Chapter 2

🔐 Privacy

- A **human right** central to computer ethics.
- About **controlling personal information** and **avoiding intrusion**.
- In the digital world, this is a growing concern due to data collection, storage, and analysis.

💡 Information

- **Definition**: Processed data = *Information* (an **asset**).
- **Compared to physical assets**:
  - No physical form.
  - Easily duplicated/shared.
  - More valuable when combined.
  - Needs media to transmit.

Risks:

- Hacking, piracy, viruses.
- Ownership/control disputes.
- Digital divide between countries.

🛡️ Information Security

- Focuses on **Confidentiality, Integrity, Availability** (CIA Triad).
- Includes:
  - Preventing unauthorized access.
  - Balancing security with usability.

Cybersecurity:

- Expands to **IoT** and **SCADA** systems.

4Rs of Information:

1. Right Information
2. Right People
3. Right Time
4. Right Form

📉 Risk Management

- **Formula**: Risk = Asset Value × Threat × Vulnerability
- **Types**:
  - **Risk Reduction** – apply countermeasures
  - **Risk Acceptance** – low risk, live with it
  - **Risk Transference** – e.g. insurance
  - **Risk Avoidance** – don't engage in risky activity

📏 Security Standards

- Key organizations:
  - ISO/IEC
  - ITU-U
  - ISACA (CISA)
  - ISC^2 (CISSP)
- Covers:
  - Policies
  - Technical/physical protection
  - HR and audit management

👤 Concept of Privacy

- **Personal Information**: Names, ID, biometrics, etc.
- **Privacy** = The right to control your personal data.

Privacy Rights:

1. Freedom from unwanted access
2. Block misuse of info
3. Consent before collection
4. Data accuracy
5. Benefit from your info

Types:

- **Passive**: Right to be left alone
- **Active**: Right to manage and correct your own data

📚 OECD Privacy Principles (8):

1. Collection Limitation
2. Data Quality
3. Purpose Specification
4. Use Limitation
5. Security Safeguards
6. Openness
7. Individual Participation
8. Accountability

💻 Cybercrime & Social Issues

Why it's hard to stop:

- Borderless
- Anonymous actors
- Jurisdiction problems

🔍 Types of Cybercrime

1. Cyber Pornography

- Sharing sexual content online.
- Child pornography is a serious global issue.

2. Cyber Stalking

- Online harassment using emails, forums, etc.

3. Cyber Terrorism

- Using digital tools to threaten infrastructure, security.

4. Hacking

- Unauthorized access to systems.

5. Viruses & Contaminants *(Assignment)*

6. Financial Cybercrime

- Phishing: fake emails
- Vishing: fake calls using VoIP

7. DoS/DDoS Attacks

- Crashes systems by flooding traffic.

8. Data Theft

- Stealing confidential or valuable info.

9. Data Diddling

- Tampering with data before it's stored.

10. Email Bombing / Spamming

11. Email Spoofing

- Faking the sender's identity.

12. Logic Bombs

- Code that activates under specific conditions.

13. Internet Time Theft

- Using someone’s internet account without permission.

14. IP-Related Crimes

- Software piracy
- Domain name misuse
- Copyright violation

📱 Mobile & Wireless Crimes

- Mobile banking fraud
- SMS spoofing
- IMEI reprogramming
- Use of phones in terrorism
- Phreaking (hacking phone systems)

⚖️ Cybercrime Law

- Sets behavior rules for digital environments.
- Protects users, data, and infrastructure.
- Requires:
  - Substantive law (what is a crime)
  - Procedural law (how to investigate)
  - Preventive law (how to avoid it)
- Emphasizes **international cooperation**.

🌎 Legislation Overview

Region	Legislation (%)
Europe	91%
Americas	86%
Asia-Pacific	77%
Africa	72%
LDCs	70%
SIDS	63%