Physical and Environmental Security

From last time…
Design of security controls

Physical controls
- e.g., fences, doors, locks.

Procedural controls
- e.g., incident response processes, security awareness.

Legal and regulatory or compliance controls
- e.g., privacy laws, policy

Technical controls
- e.g., user authentication, anti-virus, firewalls.

Physical and Environment Security

- Technical security may protect our data…
- Physical security will protect the machine our data is stored on.

Physical and Environment Security

- What are the threats to physical security?
- What can we do to improve physical security within a organisation?

What are we protecting from?

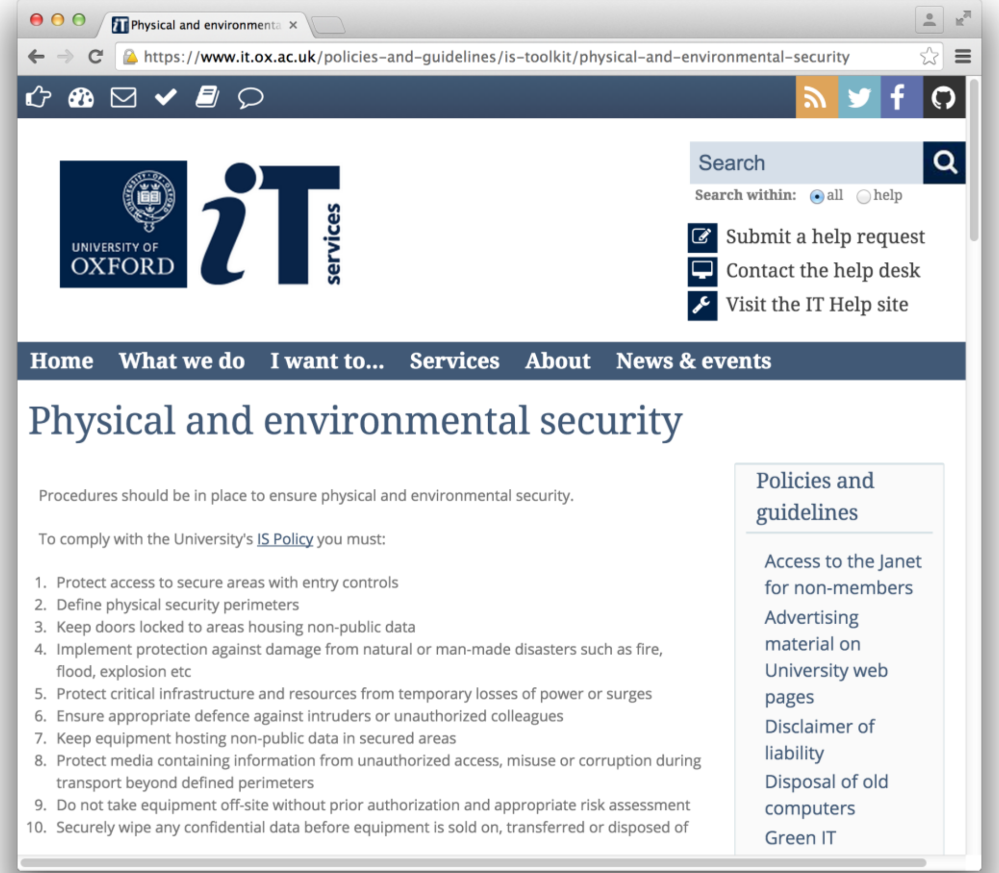
- Access, Theft, or Damage, of physical resources
  - Physical resources also include IT equipment and other data records (e.g., paper copies, contracts).
- Both external or internal attackers may attempt to evade physical security
  - Although Insider has privileged access and knowledge, and so may well be more successful…

What are we protecting from?

- Safety concerns for dangerous situations: fire alarms, flooding, earthquakes…
  - How can we maintain security whilst ensuring safety?

Physical and Environment Security Policy

- Information Security Policy should also cover physical and environmental security.
- "Only 1/3 of IS policy is technical, the other 2/3 focus on human factors"



Physical and environmental security

Procedures should be in place to ensure physical and environmental security.

To comply with the University's IS Policy you must:

1. Protect access to secure areas with entry controls
2. Define physical security perimeters
3. Keep doors locked to areas housing non-public data
4. Implement protection against damage from natural or man-made disasters such as fire, flood, explosion etc
5. Protect critical infrastructure and resources from temporary losses of power or surges
6. Ensure appropriate defence against intruders or unauthorized colleagues
7. Keep equipment hosting non-public data in secured areas
8. Protect media containing information from unauthorized access, misuse or corruption during transport beyond defined perimeters
9. Do not take equipment off-site without prior authorization and appropriate risk assessment
10. Securely wipe any confidential data before equipment is sold on, transferred or disposed of

Policies and guidelines
Access to the Janet for non-members
Advertising material on University web pages
Disclaimer of liability
Disposal of old computers
Green IT

Lock and key

- Most basic of security methods
  - What if more than one person needs access?
  - What we we want to know who has accessed?
  - What if our attacker owns a pair of bolt cutters…?

Radio-Frequency Identification Card

- RFID Access cards are widely used by many organisations.
  - Allows managed access to restricted areas for each user.
  - Provides a physical ID of the individual.
  - Maintains an electronic record of who has accessed an area.

Radio-Frequency Identification Card

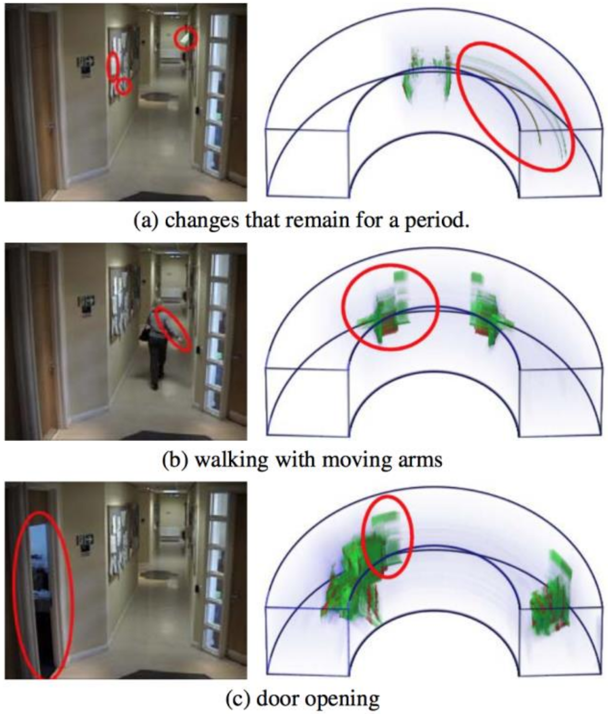
- Swipe on entry only?
- Swipe on entry and exit?
- What are the pros and cons for each?
  - Cost? Efficiency? Effectiveness?

Closed Circuit Television (CCTV)

- Video surveillance of multiple areas of organisation.
- Security officer can view in real-time, or retrieve archive video from reported incident.
- What are the pros and cons of CCTV?
  - Cost? Placement of cameras? Demands on the security officer?

Closed Circuit Television (CCTV)

- How can we improve CCTV?
  - Video Visualization
    - (http://www.oerc.ox.ac.uk/projects/video-visualization)
  - "Fight-sensing cameras to cut crime on Britain's streets" – video scene recognition
    - (http://www.cardiff.ac.uk/news/view/78769-fight-sensing-cameras-to-cut-crime-on-britains-streets)


(a) changes that remain for a period.

(b) walking with moving arms

(c) door opening

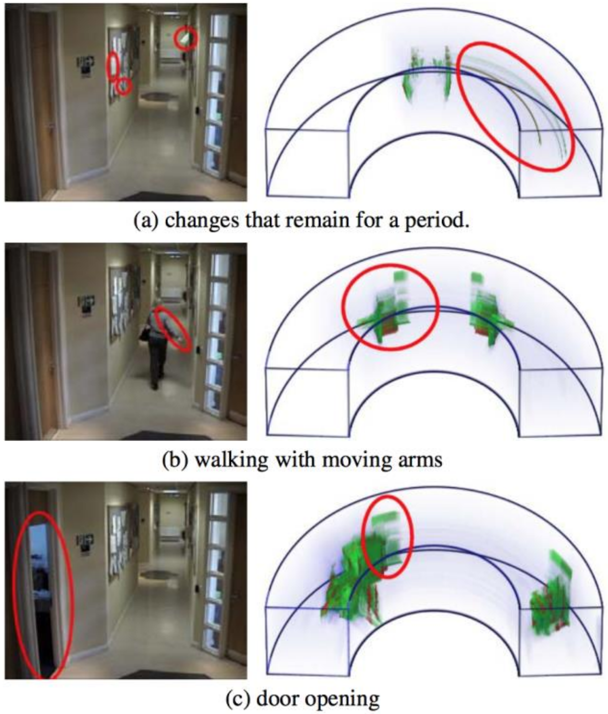
Activity

Discussion:

What else could be done to improve physical or environmental security?

Are there better measures that could be introduced once people are 'inside' the building?

What may be the future of physical security?



(a) changes that remain for a period.

(b) walking with moving arms

(c) door opening

Processes to handle intrusion alerts

- Preventative controls
  - E.g, Reception area as a first point of entry
  - E.g., Locked doors
- Detective controls
  - E.g., Alarmed areas
- Corrective / Reactive controls
  - E.g., Electric fence

Clear screen and desk policy

- How do we manage sensitive detail on a computer screen?
  - – What if the user is distracted away from their desk? (e.g., making a coffee, vs. fire alarm).
  - – Screensaver password – too short may cause frustration, too long may not be effective.
- How do we manage sensitive printed details?
  - – Clear desk policy aims for no detail to be left on view.

Moving property on and off site

- How do we manage data when it needs to be used offsite?
  - Need to avoid the "left it in the taxi" scenario!
- Inventory of offsite equipment – what is the procedure if this is lost/stolen/damaged?
- Remote access – only store the bare minimum locally?
- BYOD – what implications does this have?

Procedures for secure disposal

- How should we securely dispose of data?
  - Many cases where data has been retrieved from hard drives after resale.
  - Secure delete by overwriting data with random data multiple times.
  - Better yet, physically destroy the disk! *(Recent price drops make this more feasible).*
  - Printed data should also be shredded
  - Avoid ‘dumpster divers’.

Summary

- How can we maintain physical security?
- Processes and policies for physical security?
- Security policy exists to instruct how to manage security, and how to prevent vulnerabilities that can be exploited.

Tutorial: Physical and Environmental Security

- What are the physical security measures required to protect our organisation?
- What are the potential social engineering attacks that our organisation should protect against?
- How can we represent these within our ISMS?
- How can we ensure that these procedures are followed?