 skilled professionals in the next 5 years
- Fiscal Benefits for Businesses:
  - Provide incentives for adopting standard security practices
- Protect Information:
  - Safeguard privacy and reduce economic losses from cybercrime

Objectives

- Enhance Law Enforcement:
  - Improve prevention, investigation, and prosecution of cybercrime
- Promote Cybersecurity Culture:
  - Foster responsible behavior through communication and promotion
- Develop Public-Private Partnerships:
  - Enhance security through technical and operational cooperation
- Enhance Global Cooperation:
  - Promote shared understanding and leverage relationships for cybersecurity

Strategies: Creating a secure cyber ecosystem

- **National Nodal Agency:** Designate a central agency to coordinate all cybersecurity matters in the country with clearly defined roles and responsibilities.
- **Chief Information Security Officer (CISO):** Encourage all organizations, public and private, to appoint a senior management member as CISO to lead cybersecurity efforts.
- **Information Security Policies:** Promote the development and integration of cybersecurity policies aligned with business plans and international best practices.
- **Cybersecurity Budgets:** Ensure organizations allocate a specific budget for cybersecurity initiatives and emergency response to cyber incidents.

Strategies: Creating a secure cyber ecosystem

- **Fiscal Incentives:** Provide financial schemes and incentives to encourage organizations to strengthen and upgrade cybersecurity infrastructure.
- **Incident Prevention:** Promote incentives for technology development, cybersecurity compliance, and proactive actions to prevent cyber incidents.
- **Incident Response Mechanism:** Establish frameworks for sharing cybersecurity threat information and ensuring coordinated response and restoration efforts.
- **Trustworthy ICT Procurement:** Encourage organizations to adopt secure procurement guidelines and prioritize indigenously manufactured ICT products with cybersecurity considerations.

Strategies: Creating an assurance framework

- **Promote Best Practices**: Enhance cybersecurity by adopting global information security and compliance standards.
- **Build Compliance Infrastructure**: Establish systems for assessing and certifying compliance to cybersecurity standards (e.g., ISO 27001, system audits, penetration testing).
- **Implement Risk Management**: Integrate global security best practices in risk assessment, continuity, and crisis management in government and critical sectors.
- **Classify Infrastructure**: Identify and classify information infrastructure based on risk to ensure proper security measures.

Strategies: Creating an assurance framework

- **Secure Development**: Encourage secure application and software development following global best practices.
- **Create Assessment Framework**: Develop a framework for regular compliance verification with cybersecurity standards.
- **Evaluate Security Measures**: Regularly test and assess the effectiveness of technical and operational security controls in IT systems and networks.

Strategies : Encouraging Open Standards

- **Encourage Open Standards**: Promote interoperability and data exchange among various products or services.
- **Government-Private Consortium**: Enhance availability of certified IT products using open standards through collaboration between the government and private sector.

Examples of IT Products & Initiatives

- **Cyber Swachhta Kendra (Botnet Cleaning & Malware Analysis Centre)**
  - **Collaboration: Government (MeitY, CERT-In) + Private cybersecurity firms**
  - **Product: Free cybersecurity tools like USB Pratirodh, Browser JSGuard, and AppSamvid for malware protection.**
- **e-Governance Solutions (e-Pramaan, DigiLocker, eSign)**
  - **Collaboration:** Government (MeitY, NIC) + Private IT firms
  - **Product:** Secure authentication and document management solutions following open security standards.

Examples of IT Products & Initiatives

- **Data Localization & Cloud Services (MeghRaj Cloud)**
  - **Collaboration:** Government (MeitY) + Private Cloud Service Providers (CSPs) like TCS, Infosys, and AWS India
  - **Product:** Government cloud computing framework ensuring security and compliance with open cloud standards.
- **Indigenous Operating System (BOSS Linux)**
  - **Collaboration:** CDAC (Government) + Open-source Community + Indian IT companies
  - **Product:** Bharat Operating System Solutions (BOSS), a secure OS for government and public sector use.

Strategies : Strengthening the Regulatory framework

- **Dynamic Legal Framework:** Regularly update laws to address cybersecurity challenges (cloud computing, mobile computing, encryption, social media) and align with global standards.
- **Security Audits & Evaluations:** Mandate periodic audits to assess the effectiveness of cybersecurity measures in compliance with regulations.
- **Regulatory Awareness:** Promote awareness and education about cybersecurity laws and compliance requirements.

Examples

- Dynamic Legal Framework
  - **DPDP Act, 2023:** Addresses cybersecurity challenges like cloud computing, encryption, and social media, aligning with global data protection standards.
  - **Draft DPDP Rules (2025):** Proposes data localization and parental consent for minors on social media, enhancing data security.
- Security Audits & Evaluations
  - **RBI Directive (2025):** Mandates stronger cybersecurity measures and regular audits in banks to prevent digital fraud.
- Regulatory Awareness
  - **CCI Actions (2024):** Enforced data-sharing restrictions and fines on tech companies, increasing compliance awareness.

Strategies: Security Threat Management

- **National Cyber Threat Monitoring:** Establish systems for real-time threat detection and information sharing.
- **24x7 CERT-In Operations:** CERT-In acts as the national nodal agency for cyber emergency response and crisis management.
- **Sectoral CERTs:** Operationalize industry-specific CERTs for rapid response and coordination.
- **Cyber Crisis Management Plan:** Implement a structured response for cyber incidents affecting critical national infrastructure and public safety.
- **Cybersecurity Drills & Exercises:** Conduct regular national and sectoral drills to assess preparedness and response effectiveness.

Examples of Sectoral CERTs in India

- **CERT-Fin (Financial Sector)**
  - **Sector:** Banking, financial services, and insurance (BFSI)
  - **Objective:** Protect financial institutions from cyber threats and fraud
  - **Managed by:** Reserve Bank of India (RBI)
- **CERT-POWER (Energy Sector)**
  - **Sector:** Power and electricity infrastructure
  - **Objective:** Secure critical power grids and energy networks
  - **Managed by:** Ministry of Power

Examples of Sectoral CERTs in India

- **CERT-Health (Healthcare Sector)**
  - **Sector:** Hospitals, medical research, pharmaceuticals
  - **Objective:** Safeguard patient data, medical records, and healthcare IT systems
  - **Managed by:** Ministry of Health & Family Welfare
- **CERT-Telecom (Telecommunication Sector)**
  - **Sector:** Telecom operators, ISPs, mobile networks
  - **Objective:** Secure communication networks and prevent cyberattacks on telecom infrastructure
  - **Managed by:** Department of Telecommunications (DoT)

Examples of Sectoral CERTs in India

- **CERT-In Rail (Railways Sector)**
  - **Sector:** Indian Railways and metro networks
  - **Objective:** Protect railway operations from cyber threats and ensure safe digital transactions
  - **Managed by:** Ministry of Railways
- **CERT-Defence (Defense Sector)**
  - **Sector:** Military, defense research, strategic communication systems
  - **Objective:** Protect national security assets from cyber espionage and attacks
  - **Managed by:** Ministry of Defence

Strategies: Securing E-Governance services

- **Secure e-Governance:** Implement global security best practices and crisis management plans to reduce risks.
- **Public Key Infrastructure (PKI):** Promote PKI for secure government communication and transactions.
- **Expert Involvement:** Engage cybersecurity professionals to ensure compliance with security standards.

Protection and resilience of Critical Information Infrastructure

- **Critical Infrastructure Protection:** Develop security plans for protecting vital IT systems and ensure secure data flow.
- **24x7 NCIIPC Operations:** NCIIPC functions as the national nodal agency for securing critical infrastructure.
- **Risk Assessment & Protection:** Identify, prioritize, and safeguard key infrastructure from cyber threats.
- **Global Security Standards:** Mandate best practices, business continuity, and cyber crisis management for critical sectors.

Protection and resilience of Critical Information Infrastructure

- **Certified IT Products:** Promote the use of validated and secure IT solutions.
- **Security Audits:** Conduct periodic security assessments for critical infrastructure.
- **Certification for Security Roles:** Require certification for professionals managing critical IT infrastructure.
- **Secure Software Development:** Enforce global best practices for secure application development.

Promotion of Research & Development in cyber security

- **Cybersecurity R&D:** Focus on short, medium, and long-term security advancements.
- **Indigenous Security Solutions:** Develop cost-effective, customized cybersecurity products for domestic and global markets.
- **Commercialization of R&D:** Convert research outputs into market-ready cybersecurity products and services.
- **Centres of Excellence:** Establish specialized research hubs for strategic cybersecurity areas.
- **Industry-Academia Collaboration:** Partner with businesses and universities for advanced cybersecurity research.

Reducing supply chain risks

- **IT Security Testing:** Establish facilities for product evaluation and compliance with global standards.
- **Secure Supply Chain:** Collaborate with vendors to enhance security across the IT supply chain.
- **Risk Awareness:** Educate entities on threats, vulnerabilities, and security risks in IT procurement.

Human Resource Development

- **Cybersecurity Education & Training:** Develop programs to build national cybersecurity skills.
- **Training Infrastructure:** Set up nationwide cybersecurity training centers through public-private partnerships.
- **Cybersecurity Labs:** Create concept labs for awareness and hands-on skill development.
- **Law Enforcement Training:** Strengthen cybersecurity capacity for law enforcement agencies.

Creating Cyber Security Awareness

- **National Cyber Awareness Program:** Promote cybersecurity education across the country.
- **Public Awareness Campaigns:** Use media to educate citizens on cyber threats and safety.
- **Workshops & Certifications:** Organize training sessions to enhance cybersecurity skills.

Developing effective Public Private Partnerships

- **Cybersecurity Collaboration:** Partner with stakeholders to tackle cyber threats and protect critical infrastructure.
- **Engagement Models:** Develop frameworks for effective cooperation.
- **Cybersecurity Think Tank:** Establish a policy advisory group for discussions and strategy.

Information sharing and cooperation

- **International Cybersecurity Partnerships:** Strengthen global cooperation with other countries.
- **Security & Law Enforcement Collaboration:** Enhance coordination among national and global security agencies.
- **Industry Dialogue:** Establish mechanisms for system recovery and resilience, including critical infrastructure protection.

- **Prioritized approach for implementation**
  - **Priority-Based Implementation:** Focus on the most critical cybersecurity areas first.

- **Operationalisation of the Policy**
  - **Multi-Level Implementation:** Execute through detailed guidelines at national, sectoral, state, and organizational levels.

Cybersecurity policy of Government of India

CYBERSECURITY POLICIES OF AN ORGANIZATION

Policy Outline

- Purpose
- Scope
- Governance and Risk Management
- Access Control & Identity Management
- Data Protection & Privacy
- Network & Endpoint Security

Policy Outline

- Incident Response & Crisis Management
- Security Awareness & Training
- Third-Party & Vendor Risk Management
- Compliance & Audit Requirements
- Business Continuity & Disaster Recovery (BC/DR)
- Policy Enforcement & Review

Purpose and Scope

- Purpose
  - This policy establishes a cybersecurity framework to protect the organization's digital assets, comply with Indian cybersecurity laws, and safeguard sensitive data from cyber threats.
- Scope
  - This policy applies to all employees, contractors, vendors, and third parties accessing organizational IT resources, data, and networks.
  - This policy applies to all employees, contractors, vendors, and third parties accessing the organization’s IT infrastructure, including on-premises, cloud, and hybrid environments.

Governance and Risk Management

- The organization will implement a risk-based approach to cybersecurity, assessing threats and vulnerabilities regularly.
- A Cybersecurity Governance Board (CGB) will oversee policy enforcement and risk mitigation strategies.
- Security policies will align with industry frameworks such as NIST, ISO 27001, CIS Controls, and regulatory mandates (e.g., GDPR, HIPAA, or CCPA).

Cloud: Governance and Risk Management

- Implement a Cloud Security Governance Framework (CSGF) that aligns with industry standards such as NIST CSF, ISO 27017 (Cloud Security), and CSA Cloud Controls Matrix (CCM).
- Define a Shared Responsibility Model between the organization and the Cloud Service Provider (CSP) (e.g., AWS, Azure, Google Cloud).
- Conduct regular cloud risk assessments to evaluate security risks related to data residency, compliance, and third-party access.

Access Control & Identity Management

- Role-based access control (RBAC) will be enforced based on the principle of least privilege (PoLP).
- Multi-factor authentication (MFA) is required for access to critical systems.
- Regular access reviews will be conducted to eliminate unauthorized or outdated user accounts.

Cloud: Access Control & Identity Management

- Enforce Zero Trust Architecture (ZTA) principles, ensuring continuous authentication and least-privilege access.
- Require Cloud Identity and Access Management (CIAM) solutions, including role-based access control (RBAC) and attribute-based access control (ABAC).
- Implement Just-in-Time (JIT) access provisioning to minimize standing privileges for administrative accounts.

Data Protection & Privacy

- All sensitive data must be classified and protected according to Confidentiality, Integrity, and Availability (CIA) principles.
- Encryption will be applied to data at rest and in transit following industry standards (e.g., AES-256, TLS 1.3).
- Data retention and disposal must comply with legal and regulatory requirements.

Cloud: Data Protection & Privacy

- Encrypt data at rest, in transit, and in use using cloud-native encryption services (e.g., AWS KMS, Azure Key Vault, Google Cloud KMS).
- Apply Data Loss Prevention (DLP) policies to prevent unauthorized sharing of sensitive data across cloud applications.
- Ensure compliance with data residency laws by selecting appropriate cloud regions based on regulatory requirements (e.g., GDPR, CCPA).

Network & Endpoint Security

- Firewalls, IDS/IPS, and secure configurations will be deployed to monitor and restrict network traffic.
- Endpoint Detection & Response (EDR) solutions will be implemented to protect devices from malware, ransomware, and unauthorized access.
- Regular vulnerability assessments and penetration testing will be conducted.

Cloud Security Monitoring & Threat Detection

- Deploy Cloud Security Posture Management (CSPM) tools to continuously monitor misconfigurations and compliance violations.
- Implement Cloud Workload Protection Platforms (CWPP) to secure cloud-based applications and virtual machines.
- Enable Security Information and Event Management (SIEM) integration with cloud-native logs (e.g., AWS CloudTrail, Azure Monitor, Google Cloud Logging).

Incident Response & Crisis Management

- A formal Incident Response Plan (IRP) will be maintained to address cyber incidents effectively.
- Incident response teams will follow a detect, contain, eradicate, recover, and review methodology.
- Regular tabletop exercises and simulations will ensure preparedness for cyber incidents and business continuity.

Cloud: Incident Response & Crisis Management

- Establish a Cloud Incident Response Plan tailored to cloud-specific threats (e.g., API abuse, account hijacking, supply chain attacks).
- Automate incident detection and response using Security Orchestration, Automation, and Response (SOAR) platforms.
- Develop forensic capabilities for cloud environments, ensuring access to necessary logs and evidence for investigation.

Security Awareness & Training

- All employees must complete mandatory cybersecurity training annually.
- Social engineering and phishing simulations will be conducted periodically.
- A security culture will be fostered through ongoing awareness programs and "report suspicious activity" mechanisms.

Cloud Security Awareness & Training

- Train employees and IT teams on cloud security threats, such as misconfigured storage (e.g., open S3 buckets), container security, and API security.
- Conduct phishing and social engineering simulations tailored to cloud-based email and collaboration tools (e.g., Microsoft 365, Google Workspace).
- Establish guidelines for secure SaaS application usage, preventing unauthorized third-party integrations.

Third-Party & Vendor Risk Management

- All third parties must undergo a security assessment before integrating with organizational systems.
- Contracts with vendors must include cybersecurity requirements such as data protection, compliance, and incident response obligations.

Third-Party & Vendor Risk Management

- Require CSP security certifications (e.g., SOC 2, ISO 27001, FedRAMP) before selecting cloud providers.
- Conduct Continuous Security Monitoring (CSM) of third-party cloud services for potential security gaps.
- Define Service Level Agreements (SLAs) with CSPs that include incident response times, data protection commitments, and compliance support.

Compliance & Audit Requirements

- Regular audits will be performed to ensure adherence to cybersecurity policies.
- Compliance assessments will align with regulatory frameworks such as NIST CSF, PCI-DSS, HIPAA, or GDPR based on organizational needs.

Compliance & Audit Requirements

- Maintain Cloud Compliance Mapping, ensuring adherence to industry regulations (e.g., PCI DSS for cloud-based payment systems, HIPAA for healthcare).
- Perform continuous compliance monitoring using Cloud Governance, Risk, and Compliance (Cloud GRC) tools.
- Establish regular cloud security audits to validate CSP compliance with security controls and internal security policies.

Business Continuity & Disaster Recovery (BC/DR)

- A Business Continuity Plan (BCP) will outline procedures for maintaining operations during cyber disruptions.
- Regular data backups will be conducted, stored securely, and tested for recovery.
- A Disaster Recovery Plan (DRP) will be implemented to restore critical systems within defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

Business Continuity & Disaster Recovery (BC/DR) in Cloud

- Implement a Multi-Cloud or Hybrid Cloud Strategy to reduce vendor lock-in and enhance resilience.
- Automate cloud-based backups with defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- Ensure Disaster Recovery as a Service (DRaaS) is in place to restore critical workloads in the event of cloud outages.

Policy Enforcement & Review

- Violations of this policy may result in disciplinary action, including termination or legal consequences.
- The cybersecurity policy will be reviewed and updated annually or as needed based on emerging threats and business changes.

Policy Enforcement & Review

- Define cloud-specific security KPIs, such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) for cloud incidents.
- Conduct frequent policy reviews to adapt to evolving cloud security threats and CSP feature updates.
- Enforce automated security policy compliance checks using Infrastructure as Code (IaC) security scanning tools.

Cybersecurity policies of an organization

CYBERSECURITY POLICIES OF AN ORGANIZATION BASED ON GOI 2013 POLICY

Policy Outline

- Purpose
- Scope
- Organizational Structure for Cybersecurity
- Governance & Compliance
- Access Control & Identity Management
- Data Protection & Privacy
- Network & Endpoint Security

Policy Outline

- Cybersecurity Incident Response
- Employee Awareness & Training
- Vendor & Third-Party Security
- Business Continuity & Disaster Recovery (BC/DR)
- Compliance & Audit Requirements
- Policy Enforcement & Review

Policy Purpose and Scope

- Purpose
  - This policy establishes a cybersecurity framework to protect the organization's digital assets, comply with Indian cybersecurity laws, and safeguard sensitive data from cyber threats.
- Scope
  - This policy applies to all employees, contractors, vendors, and third parties accessing the organization’s IT infrastructure, including on-premises, cloud, and hybrid environments.

Organizational Structure for Cybersecurity

- Cybersecurity Leadership & Governance
  - Chief Information Security Officer (CISO):
  - Leads cybersecurity initiatives and ensures policy enforcement.
  - Reports to senior leadership (CIO/Board of Directors).
  - Ensures compliance with CERT-In, IT Act, DPDP Act, RBI, SEBI guidelines.
- Cyber Security Governance Board (CGB):
  - Oversees cybersecurity policies, risk management, and compliance.
  - Conducts periodic cybersecurity strategy reviews.
- Information Security Committee (ISC):
  - Composed of representatives from IT, legal, HR, and risk management.
  - Assists in policy implementation and security awareness programs.

Governance & Compliance

- The organization will implement a risk-based cybersecurity framework in compliance with:
  - IT Act, 2000 (Amended 2008)
  - National Cyber Security Policy (NCSP) 2013
  - Digital Personal Data Protection (DPDP) Act, 2023
  - CERT-In Cybersecurity Directives, 2022
  - Industry-Specific Guidelines (RBI, SEBI, IRDAI, DoT, NCIIPC, etc.)
- A Cybersecurity Governance Board (CGB) will oversee security policy enforcement and audits.

Access Control & Identity Management

- Implement Role-Based Access Control (RBAC) and Principle of Least Privilege (PoLP).
- Use Multi-Factor Authentication (MFA) for accessing critical systems.
- Conduct periodic access reviews and revoke inactive accounts.

Data Protection & Privacy

- Data Classification Policy: Data will be categorized as Public, Confidential, and Restricted.
- Encryption Standards: Use AES-256 for data at rest and TLS 1.3 for data in transit.
- Data Localization: Adhere to DPDP Act, 2023, ensuring sensitive data storage within Indian data centres (as per RBI & CERT-In rules).
- Data Retention Policy: Define timelines for data storage and secure disposal.

Network & Cloud Security

- Enforce Zero Trust Architecture (ZTA) for access control.
- Deploy firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and Endpoint Detection & Response (EDR).
- Cloud security policies must align with MeitY's Cloud Security Guidelines and include Continuous Security Monitoring (CSM).

Cybersecurity Incident Response

- Follow CERT-In guidelines, ensuring:
  - Mandatory reporting of cyber incidents within 6 hours.
  - Incident Response Plan (IRP) to detect, contain, and recover from cyberattacks.
  - Security Operations Center (SOC) monitoring 24/7.

Employee Awareness & Training

- Conduct mandatory cybersecurity awareness training annually.
- Regular phishing attack simulations and reporting mechanisms.
- Compliance with Cyber Surakshit Bharat awareness programs.

Vendor & Third-Party Security

- Vendors handling sensitive data must comply with ISO 27001, NIST, and RBI guidelines.
- Conduct Third-Party Risk Assessments (TPRA) before onboarding vendors.
- Enforce Data Protection Agreements (DPA) for all third-party integrations.

Business Continuity & Disaster Recovery (BC/DR)

- Maintain a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).
- Conduct quarterly DR drills to test system recovery capabilities.
- Ensure real-time backup mechanisms and compliance with RBI’s data resiliency guidelines.

Compliance & Audit Requirements

- Perform annual cybersecurity audits aligned with CERT-In, RBI, and SEBI requirements.
- Ensure compliance with industry-specific security frameworks (ISO 27001, PCI-DSS, NIST, GDPR, HIPAA).
- Maintain logs for 180 days as per CERT-In compliance.

Threat Intelligence & Cyber Collaboration

- Participate in threat intelligence sharing with:
  - CERT-In (Indian Computer Emergency Response Team)
  - NCIIPC (National Critical Information Infrastructure Protection Centre)
  - National Cyber Coordination Centre (NCCC)
- Subscription to Indian Cyber Threat Exchange Programs and global ISACs (Information Sharing and Analysis Centres).
- Conduct periodic threat assessments using cyber intelligence feeds.

Legal Compliance & Cyber Law Enforcement

- Compliance with Indian IT Act, 2000 (Amended 2008) and DPDP Act, 2023.
- Cyber frauds and insider threats will be reported to:
  - Local Cyber Police & Indian Cyber Crime Coordination Centre (I4C).
  - RBI’s Financial Cyber Fraud Reporting System (for banks & fintech).

Policy Enforcement & Review

- Violations of this policy will lead to disciplinary action, including termination or legal consequences.
- The cybersecurity policy will be reviewed annually and updated based on emerging threats, business needs, and regulatory changes.

Cybersecurity policies of an organization based on GOI 2013 policy

INFORMATION TECHNOLOGY ACT 2000

Key Cybersecurity Laws in India

- IT Act 2000: First cyber law passed by the Indian Parliament, safeguarding e-governance, e-banking, and e-commerce through penalties and sanctions.
- Indian Penal Code 1860 (IPC): Addresses cyber offenses through existing criminal laws.
- Information Technology Rules (IT Rules): Regulate online content and data protection practices.
- Companies Act 2013: Enforces data protection and cybersecurity compliance in corporate governance.
- Cybersecurity Framework (NCFS): Establishes guidelines for secure digital infrastructure.

Information Technology Act 2000

- Primary legislation in India dealing with cybercrime and electronic commerce.
- Formulated to ensure the lawful conduct of digital transactions and the reduction of cyber crimes.
- Basis of the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model).
- It has 94 sections, divided into 13 chapters and 2 schedules
- Signed by the President on 9 May 2000, came into effect on October 17

Objectives of the I T Act 2000

- Enable efficient delivery of government services and facilitate seamless digital transactions for businesses and individuals.
- Establish penalties for cybercrimes like data theft, identity theft, and cyberstalking to ensure a secure cyber environment.
- Develop regulations to monitor cyber activities and oversee electronic communication and commerce.
- Drive the growth of the Indian IT/ITES sector by fostering innovation and entrepreneurship.

Importance of IT Act 2000

- Legal recognition of electronic records has accelerated e-commerce and digital transactions in India.
- Electronic signatures are now legally equivalent to physical ones.
- The Act established the Controller of Certifying Authorities (CCA) to manage and secure digital signatures and certificates.
- Companies must now obtain consumer consent for collecting or using personal information.

Importance of IT Act 2000

- Individuals can claim compensation for damage or misuse of their personal data by unauthorized parties.
- The Act criminalizes cybercrimes such as hacking and spreading viruses.
- It authorized the creation of the Cyber Appellate Tribunal to handle appeals against Adjudicating Officers' decisions.
- Provisions in the Act safeguard critical infrastructures like communication networks and power grids.

Features of the IT Act 2000

- The Act empowers the Central Government to regulate e-commerce and penalize cybercrime effectively.
- It defines intermediary roles and conditions for liability exemption.
- Associated with CERT-In, the nodal agency for cybersecurity and incident response.
- Two amendments address technological advancements, implementation challenges, and anomalies.

Digital Signature Under IT Act 2000

- The IT Act 2000 legally introduced digital signatures for secure and authentic online document submission.
- Mandates the use of digital signatures by companies/LLPs under the MCA21 e-Governance program for document filing.

Electronic Governance Under IT Act 2000

- E-Governance applies legal rules to manage and administer government processes electronically.
- The IT Act 2000 establishes a framework for electronic governance, ensuring transparency, efficiency, and secure digital interactions.
- It enables electronic records and digital signatures to streamline government processes and service delivery.

Electronic Governance Under IT Act 2000

- Section 4: Grants legal recognition to electronic records, equating them with paper-based documents.
- Section 5: Gives digital signatures the same legal status as handwritten signatures, with authentication governed by the Central Government.
- Section 6: Promotes the use of electronic records and digital signatures by government agencies for filing documents, issuing licenses, and handling payments digitally, reducing red tape.
- Section 7: Authorizes the retention of electronic records to meet legal requirements for record-keeping.

IT Act 2000 Sections

- The Information Technology Act 2000 comprises **94 sections** dedicated to regulating electronic exchanges and ensuring secure digital transactions.

Section 43 of IT Act 2000

- Section 43 (Chapter IX): Imposes penalties for unauthorized actions involving computer systems, such as accessing, damaging, or disrupting them without the owner's consent.
- Access information from the system
- Download or copy data with proper authorization
- Introduce virus or other malicious software into the system
- Cause damage to a computer network or database

Section 43 of IT Act 2000

- Prevent an authorized user from accessing the system
- Assist others in breaching the provisions of the law
- Charge someone for services they have not utilized
- Alter or remove information to reduce its value or cause harm
- Steal or mess with the code that makes a computer program work

Section 66 of IT Act 2000

- Punishes actions under Section 43 when carried out with dishonest or fraudulent intent.
- Penalty: Imprisonment of up to 3 years, a fine of up to ₹5 lakh, or both.

Section 66A of IT Act 2000

- Section 66A (Amendment to IT Act 2000): Introduced to address cybercrimes linked to emerging technologies.
  - Penalizes sending offensive or menacing messages via communication services.
  - Punishes the use of communication devices to send false information with intent to cause annoyance, inconvenience, harm, or hatred.
  - Covers sending emails/messages to deceive, mislead, or intentionally annoy recipients.

Section 66B of IT Act 2000

- Prescribes punishment for dishonestly receiving stolen computer resources or communication devices.
- Penalty: Imprisonment of up to 3 years, a fine of up to ₹1 lakh, or both.

Advantages of IT Act 2000

- Before the IT Act 2000, emails and electronic communications lacked legal recognition as evidence in court.
- The Act legally recognizes electronic communications, enabling companies to engage in e-commerce and e-business.
- Legalization of digital signatures has simplified online transactions and identity verification.
- Provides statutory remedies for corporations in cases of unauthorized access or hacking of their systems.

Advantages of IT Act 2000

- Offers monetary compensation to individuals for damages incurred in their computer systems.
- Identifies and penalizes cybercrimes such as hacking, spamming, identity theft, and phishing.
- Permits companies to act as certifying authorities and issue digital certificates.
- Empowers the Indian Government to issue notices online via e-governance.

Information Technology Rules (IT Rules)

- Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009
- Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009
- Information Technology (Guidelines for Cyber Cafe) Rules, 2011
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- Information Technology (Security of Critical Information Infrastructure) Rules, 2018
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

I T (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

- **Authority to Block Content (Section 69A)**
  - Authorizes the **Central Government** to block public access to any information in the interest of:
    - National security
    - Sovereignty and integrity of India
    - Friendly relations with foreign states
    - Public order or prevention of crime
- **Request for Blocking**
  - Requests to block content can come from:
    - Government agencies.
    - Courts.
- **Adjudication Process**
  - A **Designated Officer** reviews requests and recommends actions.
  - Approval from a government committee is required before blocking content.

I T (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009

- **Government Powers (Section 69)**
  - Government agencies can intercept, monitor, or decrypt information in the interest of:
    - National security.
    - Public order.
    - Prevention of crime.
- **Procedure for Interception**
  - Authorized agencies require approval from the Union Home Secretary.
  - Interception orders must specify the duration and scope of monitoring.
- **Periodic Review**
  - A review committee evaluates compliance with these rules.

I T (Guidelines for Cyber Cafe) Rules, 2011

- **User Identification**
  - Cyber cafes must verify and maintain a record of customer identities using valid ID proofs.
- **Data Storage Requirements**
  - Browsing history and logs must be maintained for a minimum of 1 year.
- **Monitoring Obligations**
  - Install CCTV cameras to monitor user activity.

I T (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

- **Definition of Sensitive Personal Data (SPD)**
  - Includes passwords, financial information, health records, biometrics, etc.
  - Organizations must implement "**reasonable security practices**" to protect sensitive data.
- **Consent Requirement**
  - Entities must obtain **explicit consent** before collecting or sharing sensitive data.
  - Data collected should be used only for lawful purposes.

I T (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

- **Privacy Policy Disclosure**
  - Organizations must publish a **clear privacy policy** outlining:
    - Type of data collected.
    - Purpose of data collection.
    - Disclosure practices.
- **Right to Withdraw Consent**
  - Users have the right to withdraw their consent and request deletion of data.
- **Compensation for Negligence**
  - Individuals can claim compensation for data breaches caused by organizational negligence.

I T (Security of Critical Information Infrastructure) Rules, 2018

- **National Critical Information Infrastructure Protection Centre (NCIIPC)**
  - Designated to protect **critical information infrastructure (CII)**.
  - CII includes systems that impact:
    - National security.
    - Public health.
    - Economy.
- **Compliance for CII Providers**
  - Organizations handling CII must:
    - Implement stringent security controls.
    - Report security incidents to NCIIPC.

I T (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

- **Due Diligence for Intermediaries (Section 79)**
  - Platforms such as social media, search engines, and hosting services must follow due diligence while hosting user content.
  - Mandates removal of unlawful content within **36 hours** of receiving government or court orders.
  - Platforms must deploy automated tools to identify and remove offensive content.
- **Grievance Redressal Mechanism**
  - Mandatory appointment of:
    - **Grievance Officer** – To resolve complaints within 15 days.
    - **Chief Compliance Officer** – Ensures platform compliance.
    - **Nodal Contact Person** – Available 24/7 for law enforcement.

I T (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

- **Identification of First Originator (Section 4(2))**
  - Significant Social Media Intermediaries (SSMIs) providing messaging services must enable tracing of the **first originator** of messages related to crimes like national security or child exploitation.
- **Code of Ethics for Digital Media**
  - Applicable to online news publishers, Over-the-Top (OTT) platforms, and digital media.
  - Publishers must adhere to a **three-tier grievance redressal mechanism**:
    - Self-regulation by the publisher.
    - Self-regulation by industry associations.
    - Oversight by an inter-departmental government committee.

Information Technology Act 2000

IMPORTANCE OF INCIDENT REPORTING

Incident Reporting

- **What is Incident Reporting?**
  - Incident reporting is the process of documenting and communicating security breaches, cyber threats, or system failures. It ensures a timely response and mitigation of risks.
- **Types of Incidents:**
  - Cyberattacks (e.g., malware, ransomware, phishing)
  - Data breaches and leaks
  - Unauthorized access and insider threats
  - Compliance violations (e.g., GDPR, HIPAA, PCI-DSS)

Why is Incident Reporting Important?

- **Early Detection & Response**
  - Rapid reporting helps contain threats quickly.
  - Prevents minor incidents from escalating into major crises.
- **Legal & Regulatory Compliance**
  - Regulations such as **GDPR, HIPAA, PCI-DSS** mandate timely reporting.
  - Failure to report can result in severe penalties (e.g., GDPR requires reporting within 72 hours).

Why is Incident Reporting Important?

- **Prevents Financial Losses**
  - Cyber incidents can cause **millions in damages**.
  - Delayed responses lead to **lawsuits, compensation claims, and loss of revenue**.
- **Maintains Reputation & Customer Trust**
  - Transparency builds trust with stakeholders.
- **Enhances Cybersecurity & Incident Response**
  - Helps identify and address vulnerabilities in security systems.
  - Enables better defenses against future attacks.

Best Practices for Effective Incident Reporting

- **Report Immediately:** Follow legal timelines (e.g., **GDPR: 72 hours**).
- **Be Transparent:** Clearly communicate risks and response actions.
- **Document Everything:** Maintain logs for audits and legal protection.
- **Train Employees:** Ensure all staff understand how to report incidents.
- **Follow an Incident Response Plan:** Have a structured approach for handling cyber incidents.

Importance of incident reporting

CREATING INCIDENT REPORTS

Key Elements of an Incident Report

- Title and Summary
  - Concise summary of the incident.
  - Example: “Unauthorized Access Attempt on Web Server.”
- Date and Time Information
  - Time of detection and time of resolution.
  - Use **UTC timestamps** for consistency.

Key Elements of an Incident Report

- Incident Description
  - What happened?
  - How was it discovered?
  - Which systems were affected?
  - Describe the impact and affected assets.
- Root Cause Analysis (RCA)
  - Explain how the incident occurred.
  - Identify vulnerabilities exploited.

Key Elements of an Incident Report

- Containment and Mitigation Steps
  - Describe actions taken to contain the incident.
  - Include temporary and permanent mitigation strategies.
- Investigation Details
  - Timeline of events.
  - Tools and techniques used (e.g., log analysis, forensic tools).

Key Elements of an Incident Report

- Recommendations and Lessons Learned
  - Propose actions to prevent recurrence.
  - Highlight areas for process improvement.
- Signatures and Approvals
  - Ensure accountability by documenting who reviewed and approved the report.

Creating incident reports

COMMUNICATING WITH STAKEHOLDERS

Why Stakeholder Communication Matters

- Purpose of Communication During an Incident
  - Keep stakeholders informed and aligned.
  - Manage expectations and reduce panic.
  - Enable better decision-making.
  - Preserve the organization’s reputation.
- Consequences of Poor Communication:
  - Loss of trust.
  - Legal or regulatory non-compliance.
  - Increased confusion and mismanagement.

Identifying Key Stakeholders

- Internal Stakeholders:
  - Executive Leadership (CISO, CIO, CEO)
  - IT and Security Teams
  - Legal and Compliance Teams
  - Human Resources (for insider threats or policy violations)
  - Public Relations/Communications Team

Identifying Key Stakeholders

- External Stakeholders:
  - Customers/Clients
  - Law Enforcement/Regulatory Bodies
  - Vendors/Third-Party Partners
  - Media (in high-profile incidents)

Communication for Different Stakeholders

- Executives:
  - Focus on business impact, risk, and mitigation.
  - Use high-level summaries and actionable insights.
  - **Example:** “A ransomware incident affected 20% of operations. Containment measures have been implemented, and full system restoration is expected in 12 hours.”
- Technical Teams:
  - Include detailed technical information, timelines, and next steps.
  - Share log analysis, affected systems, and investigation progress.
  - **Example:** “The firewall logs indicate a series of brute-force login attempts from IP 192.168.0.5, triggering a block at 03:45 UTC.”

Communication for Different Stakeholders

- Legal/Compliance Teams:
  - Provide details on regulatory requirements, data exposure, and possible legal implications.
  - **Example:** “A potential data breach may have exposed 5,000 customer records. GDPR notification requirements apply, and a formal report is in preparation.”
- Public/Clients:
  - Be transparent but avoid excessive technical details.
  - Focus on how the organization is addressing the issue.
  - **Example:** “We are investigating an incident affecting some customer accounts. Security measures have been enhanced, and affected users are being contacted.”

Effective Incident Communications

- Situation Overview
  - What happened?
  - When was it discovered?
  - What is the potential impact?
- Response and Current Status
  - What actions have been taken?
  - Is the incident contained or ongoing?

Effective Incident Communications

- Next Steps and Timeline
  - Estimated time for resolution.
  - Any immediate actions required from stakeholders.
- Contact Information
  - Point of contact for further inquiries.

Communicating with stakeholders

DIGITAL PERSONAL DATA PROTECTION ACT 2023

Rights of Data Principals (Individuals):

- **Right to Access:** Individuals have the right to access their personal data.
- **Right to Correction and Erasure:** Individuals can seek correction and erasure of inaccurate or irrelevant data.
- **Right to Revoke Consent:** Individuals can withdraw their consent for data processing at any time.
- **Right to Data Portability:** Individuals have the right to transfer their data to another data fiduciary.
- **Right to Grievance Redressal:** Individuals have the right to seek redressal for data privacy violations.
- **Right to Nominate a Consent Manager:** Individuals can nominate a person to manage their data-related requests on their behalf, or to exercise rights in case of death or incapacity.

Data Fiduciaries and Their Obligations:

- **Definition:**
  - A data fiduciary is any person who determines the purpose and means of processing personal data.
- **Obligations:**
  - Data fiduciaries must ensure data security, maintain data accuracy, and delete data once its purpose is met.
- **Significant Data Fiduciaries (SDFs):**
  - Entities handling large volumes or sensitive data are designated as SDFs and face additional obligations.

Data Fiduciaries and Their Obligations:

- **Data Protection Officer:**
  - SDFs are required to appoint a Data Protection Officer.
- **Data Processing Agreements:**
  - Data fiduciaries must have data processing agreements with third-party processors.
- **Data Protection Impact Assessments:**
  - Periodic Data Protection Impact Assessments are mandatory for Significant Data Fiduciaries.

Consent and Legitimate Use:

- **Explicit Consent:**
  - Personal data can be processed only with the explicit consent of the data principal, unless processing is for a legitimate use or is exempted by the Act.
- **Legitimate Uses:**
  - Data fiduciaries can process data without consent for purposes like performing functions under law, complying with court orders, addressing medical emergencies, or fulfilling employment-related purposes.
- **Consent Management:**
  - The Act emphasizes the importance of clear and transparent consent management mechanisms.

Data Security and Breach Notification:

- **Data Security:**
  - Data fiduciaries are responsible for implementing reasonable security safeguards to protect personal data.
- **Data Breach Notification:**
  - Data fiduciaries must notify the Data Protection Board and data principals of any data breach that compromises the confidentiality, integrity, or availability of personal data.

Data Protection Board:

- **Role:**
  - The Data Protection Board is an independent body responsible for overseeing the implementation of the Act, resolving privacy-related grievances, and imposing penalties for non-compliance.
- **Powers:**
  - The Board has the power to investigate complaints, issue fines, and order organizations to comply with the Act.

Penalties:

- **Financial Penalties:** The Act imposes financial penalties for non-compliance, with penalties ranging from INR 10,000 to INR 250 crore depending on the severity of the breach.
- **No Criminal Penalties:** The Act does not impose criminal penalties for non-compliance.

Communicating with stakeholders

LEGAL AND ETHICAL CONSIDERATIONS IN REPORTING

Key Legal Considerations

- The Digital Personal Data Protection Act, 2023 (DPDP Act)
  - Organizations must notify the **Data Protection Board of India (DPBI)** of a **personal data breach**.
  - Reporting timeline: Notification must be provided **as soon as possible** and within a **reasonable timeframe** after becoming aware of the breach.

Key Legal Considerations

- Information Technology (The Indian Cybersecurity Directions), 2022
- Organizations must report **cybersecurity incidents** to CERT-In within **6 hours** of detecting the incident.
- Types of Reportable Incidents:
  - Unauthorized access of IT systems.
  - Data breaches and exfiltration.
  - Malware and ransomware attacks.
  - Phishing, DDoS, and identity theft.
  - Security breaches affecting cloud services.

Key Legal Considerations

- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules)
  - Organizations handling **sensitive personal data** must report any security breach.
  - Affected individuals must be notified promptly in the event of a breach.
- Types of Sensitive Personal Data:
  - Passwords
  - Financial information
  - Medical records
  - Biometric data

Key Legal Considerations

- General Data Protection Regulation (GDPR - EU):
  - Requires notification within **72 hours** of discovering a breach.
  - Notification to both regulators and affected individuals when applicable.
- California Consumer Privacy Act (CCPA - USA):
  - Mandates disclosure of data breaches affecting California residents.
  - Organizations must notify affected individuals “without unreasonable delay.”

Key Legal Considerations

- Industry-Specific Regulations
- Reserve Bank of India (RBI) Guidelines:
  - **Applicability:** Banks, NBFCs, and payment service providers.
  - **Reporting Timeline:** Security breaches must be reported to RBI within **2 to 6 hours** of detection.
- Insurance Regulatory and Development Authority of India (IRDAI):
  - **Applicability:** Insurance companies.
  - **Incident Reporting:** Must report cybersecurity breaches that impact customer data.
- SEBI (Securities and Exchange Board of India):
  - **Applicability:** Stock exchanges, depositories, and brokers.
  - **Reporting Obligation:** Report cybersecurity incidents impacting critical systems.

Key Legal Considerations

- Industry-Specific Regulations
- Health Insurance Portability and Accountability Act (HIPAA - USA):
  - Requires reporting breaches involving Protected Health Information (PHI).
  - Notifications to the Department of Health and Human Services (HHS) and affected individuals.
- Payment Card Industry Data Security Standard (PCI-DSS):
  - Requires reporting security incidents related to payment card data.

Ethical Considerations

- Accuracy and Integrity
  - Report only verified facts.
  - Avoid exaggerating or downplaying the impact of the incident.
- Timeliness and Transparency
  - Disclose incidents as soon as feasible while ensuring accuracy.
  - Avoid unnecessary delays that could increase harm to affected parties.

Ethical Considerations

- Confidentiality and Privacy
  - Protect sensitive data, even while disclosing necessary information.
  - Anonymize personal information where possible.
- Avoiding Conflict of Interest
  - Ensure decisions made during incident reporting are objective and not influenced by personal or organizational gain.

Ethical Dilemmas in Reporting

- **Scenario 1:** A minor security breach occurs, but disclosing it might lead to public panic.
- **Scenario 2:** A third-party vendor's security lapse affects your organization's clients.
- **Scenario 3:** An insider threat incident is discovered, but the individual is a high-profile executive.

Case Studies

- **British Airways (2018):** Late reporting of a data breach → **£183M fine under GDPR**.
- **Equifax (2017):** Delayed breach reporting → **$700M settlement** + **executives charged with insider trading**.
- **Uber (2016):** Attempted cover-up → **CSO convicted** + **$148M fine**.
- **Yahoo Data Breach (2013-2014):** Failure to disclose breaches led to a $35 million settlement.

Case Studies

- **Maersk (2017):** Prompt response to **NotPetya ransomware attack**, recovered in **10 days**.
- **Norsk Hydro (2019):** Publicly disclosed a ransomware attack, refused to pay ransom, and gained industry respect.