

School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 171 T1 2023

Ngā whakapūtanga o Te Haumarū rorohiko
Cybersecurity Fundamentals

Week 10 - Physical Security

Objectives

- Understanding the importance of physical security
- Looking for physical security vulnerabilities
- Implementing countermeasures for physical security attacks

What is Physical Security?

- *Physical security* is concern with the protection of physical property.
- It encompasses both **technical** and **nontechnical** components, both of which must be addressed.

Safety vs security

- **Safety** refers to the systems that react to/in abnormal events by minimising their impact, preserving human life, and protecting property.
 - **Examples:** Earthquake, fire, flood, and natural or human accidents.
- **Security** represents the systems that **prevent**, detect, alarm, delay and respond to, interrupt, and neutralise a malevolent human adversary.
 - **Examples:** Insider theft, direct attack, and material diversion.

Safety vs security (cont.)

Fail-Safe



Fail-Secure



Physical Protection System Integration Objectives

- Security—the layered “wrapper” around asset(s)
- Protection/Defense in depth
- Minimised consequences of component failure, e.g., power generation
- Balanced protection (equally bad choices)



Technology and security

“If you think technology can solve your problems, then you don’t understand the problems and you don’t understand the technology.”

—*Bruce Schneier*

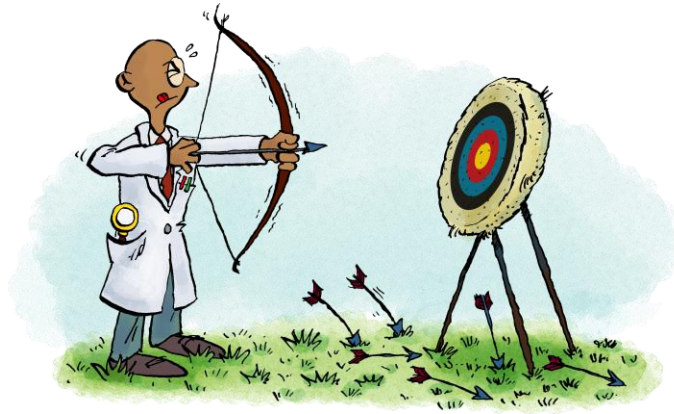
What is the problem?

- Physical security is an **often-overlooked** but critical aspect.
- Securing your information depends on your ability to physically secure your office, building, or campus.
- Regardless of your security technology, practically any **breach** is possible if an attacker is in your building or data centre.

Security focus

“Let us not look back in anger or forward in fear, but around in awareness.”

—*James Thurber*





PHYSICAL SECURITY VULNERABILITIES



Physical Security Vulnerabilities

- Depend on, *but not limited to*:
 - Size of building.
 - Number of buildings or office locations.
 - Number of employees.
 - Presence of a receptionist or security guard.
 - Location and number of building **entrance** and **exit** points.
 - Placement of server rooms, wiring closets, and data centres.

Assessing Your Organization's Physical Security

- Building infrastructure
- Utilities
- Office layout and use
- Network components and computers





BUILDING INFRASTRUCTURE



Attack Points

- Doors
 - Propped open
 - Gaps at the bottoms
 - Easy to force open
 - Hinges
 - Material
 - Look-through
- What is the building or data centre made of?
 - walls and entryways
 - slab-to-slab walls
 - how resilient the material is to earthquakes, tornadoes, strong winds, heavy rains, and vehicles driving into the building
- Windows
- Drop ceilings with tiles that can be pushed up

Countermeasures

- Strong doors and locks.
- Motion detectors.
- Cameras to discourage criminal activity
- Windowless walls around data centres.
- Signage that makes it clear what's where and who's allowed.
- A continuously monitored alarm system
- Lighting
- Entrances that allow only one person at a time
- Fences (with barbed wire or razor wire if necessary).



UTILITIES



Attack Points

- Power-protection
 - Surge protectors, generators, UPSes
 - On/off power switch
 - When the power fails
 - fail open
 - fail closed
 - Fire-detection and -suppression devices
 - Alarm sensors, extinguishers, and sprinkler systems
- position
 - accessibility (network and default login credentials)
 - Water and gas shutoff valves
 - Can you access them or a maintenance personnel is needed
 - Local telecom wires that run outside the building
 - aboveground,
 - buried,
 - on telephone poles

Countermeasures

- Major utility controls are placed
 - behind closed and lockable doors
 - fenced areas
 - out of the sight of people passing through or nearby
- Cameras with ample coverage
- Devices accessible over the network
 - tested
 - disable that feature if not needed
 - limit who can access the systems



OFFICE **LAYOUT** AND **USE**



Attack Points


- Main doors of the building
- Desks
- Mail and packages
- Trash cans and bins, recycling bins, and shredders (**dumpster diving**)
- Copy rooms and fax machines
- Network cameras and digital video recorders (**default settings**)
- Access controls on the doors
 - regular keys
 - card keys
 - combination locks
 - biometrics
- Keys and programmable keypad combinations



Countermeasures

- A receptionist or a security guard
- Make it policy for all employees to
 - **question** strangers
 - **report** strange behaviour
- A single entry and exit points to a data centre
- Place trash bins in secure areas.
- Use cameras to monitor critical areas
- Dispose of hard-copy documents in cross-cut shredders or secure recycling bins
- Limit the numbers of keys distributed
- Ensure that access is also logged and monitored
- Use electronic badges
- Use biometric identification systems





NETWORK COMPONENTS AND COMPUTERS



Attack Points

- Network
 - servers, firewalls, and routers
 - network diagrams
 - switches
- Computer
 - Passwords
 - Files
 - Installing network analyser software
 - accessibility
- Penetration drop boxes <https://video.link/w/T6vo>
- Contact lists
- Disaster recovery plans
- Laptops, mobile phones and tablets
- Sticky notes
- Backup media
- Safes (if used to store backup media)
- Cables and patch panel



Countermeasures

- Make your users aware of what to look out for
- Require users to lock their screens
- Ensure that strong passwords are used
- Laptops and PCs are locked to the desks
- Full disk encryption technologies for laptops
- Server rooms and wiring closets (locked and Monitored)
- Use modern access control systems instead of traditional door locks and keys
- Scan for rogue wireless access points, and shut them down
- Secure patch panels
- Use a bulk eraser on magnetic media and shred them **before they are discarded**



REMARKS



Remarks

- Detectors and responders
 - Human vs technology (automatic/manual)
- Multiple systems
 - Harder and stronger every level
- Do not make it too attractive
- Balanced security
- Secure your assets don't just hide them
- Think about other elements, e.g., birds, rain, and lightning strikes

Remarks (cont.)

- Understand the **motivations** of your attackers, e.g., sabotage and espionage
- Estimate the **number** of your attackers
 - One attacker, multiple roles
- What **tools** do they have or can get
 - How heavy are these tools?
- What **equipment** are you have at the facility?
- How much **knowledge** about your system do they have?
 - You must assume that they know everything
- Do people count as assets?
 - Patents

“We only need to be lucky once. You need to be lucky every time.”

—*The IRA to Margaret Thatcher*

What we covered...

- Discussed common physical security weaknesses.
- Outlined some low-cost countermeasures.