

Week 01 – Lecture 01: Cybersecurity and Privacy

2. Meaning of Cybersecurity

- Protection of **data, systems, and networks** from unauthorized access.
 - Involves **vulnerability management** and **threat prevention**.
 - Goal: Ensure confidentiality, integrity, and availability of information.
-

3. Meaning of Privacy

- Deals with **personal control over data**.
 - Deciding what information to disclose or keep private.
 - Focuses on individual rights and data ownership.
-

4. Relationship Between Cybersecurity and Privacy

- Cybersecurity → Protects systems and data.
 - Privacy → Protects individual information and consent.
 - Both overlap; strong cybersecurity ensures better privacy protection.
-

5. Importance and Relevance

- Cybersecurity is a **current and critical issue**.
 - Affects individuals, organizations, and governments.
 - Managers must be aware of cybersecurity threats and risks.
-

6. Example 1 – Phishing Email Case (IIT Madras)

- Fake email impersonating IITM Director.
 - Suspicious signs:
 - Informal tone (“Can I have a quick moment with you?”).
 - Sent from **Gmail**, not official domain.
 - **Type of attack:** *Spear Phishing* (targeted attack using social engineering).
 - **Lesson:** Always verify sender’s email address and message authenticity.
-

7. Example 2 – Fake SBI PAN Verification Message

- Received text message with fake link to SBI website.
 - Website copied design of real SBI login page.
 - **Lesson:** Always check website URL/domain before entering credentials.
-

8. Common Cyber Threats

1. **Phishing:** Fake emails or messages to steal information.
 2. **Spear Phishing:** Targeted phishing using personal or professional details.
 3. **Ransomware:**
 - Hacker encrypts data and demands money to unlock it.
 - Example:
 - **Kaseya POS attack (2021)** – \$70 million ransom demand.
 - **Chennai Corporation** ransomware attack – refused ransom.
-

9. Example – AIIMS Cyber Attack (2022)

- Five servers hacked; patient data compromised.
 - **Healthcare data = highly sensitive** (embarrassment, misuse, job loss).
 - **HIPAA (U.S. law)** – Protects healthcare data privacy.
-

10. Rising Global Concern

- Cyber attacks impact all sectors: manufacturing, healthcare, government.
 - **91% of organizations** reported at least one cyber incident per year (E&Y).
 - Cybersecurity now a **top priority** for business leaders and CEOs.
-

11. Final Takeaways

- Cybersecurity and privacy are **essential in the digital world**.
- Need for awareness, vigilance, and system updates.
- Everyone must protect personal data and respect privacy.

lecture 02 Key Points on Cyber Security

1. Digital Dependence and Risk

- Modern cars and devices are controlled by computers and connected to the internet.
- Example: Tesla cars get automatic updates online.

- Cyber attacks on connected cars can endanger human lives.
 - Hence, cars are now tested for **cybersecurity** before release.
-

2. Real-World Cyber Attacks

- **Saudi Aramco refinery (2019)** was shut down due to a **cyber attack** using **drones**.
 - Industries like **banking, energy, and manufacturing** depend heavily on IT systems.
 - If systems fail, **entire operations stop**.
-

3. Internet of Things (IoT) Risks

- IoT devices (sensors, controllers) connect to the internet to transmit data.
 - **Any internet-connected device is vulnerable.**
 - Hacked sensors can send wrong data and cause **major damage** in industries.
 - Example: A hacker changing a temperature sensor reading can disrupt the entire process.
-

4. Evolution: From Information Security to Cyber Security

- Earlier: Focus on **data protection** only.
 - Now: Protecting **people, infrastructure, and nations**.
 - Cyber attacks can cause **physical harm** and **loss of life**, not just data theft.
-

5. Famous Cyber Incidents

- **Air India data breach** – exposed passenger information.
 - **Twitter hack** – celebrity accounts like Bill Gates compromised.
 - **TCS website hack** – even IT companies face attacks.
-

6. Cybersecurity Affects All Levels

- **Individuals** – bank frauds, data theft.
 - **Organizations** – ransomware, operational halts.
 - **Governments** – system attacks, data leaks, citizen privacy issues.
 - Governments must ensure **policy, regulation, and public safety**.
-

7. Privacy and Data Protection

- Huge concern due to large-scale data collection (e.g., Aadhaar).
 - **Privacy** and **cybersecurity** are interconnected.
 - Governments must **balance technology growth** with **data safety**.
-

8. Technology's Triple Role in Cyber Security

1. **Source of Threat** – used for attacks (malware, DoS).
 2. **Asset to Protect** – systems, data, and networks.
 3. **Defense Tool** – firewalls, encryption, and protection technologies.
-

9. Growing Cyber Threats

- Cyber attacks are **real and increasing**.
 - More digitalization → more cyber risks.
 - Stopping technology is not an option; **safe use and protection** are essential.
-

10. Key Takeaway

- The **digital world empowers** but also **exposes** us.
- Cybersecurity is a **must** to protect people, systems, and nations.
- Focus should be on **awareness, safety, and responsible technology use**.

Here's your **Lecture 03** neatly converted into **clear, structured key points** 🤝

Lecture 03 – Introduction to Security & Cyber Security

1. Meaning of Security

- **Security** = *State of being safe or feeling secure*.
 - It's both a **physical** and **psychological** sense of safety.
 - Involves protection from threats to:
 - Life and body (individual level)
 - Property and assets (organizational level)
 - Information and systems (digital level)
-

2. Types of Security

- **Physical Security** – Protecting physical assets (e.g., institute gates, security guards).

- **Information Security** – Protecting information assets (data, databases, systems).
 - **Cyber Security** – Broader scope: includes information, systems, people, and infrastructure.
-

3. Security Example (Institution Gate)

- Security ensures only **authorized access** to assets.
 - **Authorized persons** can enter; unauthorized persons are denied.
 - **False positives** (denying access to valid users) and **false negatives** (allowing intruders) can occur.
 - Verification of identity is key in both **physical** and **cyber** security.
-

4. Cyber Security vs. Information Security

Aspect	Information Security	Cyber Security
Scope	Protects <i>data and systems</i>	Protects <i>data + systems + users + infrastructure</i>
Focus	Confidentiality, integrity, availability of data	Safety of digital world including individuals
Example	Prevent data breach in hospital servers	Prevent drone attacks, cyber crimes, user harm
Relation	Subset of cyber security	Superset including information security

5. Origin and Meaning of “Cyber”

- Comes from the Greek word **“Cybernetics”**, meaning *control or steering*.
 - In modern use, **“cyber”** relates to the **internet-connected world** — computers, networks, systems.
 - **Cyber Security** → *Security of the internet-connected world*.
-

6. Correct Usage of the Term “Cyber Security”

- Three forms:
 1. **Cyber security** (two words – European style)
 2. **Cyber-security** (hyphenated – Indian style)
 3. **Cybersecurity** (one word – US style)
- All correct — just be consistent in usage.

7. ITU Definition of Cyber Security (2008)

- Extremely broad — includes:
 - **Tools, policies, concepts, safeguards, guidelines, risk management, training, technologies, best practices.**
 - Covers **everything** related to securing the digital or cyber world.
 - Includes **systems and human users.**
-

8. Scope of Cyber Security

- Encompasses:
 - Systems
 - Networks
 - Software and hardware
 - Data
 - **Users and individuals** (protection from cyber crimes, bullying, online threats)
 - Example: Cyber crimes and bullying are part of **cyber security**, not just **information security**.
-

9. Cyber Security = Information Security + Individuals

- Protects:
 - **Information systems** (data confidentiality)
 - **People** (user safety in digital world)
 - Example: A **drone attack** involves both data breach (information) and physical harm (human safety).
-

10. The CIA Triangle

- Core principles of **Information Security**:
 1. **Confidentiality** – Only authorized users can access data.
 2. **Integrity** – Data remains accurate and unaltered.
 3. **Availability** – Systems and data are accessible when needed.
-

11. Information Security Definition (Whitman & Mattord, 2018)

"Protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information."

12. Perspectives in Cyber Security

- **Technological perspective** – Firewalls, encryption, antivirus, intrusion detection, etc.
 - **Administrative/Managerial perspective** – Policies, governance, risk, compliance, and response planning.
 - The course focuses on **management + technology**, not only the technical side.
-

13. Role of Cryptography

- Ensures **confidentiality** of information transmission.
 - Converts data into an unreadable form for unauthorized users (encryption).
 - **Analogy:** Speaking a language only the intended person understands.
 - Focus in course → *Application* of encryption, not algorithm design.
-

14. Cyber Security: Technology vs. Administration

- Debate: Is cyber security a **technical or administrative** issue?
 - Conclusion: It is **both** – technology acts as a tool, management provides the framework.
 - New trend: "**Zero Trust Systems**" – no trust in humans, rely on strong automated verification.
-

15. Cyber Security as a Multi-Level Issue

- **Technological problem** – firewalls, systems, encryption.
 - **Administrative problem** – management failures, poor controls.
 - **Regulatory problem** – lack of policies or laws (e.g., Data Protection Bill, GDPR).
-

16. Government Role & Data Protection

- Governments create **laws, standards, and regulations** for cyber safety.
- **Examples:**
 - India – Personal Data Protection Bill.
 - EU – **GDPR (General Data Protection Regulation)**.
- Regulations ensure organizations invest in and follow security standards.

17. Cyber Security Management Focus

- Two main planning types:
 1. **Risk Management (Preventive)** – Identify and prevent potential threats.
 2. **Contingency Planning (Reactive)** – Manage damage after incidents occur.
 - Goal: Protect systems and restore them after failure or attack.
-

18. Course Focus and Structure

- Based on **Whitman & Mattord (2018)** textbook – *Information Security*.
- Additional readings & case studies cover **Cyber Security** aspects.
- Course includes:
 - Guest lecture from cybersecurity professional.
 - Case studies (e.g., **Target 2016, Sony 2014** breaches).
 - Discussion of standards: ISO, GRC (Governance, Risk, Compliance).
 - Topics: Confidentiality, Integrity, Availability, Privacy, Policy, Regulation.

19. Course Learning Objectives (CLO)

1. Recognize cyber security from **technological** and **administrative** perspectives.
 2. Understand **foundations and principles** of cyber and information security.
 3. Learn **risk and contingency management**.
 4. Explore **policy, governance, and regulatory frameworks** for cybersecurity.
-

20. Final Takeaways

- **Cyber Security = Technology + Management + Regulation.**
 - Covers protection of **information, systems, and people** in the digital world.
 - Goal: Build a **secure, trustworthy, and resilient cyber ecosystem**.
-