Fundamentals of Information Systems Security

Unit 1
Information Systems Security Fundamentals
Learning Objective

Explain the concepts of information systems security (ISS) as applied to an IT infrastructure.
Key Concepts

- Confidentiality, integrity, and availability (CIA) concepts
- Layered security solutions implemented for the seven domains of a typical IT infrastructure
- Common threats for each of the seven domains
- IT security policy framework
- Impact of data classification standard on the seven domains
DISCOVER: CONCEPTS
Introducing ISS

ISS

Information Systems

Information
The CIA Triad

Confidentiality

Integrity

Availability
Confidentiality

Personal Data and Information
- Credit card account numbers and bank account numbers
- Social Security numbers and address information

Intellectual Property
- Copyrights, patents, and secret formulas
- Source code, customer databases, and technical specifications

National Security
- Military intelligence
- Homeland security and government-related information
Integrity

Maintain valid, uncorrupted, and accurate information.

- User names and passwords
- Patents and copyrights
- Source code
- Diplomatic information
- Financial data
Availability
Conduct and Ethics in ISS

- ISS is a classic battle of “good vs. evil.”
- No global laws, rules, or regulations govern cyberspace.
- U.S. government and Internet Architecture Board (IAB) have developed joint Internet acceptable use policy (AUP).
- Security professionals are in high demand as the “good guys.”
Compliance Laws Driving ISS

Health Insurance Portability and Accountability Act (HIPAA)

Sarbanes-Oxley (SOX) Act

Children’s Internet Protection Act (CIPA)
IT Security Policy Framework

**POLICY**
- A short written statement that defines a course of action that applies to the entire organization

**Standard**
- A detailed written definition of how software and hardware are to be used

**Procedure**
- Written instructions for how to use the policy and standard

**Guideline**
- Suggested course of action for using the policy, standard, or procedure
Seven Domains of a Typical IT Infrastructure
Common Threats in the User Domain

- Lack of user awareness
- User apathy toward policies
- User violating security policy
- User inserting CD/DVD/USB with personal files
Common Threats in the User Domain (Continued)

- User downloading photos, music, or videos
- User destructing systems, applications, and data
- Disgruntled employee attacking organization or committing sabotage
- Employee blackmail or extortion
Common Threats in the Workstation Domain

- Unauthorized workstation access
- Unauthorized access to systems, applications, and data
- Desktop or laptop operating system vulnerabilities
- Desktop or laptop application software vulnerabilities or patches
Common Threats in the Workstation Domain (Continued)

- Viruses, malicious code, and other malware
- User inserting CD/DVD/USB with personal files
- User downloading photos, music, or videos
Common Threats in the LAN Domain

- Unauthorized physical access to LAN
- Unauthorized access to systems, applications, and data
- LAN server operating system vulnerabilities
- LAN server application software vulnerabilities and software patch updates
Common Threats in the LAN Domain (Continued)

- Rogue users on WLANs
- Confidentiality of data on WLANs
- LAN server configuration guidelines and standards
Common Threats in the LAN-to-WAN Domain

- Unauthorized probing and port scanning
- Unauthorized access
- Internet Protocol (IP) router, firewall, and network appliance operating system vulnerability
- Local users downloading unknown file types from unknown sources
Common Threats in the WAN Domain

- Open, public, and accessible data
- Most of the traffic being sent as clear text
- Vulnerable to eavesdropping
- Vulnerable to malicious attacks
- Vulnerable to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
Common Threats in the WAN Domain (Continued)

- Vulnerable to corruption of information and data
- Insecure Transmission Control Protocol/Internet Protocol (TCP/IP) applications
- Hackers and attackers e-mailing Trojans, worms, and malicious software freely and constantly
Common Threats in the Remote Access Domain

- Brute force user ID and password attacks
- Multiple logon retries and access control attacks
- Unauthorized remote access to IT systems, applications, and data
- Confidential data compromised remotely
- Data leakage in violation of data classification standards
Common Threats in the Systems/Applications Domain

- Unauthorized access to data centers, computer rooms, and wiring closets
- Difficult-to-manage servers that require high availability
- Server operating systems software vulnerability management
- Security required by cloud computing virtual environments
- Corrupt or lost data
DISCOVER: PROCESSES
Implementing the CIA Triad

Confidentiality

AUP

Security Awareness Policy

Enhanced Access Control
Implementing the CIA Triad (Continued)

Integrity

AUP
Threat Assessment and Monitoring
Security Awareness Policy
Vulnerability Assessment and Management
Enhanced Access Control
Asset Protection Policy
Implementing the CIA Triad (Continued)

Availability

Data Classification Standard
AUP
Threat Assessment and Monitoring
Security Awareness Policy
Vulnerability Assessment and Management
Enhanced Access Control
Asset Protection Policy
DISCOVER: ROLES
## Who Implements the CIA Triad?

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User</td>
<td>IT administrator</td>
</tr>
<tr>
<td>IT administrator</td>
<td>IT administrator</td>
<td>Network administrator</td>
</tr>
<tr>
<td>Network administrator</td>
<td>Network administrator</td>
<td>Third-party vendor, for example, telecommunication company</td>
</tr>
<tr>
<td>Human resources</td>
<td>Human resources</td>
<td></td>
</tr>
<tr>
<td>Senior management</td>
<td>Senior management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Third-party vendor, for example, telecommunication company</td>
</tr>
</tbody>
</table>
Summary

- Terms associated with ISS include risks, threats, and vulnerabilities.
- Layered security strategy protects an IT infrastructure’s CIA.
- IT policy framework includes policies, standards, procedures, and guidelines.
- Data classification standard defines how data is to be handled within an IT infrastructure.