Site and Facility Secure Design

Evan Morgan, CISSP, CISM

@1evanski www.evanski.com

Overview

Discuss how physical security improvements can improve your organization's overall security posture (both physical and logical)

This is the 10th and 11th objectives of the Security Engineering domain of the CISSP® Exam

Strong information security cannot exist without strong physical security

Before using a physical site for technology assets, a security survey should be performed

A security survey helps identify threats to the facility and vulnerabilities the facility has, along with what can be done to mitigate them

Probability of a threat being realized, and the consequences for its realization are important to understand for the development of effective controls

Once threats are identified, vulnerabilities can be addressed

Physical security controls must exist in balance with effective organization operations

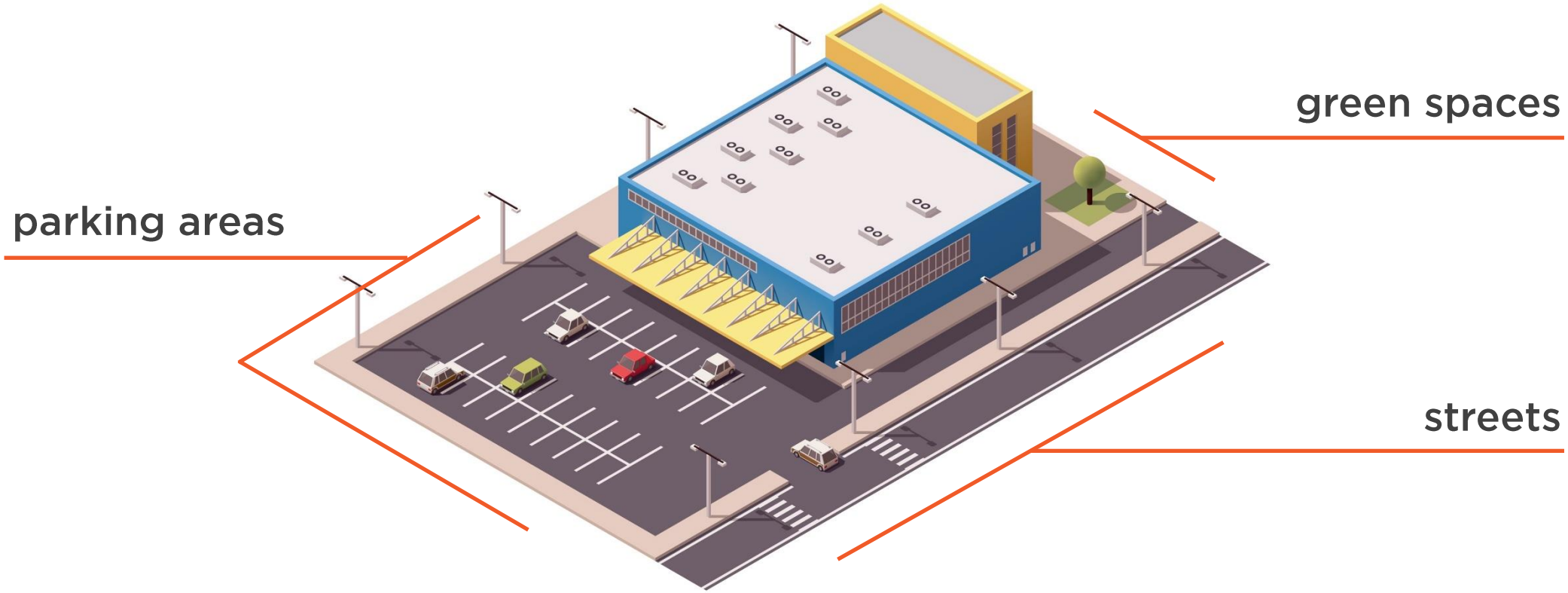
Cost of controls vs. value of assets should also be considered when developing controls

CPTED

Crime Prevention Through Environmental Design

— Reduce crime potential through environmental design

Design Environment Scope



Underlying idea is to not make a facility look like a fortress, but still have the same security value

Example: New Zealand's Ministry of Justice

Use security glass instead of bars

Adding thorny shrubbery to fences to increase aesthetics and security

Use different shutters with security value than industrial rolling shutters

Depending on your organization's industry, there may be specific physical security requirements that must be put in place

Resources and Guidance

Federal Emergency Management Agency (FEMA)

- Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks (FEMA 427)
- A How-To Guide to Mitigate Potential Terrorist Attacks (FEMA 452)
- Safe Rooms and Shelters: Protecting People Against Terrorist Attacks (FEMA 453)

The American Institute of Architects

Security Concerns from American Institute of Architects

1. Facility security control during and after hours of operation
2. Personnel and contract security policies and procedures
3. Personnel screening
4. Site and building access control
5. Video surveillance, assessment, and archiving
6. Natural surveillance opportunities
7. Protocols for responding to internal and external security incidents
8. Degree of integration of security and other building systems
9. Shipping and receiving security

Security Concerns from American Institute of Architects

10 Property identification and tracking

11 Proprietary information security

12 Computer network security

13 Workplace violence prevention

14 Mail screening operations, procedures, and recommendations

15 Parking lot and site security

16 Data center security

17 Communications security

18 Executive protection

19 Business continuity planning and evacuation procedures

Key Facility Protection Points

Access Control to and Within the Facility

Support Equipment Rooms

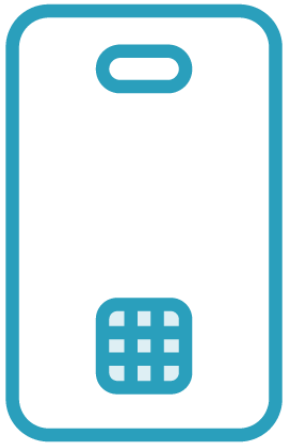
Server and Technology Component Rooms

Restricted Work Areas

Facility Access

the first control point before anyone can access your controlled environment

Examples of Facility Access Security



Electronic Key Card

Posted Guard

Receptionist

Support equipment rooms

house all of the components needed to support operations

Example Support Equipment Rooms

Electrical Power

Uninterruptible Power Supplies (UPS)

HVAC and Generator Inputs

Telecommunications

Networking Equipment

Additional support equipment, such as the generators and HVACs themselves will most likely be placed outside of the facility itself, but should be protected from tampering

Server Room

Contains all of the main technology components that make up the technology operations of a facility.

(essentially the core of the datacenter)

Controls Typically Found in Datacenters

Fire Detection and Suppression

Water Detection

Electrical Power Continuity

Lightning Protection

HVAC Continuity

Restricted Work Areas

Security Operations work areas

Human Resources work areas

Sensitive Compartmented Information Facility (SCIF)

SCIFs

Designed to allow for consistent operations within a contained area within a facility that is more sensitive than the rest of the facility

(e.g., Secret level facility with Top Secret SCIF)

SCIFs also have numerous physical construction requirements to be certified as a SCIF

Summary

Discussed how physical security improvements can improve your organization's overall security posture (both physical and logical)

This is the 10th and 11th objectives of the Security Engineering domain of the CISSP® Exam

What's Next?

If you've reviewed all of the other modules and their clips then...

You're done with this course!

If you're looking for additional information on the CISSP® then feel free to watch the other courses on the topic

As well as, watch any other relevant security or IT courses