Physical Security, Human Factors

Paolo Falcarin

Ca' Foscari University of Venice

Department of Enviromental Sciences, Informatics and Statistics

paolo.falcarin@unive.it

CM0626 – Software Security

18 March 2025

Three Security Disciplines

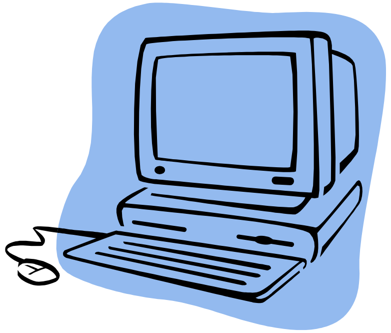
- Information Security
  - Network, Software, Hardware, Data
  - Physical environment security – Side Channels Attacks
- Physical
  - Most common security discipline
  - Protect facilities and contents
    - Plants, labs, stores, parking areas, loading areas, warehouses, offices, equipment, machines, tools, vehicles, products, materials
- Personnel
  - Protect employees, customers, guests
  - Protect from employees (insider threat)

Information Revolution

- Information Revolution as pervasive as the Industrial Revolution
- Impact is Political, Economic, and Social as well as Technical
- Information has an increasing intrinsic value
- Protection of critical information now a critical concern in Government, Business, Academia

The New World

- The Internet allows global connectivity
- Cyber-space has no borders
- Anonymity easy to accomplish
- New breed of threat
    - Technically smart
    - Determined, knowledgeable
- Physical Security often overlooked in the new threat environment



Nature of the Threat

- Threat environment changes
- Nation-state threat
  - Countries see computers as equalizers
  - New balance of power through information control
- Non-state actors
  - New levels of potential threat
  - “Strategic Guns for Hire”
- Physical attacks against information sources requires minimal effort for maximum effect
- Cyber events can have physical consequences

Threat and Physical Security

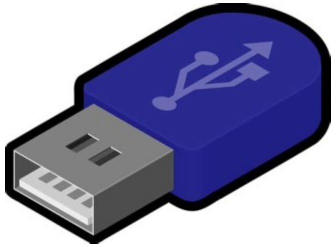
- Physical Attacks require little resources
- Insider threat very real
    - Disgruntled employee
    - Agent for hire
- Tactics well known and hard to stop
    - World Trade Center
    - Aldrich Aimes
- Financial network facilities viable target
- Target information readily available

Why Physical Security?

- Not all threats are “cyber threats”
- Information one commodity that can be stolen without being “taken”
- Physically barring access is first line of defense
- Forces those concerned to prioritize!
- Physical Security can be a deterrent
- Security reviews force insights into value of what is being protected

Layered Security

- Physical Barriers
  - Fences
  - Alarms
  - Restricted Access Technology



- Physical Restrictions
  - Air Gapping
  - Removable Media
  - Remote Storage

- Personnel Security Practices
  - Limited Access
  - Training
  - Consequences/Deterrence

Physical Barriers

Hardened Facilities

- Fences
- Guards
- Alarms
- Locks
- Restricted Access Technologies
    - Biometrics
    - Coded Entry
    - Badging
- Signal Blocking (Faraday Cages)

Outer Protective Layers

- Structure
  - Fencing, gates, other barriers
- Environment
  - Lighting, signs, alarms
- Purpose
  - Define property line and discourage trespassing
  - Provide distance from threats

Middle Protective Layers

- Structure
  - Door controls, window controls
  - Ceiling penetration
  - Ventilation ducts
- Environment
  - Within defined perimeter, positive controls
- Purpose
  - Alert threat, segment protection zones

Inner Protective Layers

- Several layers
- Structure
  - Door controls, biometrics
  - Signs, alarms, CC-TV
  - Safes, vaults
- Environment
  - Authorized personnel only
- Purpose
  - Establish controlled areas and rooms

Other Barrier Issues

- Handling of trash or scrap
- Fire:
  - Temperature
  - Smoke
- Pollution:
  - CO
  - Radon
- Flood
- Earthquake

Physical Restrictions

- Air Gapping Data
  - Limits access to various security levels
  - Requires conscious effort to violate
  - Protects against inadvertent transmission

- Removable Media
  - Removable Hard Drives
  - Floppy Disks/CDs/ZIP Disks

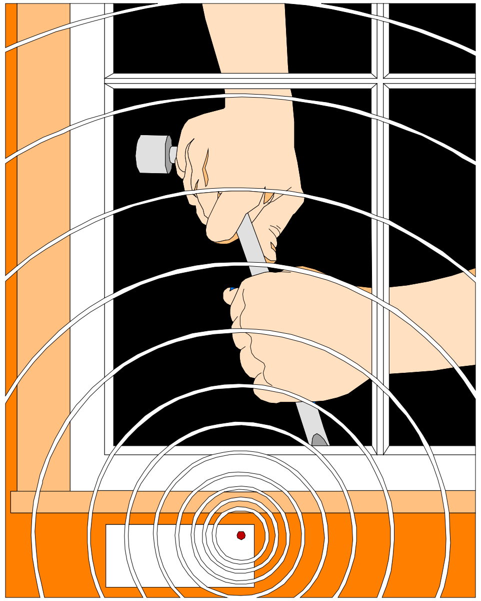
- Remote Storage of Data
  - Physically separate storage facility
  - Use of Storage Media or Stand-Alone computers
  - Updating of Stored Data and regular inventory

Activities or Events

- Publications, public releases, etc.
- Seminars, conventions or trade shows
- Survey or questionnaire
- Plant tours, “open house”, family visits
- Governmental actions: certification, investigation
- Construction and Repair

Technical Security

- Alarms
  - Loud and Noisy
  - Silent
  - Integrated into barrier methods
- Video/Audio
  - Deterrent factor
  - Difficult to archive
- Bio-Metrics
  - Identification
  - Reliability questions



NISPOM

- National Industrial Security Operating Manual
- Prescribes requirements, restrictions and other safeguards that are necessary to prevent unauthorized disclosure of information
- Protections for special classes of information: Restricted Information, Special Access Program Information, Sensitive Compartmented Information
- National Security Council provides overall policy direction
- Governs oversight and compliance for 20 government agencies

- https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom

The Place of Physical Security

- Physical Security is part of integrated security plan
- Often overlooked when considering Information Security
- No information security plan is complete without it!

Personnel Security

Personnel Security Practices

- Insider Threat the most serious
  - Disgruntled employee
  - Former employee
  - Agent for hire
- Personnel Training
  - Critical Element
  - Most often overlooked
- Background checks
  - Critical when access to information required
  - Must be updated

People

- Disgruntled employee / former employee
- Moonlighter (one who works another job, often at night, for extra income)
- Marketing, sales representatives, etc.
- Purchasing agents, buyers, subcontract administrators
- Consultants
- Vendor/Subcontractor
- Clerks
- Applicants, Visitors, Customers

Personnel Management

- Job descriptions
- Separation of duties
- Job responsibilities
- Job rotation
- Cross-training
- Collusion

Employment Candidate Screening

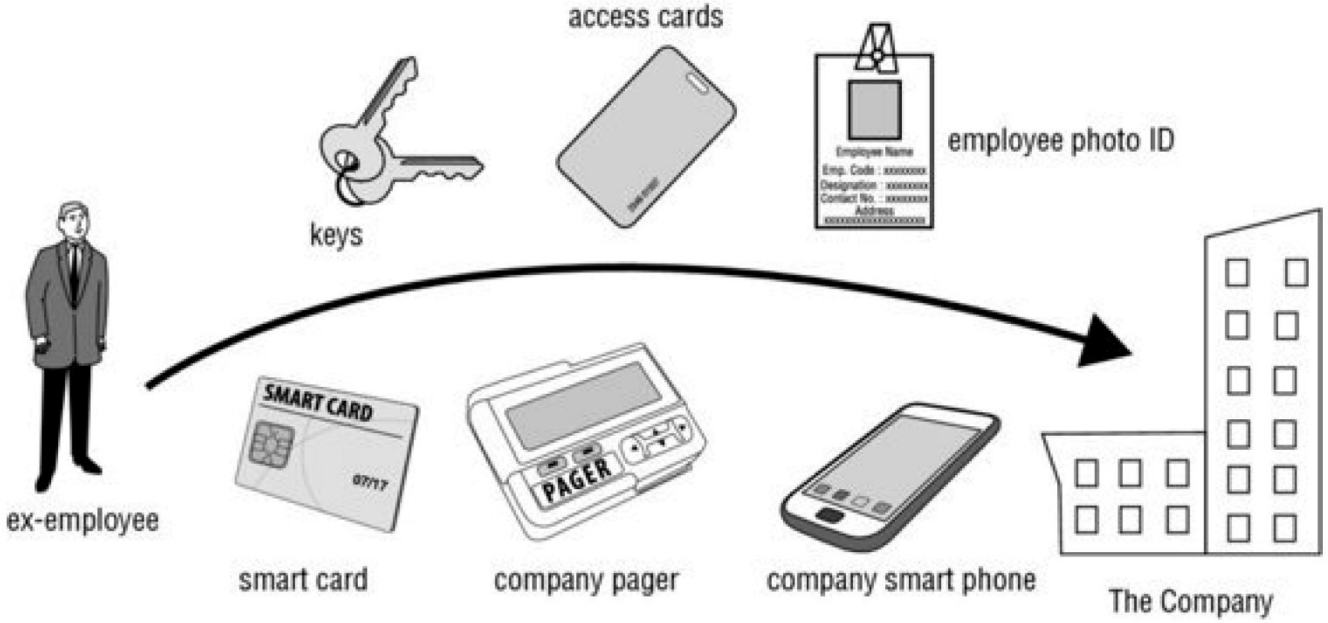
- Based on job description
- Background checks
- Reference checks
- Education verification
- Security clearance validation
- Online background checks

Employment Agreements and Policies

- Nondisclosure agreement
- Noncompete agreement
- Audit job descriptions, work tasks, privileges, and responsibilities
- Mandatory vacations

Employment Termination Processes

- Maintain control and minimize risks
- Exit interview
- Terminate access
- Return company property



Privacy

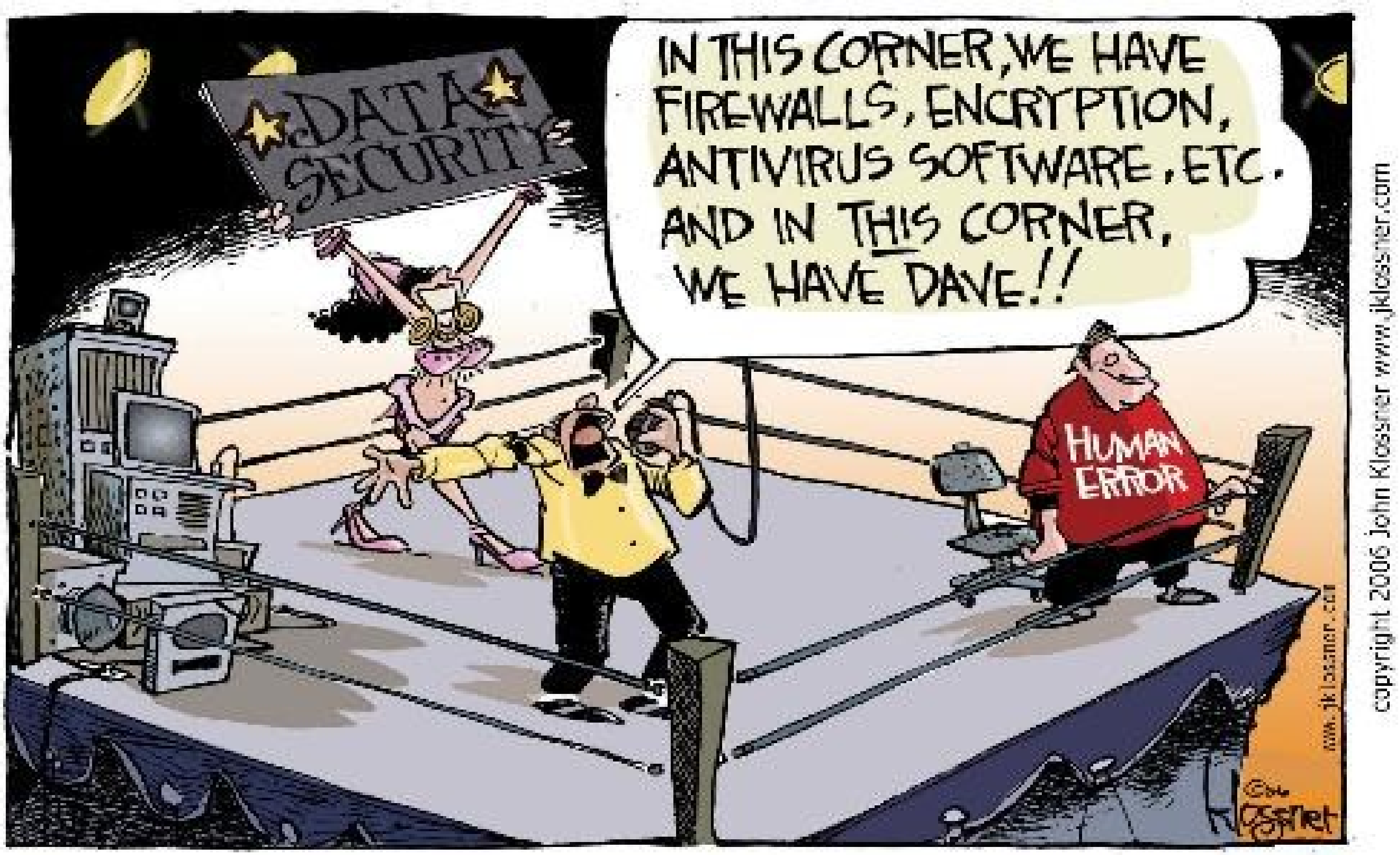
- Active prevention of unauthorized access to information that is personally identifiable
- Freedom from unauthorized access to information deemed personal or confidential
- Freedom from being observed, monitored, or examined without consent or knowledge
- Legislative and regulatory compliance issues

Security Governance

- Maintain business processes while striving toward growth and resiliency
- Third-party governance
- Auditing
- Compliance
    - Conforming to or adhering to rules, policies, regulations, standards, or requirements
    - Maintaining high levels of quality, consistency, efficiency, and cost savings
- Documentation review

Human Factors in Security

Human Errors


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
copyright 2006 John Klossner www.jklossner.com
www.jklossner.com
Klossner

Phishing

- Phishing is the fraudulent attempt to obtain sensitive information by disguising oneself as trustworthy entity in an e-mail
- According to US Secrete Service, 91% of all cyber attacks begin with phishing
- Objectives:
  - Personally Identifiable Information (PII)
  - Financial Information, account info, payment processes
  - Owed invoices or outstanding debts
  - Company structure info and internal comms
  - Login credentials, passwords, defece posture
  - Deployment of malware
  - Ransomware

Phishing

- Globally June 2016 to present, current losses over 26 Billion US $
- Red flags:
  - Urgency, out of contact
  - Language and grammar errors
  - Links or attachments
  - No prior web presence or footprint
  - Use of chat apps Whatsapp, Telegram
  - Use of non-traditional payments: money orders, gift cards
  - Use of irreversible/hard to track payments: wires, virtual currency

Spear-Phishing

- Sending emails to specific and well-researched targets while pretending to be a trusted sender
- The purpose is to either infect devices with malware of convince victim to hand over information or money
- Often uses social engineering or social media to research the victim

- https://www.youtube.com/watch?v=F7pYHN9iC9I

Whaling (CEO fraud)

- Fraudulent use of a compromised email account of a EO or other high-ranking executive
- More targeted form of spear-phishing
    - Whales are big fishes in an organization
- Subordinates tend to be reluctant to disobey important members of their organization
- Objectives:
    - Gain access to information/accounts of a senior member of a company
    - Authorize fraudulent wire transfers to a financial institution chosen by the attacker
    - Obtain information for all employees
        - File fake tax returns posing as employees
        - Sell employee data on the dark web

Smishing (SMS + Phishing)

- Smishing is the fraudulent practice of sending text messages pretending to be from reputable companies in order to induce individuals to reveal personal information (passwords, credit card numbers)
- Gain personal information
  - Install malware on your mobile phone
  - Link takes you to a fake site
- Risk for companies with BYOD (Bring Your Own device)
- Threaten daily charges for a service unless you click their link and enter personal information
- Red flags: text from someone you do not know, Phone number does not look like a real one

Examples

- Urgent “Your bank account is locked”
- Urgent “Credit card attack”
- You won a prize, click here to get it
- It must be fake but it’s also funny (fake Amazon account)
- Unusual account activity from fake “Apple support”

What to do

- Be suspicious on urgent messages
- Never click link or a phone number you are not sure about
- Look for suspicious phoen numbers
- Do not score credit card or banking data on your mobile phone
- Do not respond and report it

Vishing (Voice Phishing)

- Vishing is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information
- Objectives
  - Gain access to personal information
  - Convince you to pay money
- Older people targets
  - Caller claims to represent the Social Security Administration, Police or the court
  - Frantic sense of urgency
  - Caller asks for your personal information

Vishing Tactics

- Supposed fraud or suspicious activity on your bank account
- Overdue or unpaid taxes
- Prize or contest winnings
- Fake computer tech support calling to remotely access your PC to fix a problem
- Faked government agencies

What to do

- Join the National “Do Not Call Registry” (in USA)
- Don’t answer the phone
- Hang up
- Do not press buttons or respond to prompts
- Verify caller’s identity

Dumpster Diving

- Dumpster Diving is searching through trash for information that could be used in a cyber attack
  - “One man’s trash is another man’s treasure”
- Objectives;
  - Full names of employees, business partners, and contractors
  - Account login credentials
  - Marketing information
  - Email addresses of employees
  - Sensitive customer information
  - Employee information
  - Corporate secrets
  - Medical records
  - Bank statements and other financial information
  - Technical support logs

Red flags

- Potential attackers have access to discarded information
  - Paper, Electronic, Hardware
- Tactics
  - Network and security information can be used directly in a hacking attack
  - Personal information can be used in a phishing, spear-phishing, whaling, smishing, or vishing attack

Mitigations of Dumpster Diving

- Never underestimate the importance of physical security
- Destroy any CDs/DVDs containing personal data
- When disposing of a computer, delete all data
- Use a firewall to prevent attackers from accessing discarded data
- Permanently destroy / shred paper documents (wood oven heat)
- Have a safe disposal policy
- Lock waste bins

Tailgaiting

- Tailgaiting is also known as piggybacking and takes place when some one without proper authentication follows an authenticated employee into a restricted area
- Digital tailgating is requesting the use of a digital resource without proper authentication
- Objectives:
  - Physical access or digital access to a restricted area
- Red flags Tactics:
  - Someone attempts to flow you into a restricted area
  - Another “employee” forgot thei badge to access the restricted area
  - “hold the door”, attacker has hands full, “forgot my badge”
  - “Can I use your computer for just a minute?”

What to do

- Never underestimate the importance pf physical security
- Never allow someone with proper authentication into a restricted ara
- Never allow someone without proper authentication to use your electronic devise
- Contact your facility security team
- Implement Man Trap door in critical areas

Baiting

- Baiting attacks use a false promise to appeal to a victim’s greed or curiosity
- Users are lured into a trap that steals their personal information or infects their system with malware
- Frequently uses physical media, like USB thumb drives
- Objective
  - Stealing information
  - Infect network with malware

Baiting Red Flags

- Someone gives you a USB thumb drive or find one in a conspicuous place
- “Free stuff” or “swag” at a conference or event – Stuxnet!
- You win a prize in a contest you did not enter
- “Sorry we missed you” - You missed a delivery for a package you were not expecting

Impersonation

- Impersonation is another type of social engineering attack used to gain access to a system or network to commit fraud, industrial espionage, or identity theft
- The social engineer plays the role of someone you are likely to trust or obey enough to fool you into allowing access to your restricted space, to information, or to your network
- Objectives:
  - Gain trust
  - Access to restricted space
  - Anyone who could be tricked

Impersonation: red flags and warning signs

- Someone makes a suspicious request
- A person is acting especially friendly to gain your trust
- A new acquaintance seems very interested in your work or workplace
- Someone who would be ina position of authority asks you to do something that would violate policies or procedures
  - “Friday afternoon” attack

Impersonation Tactics

- Stalking employees on social networking sites
- Company websites
- Email phishing
- Phone pretexting
- Dumpster diving
- Eavesdrpping on employee conversations
- Black market websites or other social engineers

Impersonation Example: Mia Ash

- Photographer with more than 500 friends on FB and LinkedIn
- Most of her friends were Middle Eastern and Asian men aged 20-40
- Asks acquaintances to help with a photography project by taking a survey to their contacts
- The Excel Xslm document she sent contained Trojan malware “Puppy Rat” installing a backdoor in your company network to steal information.
- Mia Ash is not real, but a persona created by the Iranian APT called Cobalt Gypsy

https://www.wired.com/story/iran-hackers-social-engineering-mia-ash/

Impersonation Example: HVAC

- HVAC (Heating, Ventilation, & Air Conditioning) contractors tell receptionist they got a call the server room is overheating
- This is an emergency – if the room gets any hotter, your servers are going to overheat with disastrous consequences
- They ask you to call ahead your IT dept to give them access to the secure server room.

What to do

- When in doubt about someone’s identity, contact your manager
- Never give out passwords
- Avoid revealing information, out of trust or fear
- Be aware of your surroundings
    - Who is in range on hearing your conversation or seeing your work?
- Be sceptical about anything out of the ordinary
- Adhere to your organization’s policies or procedures