INFORMATION SECURITY

Bachelor of Information Systems

INTRODUCTION TO
DATABASE AND INFORMATION SYSTEM

Learning Objective(s)

This material should address the following question(s).

- What is the information security?
- What are factors that contribute to the increased vulnerability of information resources?
- What are the threats for information security?
- What are the information security risk mitigation strategies?

Question

What is the **information security**?

Information Security

- **Security** can be defined as the level of protection against criminal activity, danger, damage, and/or loss.
- **Information security** refers to all processes and policies designed to protect an organization's information and information systems (IS) from unauthorized access, use, disclosure, interference, modification or destruction.

Threat-Exposure-Vulnerablity

- **Threat** — a resource is in danger.
  e.g., malware
- **Exposure** — the amount of loss or damage.
  e.g., insecurely stored login credentials
- **Vulnerability** — the possibility (chance) that the system will experience damage.
  e.g., vulnerabilities in firewall or antivirus software configurations.

TEV framework can be used to help organizations in:

- Identify and assess cybersecurity risks.
- Develop and implement security controls to reduce risk.
- Monitor and manage cybersecurity risks on an ongoing basis.

Question

What are **factors** that **contribute** to the increased **vulnerability** of information resources?

Vulnerability of Information Resources

- Five factors that increase the vulnerability of information resources:
  - Today's business environment is interconnected, interdependent, and wirelessly connected
  - Smaller, faster, cheaper computers and storage devices
  - Decreased skills required to become a hacker.
  - Organized crime is taking over cybercrime.
  - Lack of management support.

Question

What are the **threats** for **information security**?

Threats

- Information systems are vulnerable to many potential dangers and threats.

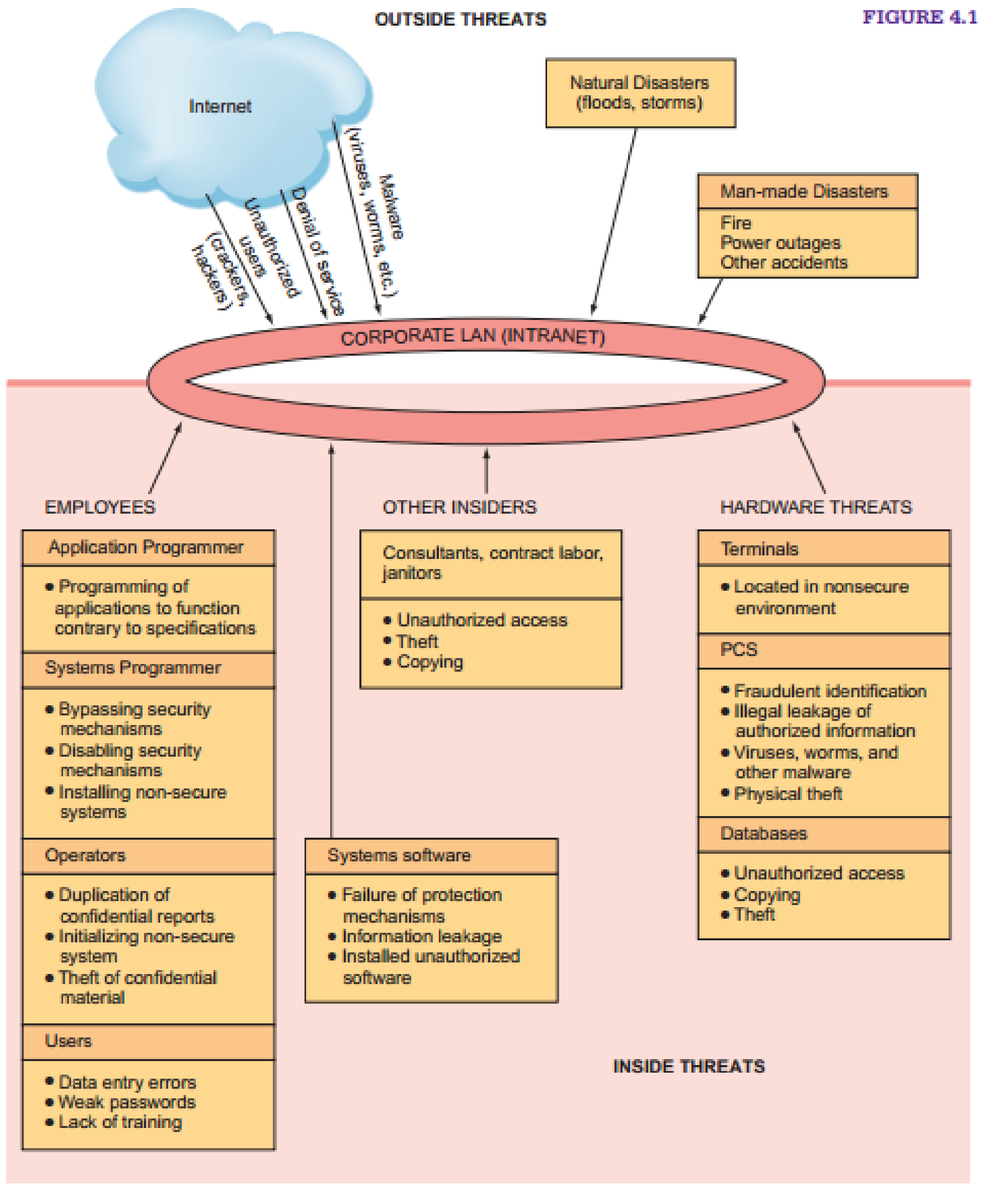

FIGURE 4.1 Security threats.

Question

What are the information security **risk mitigation** strategies?

Risk Mitigation Strategy

- There are several risk mitigation strategies that organizations can adopt.
- The three most common:
  - **Risk acceptance**: Accept the potential risk, continue operating without control, and absorb any damage that occurs.
  - **Risk limitation**: Limit risks by implementing controls that minimize the impact of threats.
  - **Risk transference**: Transferring risk by using other means to compensate for losses, such as purchasing insurance.

Conclusion

- Information security refers to all processes and policies designed to protect an organization's information and information systems (IS) from unauthorized access, use, disclosure, interference, modification or destruction.
- There are five factors that increase the vulnerability of information resources.
- Information systems are vulnerable to many potential dangers and threats.

Conclusion

- The three most common risk mitigation strategies that organizations can adopt are risk acceptance, risk limitation, and risk transference.

References

- R, Elmasri, et. al., Fundamentals of Database Systems.
- A. Silberschatz, et. al., Database System Concepts.
- R. K. Rainer, et. al., Introduction to Information Systems.
- G. M. Marakas et. al., Introduction to Information Systems: Essentials for The e-Business Enterprise.

Course

Mario E. S. Simaremare

@simaremare

Lecturer

Samuel I. G. Situmeang

@exemuel