

Student Note:

**UNIT 6 – SECURING ASSETS;**  
**INFORMATION & INTELLECTUAL PROPERTY**

**HOMEWORK PREPARATION FOR CLASS**

**READING**

*Proactive Security Administration*, Chapter 5: Securing Assets— Information and Intellectual Property, pp. 105–122

**WRITTEN ASSIGNMENT: UNIT 5-1**

**Title: Perimeter Security**

**Introduction:** You are a security consultant. You have been hired to ensure security for the convenience store in your neighborhood.

**Tasks:** The peak period for convenience store robberies is between 9 PM and 11 PM. As a security professional, what ideas can you implement to deal with the risk of a robbery? Try to make your suggestions as innovative (yet practicable) as possible. Provide at least three viable ideas.

**VIDEO PRESENTATION:** If time allows...

**A & E: Bodyguard Training Camp**

The bodyguard training for professionals and business executives.

**QUIZ PREVIEW QUESTIONS:** From your reading and today's lecture

1. Define information, information security, and intellectual property.
2. Explain the two general categories of threats to information.
3. Describe the process for establishing an information security policy.
4. Identify commonly used methods for protecting information and sensitive data.

**LECTURE:**

**I. THE INFORMATION AGE**

A. The short history of the computer age...

1. 1980 –

2. 1990 –

3. 2000 –

4. Today –

B. The Lessons from September 11, 2001

1. Electronic transactions disabled and records destroyed
2. Stored Data and other information destroyed

C. How can we protect our Information and Intellectual Property?

1. Information has value:

a) Information is

b) Intellectual Property is

2. Information Security:

a) Information Security is

(1) Availability:

(2) Accuracy:

(3) Authenticity:

(4) Confidentiality:

b) The process is known as

D. Threats to Information (Pages 110 – 114)

1. Physical Threats (Physical Damage)

a) Human Error

b) Criminal Acts or Malicious Acts

- c) Natural Disasters
- 2. Technological Threats (Software & Data Damage)
  - a) Human Error
  - b) Criminal Acts or Malicious Acts
  - c) System Failures
- E. Misuse or Abuse of Networks (Pages 114 – 115)
  - 1. Four areas of employee abuse
    - a)
    - b)
    - c)
    - d)
  - 2. Defense: Use policies limiting employee access with a combination of rules and software tracking.
  - 3. Malicious Attacks on Networks (Pages 115 – 117)
    - a) Attack to obtain information: Social security, credit card or other...
      - (1) Most often disgruntled employees and independent hackers (a smaller percentage are business competitors)
      - (2) Most attacks are viruses or worms
      - (3) Other attack devices are Trojan horse and Logic Bombs
  - 4. Attacks on Web Sites
    - a) Two major threats to the business
      - (1)
      - (2)
  - 5. Vulnerability Assessments
    - a) Vulnerabilities are conditions or weaknesses in security that could be exploited by a threat. The threat can be physical or technological...
    - b) A two step process:

- (1) **Identification of Vulnerabilities** (an organizational process – all departments in the organization should be involved in the process to identify all known vulnerabilities)
  - (2) **Assess the Importance of the Vulnerability** (how do you fix or mitigate the damage)
- F. Countermeasures (Pages 118 – 122)
1. Countermeasures are policies and activities that address identified vulnerabilities in an effort to prevent or mitigate threats.
    - a) Identification and selection of countermeasures are unique to each organization.
  2. Standard Countermeasures (Page 118 – 119)
    - a) Security policies
    - b) Employee training
    - c) Confidentiality agreements
    - d) Criminal Prosecution of offenders
    - e) Physical Security
    - f) Hardware and Software security
    - g) Biometrics
  3. Use of Cost-Benefit Analysis (process for establishing an information security policy)
    - a) A four step process
      - (1) Identify All Vulnerabilities
      - (2) Rank by their likelihood of occurrence
      - (3) Rank by their potential damage to the company
      - (4) Combine the lists and work to mitigate or eliminate
        - (a) Concentrate on top 20 percent of your list...
- G. Protecting Information and Sensitive Data (Pages 120 – 122)
1. Access Controls
  2. Firewalls
  3. Antivirus Software
  4. Spyware
  5. Encryption
  6. Virtual Private Network
  7. Biometric Devices

**QUIZ/LAB**

Security Terminology

**HOMEWORK**

**READING:** *Proactive Security Administration*, Chapter 6: Investigation of Crime and Security Incidents, pp. 125–149

**Homework Assignment Unit 6- 1****Title: Protecting Information and Sensitive Data**

**Introduction:** Your supervisor has assigned you the task of collecting information on available security technologies.

**Tasks:** Using the material in the textbook, the ITT Tech Virtual Library, and the Internet, locate and pull information on emerging security technologies used by organizations to protect sensitive data. Identify at least five such technologies and explain the pros and cons of using these technologies.

**Deliverables and format:** Submit answers in a Microsoft Word document of not more than 300 words. Font: Arial, 12 pt. Line Spacing: Double