Topic 3
Physical Security

Dr Diarmuid Ó Briain

2 Oct 2024

Licence

Learning objectives

By the end of this topic you will be able to:

- Compose a secure facility plan
- Integrate physical access controls into a secure facility plan
- Formulate a plan for physical security controls as part of a secure facility plan
- Incorporate environmental and safety concerns into a secure facility plan

---

Site facility and design

- Group exercise

- In terms of site facility and design for a small Manufacturing Plant making widgets, consider the:
  - Location
  - Threats

5

Site & Facility Design

- **Location**
  - Emergency Services
  - Hazards and threats
  - Adjacency to services
    - Power
    - Fibre
    - Height for radio
    - Water

- **Threats**
  - Fire
  - Water and flooding
  - Storms
  - Vandalism
  - Sabotage
  - Explosions
  - Building failure, collapse
  - Utility failure and continuity
  - Equipment failures
  - Access
  - Strikes

Secure Facility Plan

- Planning process:
  - What are we securing against?
  - What levels of security do we need and are we willing to provide?
- List of threats
- Systematically relate the company applications with all the possible threats to it
  - A Database Server will require, hardware, software, power, temperature control
  - Critically analyse any dependencies for this server, what if the electricity goes down, what if the hardware overheats

Physical Security Controls

- **Physical Group**
  - Walls
  - Fences
  - Gates
  - Locks
  - Lighting
  - Guards
  - Guard dogs

- **Administrative Group**
  - Site Management
  - Personnel Access Controls
  - Security Training
  - Procedures in the event of security breaches

- **Technical Group**
  - Intrusion detection systems
  - Alarms
  - CCTV
  - Fire detection
  - Fire Suppression

Server rooms

- Enclosed
- Restricted
- Protected rooms
- Mission critical equipment in controlled environment
  - Temperature
  - Humidity
- Fire detection and extinguishing systems
  - Halon type oxygen displacement

Work areas

- Designed to prevent shoulder surfing
  - Act of gathering info by watching a monitor and keyboard
- The level of access an employee has should determine the work area they have
- High level access employees work area not in proximity of level access employees

Physical Access Controls - Fence

Physical Access Controls - Fence

- First line of defence
- Fence guidelines:

  - 1 metre   Deter casual trespassers
  - 2 metres   Hard to climb easily
  - 2.5 metres   Delay determined intruders

- Planning laws in locality
  - May impact the type or look of the fence in plan
- A grass or gravel clearway deter vehicles from parking
- Bollards

Physical Access Controls - Fence

- **Access points**
  - These points can be a weakness in the first layer of defence
  - By their nature gates provide access through the fence and therefore should be afforded the appropriate management

Intrusion detection devices

- Photoelectric beams
- Ultrasonic
- Passive infrared
- Microwave
- Pressure sensitive pads

- The use of intrusion detection systems can be mixed, for example
  - Trigger audio or silent alarms or drown the area in light
- Consideration: the triggering of alarms by non intruders ie animals and birds

Light

- **Continuous Lighting**
  - Fixed lights should be installed 2.5 metres above ground
  - Light on the ground should be at least 2 lumens
- **Motion sensitive/trip lighting**
  - Sensor activated light can be both a good security deterrent and a cost effective alternative to continuous lighting
- **Standby lighting**
  - Lights that come on in the event of power failure
- **Exit lighting**
  - Lights to indicate the exit points

Closed Circuit Television (CCTV)

- CCTV equipment may be used to observe parts of a process from a central control room;
  - for example, the environment is not suitable for humans

- Points to consider when installing CCTV systems:
  - The ability to **detect** an object
  - The ability to **recognise** a detected object
  - The ability to **identify** object details

Security Guards

- Privately and formally employed person who is paid to protect property, assets, and people
- Is uniformed, overt and visible presence as a deterrent
- Practice:
  - *Detect*
  - *Deter*
  - *Observe*
  - *Report*
- Call on the Gardaí or police when necessary
- Perform access control at building entrances and vehicle gates

Access Logs

- Maintained either in paper form though more commonly in electronic form to record the comings and goings of non employees

Company: Date:

Name	Company	Name of person visiting	Security Guard	Time in	Time out

Perimeter Security - Doors

- Panels and glass protected against being kicked in or knocked out
- Install metal lining on exterior wooden doors to resist drilling or sawing
- Secure double doors with heavy duty, multiple-point, long flush bolts
- Make sure the frame is as strong as the door
- All exterior doors should be;
    - Constructed of steel, aluminium alloy, or solid-core hardwood
    - Minimum 15mm steel on side and rear doors
- Door frames should be securely fixed to the walls
- Glass doors should have burglar-resistant glass installed
- Doors should be secured with a minimum of 3 hinges
- Doors should be clearly lit
- Emergency doors should be clearly marked
- Doors provide entry and exit for emergencies like power failure
- Doors should have the same fire rating as the walls

Perimeter Security - Locks

- Exterior swinging doors should have a minimum 25mm deadbolt lock, 25mm throw bolt with a hardened insert, and free turning steel or brass tapered-cylinder guard
- Steel strike plates should be used on aluminium door frames
- Outside hinges should have non-removable hinge pins
- Electronic/Electrical Locks connected to an access control system, advantages which include:
    - Key control, where keys can be added and removed without re-keying the lock cylinder
    - Fine access control, where time and place are factors
    - Transaction logging, where activity is recorded

Electronic lock authentication methods

- Numerical codes, passwords and passphrases
- **Security tokens**
    - Cards
- **Biometrics**
    - Fingerprint
    - Retinal scanning
    - Iris scanning
    - Voice print identification

Padlocks

- The most common assaults on padlocks are made with bolt cutters or crowbars
- Quality padlocks should have the following features:
  - Laminated or solid body case
  - Hardened steel shackle with a minimum diameter of 8 mm
  - A double locking mechanism providing *heel and toe* locking, and at least 5 pin tumblers in the cylinder

Turnstiles (Baffle gate) or Man-trap

- Allows one person to pass at a time
- Can enforce one-way traffic
- Restrict passage to people with a security pass
- Patrons to enter single-file, so security have a clear view
- With mantraps when alarm, all doors lock
  - Suspect trapped between the doors in the *dead-space*
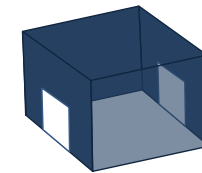
Windows

- **Light, ventilation, and visibility, but not easy access**
- **Locks**: Cannot be reached and opened by breaking the glass
- **First floor windows**: Protected with burglar-resistant glass, bars, grilles, grates
- **Plate Glass**: Most common type of glass found in windows It tends to shatter in shards when broken or subject to an explosion, a safety hazard
- **Tempered Glass**: Processed by controlled thermal or chemical treatments to increase its strength compared with normal glass
  - Does not shatter into shards when broken
- **Polycarbonate Glass**: Thermoplastic polymer moulded to look like glass and is the toughest glazing available

Environment and Safety - Power

- Power problem terms:
  - **Fault** – This is a momentary loss of power
  - **Blackout** – Complete loss of power
  - **Sag** – Lowering of the power supply voltage
  - **Brownout** – Prolonged period of low voltage
  - **Spike** – Momentary increase in voltage
  - **Surge** – Prolonged period of high voltage
  - **Noise** – A continuous power fluctuation
  - **Transient** – A short period of noise
  - **Ground** – Electrical earth
  - **Clean** – Continuous non fluctuating power
  - **Inrush** – Surge of voltage given initially after a device is connected to power

Uninterruptible Power Supply (UPS)

- Battery backup, emergency power source
- Unlike generator provides instantaneous power
- On-battery runtime can be relatively short 5 – 15 minutes being typical for smaller units
  - Sufficient to allow time to bring an auxiliary power source on line, or to properly shut down the protected equipment

Water and Fire

- A fire develops typically in four stages, and fire detectors are designed to detect some characteristic effect of one or more of these stages:

  - **Incipient stage**
  - **Smouldering/smoke stage**
  - **Flame stage**
  - **Heat stage**

Water and Fire – Fire triangle

O₂ | Fuel | Heat
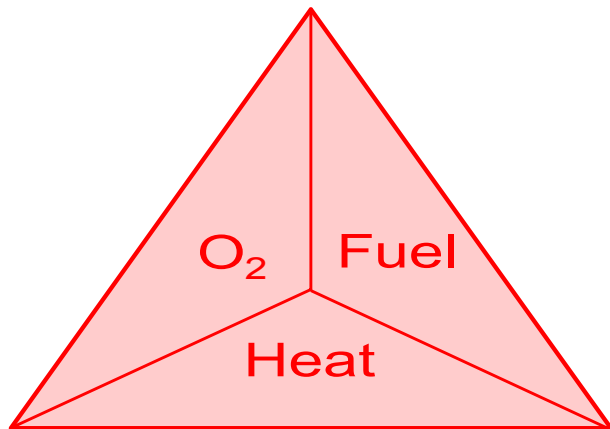
Fire management in data centres and labs

- Water ? electronic equipment ?
- Halon 1301 Gas was used in such environments
  - Damage the ozone layer
- The Montreal Protocol of 1987, limited the production of Halon 1301 to roles like aircraft emergency equipment where another alternative did not exist
- Halon 1301 replaced
  - Argon
  - Inergen

Fire management in data centres and labs

- **Halocarbon gases**
  - Remove heat from the fire
  - Evacuation necessary before the release of these agents
  - Lower storage space requirement compared to inert gasses
  - Fast fire suppression time (10sec)
  - Must be very near point of use (max 30m)
  - More expensive than inert gasses
- **Inert gases**
  - Lower the oxygen concentration in the room
  - Perform more effectively in rooms that aren't well sealed
  - More gas required than Halocarbon gasses
  - These can be piped long distances (100 – 200m) to a room and still retain their effectiveness

Pre-action sprinklers

- Pre-action sprinkler systems also are an option
- Water not retained in pipes which reduces the risk of leaks:
  - Valve located outside keeps water from entering
  - Smoke detector triggers and temperature threshold must be reached before water flows
  - Two trigger events reduces risk of an accidental leak

Water threat

- Water damage is a threat in itself:
  - Information systems
  - Paper records
- Water detection sensors that can trigger an alarm
- Raised floors to allow time for a water threat to be reacted to are common
  - though these are also used for conduits to carry room power and network cabling
- Water threats are another reason to place such rooms above ground level

Heating, Ventilating, and Air Conditioning

- Temperature and humidity control
- Positive Pressure:
  - Ensures that should there be any leakage it will be out and thus prevent any unwanted air in
  - Monitoring of air pressure by alarm system
  - Should the pressure change suddenly it is an indication of the possibility of unauthorised access
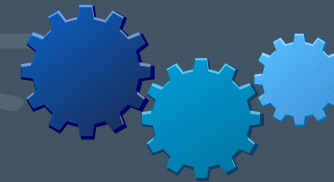
Learning objectives

You should now be able to:

- Compose a secure facility plan ✓
- Integrate physical access controls into a secure facility plan ✓
- Formulate a plan for physical security controls as part of a secure facility plan ✓
- Incorporate environmental and safety concerns into a secure facility plan ✓

Exercise #3

Scenario

TUS
Ollscoil Teicneolaíochta na Sionainne:
Lár Tíre, An tIarthar Láir
Technological University of the Shannon:
Midlands Midwest

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir
Sinsearach

E diarmuidobriain@tus.ie | W tus.ie
Campas Maoilis, Páirc Maoilis,
Luimneach, V94 EC5T, Éire

CEng, FIEI   CISSP®

Thank you

TUS