

# CS42600: Computer Security

*Personnel and Physical Security*

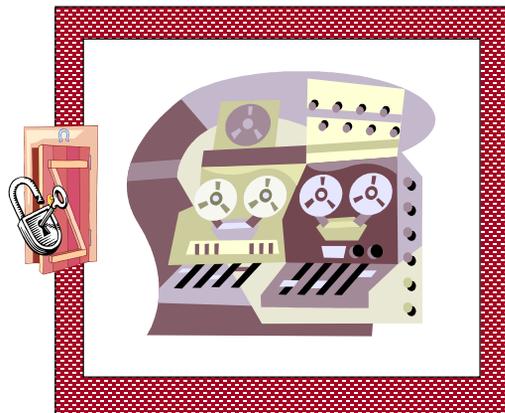
Prof. Chris Clifton

24 January 2019



## 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



16

## Solutions: Availability

---

- Control access
  - Authentication
  - Access control
- Redundancy
  - Reduce / harden “single point of failure”
  - Physical separation of redundant systems

17

## Physical Attacks: Integrity

---

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



18

## 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)

19

## 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

20

## 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*

21

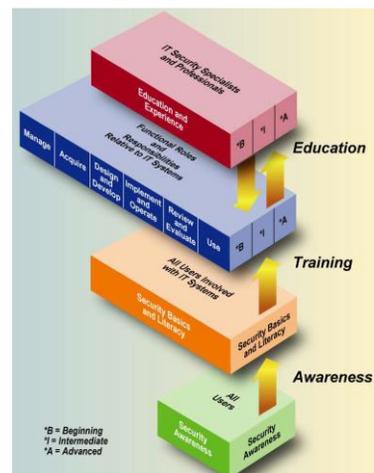
# Personnel and Physical Security: Training

- 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

24

## Security Awareness: Developing a Program

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



25

## 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

26

## Needs Assessment



27

## 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
- ...

28

## 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)

29

## IT Security Training Matrix *SysAdmin*

Training Areas	Functional Specialities						
	A Manage	B Acquire	C Design and Develop	D Implement and Operate	E Review and Evaluate	F Use	G Other
1. Laws and Regulations				1D ✓			
2. Security Program							
2.1. Planning							
2.2. Management				2.2D ✓			
3. System Life Cycle Security							
3.1 Initiation				3.2D ✓			
3.2. Development				3.3D ✓			
3.3. Test and Evaluation				3.4D ✓			
3.4. Implementation			3.4C ✓	3.4D ✓			
3.5. Operations	3.5A ✓		3.5C ✓	3.5D ✓			
3.6. Termination				3.6D ✓			
4. Other							

30

## 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?

31

## 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*

32

## 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

33