Learning Objectives

• Describe the business value of security and control.

• Describe the components of an organizational framework for security and control.

• Describe the tools and technologies used for safeguarding information resources.
System Vulnerability and Abuse

- **Security:**
  - Policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems

- **Controls:**
  - Methods, policies, and organizational procedures that ensure safety of organization’s assets; accuracy and reliability of its accounting records; and operational adherence to management standards

**CONTEMPORARY SECURITY CHALLENGES AND VULNERABILITIES**

![Diagram of system vulnerability and abuse](image)

The architecture of a Web-based application typically includes a Web client, a server, and corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network.
System Vulnerability and Abuse

• **Internet vulnerabilities**
  – Network open to anyone
  – Size of Internet means abuses can have wide impact
  – Use of fixed Internet addresses with cable / DSL modems creates fixed targets for hackers
  – Unencrypted VOIP
  – E-mail, P2P, IM
    • Interception
    • Attachments with malicious software
    • Transmitting trade secrets

System Vulnerability and Abuse

• **Wireless security challenges**
  • Radio frequency bands easy to scan
  • SSIDs (service set identifiers)
    • Identify access points
    • Broadcast multiple times
    • Can be identified by sniffer programs
    • War driving
      • Eavesdroppers drive by buildings and try to detect SSID and gain access to network and resources
      • Once access point is breached, intruder can use OS to access networked drives and files
Many Wi-Fi networks can be penetrated easily by intruders using sniffer programs to obtain an address to access the resources of a network without authorization.

**Organizational Frameworks for Security and Control**

- **Information systems controls**
  - Manual and automated controls
  - General and application controls

- **General controls**
  - Govern design, security, and use of computer programs and security of data files in general throughout organization’s information technology infrastructure
  - Apply to all computerized applications
  - Combination of hardware, software, and manual procedures to create overall control environment
• **Application controls**
  
  – Specific controls unique to each computerized application, such as payroll or order processing
  
  – Include both automated and manual procedures
  
  – Ensure that only authorized data are completely and accurately processed by that application
  
  – Include:
    
    • Input controls
    • Processing controls
    • Output controls

---

**Organizational Frameworks for Security and Control**

• **Risk assessment**: Determines level of risk to firm if specific activity or process is not properly controlled
  
  • Types of threat
  
  • Probability of occurrence during year
  
  • Potential losses, value of threat
  
  • Expected annual loss

<table>
<thead>
<tr>
<th>Exposure</th>
<th>Probability</th>
<th>Loss Range (Avg)</th>
<th>Expected Annual Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power failure</td>
<td>30%</td>
<td>$5K–$200K ($102,500)</td>
<td>$30,750</td>
</tr>
<tr>
<td>Embezzlement</td>
<td>5%</td>
<td>$1K–$50K ($25,500)</td>
<td>$1,275</td>
</tr>
<tr>
<td>User error</td>
<td>98%</td>
<td>$200–$40K ($20,100)</td>
<td>$19,698</td>
</tr>
</tbody>
</table>
Organizational Frameworks for Security and Control

• **Security policy**
  - Ranks information risks, identifies acceptable security goals, and identifies mechanisms for achieving these goals
  - Drives other policies
    - Acceptable use policy (AUP)
      - Defines acceptable uses of firm’s information resources and computing equipment
    - Authorization policies
      - Determine differing levels of user access to information assets

Organizational Frameworks for Security and Control

• **Identity management**
  - Business processes and tools to identify valid users of system and control access
    - Identifies and authorizes different categories of users
    - Specifies which portion of system users can access
    - Authenticating users and protects identities
  - Identity management systems
    - Captures access rules for different levels of users
Disaster recovery planning: Devises plans for restoration of disrupted services

Business continuity planning: Focuses on restoring business operations after disaster
  • Both types of plans needed to identify firm’s most critical systems
  • Business impact analysis to determine impact of an outage
  • Management must determine which systems restored first

Information systems audit
  • Examines firm’s overall security environment as well as controls governing individual information systems
  • Reviews technologies, procedures, documentation, training, and personnel
  • May even simulate disaster to test response of technology, IS staff, other employees
  • Lists and ranks all control weaknesses and estimates probability of their occurrence
  • Assesses financial and organizational impact of each threat
Tools and Technologies for Safeguarding Information Resources

• **Identity management software**
  – Automates keeping track of all users and privileges
  – Authenticates users, protecting identities, controlling access

• **Authentication**
  – Password systems
  – Tokens
  – Smart cards
  – Biometric authentication
  – Two-factor authentication

Tools and Technologies for Safeguarding Information Resources

• **Firewall:**
  – Combination of hardware and software that prevents unauthorized users from accessing private networks
  – Technologies include:
    • Static packet filtering
    • Stateful inspection
    • Network address translation (NAT)
    • Application proxy filtering
The firewall is placed between the firm’s private network and the public Internet or another distrusted network to protect against unauthorized traffic.

**FIGURE 8.5**

A CORPORATE FIREWALL

Tools and Technologies for Safeguarding Information Resources

- **Intrusion detection systems:**
  - Monitors hot spots on corporate networks to detect and deter intruders
  - Examines events as they are happening to discover attacks in progress

- **Antivirus and antispyware software:**
  - Checks computers for presence of malware and can often eliminate it as well
  - Requires continual updating

- **Unified threat management (UTM) systems**
• Securing wireless networks
  • WEP security can provide some security by:
    • Assigning unique name to network’s SSID and not broadcasting SSID
    • Using it with VPN technology
  • Wi-Fi Alliance finalized WPA2 specification, replacing WEP with stronger standards
    • Continually changing keys
    • Encrypted authentication system with central server

• Encryption:
  – Transforming text or data into cipher text that cannot be read by unintended recipients
  – Two methods for encryption on networks
    • Secure Sockets Layer (SSL) and successor Transport Layer Security (TLS)
    • Secure Hypertext Transfer Protocol (S-HTTP)
Tools and Technologies for Safeguarding Information Resources

• **Two methods of encryption**
  • **Symmetric key encryption**
    • Sender and receiver use single, shared key
  • **Public key encryption**
    • Uses two, mathematically related keys: Public key and private key
    • Sender encrypts message with recipient’s public key
    • Recipient decrypts with private key

---

**PUBLIC KEY ENCRYPTION**

A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock the data when they are received. The sender locates the recipient’s public key in a directory and uses it to encrypt a message. The message is sent in encrypted form over the Internet or a private network. When the encrypted message arrives, the recipient uses his or her private key to decrypt the data and read the message.
Tools and Technologies for Safeguarding Information Resources

• **Digital certificate:**
  - Data file used to establish the identity of users and electronic assets for protection of online transactions
  - Uses a trusted third party, certification authority (CA), to validate a user's identity
  - CA verifies user's identity, stores information in CA server, which generates encrypted digital certificate containing owner ID information and copy of owner’s public key

• **Public key infrastructure (PKI)**
  - Use of public key cryptography working with certificate authority
  - Widely used in e-commerce

References and recommended readings