ACS-2821-001
Information Security in Business

Physical Security Control

ACS-2821-001 – Slides Used In The Course

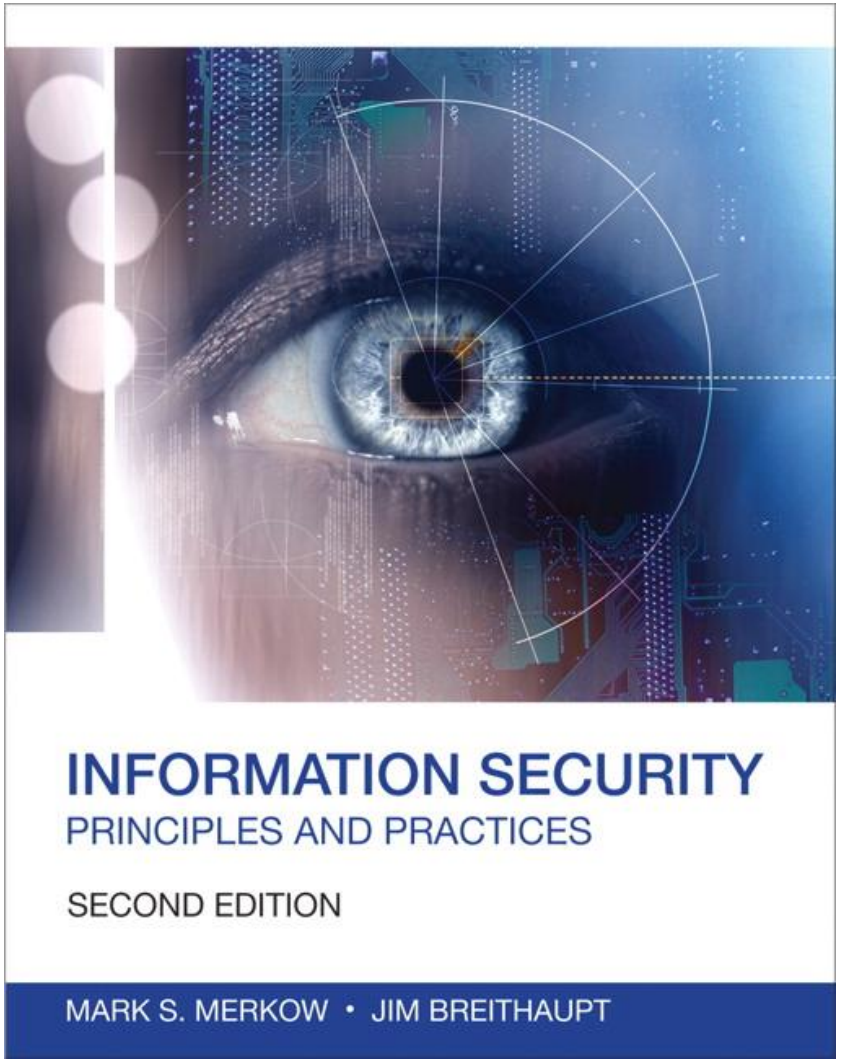
THE UNIVERSITY OF WINNIPEG

A note on the use of these slides:

These slides has been adopted and/or modified from the original for the use in this course. The author of the text have make these slides available to all (faculty, students, readers) and they obviously represent a *lot* of work on their part.

In return for use, please:

- If slides are being used (e.g., in a class) that the source be mentioned (after all, the author like people to use our book!)
- If any slides are being posted on a www site, note that they are adapted from (or perhaps identical to) the author original slides, and note their copyright of this material.



Objectives

- Distinguish between logical and physical security, and explain the reasons for placing equal emphasis on both
- Recognize the importance of the Physical Security domain
- Outline the major categories of physical security threats
- Classify the techniques to mitigate risks to an organization's physical security
- Classify the five main categories of physical security controls
- Identify how to use smart cards for physical access control
- Categorize the different types of biometric access controls and determine their respective strengths and weaknesses

Overview

- To protect logical systems, the hardware running them must be physically secure
- Physical security deals with who has access to buildings, computer rooms, and the devices within them

Understanding the Physical Security Domain

- Four focus areas
  - How to choose a secure site (location) and guarantee the correct design
  - How to secure a site against unauthorized access
  - How to protect the people and property within an installation
  - How to protect equipment against theft

Physical Security Threats

- **Weather**: Tornadoes, hurricanes, floods, fire, snow, ice, heat, cold, humidity, and so forth
- **Fire/chemical**: Explosions, toxic waste/gases, smoke, and fire
- **Earth movement**: Earthquakes, and mudslides
- **Structural failure**: Building collapse because of snow/ice or moving objects (cars, trucks, airplanes, and so forth)
- **Energy**: Loss of power, radiation, magnetic wave interference, and so forth
- **Biological**: Virus, bacteria, infestations of animals or insects.
- **Human**: Strikes, sabotage, terrorism, and war

Providing Physical Security

- Five Areas of Physical Security
  - Educating personnel
  - Administrative controls
  - Physical security controls
  - Technical controls
  - Environmental/Life-safety control

Educating Personnel

- An educated staff is the best weapon a company can have against illegitimate and accidental acts by others
  - Being mindful of physical and environmental considerations required to protect the computer systems
  - Adhering to emergency and disaster plans
  - Monitoring the unauthorized use of equipment and services
  - Recognizing the security objectives of the organization
  - Accepting individual responsibilities associated with their own security as well as the equipment they use

Administrative Access Controls

- Restricting Work Areas
- Escort Requirements and Visitor Control
- Site Selection
  - Visibility
  - Locale considerations
  - Natural disasters
  - Transportation

Physical Security Controls

- Perimeter Security Controls
  - Controls on the perimeter of the data center are designed to prevent unauthorized access to the facility
- Include gates, fences, turnstiles, and mantraps
- Badging
  - The photo identification badge is a perimeter security control mechanism that not only authenticates an individual but also continues to identify the individual while inside the facility
- Keys and Combination Locks
  - Keys and combination locks are the least complicated and least expensive devices

Physical Security Controls

- Security Dogs
  - Dogs are a highly effective and threatening perimeter security control when handled properly and humanely
- Lighting
  - Lighting is another form of perimeter protection that discourages intruders or other unauthorized individuals from entering restricted areas

Technical Controls

- The more prominent technical controls include
  - Smart/Dumb cards
  - Audit trails/access logs
  - Intrusion detection
  - Biometric access controls

Technical Controls

- Smart Cards
  - Similar to a credit card but it has a semiconductor chip
  - The smart card has many purposes
    - Storing value for consumer purchases
    - Medical identification
    - Travel ticketing and identification
    - Building access control
  - The smart card can facilitate file encryption and digital signature
  - The use of smart cards with biometrics authentication can be extremely effective

Technical Controls

- Audit Trails/Access Logs
  - Should contain
    - The user ID or name of the individual who performed the transaction
    - Where the transaction was performed
    - The time and date of the transaction
    - A description of the transaction—what function did the user perform, and on what
  - The retention period of the audit logs, recovery time, and the integrity of the data must also be considered and the logging system designed appropriately.

Technical Controls

- Intrusion Detection
  - Perimeter intrusion detectors
    - These devices are based on dry contact switches or photoelectric sensors. An alarm is set off when the switches are disturbed or the beam of light is broken
  - Motion detectors
    - These devices detect unusual movements within a well-defined interior space, including
    - Wave pattern detectors that detect changes to light-wave patterns
    - Audio detectors that passively receive un-usual sound waves and set off an alarm

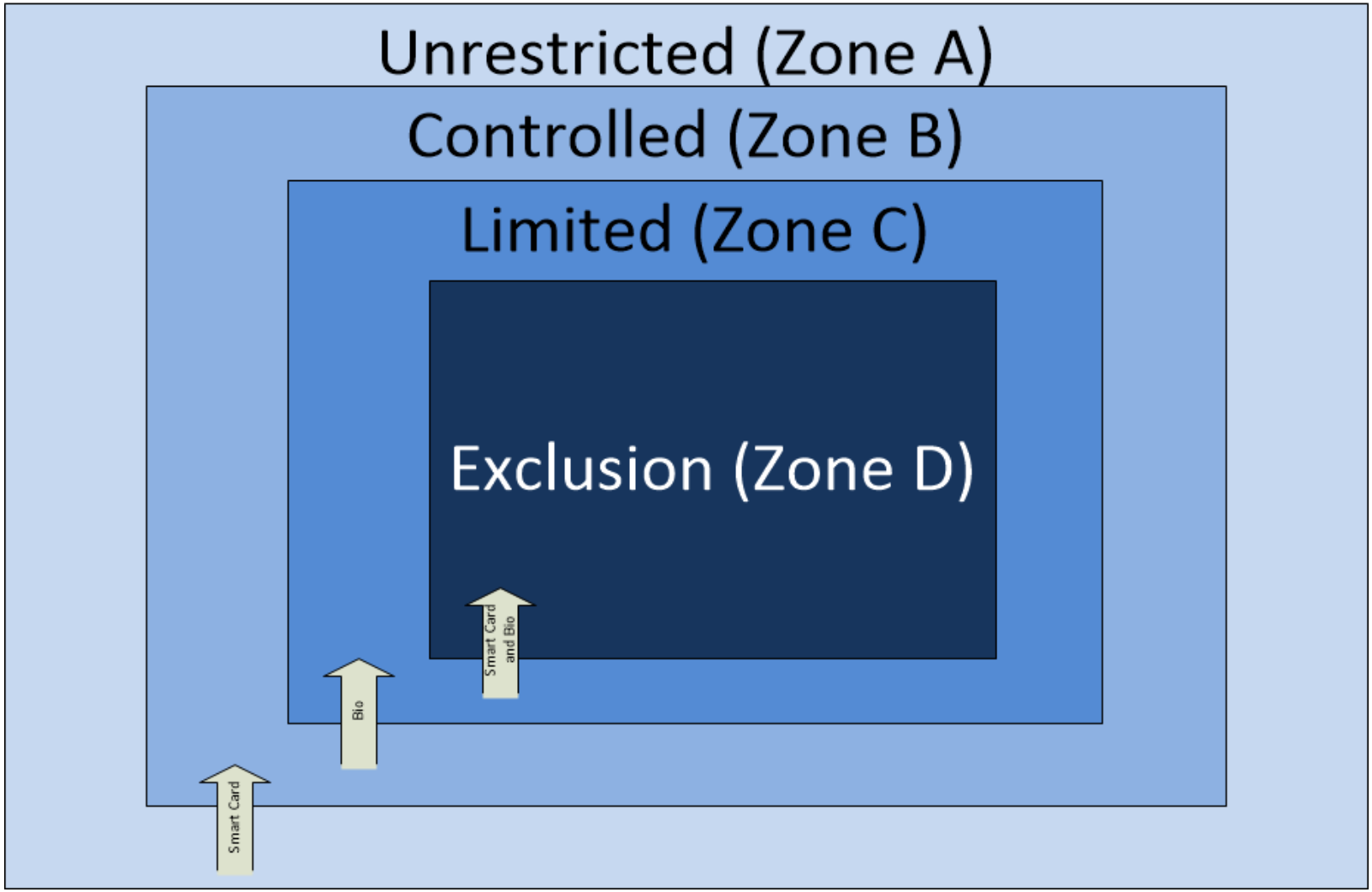
Technical Controls

- Alarm systems
  - Sets off an alarm to alert guard on the premises or in a remote location
- Biometrics
  - Biometrics authentication uses physiological or behavioral characteristics such as the human face, eyes, voice, fingerprints, hands, signature, and even body temperature
  - Biometric is data stored and used for the authentication procedure

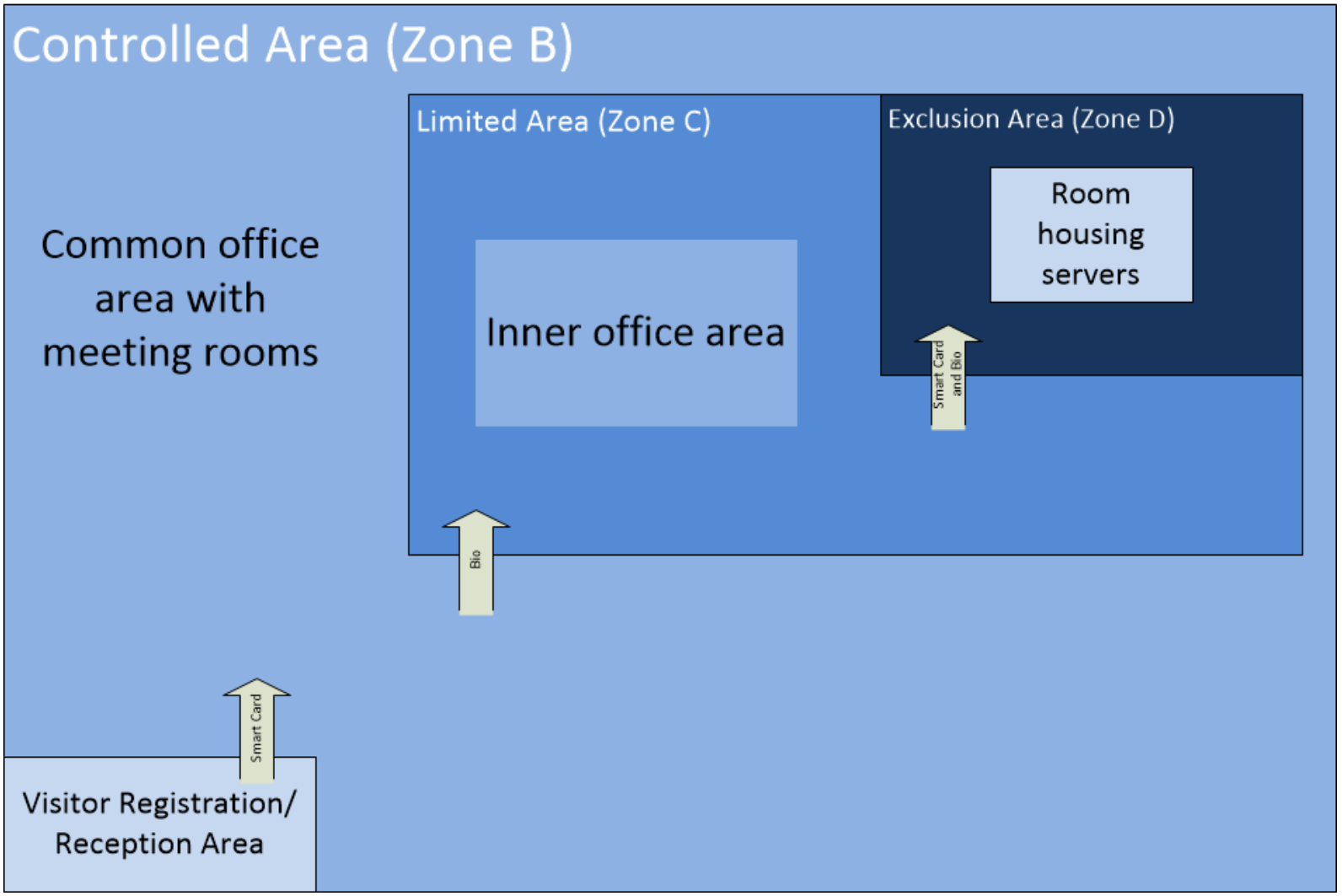
Environmental/Life-Safety Controls

- The three most critical areas are
  - Power (electrical, diesel)
  - Fire detection and suppression
    - Fire types
    - Fire detectors
    - Fire-extinguishing systems
  - Heating, ventilation, and air conditioning (HVAC)

Physical and Logical Access Control



Physical and Logical Access Control



Eli Lilly Warehouse Heist

Date: March 14, 2010
Time: Late Saturday/Early Sunday
Location: Enfield, CT
Value: $76 million
Drugs Stolen: Prozac, ADHD treatment Stattera, Cymbalta, Zyprexa, Gemzar, Alimta, Efient

- The thieves vaulted over a wall, climbed onto the roof of the warehouse and the then cut a hole in the roof. They rappelled down into the warehouse, disabled the alarm, and worked for a couple of hours loading trucks before taking off with the stolen goods.
- The alarm system was believe to be top of the line.
- An insider helped to provide them a security and floor plan.
- The thieves plan this heist for months doing reconnaissance outside the warehouse.
- The warehouse was located in a country side.
- There were no sign indicating that it was the company's warehouse.
- No gates, fences or walls around the warehoused.
- No physical guards was posted at the ground.

Summary

- Physical security is often underemphasized by security experts when discussing strategies for protecting critical resources
- Physical security domain includes traditional safeguards against intentional and unintentional threats
- Physical security addresses the following areas
  - Educating personnel
  - Administrative controls
  - Physical controls
  - Technical controls
  - Environmental/Life-safety controls

ACS-2821-001 – Questions?