Eötvös Loránd University (ELTE)
Faculty of Informatics (IK)
Pázmány Péter sétány 1/c
1117 Budapest, Hungary

PHYSICAL AND PERSONNEL SECURITY

Introduction to Data Security

Imre Lendák, PhD, GICSP

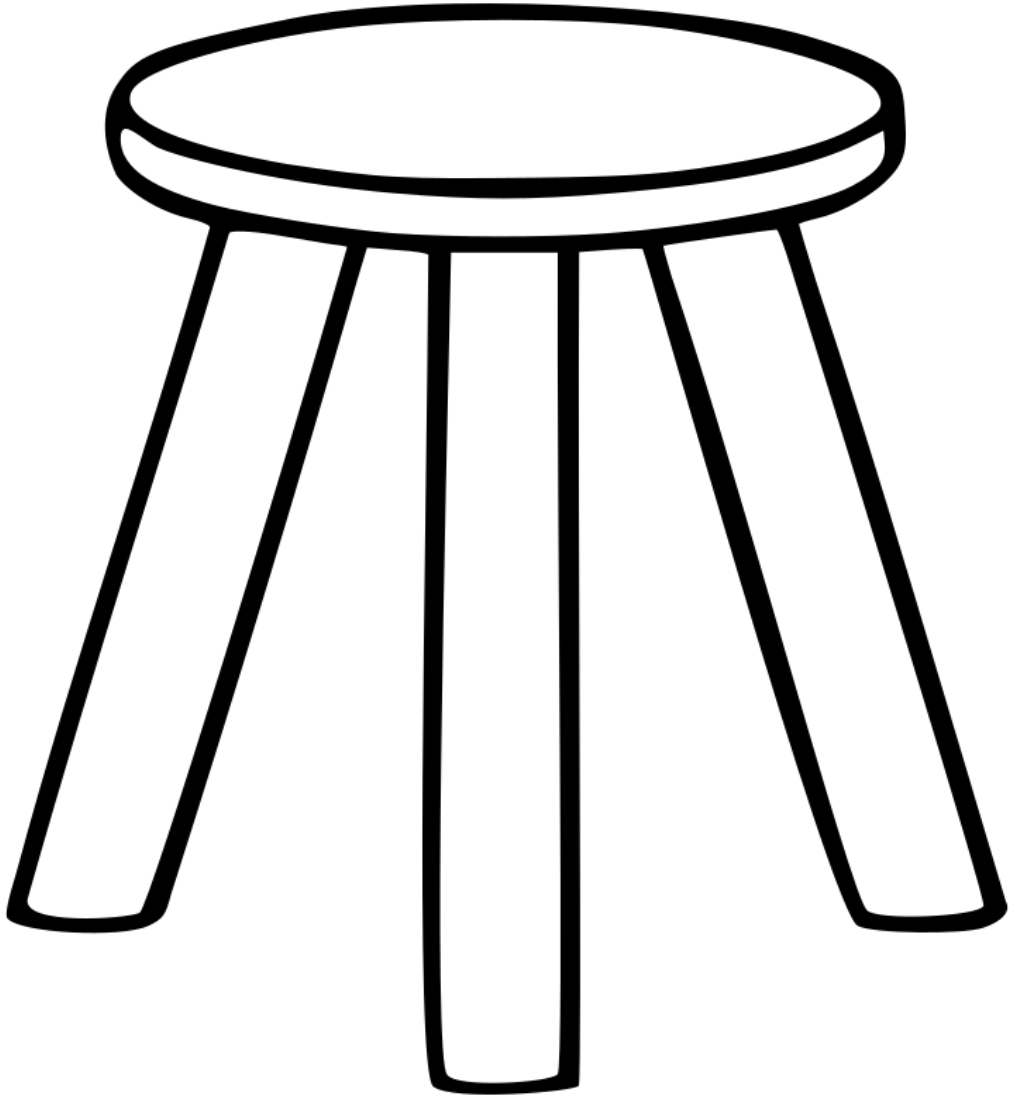
2025
Budapest, Hungary

Presentation outline

- Basic definition and data lifecycle
- Attackers and attack types
- Methods
- Physical security
  - Outside the facility
  - Physical access points
  - Inside the facility
  - Inside the control room
- Personnel security in brief

The CIA triad & CIA+AN

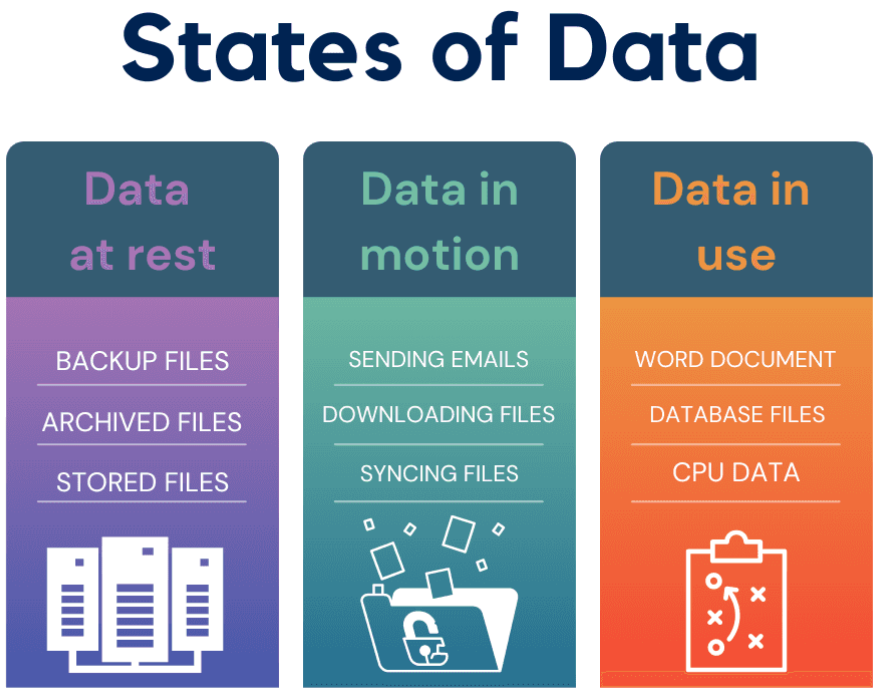
- **Confidentiality** = Authorized entities can access data & services
- **Integrity** = Authorized entities modify system configuration
  - **Discuss:** What is configuration in different contexts?
- **Availability** = Data and services are accessible within predefined time constraints
- +**Authentication** = Verify the identity of a user, process, or device
- +**Non-repudiation** = 3rd-party validation of message integrity and origin (from specific entity with key)



Additional key definitions

- Definitions based on the NIST Glossary
- **Cybersecurity** = Damage prevention, protection and restoration of information infrastructure and data to ensure its confidentiality, integrity, availability, authentication, and nonrepudiation.
- **Vulnerability** = Weakness in an information system (system security procedures, internal controls, or implementation) that could be exploited or triggered by a threat source.
  - TTP = Tools, Technology and Process
- **Threat** = Any circumstance or event with the potential to adversely impact an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service → Potential negative impact on the CIA of an information system.
- **Threat actor** = An individual or a group posing a threat.
- **Attack** = Malicious activity which attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself → Activity which negatively impacts CIA.
- **Risk** = A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of likelihood and impact.
- **Security control** = A safeguard or countermeasure prescribed for an information system, or an organization designed to protect information and meet security requirements.

Data in…



https://estuary.dev/data-in-motion/

- Data at rest
  - Storage (electronic, paper)
  - Cloud
  - Backup (we really need this!)
  - **Discussion:** anywhere else?
- Data in transit
  - Data communicated over critical information infrastructures
- Data in use
  - Data is loaded into RAM
  - Calculations are performed in a single or multiple physical or virtual computers (or containers)

Attackers and attack types

Adversaries

Adversary	Description (as defined in NIST IR 7628)
Nation states	State-run, well organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having an economic, military or a political advantage.
Hackers	A group of individuals (e.g., hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems or other flaws.
Terrorists / Cyberterrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands.
Organized crime	Coordinated criminal activities including cyber extortion, IP theft and other. Organized and well-financed criminal organization.
Other criminal elements	Other facets of the criminal community, which is normally not well organized or financed. Normally consists of a few individuals, or of one individual acting alone.
Industrial competitors	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments in the form of corporate espionage.
Disgruntled employees	Angry, dissatisfied individuals with the potential to inflict harm on critical infrastructures. This can represent an insider threat depending on the current state of the individual's employment and access to the systems.
Careless or poorly trained employees*	Those users who, either through lack of training, lack of concern, or lack of attentiveness pose a threat to a CI. This is another example of an insider threat or adversary.

Cyber attacks targeting individuals (2025)

- **Spam:** Unwanted email. Often contains malicious links or attachments. Countermeasures: anti-malware.
- **Online scams:** Nigerian prince and its novel variants. Countermeasures: check message source, follow trends.
- **Hijacking of electronic accounts:** Weak password or other vuln is used to hijack account. Countermeasures: multi-factor auth (MFA).
- **Ransomware:** Vuln is used to obtain access, encrypt files and request ransom for decode key. Countermeasure: training, backup.
- **Discussion:** Other?

Cyber attacks in business envs (2025)

- **Ransomware:** The same as against individuals, but potentially higher impact → higher ransom. Examples: UNIX, healthcare providers, Maersk.
- **Business account compromise:** Hijack and misuse business account(s) (e.g., send spam) → negative impact on business.
  - **Discuss:** Which?
- **Data breaches:** Trick employee to send data or exfiltrate after system breach.
  - **Discuss:** Often combined with ransomware. How?
- **Internet scams:**
  - **CEO fraud:** Attacker claims to be the CEO and instructs employee to perform unwanted action.
    - **Discuss:** Since ~2024 the use of deepfakes (audio, video) further aggravates this threat.
  - **Unwanted invoice actions:** Attackers inject unwanted invoices into legitimate exchanges and trick employees into transmitting funds to their accounts.
    - **Discuss:** Anybody heard about such attacks?
- **Supply chain attacks:** Adversary hacks a solution or hardware provider, introduces a vulnerability into a product (backdoor) which is subsequently delivered to a large public service organization or multinational company, allowing the adversary to gain the initial foothold easier
  - Examples: Solarwinds 2020, Kaseya 2021, Hezbollah pager attack 2024

ATTACK & DEFENSE METHODS

Cyber Kill Chain model

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions on Objectives

Stuxnet in a nutshell

- **Date:** June 2010 (detection)
- **Goal:** destroy nuclear fuel enrichment centrifuges via cyber attack
- **Motive:** hinder nuclear program via centrifuge destruction
- **Method:** cyber weapon → worm ~500kB, zero-day exploints, hard-coded passwords
- **Source:** (maybe) USA & Israel (?)
- **Outcome:** official, well-publicized start of global cyberwarfare

Stuxnet (2010) and the kill chain

Reconnaissance	• Geo location; physical security; equipment; SCADA
Weaponization	• Develop complex malware; steal digital certs (to hide malware)
Delivery	• USB drive (most probably)
Exploitation	• Windows zero days; hardcoded passwords
Installation	• Lateral movement; malware deployment on maintenance and operations workstations
Command & Control	• PLC recipe modification; hide traces
Actions on Objectives	• Send commands to destroy centrifuges

Physical and personnel security

OUTSIDE THE FACILITY

The ‘onion’ of physical security

- Well-chosen location of the industrial/infrastructure facility
- Cleared area around the location
- Fence with vehicle and personnel access points – optionally with bomb detection
- On-premise surveillance system with cameras, sensors and guards&dogs
- Secured external walls and windows
- Secured doors with multi-factor authentication between internal security zones
- Secured access to IT infrastructure e.g., server rooms
- Secured access to sensitive IT & OT equipment e.g., rack protection, locked equipment cabinets with PLCs
- Physical port security
- (Optional) Redundant utilities i.e., electricity, water, communications, transport.

Location

- Avoid locations prone no natural disasters e.g., tornadoes, floods, earthquake fault lines → tsunamis
- Choose neighbors wisely → avoid prisons, airports and chemical plants which might cause unplanned disturbances
- Cleared ground around the industrial/infrastructure facility
  - Clear overgrown trees and other large obstacles to visibility and access, e.g. large boulders
  - ~30m cleared buffer zone around the facility to improve the efficiency of the camera system and guards

Fences

- Fences are the first line of defense
  - The entire fence can be regarded as a potential physical access point (PAP)
- 2-meter-high fences deter casual intruders from trespassing
- 2.5-meter and higher fences will stop even the most determined intruders

https://te-fence.com/high-security-fences/

Vehicle and personnel entry + bomb detection

- Vehicle and personnel entry points are physical access points which allow policy-allowed physical access to the ICS facility
- Single main entrance + back entrance for delivery & shipping
- ‘Staffed’ guard station
- Retractable ram posts
- Fire doors exit only
- Entrance with badge/card swipe or PIN code + multi-factor authentication
- Strict visiting policies for guests and contractors
- (Optional) Highly sensitive, high-risk facilities need to implement manual (gate guards with mirrors to peek underneath vehicles entering the compound) or assisted bomb detection

Physical barriers

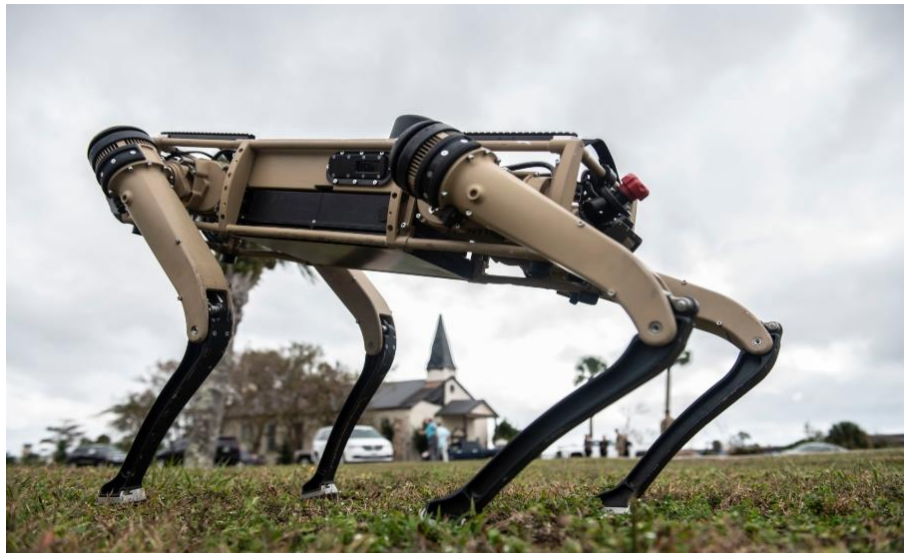
Armed guards

- Civilian clothing
- Security training is a plus (military, national guard, police)

- Which infrastructures do need physical guards → where to station them?

https://securityguardsuk.com/news/rules-security-guard-must-obey/

Dogs



- Traditionally dogs were used on physical perimeters → augment the human guards
- Living dogs might be soon partially substituted by their robotic brethren

https://www.securitymagazine.com/articles/93941-us-air-force-implements-dog-like-robots-into-patrolling-regiment-to-enhance-security-and-safety

Physical and personnel security

PHYSICAL ACCESS POINTS

Walls

- 30 cm or thicker external concrete walls provide adequate protection against severe weather, intruders and explosive devices
- Additional protection can be attained by using Kevlar
- Interior walls need to go all the way to the ceiling → do not allow intruders to crawl over in case of a dropped ceiling

https://www.indiamart.com/proddetail/precast-concrete-security-wall-22189506888.html

Doors & security portals

- Secure doors
  - Made from metal or use metal structures
  - Strong locks
  - Hinges on the more secure side
- Security portals
  - One person at a time → no piggy-backing

Rooftops

- Traditionally the focus was on safety → nobody falls off the roof
- Latest challenges
  - Drone attacks
  - Breaking and entering via roofs
  - Protecting the equipment usually mounted on rooftops → which?
- Consider basements as well (!)

Windows

https://mullerexteriors.com/better-window-safety-5-ways-to-secure-your-windows-against-burglars/

- Avoid windows as much as possible as they are the weakest elements of exterior defense
  - Exception: offices or rooms where employees take breaks
- Glass types to consider
  - Heat strengthened glass
  - Fully tempered glass
  - Heat-soaked tempered glass
  - Laminated glass
  - Wire glass

On-premise surveillance

External

- DEF: External surveillance is implemented on the outer physical perimeter of the ICS facility
- IP cameras or closed-circuit TV
- Security guards & dogs
- Use a clever combination of
  - Motion detection devices
  - Low-light cameras
  - Pan-tilt-zoom cameras
  - Fixed cameras
- Store sensor recordings offsite for planned amount of time

Internal

- DEF: Internal surveillances is implemented inside the facility
- Cover every physical access point
- Watch the entrances and exits both outside and inside, especially at the more sensitive (physical) zones
- Keep track of who was where and when → spot when equipment disappears

Sending and destroying data stores

Send data

- Might need to send data to external entities on CD/DVD, USB, paper
- Encrypt the data
- Do not mark the envelopes
- Choose postal services with electronic tracking
- Proof of receipt

Data wipes

- Always attempt to counter dumpster diving (!)
- Use a shredder to destroy paper
- Physically break CD/DVD/Blue Ray disks
- Magnetically erase and physically destroy magnetic drives
- Dumpster bins and containers keep locked whenever possible
- Consider subcontracting a data wipe specialist company

Physical and personnel security

INSIDE THE FACILITY

Computing equipment threats

- Natural events (e.g., floods, earthquakes, and tornados)
- Other environmental conditions (e.g., extreme temperatures, high humidity, heavy rains, and lightning)
- Intentional acts of destruction (e.g., theft, vandalism, and arson)
- Unintentionally destructive acts (e.g., spilled drinks, overloaded electrical outlets, and bad plumbing)

https://nces.ed.gov/pubs98/safetech/chapter5.asp

Secure access to the process environment

- Consider the process environment as a high security area and allow access via a limited number of doors
- Use strict (multi-factor) authentication e.g., swipe cards and/or biometric reading devices
- Audit each entry and exit into and out of the process/production area
- Representatives of vendors and visitors must be accompanied by an employee during 100% of their visits

Secure access to IT infrastructure

- Server rooms behind single, locked doors
  - Multi-factor authentication, e.g., biometric sensor + card
  - Strictly log physical access
- Shielded and hidden cabling (network, electricity)
- Fire protection
- Secured suspended ceiling if cabling is above
  - Similar for raised floors (!)
- Video surveillance

Data center secure storage

- Data centers might host customer-owned racks
- Physical fences
- Secure doors
- Secure rooftops
- Well-hidden cabling (electricity & network)

https://www.storagesystems.ie/products/details/data-center-cages/76

Structural lowered ceilings

- Hidden or in plain sight
- Allow on-site administrators to implement structural cabling
- Cabling should be hidden outside server rooms

Raised floors

- Structured cabling under the floor
- Often easier to access and hidden from plain sight (when compared to lowered ceilings)

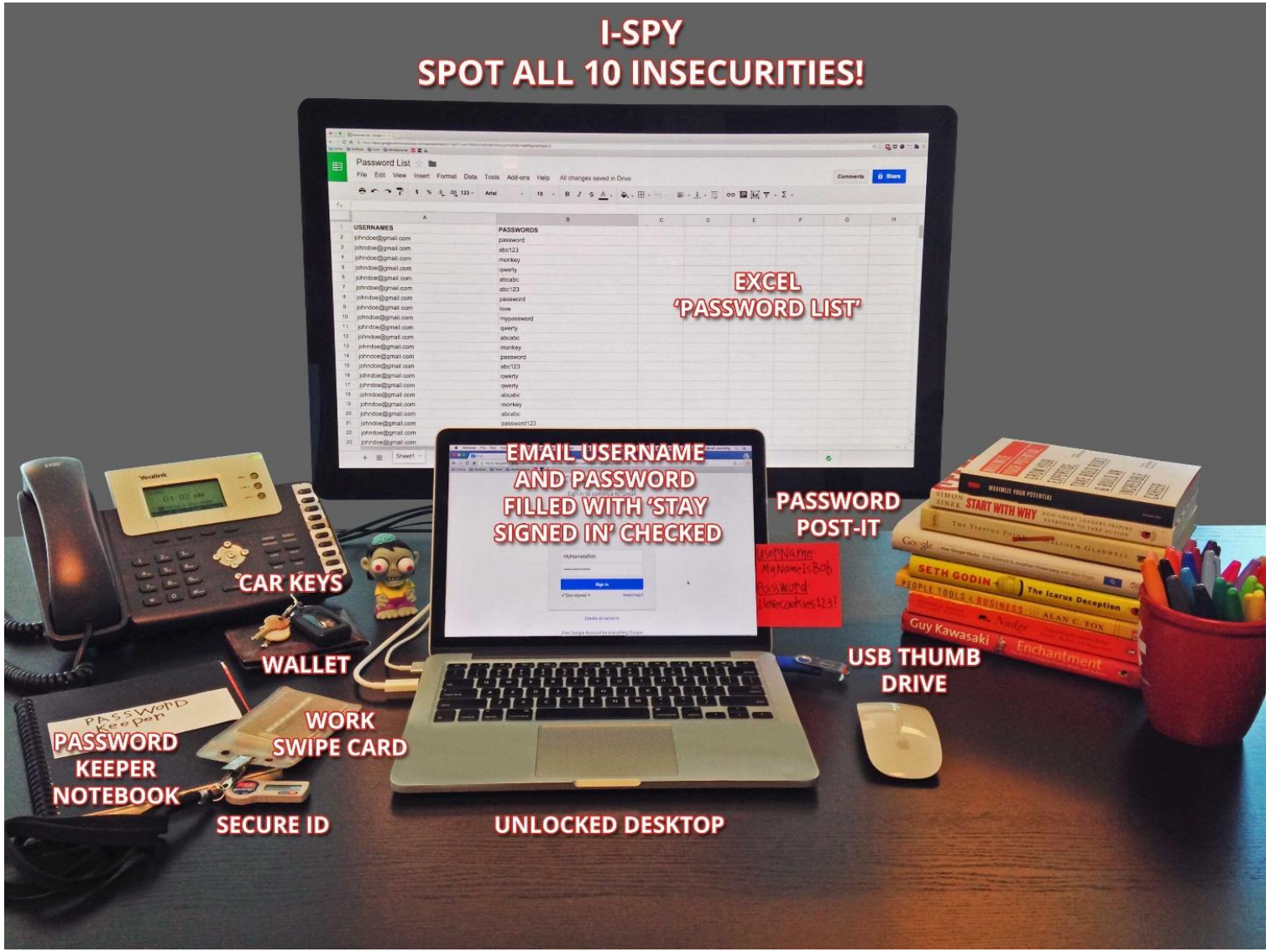
Redundant utilities

- Most facilities need at least electricity, water and telecommunications services
- Ensure that the facility has redundant (i.e. two) sources for the key utilities
- Electricity from two separate substations
- Water from two different main lines
- The redundant utilities enter the building at separate points → no single point of failure
- Underground cabling and pipes
- Separate water pipes from the other utilities → lowered risk of flooding the cabling

Physical and personnel security

INSIDE THE CONTROL ROOM

Workstation security (what not to do!)



Workstations

- Theft protection
- Encrypted file systems
- Biometric sensors and strong passwords → cards might be a better choice compared to passwords
- BIOS password
- Screen orientation → do not allow possible attackers direct view via windows to sensitive screens
- Automatic session locking when the operator leaves the WS
- Keep sensitive documents and plans in locked cabinets

Secure computer workstations

- Locked compartments for
  - Computer cases
  - Screens
  - Keyboard, mouse

- Threats:
  - Locks can be picked
  - Doors can be left unlocked by reckless employees
  - Keys can be lost

https://www.equiptowork.com/products/computer-workstations

Physical port security

- Lock-ins for network cabling
- Port blocking devices for USB ports

https://www.amazon.com/Lindy-RJ45-Port-Blocker-40470/dp/B00F3VBND4

Biometric sensors

- Sensitive workstations need strict access control
- Passwords are not a viable solution
- All types off remote access to workstations should be default deny
- MFA is a possible solution
  - Combined fingerprint and card reader

https://www.acs.com.hk/en/products/131/aet65-smart-card-reader-with-fingerprint-sensor/

Physical and personnel security

PERSONNEL SECURITY

How to tighten personnel security?

https://gcn.com/articles/2015/03/23/personnel-security?m=1

Control whom you hire…

- Check every prior position
  - Pay special attention to any ‘holes’ in a CV → the candidate might’ve served a prison sentence or worked for a classified organization
- Check key claims in a CV
  - Degrees, certificates
  - Knowledge of languages
  - Criminal record
  - Note: checking creditworthiness is not privacy-proof (!)
- Check all referrers, e.g., past employers
- Check physical and psychical capabilities → control room operators might face highly stressful situations during their work

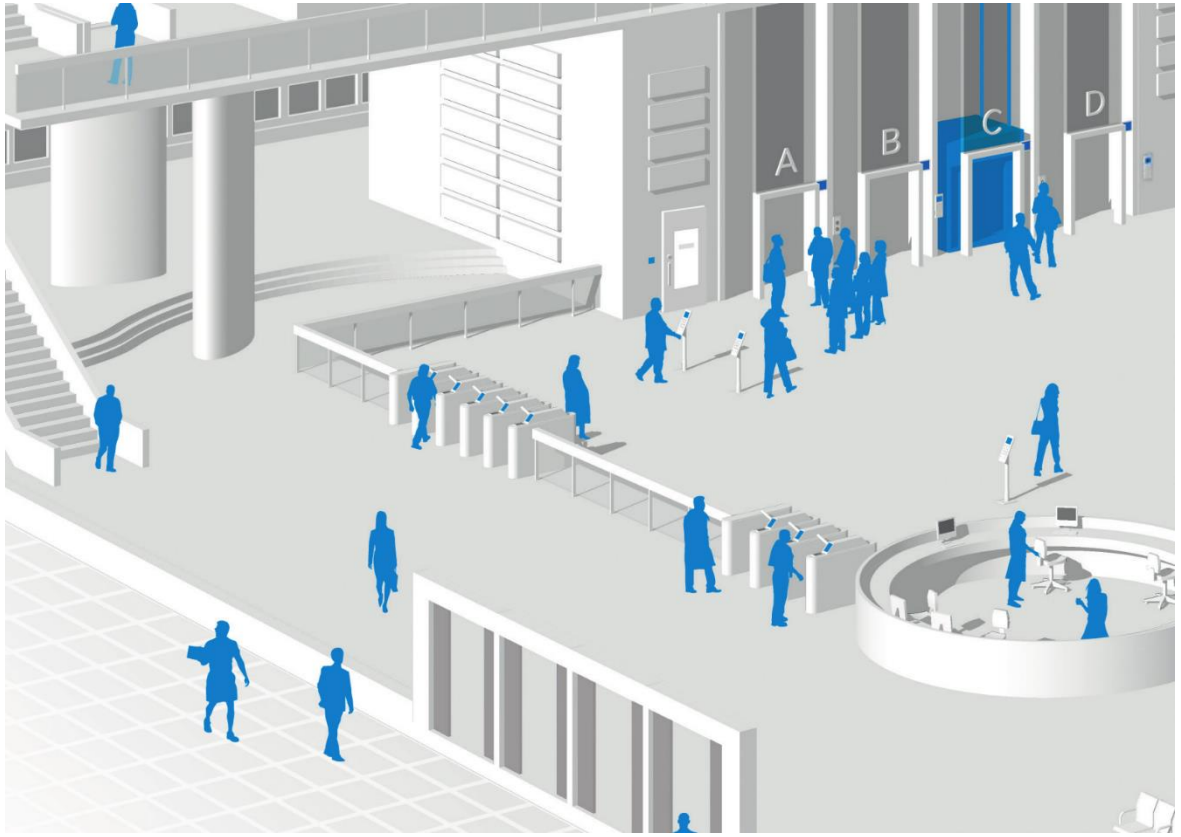
Secure & monitor your human resources

- Define persons who handle security incidents, either physical or electronic
  - Define chains of notification within departments and/or on floors within your building(s)
- Organize periodic security trainings (in person, not electronic !)
- Frequently send out short notifications about the latest known threats
- Consider offering awarding special prizes to employees who strictly follow the security policy
- Consider additional monitoring specific employees during specifically sensitive periods
  - Decreased salary
  - Reassignment, e.g., to a different department
  - Before known lay-offs

Let them go if they have to leave…

- Control the software and hardware used by the employee
- Do the following synchronously in the physical domain
  - Deny access to any workstations
  - Return company laptop
  - Return keys, magnetic and other cards
  - Escort the employee outside the facility
- Do the following synchronously in the electronic domain
  - Deny and uninstall VPN access
  - Delete and/or deactivate all electronic accounts – some industries do not require an immediate deletion
  - Delete publicly available information about the (past) employee, e.g., delete info from the company's public website
- When a high-risk employee leaves (e.g., OT server room admin) then create backups and increase the sensitivity of security monitoring solutions

Secure flow of human resources



- Well-trained employees
- Vetted contractors
- Proven subcontracted service providers
  - Garbage
  - Raw material logistics
  - Complete products leaving the facilities
- Short trainings for guests

Security onion around the ‘core’

- Ensure that anyone entering the most sensitive parts of the facilities was authenticated multiple times
  - At the entrance/gate
  - At the employee entrance ensuring that there is no piggybacking
    - Floor-to-ceiling turnstile
    - Mantrap with two separate doors and an airlock between them. Both doors require authentication
  - At the inner door to the sensitive part of the facility with multi-factor authentication, surveillance and strict auditing policy

People flow

- Employees
  - Company card with photo and color-coding aligned access level
- Contractors
  - Limited use cards
  - Food delivery services strictly controlled and any changes in schedule or personnel based on prior notification only
- Guests
  - Temporary, one-day cards
  - Receive a basic physical security training on first entry
  - Continuously escorted by at least one employee

5 Levels of Physical Security

Security level	Security controls (additive)	Examples
Zero	None	high seas; forest; open fields
Minimum	Basic security controls to keep intruders out: cleared space, lighting, fences, walls.	private residences; urban spaces
Low	Security gate, reinforced locks, bars on windows, alarm.	small shops; storage facilities
Medium	Covers internal and external threats. Internal surveillance monitors employees, customers and guests. High fence, unarmed security guard, loud alarm.	factories; large retail stores; warehouses;
High	24/7 closed-circuit television (CCTV), perimeter alarm system, gates, controlled access in and out, security lighting, armed guards, security dogs, audit, cooperation with law enforcement.	prison; defense; electronics; pharmaceuticals;
Maximum	24/7 security personnel (combat-trained, well-equipped), stricter internal control of movement, tamper-proof alarm.	military installations; embassies; nuclear; some gov facilities;

Conclusion

- Basic definition and data lifecycle
- Attackers and attack types
- Methods
- Physical security
  - Outside the facility
  - Physical access points
  - Inside the facility
  - Inside the control room
- Personnel security in brief

Thank you for your attention!