UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Chapter 10

Always A Pioneer, Always Ahead

Elements of Physical Security

Dr Zaheera Zainal Abidin
zaheera@utem.edu.my

MyUTeM

OVERVIEW

- Introduction
- Combination of Physical Security with Existing Information Security
- Physical Security as a Data Center and Mission-Critical Facility
- Physical Security as a Controlled Access and Layered Defense
- Computing Facility based Physical Security
- Conclusion

INTRODUCTION

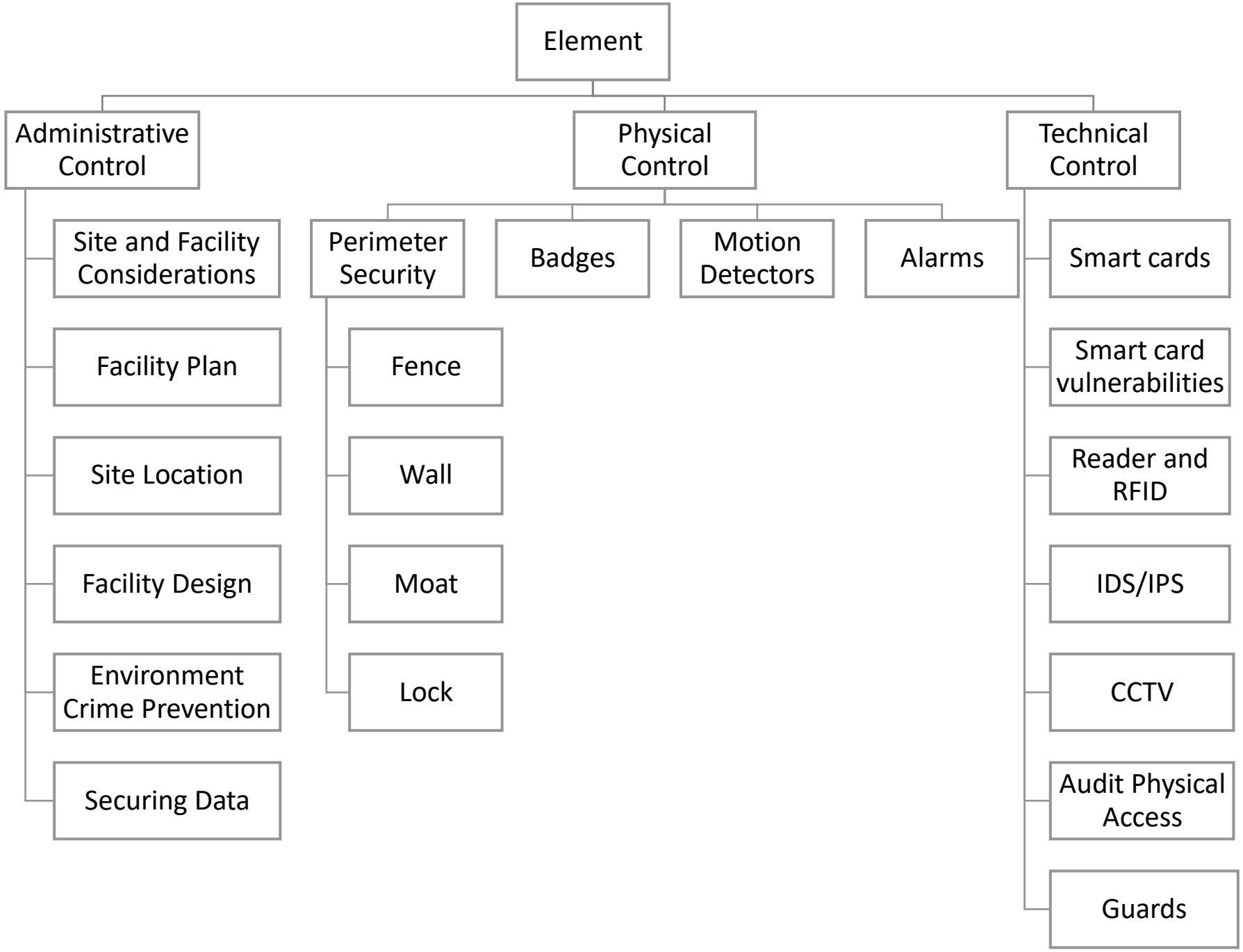
ELEMENTS OF PHYSICAL SECURITY

- What Elements of Physical Security means?
  - Lecture 10 teaches on the crucial elements needed in the implementation of physical security system in organizations.
- Why does Elements of Physical Security so important in a company?
  - If the implementation of physical security is not properly done in the organization, the company could face civil or criminal penalties for negligence due to not using proper security controls and not follow the security standards.

ELEMENTS OF PHYSICAL SECURITY

- What is the element?
  - The element of physical security follows the 3 category of Information Security Control in Lecture 3 that is Administrative Control, Technical Control and Operational Control. Recall from Lecture 3, which explains the definition and function of each category of Information Security Control. However, in this lecture, the element needed for 3 categories are discussed.
  - For example, the operational control in an organization or premise has is fence that comes in various shapes, sizes and heights. Thus, fence is the element of physical security under operational control.

MyUTeM



Reference: David Hutter and Manuel Santander, Physical Security and Why It Is Important, SANS Institute, (2016), pp. 1-30.

Administrative – Site and Facility Considerations

- A holistic control to protect the physical environment depends on layers such as first layer of defense is administrative, technical and physical security. Meanwhile, the last layer is the employee.
- Need a data centre to apply, sustain and monitor people, IT infrastructure and operations (Stewart, J., Chapple, M, and Gibson, D., 2012).

Administrative – Facility Plan

- A critical path analysis uses a systematic approach that identifies relationships between processes, operations, and applications.
- Recourses require security identification plan.
- Critical path analysis is the first stage securing the IT infrastructure. IT infrastructure includes computers, servers, networking equipment, water, electricity, climate control, and buildings.
- It is necessary to strategize how the older legacy systems and the new systems will merge together. The integration of old and new systems is called technology convergence.

Administrative – Site Location

- Geographical location, price, and size are factors that involve thought when purchasing a site location. Security requirements should always be the primary concern when determining a location. Buying an existing facility or building a new one also needs to be considered.
- It is important to take into account that looting, riots, vandalism, and break-ins can occur (Stewart, J., Chapple, M., & Gibson, D., 2012).
- Accessibility to the site is important. Road access, traffic, and distance to train stations, freeways and airports are important aspects.
- Geographical areas prevalent to natural disasters are not ideal site locations.

Administrative – Facility Design

- The security analyst needs to learn the basic infrastructure of a building and study for issues before constructing a site. Example, green building concept, using solar power for electricity, energy safe premise and less carbon printed building for sustainability and optimum use of resources.
- In the planning design, security analyst should think of unauthorised entry for visitor, the lift design (for staff and visitor), emergency evacuation, meeting place when fire and safety measures.
- The materials and process of implementation the security procedures must follow the standards. For example, the hinge durability, door opening direction, locks needed, glass requirements, ceiling must be fire-resistance, windows selection approval, flooring and HVAC specifications.

Administrative – Environmental Crime Prevention

- Crime prevention through environmental design (CPTED) attempts to reduce crime utilizing facility construction, environmental elements, and procedures to modify human behavior.
- An example of CPTED is mission critical servers located near an exterior wall should be moved in case of external force to the middle of the building where there is less chance of impact.

Administrative – Securing Data

- Data centers and server rooms that house IT or communications equipment must be off limits to unauthorized individuals. These rooms have to be locked down to prevent attacks.
- These rooms should be protected and have limited access to those employees that require access for job duties. The more human-incompatible these rooms are, the less likely attacks are executed.
- Oxygen displacement, extremely dim lighting, cold temperatures and hard to maneuver due to little space, are methods used in creating a human inhospitable environment. These data center rooms store mission critical equipment and should be located in the middle of the facility and not in the basement, ground or top floors.

Physical – Perimeter Security

- To implement the physical security in the organization, the security analyst plans for developing the mantraps, gates, fences and turnstile at the outside of the facility that creating an additional layer of security for someone accessing the building.

Physical – Badges

- The security analyst must design the registration procedure and approval method to determine that the visitor or employee carry the true identity.
- After the approval of identity has been made, then only badge or identification card (ID) is given to the individual to access the building.
- A continues monitoring of movement system on employee or visitor need to be implemented in the organization to observe the pattern movements.

Physical – Motion Detectors

- Infrared motion detectors observe changes in infrared light patterns. Heat-based motion detectors sense changes in heat levels. Wave pattern motion detectors use ultrasonic or microwave frequencies that monitor changes in reflected patterns.
- Capacitance motion detectors monitor for changes in electrical or magnetic fields.
- Photoelectric motion detectors look for changes in light and are used in rooms that have little to no light. Passive audio motion detectors listen for unusual sounds.

Physical – Alarms

- Alarms monitor various sensors and detectors. These devices are door and window contacts, glass break detectors, motion detectors, water sensors, and so on. Status changes in the devices trigger the alarm. In hardwired systems, alarms notice the changes in status by device by creating a wiring short. Types of alarms are deterrent, repellant, and notification.
- Repellant alarms utilize loud sirens and bright lights in the attempt to force attackers off the site.
- Notification alarms send alarm signals through dial-up modems, internet access or GSM (cellular) means. The siren output may be silenced or audible depending on if the organization is trying to catch criminals in the act.

Technical – Smart Cards

- Smart cards come in two types, contact and contactless. Contact smart cards have a contact point on the front of the card for data transfer. When the card is inserted, fingers from the device make a connection with chip contact points. The connection to the chip powers it and enables communication with the host device.
- Contactless smart cards use an antenna that communicates with electromagnetic waves. The electromagnetic signal provides power for the smart card and communicates with the card readers.

Technical – Smart Card Vulnerabilities

- Malicious individuals are encouraged to steal valuable information that can be compromised. Attackers attempt to bypass smart card vulnerabilities by various methods including fault generation, side-channel attacks, software attacks and micro probing.
- Side-channel attacks expose data about how the smart card works without cracking it.
- The attacker observes how the device reacts to diverse situations making it a stealthier approach to uncover data. The attacker gathers information about the card through timing, differential power analysis, and electromagnetic analysis. Timing verifies the duration that the process takes to finish.
- Micro probing is a more intrusive attack because it involves connecting probes to the access token card microchip and interacting directly with it the internal parts.

Technical – Readers and RFID

- Access control systems use proximity readers to scan cards and determines if it has authorized access to enter the facility or area. Access control systems evaluate the permissions stored within the chip sent via radio frequency identification RFID. This technology utilizes the use of transmitters (for sending) and responders (for receiving).
- Two types of RFID: Active and Passive. Active means active tag contains self-power batteries and passive relies on the reader to scan and capture the information in the RFID tag.
- Readers can track movements and locate items when connected to the network and detection systems. If an asset is removed from certain areas, the organization can have the access control system trigger an alarm.

Technical – Intrusion Detection, Guard & CCTV

- IDSs are essential to security because the systems send a warning if a specific event occurs or if access was attempted at an unusual time.
- Guards are a significant part of an intrusion detection system because they are more adaptable than other security aspects.
- While making rounds, guards can verify doors and windows are locked, and vaults are protected. Guards may be accountable for watching IDSs and CCTVs and react to suspicious activity. They can call for backup or local police to help capture a suspect if necessary.
- Closed-circuit television or surveillance systems utilize cameras and recording equipment to provide visual protection. In areas that cameras monitor, having enough light in the right areas is essential. It might be too dim for the camera to capture decent video quality necessary to prosecute or identify persons of interest without enough light

Technical – Audit Physical Access

- Auditing physical access control systems require the use logs and audit trails to surmise where and when a person gained false entry into the facility or attempted to break-in.
- The software and auditing tools are detective, not preventive. Consistent monitoring of audit trails and access logs are needed to act swiftly. The system has no value if the organization does not respond or response time is limited. Management needs to know when there are incidents so they can make security decisions.
- Adding additional resources to particular areas or at certain times might be necessary to protect the environment. Access logs and audit trails must include the date and time that the incident occurred. These logs should capture all failed access attempts, the person's employee information, and location where the attacker tried to gain entry.

A COMBINATION OF PHYSICAL SECURITY WITH EXISTING INFORMATION SECURITY OR CONVERGENCE OF PHYSICAL SECURITY

COMBINATION OF PHYSICAL SECURITY WITH THE EXISTING SECURITY SYSTEM

- The combination of physical security with cyber security
- The combination of physical security with Internet-of-Things
- The combination of physical security with cloud
- The combination of physical security with RFID and biometrics
- The combination of physical security with merging security systems and technology
- The combination of physical security with policy and procedure

Life and Environmental Safety

- The most important element physical security is protecting human life. Physical security must always be taken seriously to facilitate and prevent injuries to employees and protect the basic environmental elements at site location. Element of life and environment safety are:
  1. Employee Safety and Privacy
  2. Power and Electricity – Noise, Temperature, Humidity and Static Electricity
  3. Water
  4. Fire Prevention, Detection, and Suppression – Fire Extinguishers, Fire Detection System, Water Suppression Systems, Gas Discharge system, and damage.

Privacy and Legal Requirements

- Organizations must abide by laws and regulations that govern in the industry and jurisdiction they located. The company should practice due diligence to protect lives. If proper due diligence concerning physical security is not enforced by organizations, civil and criminal lawsuits could be filed.
  1. Protection of Privacy
  2. Legal Requirements

PHYSICAL SECURITY AS A DATA CENTER AND MISSION-CRITICAL FACILITY

DATA CENTER AND CRITICAL FACILITY

- Data center security procedures maybe considerably more complex than those for other areas such as wiring and cabling located outside the data centers.
- Data center security procedures usually contain technical terminology that needs to be checked for accuracy.
- Extra levels of security are necessary for sensitive documents or critical types of equipment within the data center.

PHYSICAL SECURITY AS A CONTROLLED ACCESS AND LAYERED DEFENSE

PHYSICAL SECURITY - ACCESS CONTROL

- The access control in physical security involves the concept of availability, integrity and confidentiality.
- Availability is ensuring access to the data when needed.
- Integrity implies that the data has been unmodified; thus, access to change the data is limited to only authorized persons or programs.
- Confidentiality implies that the information is seen only by those authorized. Thus, confidentiality is controlling access to read the data. All of these concepts are different aspects of controlling access to the data. In a perfect world, one could equate assurance with the degree of control one has over access.

PHYSICAL SECURITY - LAYERED DEFENSE

- A layered defense boosts the confidence level in access controls by providing redundancy and expanded protection.

- However, the IT security specialist should be able to evaluate the benefits of a layered defense and the security it will and will not provides.

COMPUTING FACILITY BASED PHYSICAL SECURITY

PHYSICAL BASED COMPUTING FACILITY

- Cloud Computing
  - Large computing facilities of IT giants (Amazon, Google) found that offering their computing capabilities as a service provided opportunities to better utilize their infrastructure.
  - Clouds are characterized by the fact of having virtually infinite capacity, being tolerant to failures, and being always on, as in the case of mainframes.
  - The network security engineer needs to integrate the available cloud infrastructure with the new implementation of physical access control in the organization.

CONCLUSION

Conclusion

- The design and analysis of the integration of new elements from physical security must be clearly planned and implemented in a converged infrastructure to prevent cyber crimes. An excellent performance of security services and application is vital.
- Responsible employees are the most important talent that physical security has to be safeguarding. To be able to accomplish this, basic facility needs such as, food, water, electricity, and temperature control must be available at all times. Employee safety and job satisfaction should always be the top priority and then comes the facility security.

Thank You

MyUTeM

www.utem.edu.my