INFORMATION SECURITY

Prof. Suhendro Y. Irianto

28 November 2025

Information security

Safeguarding Data and Digital Assets in a Connected World

Definition of Information Security

- Information security refers to practices that protect data from unauthorized access, misuse, alteration, or destruction.
- Example: Protecting student records from unauthorized access.

The CIA Triad

- Confidentiality: Limit access to authorized users.
- Example: Password-protected documents.

- Integrity: Ensure accuracy of data.
- Example: Tamper protection on academic records.

- Availability: Data accessible when needed.
- Example: Servers running 24/7.

Core Security Principles

- Authentication: Verifying identity.
- Example: Logging in with a password.

- Authorization: Determining access rights.
- Example: Admins can edit data; students cannot.

- Accountability: Tracking user actions.
- Example: System activity logs.

Common Threats

- Malware, phishing, DDoS, insider attacks, password attacks.
- Example: Fake bank emails that trick users.

Real Cyber Attack Scenarios

- Ransomware in hospitals, e-commerce data breaches, government websites attacked.
- Example: WannaCry ransomware attack in 2017.

System Vulnerabilities

- Outdated software, weak passwords, misconfigurations, human error.
- Example: Unpatched computers targeted by malware.

Risk Management

- Identify risks, analyze impact, apply mitigation strategies.
- Example: Using antivirus to reduce malware risk.

Security Controls

- Administrative controls: Policies.
- Example: Strong password policy.

- Technical controls: Firewalls, encryption.
- Example: Firewall blocking suspicious IPs.

- Physical controls: Locks, CCTV.
- Example: Locked server room.

Security Technologies

- Firewalls, IDS/IPS, MFA, encryption, VPN.
- Example: MFA to secure Gmail accounts.

Password & Identity Management

- Use strong passwords, avoid reuse, use password managers, enable MFA.
- Example: 'F0rum@2025!' is stronger than '123456'.

Data Protection Strategies

- Encryption, masking, access control, backups.
- Example: Encrypting student grades stored in the cloud.

Security Policies

- Rules on passwords, data classification, device management, incident response.
- Example: Employees must change passwords every 90 days.

Human Factor in Security

- Most security breaches involve human error.
- Example: Opening malicious email attachments.

Incident Response Steps

- Identify, contain, eradicate, recover, learn.
- Example: Isolating infected computers to prevent malware spread.

Standards & Frameworks

- ISO 27001, NIST CSF, COBIT, GDPR.
- Example: Organizations adopt ISO 27001 for structured data protection.

Security in Daily Life

- Update devices, avoid public Wi-Fi, don't click suspicious links, backup data.
- Example: Using personal hotspot for mobile banking.

Security in Organizations

- Network segmentation, audits, staff training, monitoring.
- Example: Conducting security audits every 6 months.

Future Trends

- AI-based defense, Zero-Trust, quantum-safe encryption, IoT security.
- Example: AI detecting unusual login activity.

Conclusion

- Information security requires technology, policies, and user awareness.
- Example: Campus data stays safe through firewalls, SOPs, and staff training.