Learning Objectives

1. Understand goals of security
2. Understand tools of security management
3. Understand the need for system controls and audits
4. History

Goals

- Accuracy
- Safety
- IS Processes & Resources
- Integrity

Goals (continued)

- Minimize
  - Errors
  - Fraud
  - Losses

Goals (continued)

Increasingly Important Topic

The Sept. 11 terrorist attack has heightened interest in and concern for:

- Personal and Property Security
- Disaster Recovery
- Privacy and Civil Liberties

Goals (continued)

Homeland Security Act

Is Big Brother could really be watching you?

Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every bank deposit you make, every trip you book and every event you attend — all these transactions and communications will go into what the Defense Department describes as a virtual, centralized database.

Also add every piece of information that government has about you — birth certificate, passport application, driver’s license, judicial and divorce records, etc.
Security Comes Before Liberty

Abdul Hakim Murad was arrested in the Philippines in 1995.

When tortured he revealed nothing.

He was told that he was to be taken to Israel.

He then revealed a plan to assassinate the Pope in Manila.

Goals (continued)

Huge Implications

Steps taken by the Bush administration pale in comparison to what previous wartime administrations have done under Abraham Lincoln, Woodrow Wilson and Franklin Roosevelt.

How to balance security measures to forestall future terrorist attacks implicates our much-cherished doctrine of civil liberties.

Goals (continued)

Security Management Tools

What are the primary tools?

1. Encryption
2. Firewalls
3. Denial of Service
4. E-Mail Monitoring
   - Continuous
   - Span
5. Virus Defenses

What are the secondary tools?

1. Passwords or security codes
2. Backup
3. Security Monitors
4. Biometric
5. Computer service interruption
6. Fault tolerant systems
7. Disaster recovery

Security Management Tools (continued)

Methods to insure

• Accuracy
• Validity
• Propriety

Supported by Audit Trails

• Trace
• Throughout its lifecycle

Systems Controls & Audits

Who Commit Computer Crimes?

<table>
<thead>
<tr>
<th>Who</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programmers</td>
<td>18%</td>
</tr>
<tr>
<td>Students</td>
<td>12%</td>
</tr>
<tr>
<td>Input clerks</td>
<td>12%</td>
</tr>
<tr>
<td>Bank tellers</td>
<td>8%</td>
</tr>
<tr>
<td>Accomplices</td>
<td>8%</td>
</tr>
<tr>
<td>Unskilled workers</td>
<td>6%</td>
</tr>
<tr>
<td>Unemployed</td>
<td>6%</td>
</tr>
<tr>
<td>Employee with access</td>
<td>5%</td>
</tr>
<tr>
<td>Executives</td>
<td>3%</td>
</tr>
</tbody>
</table>
Computer Crime Profile

History
Relatively young (18 to 30 years old)
Highly motivated
Intelligent
Personable
Good worker
Happy with their job
Employed for several years
No history of job problems
Possibly overqualified for current position
Sees themselves as a borrower

San Jose Police Hi-tech Arrests
100% had graduated from high school.
80% had graduated from college.
50% had masters degrees.
25% had a PhD.

Possible Exam Questions

1. What three types of information systems controls are needed to ensure the quality and security of information systems?
2. What are the tools that are needed to ensure the security of information systems?
3. What are system controls?
4. What is an audit trail?