Physical Security

- Physical attacks often easiest way to breach computer security
  - Theft of systems or parts
  - Access to unattended systems
  - Access to unprotected networks
Physical Attacks: Availability

• Damage or steal hardware
  – Chicago Air Traffic Control Center Fire
  – Response: Improve
    • Access control
    • Personnel screening
    • Training to identify indicators of potential threats

Solutions: Availability

• Control access
  – Authentication
  – Access control

• Redundancy
  – Reduce / harden “single point of failure”
  – Physical separation of redundant systems
Physical Attacks: Integrity

• Use access to alter information
  – Typically involves non-physical attack as well
• Direct attacks on data integrity
  – Pull the plug…

Solutions: Integrity

• Similar measures as taken for availability
  – Control access to critical areas
  – Redundancy
• Measures taken for insider threat
  – Reduce chance of unattended systems
• Backups
  – Regular backup schedule
  – DBMS-style logging (take CS44800 for details)
Physical Attacks: Confidentiality

Attacks
- Steal devices
  - Whole systems
  - Disk drives
- Download data
  - USB flash drives
- Install devices
  - Cameras
  - Keystroke loggers

Responses
- Virtualization
  - Accessible devices don’t hold data
- System lockdown
  - Disable unneeded I/O
- Block access to parts of systems
  - Keyboard accessible, but not USB port it plugs in to

Physical Security: Summary

- Many measures analogous to Information Security
  - Authentication
  - Access control
- Measures for Insider Threat also address Physical Security issues
- Policies should be reasonable, implementable
  - People should understand why policy needed
- Training
Personnel and Physical Security: Training

• Security Training not always effective
  – Multiple studies of phishing attacks show this
• But still necessary
  – Alternative: Principle of No Privilege?

Security Training: Steps (NIST 800-50)

• Levels
  – Awareness
  – Training
  – Education
• Outcomes
  – Security awareness
  – Security Basics and Literacy
  – Functional Roles and Responsibilities
Security Awareness

- General understanding that security is an issue
  - Goal: Individuals recognize concerns
- Example: Computer Virus
  - What a computer virus is, potential impacts
  - How this happens
  - What to do / who to call
- Delivery: Presentation/Talk/Video

Security Awareness: Developing a Program

- Structure: Policy, Strategy, Implementation
  - Strategy and Implementation can be centralized or distributed
- Policy: Goals
- Strategy: Needs assessment
- Implementation: Methodology
Needs Assessment

*Needs Assessment requires understanding*

- Directives and Laws
  - Legal
- Security issues and challenges
  - Security experts
- System controls
- Domain-specific issues
  - User backgrounds, expectations, behaviors
Example Awareness Topics

- Password usage / management
- Protection from malware
- Policy / Compliance
- Web usage policy
- Spam / email hygiene
- Backup
- Social engineering
- Incident response
- Access control issues
- Accountability
- Visitor control/access
- ...

Security Training

- Specific skills and knowledge related to individual’s role
  - Goal: Understand specific operations / actions user should take as part of their job
  - Typically targeted to non-IT security roles
- Delivery
  - Classroom
  - On-line course
- Ensure knowledge/skills developed
  - Some form of evaluation (test/exercises)
## IT Security Training Matrix

### SysAdmin

<table>
<thead>
<tr>
<th>Training Areas</th>
<th>Functional Specialties</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A Manage</td>
</tr>
<tr>
<td>1. Laws and Regulations</td>
<td></td>
</tr>
<tr>
<td>2. Security Program</td>
<td></td>
</tr>
<tr>
<td>2.1 Planning</td>
<td></td>
</tr>
<tr>
<td>2.2 Management</td>
<td></td>
</tr>
<tr>
<td>3. System Life Cycle Security</td>
<td></td>
</tr>
<tr>
<td>3.1 Initiation</td>
<td></td>
</tr>
<tr>
<td>3.2 Development</td>
<td></td>
</tr>
<tr>
<td>3.3 Test and Evaluation</td>
<td></td>
</tr>
<tr>
<td>3.4 Implementation</td>
<td></td>
</tr>
<tr>
<td>3.5 Operations</td>
<td></td>
</tr>
<tr>
<td>3.6 Termination</td>
<td></td>
</tr>
<tr>
<td>4. Other</td>
<td></td>
</tr>
</tbody>
</table>

---

## Awareness vs. Training

- **Awareness:** What behavior do we want to reinforce?
- **Training:** What skill or skills do we want the audience to learn and apply?
Security Education

- Long-term professional development
  - Targeted to IT professionals
- Goal: Design/develop security mechanisms and policies
- Delivery
  - Course and degree programs
  - Professional certifications

  *Typically done by outside organizations*

Follow-on Steps

- Monitor compliance - Is the training being done?
  - Organizational reporting
  - Status reports
- Evaluate - Are the goals being achieved?
  - Evaluation forms/questionnaires
  - Focus groups
  - Interviews
  - Observation/analysis