Physical security

Dr. Talal Alkharobi

Physical security

- Describes measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media.
- It can be as simple as a locked door or as elaborate as multiple layers of armed guard posts.

Elements of Physical security

3

- Prevent
- Detect
- Response
- Recover

Dr. Talal Alkharobi

Prevent

4

- Placing obstacles to frustrate trivial attackers and delay serious ones

Dr. Talal Alkharobi

5

Detect

- alarms,
- security lighting,
- security guard patrols
- closed-circuit television cameras

6

Response

- To repel, catch or frustrate attackers when an attack is detected

7

Recover

- Actions necessary to restore data files of an IS and computational capability after a system failure.
- Disaster recovery plan
- Backup
- Fault-tolerant

8

Elements of Physical security

- In a well designed system, all elements must complement each other.
- The response force must be able to arrive on site in less time than it is expected that the attacker will require to breach the barriers;

9

Physical security

- Persuading attackers that the likely costs of attack exceed the value of making the attack.
- Example:
  - ATMs (cash dispensers) are protected, not by making them invulnerable, but by spoiling the money inside when they are attacked.
  - Attackers quickly learned that it was futile to steal or break into an ATM if all they got was worthless money covered in dye.

10

Physical security

- Safes are rated in terms of the *time* in minutes which a skilled, well equipped safe-breaker is expected to require to open the safe.
  - The time between inspections by a patrolling guard should be less than that *time*, or
  - Alarm response force should be able to reach it in less than that *time*.

11

Physical security

- Hiding the resources, or hiding the fact that resources are valuable, is also often a good idea as it will reduce the exposure to opponents and will cause further delays during an attack, but should not be relied upon as a principal means of ensuring security

Dr. Talal Alkharobi

12

security through obscurity

- Using secrecy (of design, implementation, etc.) to ensure security.
- A system relying on security through obscurity may have theoretical or actual security vulnerabilities, but its owners or designers believe that the flaws are not known, and that attackers are unlikely to find them.

Dr. Talal Alkharobi