BAKER COLLEGE
STUDENT LEARNING OUTCOMES

CIS2750 Securing Information Systems
3 Semester Hours

Student Learning Outcomes and Enabling Objectives

1. Examine the need for information and network security.
    a. Define key terms.
    b. Review the OSI model.
    c. Explore how to identify threats to information and network security.
    d. Assess the likelihood of a network attack.
    e. Explain the nature of the Internet and its relationship to the TCP/IP protocol.
    f. Discuss password security
    g. Discuss encryption
2. Determine management's role in the development and enforcement of information security policies and guidelines.
    a. Identify how an organization institutionalizes policies, standards, and practices using education, training, and awareness programs.
    b. Discuss the need for a contingency plan using sound backup and recovery techniques.
    c. Discuss the need for a disaster recovery plan.
3. Examine how an organization deals with network security breaches and incidents.
    a. Identify common system and network vulnerabilities.
    b. Discuss Anti-Virus selection, use, and maintenance
    c. Discuss risk assessment and management
    d. Identify some widely available scanning and analysis tools.
    e. Describe the various technologies that are used to implement intrusion detection and prevention
    f. Explore digital forensics in information technology.
4. Determine the need of a proxy server on a network.
    a. Discuss proxy servers and how they work.
    b. Determine when a proxy server isn't the best choice on a network.
    c. Evaluate the most popular proxy-based firewall products.
    d. Discuss the SOCKS protocol
5. Examine the functions of a firewall
    a. Identify what a firewall does.
    b. Discuss the differences between using a hardware firewall and a software firewall
    c. Explore firewall rules and security

    d. Discuss secure virtual private networks.
6. Explore how a firewall works.
    a. Create firewall rules that reflect an organization's overall security approach.
    b. Identify the importance of using firewall log files to identify an incident.
    c. Maintain a secure wireless router for home use.
    d. Describe common authentication protocols used by firewalls.
    e. Discuss authentication for users, clients, sessions, and administrators.

Big Ideas and Essential Questions

Big Ideas

- Network Security Policy and Procedures
- Firewall usage on a network
- Secure Authentication and Encryption
- Disaster planning and recovery

Essential Questions

1. What is meant by network security?
2. What do firewalls do?
3. What is encryption and authentication?
4. What is risk?

These SLOs are approved for experiential credit.

Effective: Summer 2022