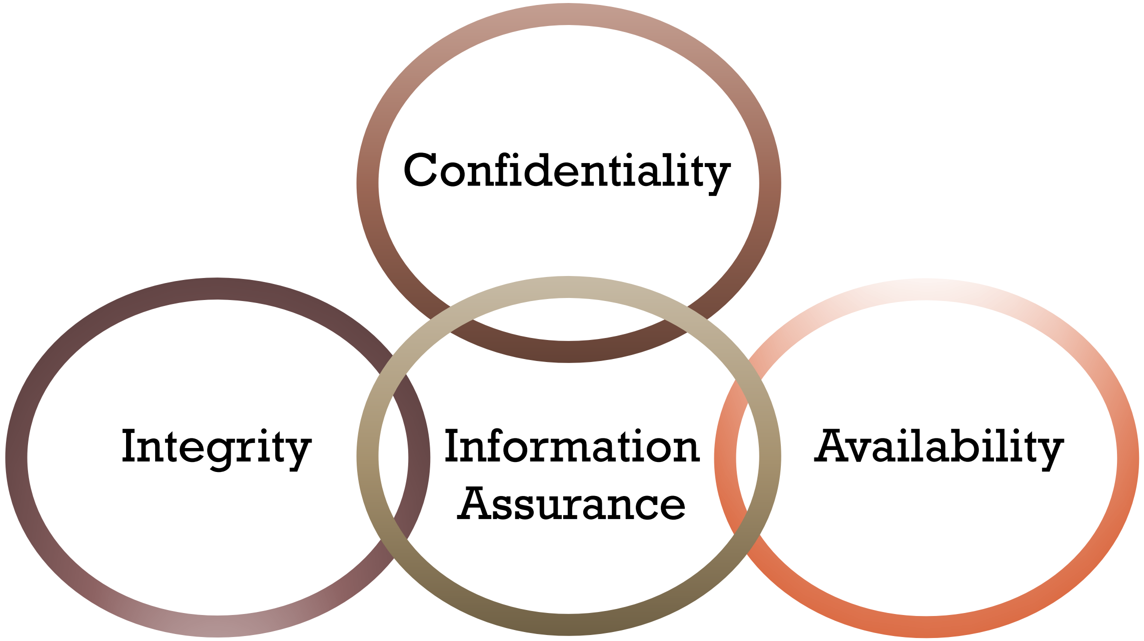
# 1.1 ELEMENTS OF INFORMATION SECURITY

- Information Security Overview
- Security Controls
- Access Control

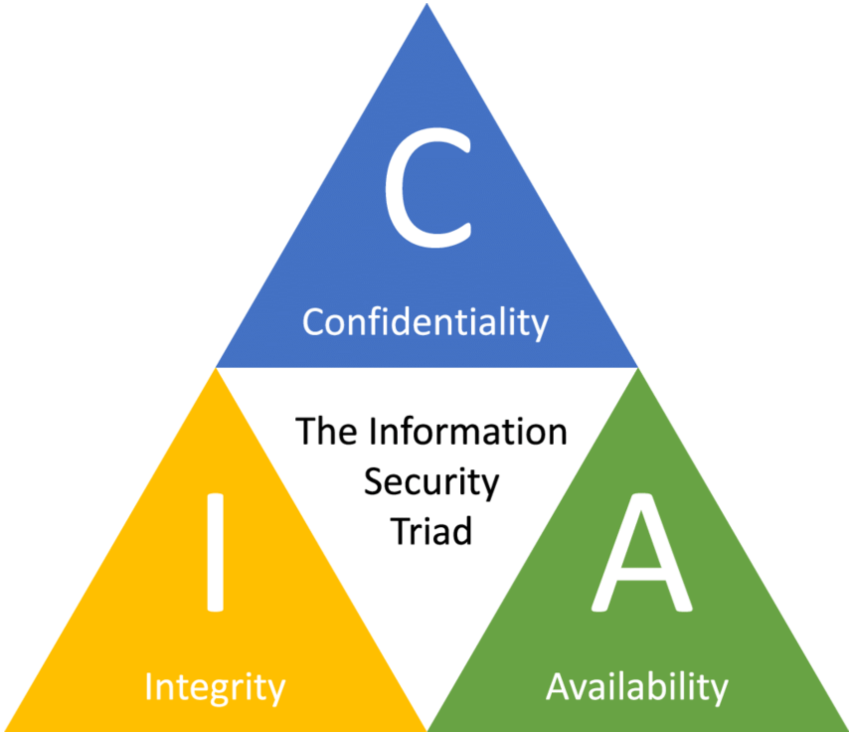
# WHAT IS INFORMATION SECURITY?

- The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction
- The goal is to provide confidentiality, integrity, and availability of systems and data



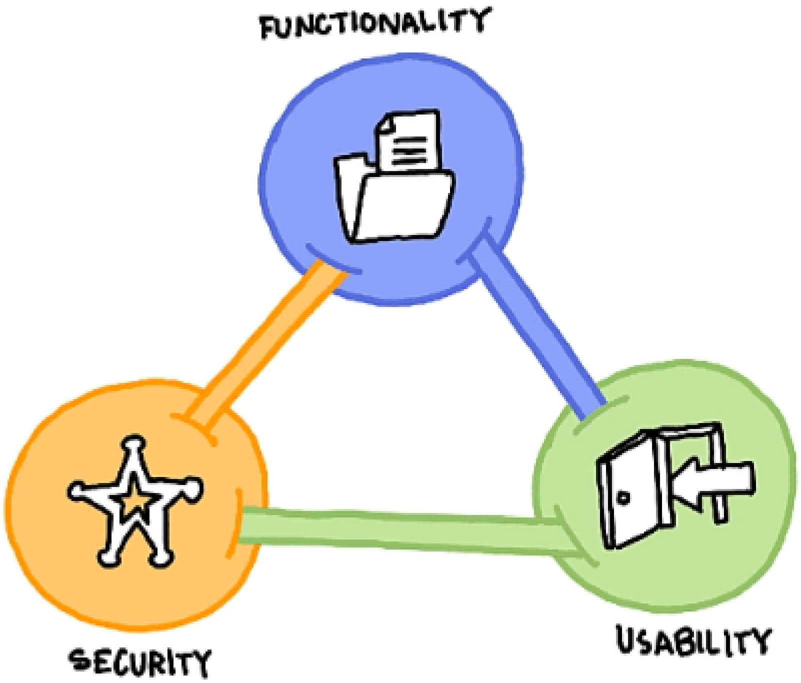
# CIA TRIAD

- **Confidentiality**
  - Only allow authorized parties to access the data or system
- **Integrity**
  - Protect the data from unauthorized modification or deletion
- **Availability**
  - Ensure that data and systems that you are protecting can still be accessed and used as needed



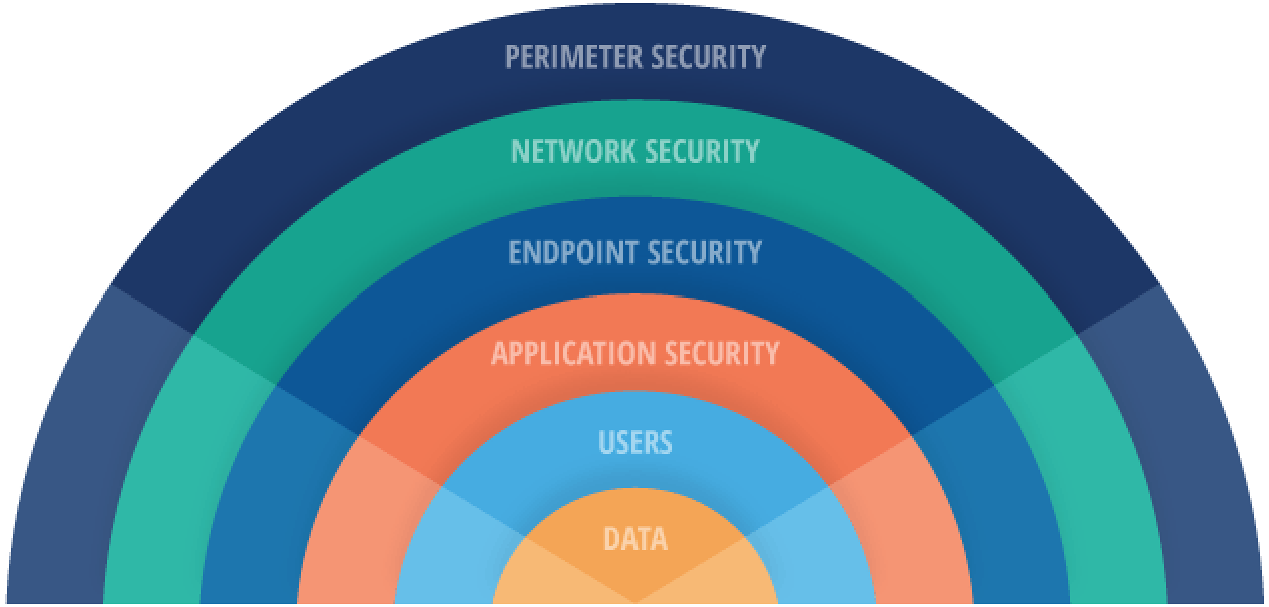
# SECURITY, FUNCTIONALITY, USABILITY

- These attributes are interlocked
- Security is at odds with nearly every other organizational process
- Increasing security usually requires decreasing functionality and usability
- You need to find an acceptable balance between these three



# DEFENSE IN DEPTH

- Multiple layers of security controls
- Provides redundancy in the event of a control failure



# THREE TYPES OF ACTIVE DEFENSE

- Annoyance
  - Involves tracking a hacker and leading them to a fake server
  - Waste their time
  - Make them easy to detect
- Attribution
  - Identify the attacker
  - Use tools to trace the source of an attack back to a specific location, or even an individual
- Attack
  - This is most controversial--and risky
  - You "hack back"
    - Access an alleged hacker's computer
    - Delete data or take revenge
    - Both steps are considered illegal

# ESSENTIAL TERMINOLOGY

| Term | Definition |
|---|---|
| Hack value | Perceived value or worth of a target as seen by the attacker |
| Vulnerability | A weakness or flaw in a system |
| Threat | Anything that can potentially violate the security of a system or organization |
| Exploit | An actual mechanism for taking advantage of a vulnerability |
| Payload | The part of an exploit that actually damages the system or steals the information |
| Zero-day attack | An attack that occurs before a vendor is aware of a flaw or is able to provide a patch for that flaw |
| Daisy Chaining / Pivoting | Using a successful attack to immediately launch another attack. |
| Doxing | Publishing personally identifiable information (PII) about an individual usually with a malicious intent |

# ESSENTIAL TERMINOLOGY (CONT'D)

| Term | Definition |
|---|---|
| Non-repudiation | The inability to deny that you did something<br>Usually accomplished through requiring authentication and digital signatures on documents |
| Control | Any policy, process, or technology set in place to reduce risk |
| Mitigation | Any action or control used to minimize damage in the event of a negative event |
| Accountability | Ensure that responsible parties are held liable for actions they have taken |
| Authenticity | The proven fact that something is legitimate or real |
| Enterprise Information Security Architecture (EISA) | The process of instituting a complete information security solution that protects every aspect of an enterprise organization |

# SECURITY CONTROL TYPES

| Control Type | Description | Example |
|---|---|---|
| Physical | Tangible mechanisms designed to deter unauthorized access to rooms, equipment, document, and other items | Guards, lights, cameras, motion detectors, walls/fences, bollards, mantraps, turnstiles, locks, alarms, disposal tools such as document and hard drive shredders |
| Administrative | Procedures and policies that inform people on how the business is to be run and how day to day operations are to be conducted. Can be enforced through management policing, physical and technical means. | Training awareness, policies, procedures, guidelines, software bug bounties, engaging an security audit team |
| Technical | Any measures taken to reduce risk via technological means | IDS/IPS, firewall, anti-virus software, encryption, authentication protocols, access control lists |

# SECURITY CONTROL TYPES (CONT'D)

| Control Type | Description | Examples |
|---|---|---|
| Preventive | • Makes it difficult or impossible for a bad actor to carry out the threat<br>• Designed to keep errors or irregularities from occurring in the first place<br>• Most security controls are preventive | Fences, gates, locks, authentication, logical access controls, encryption, segregation of duties, employee screening and training |
| Detective | Designed to detect errors, irregularities and intrusions that have already occurred<br>Assure their prompt correction | Audits, intrusion detection, cameras, motion sensors, anti-virus, mandatory vacations, job rotation |
| Deterrent | Discourages the bad actor from attempting to carry out a threat | Warning signs, lights, high fences, guards, dogs, logon banners |

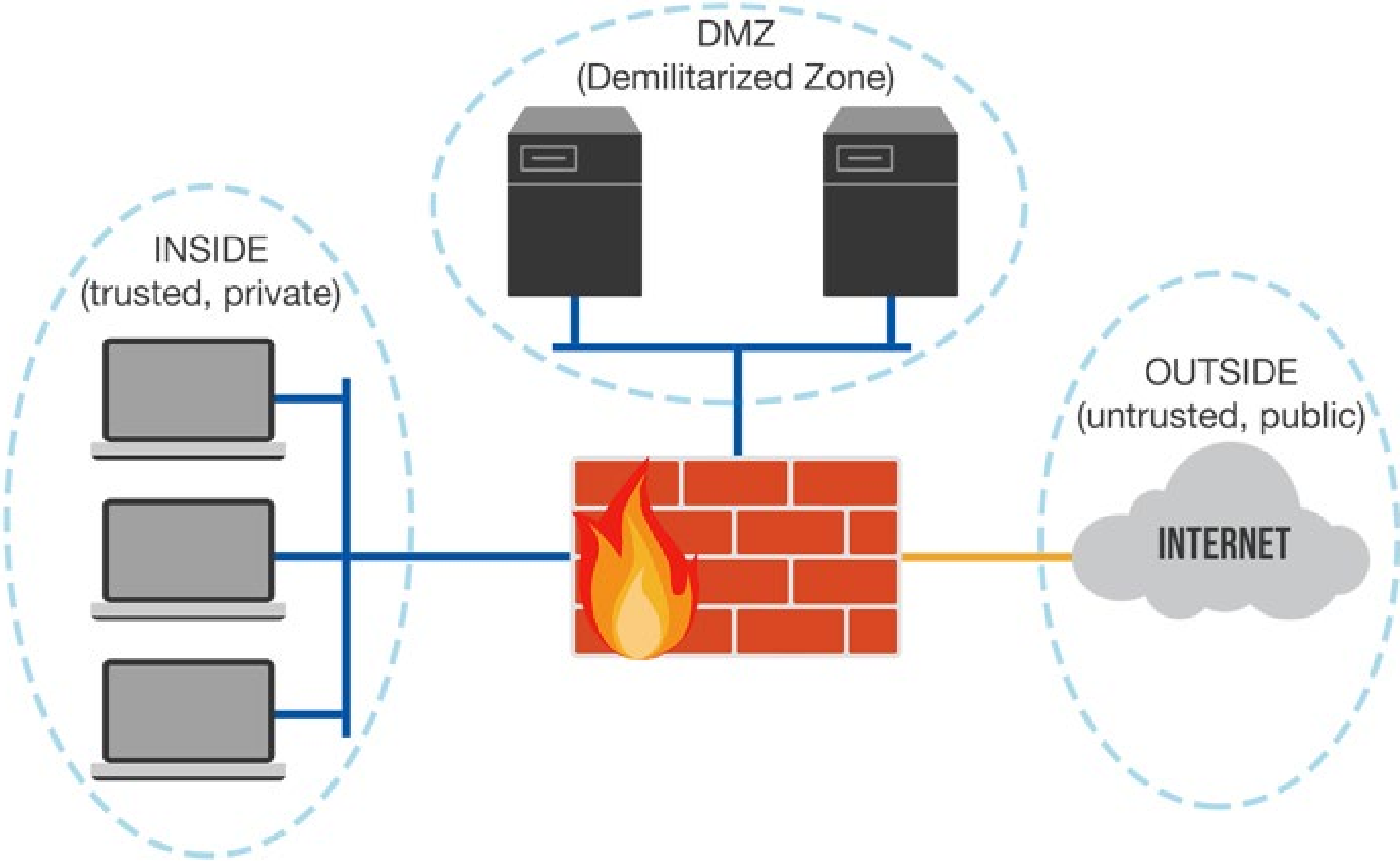
# SECURITY CONTROL TYPES (CONT'D)

| Control Type | Description | Examples |
|---|---|---|
| Mitigating/ Recovery | Minimize the impact of a security incident | System isolation, repair, restore operations, fire suppression |
| Corrective/ Compensating | • Alternative fixes to cover any gaps in the other control types<br>• Provides equivalent or comparable protection<br>• Might have to sacrifice conveniences to achieve the desired result | • A medical instrument uses an older operating system that still has unpatched vulnerabilities that could expose it to remote code execution.<br>• If the device does not need to be connected to the network to provide its primary clinical functions, the compensating control could be to disconnect it from the network. |

# NETWORK SECURITY ZONING

- Network Security Zoning allows an organization to manage different levels of network security
  - Defines security levels for specific areas of the company network
- Used to define clear security boundaries between different parts of the network
- Examples:
  - Internet Zone
    - Uncontrolled zone; outside the organization
  - Internet DMZ Zone
    - Controlled zone; defense between internal network and Internet
  - Production Zone
    - Restricted zone; access is strictly controlled
  - Intranet Zone
    - Controlled zone; no extreme restrictions
  - Management Zone
    - Secured zone; with strict policies

# NETWORK ZONES EXAMPLE



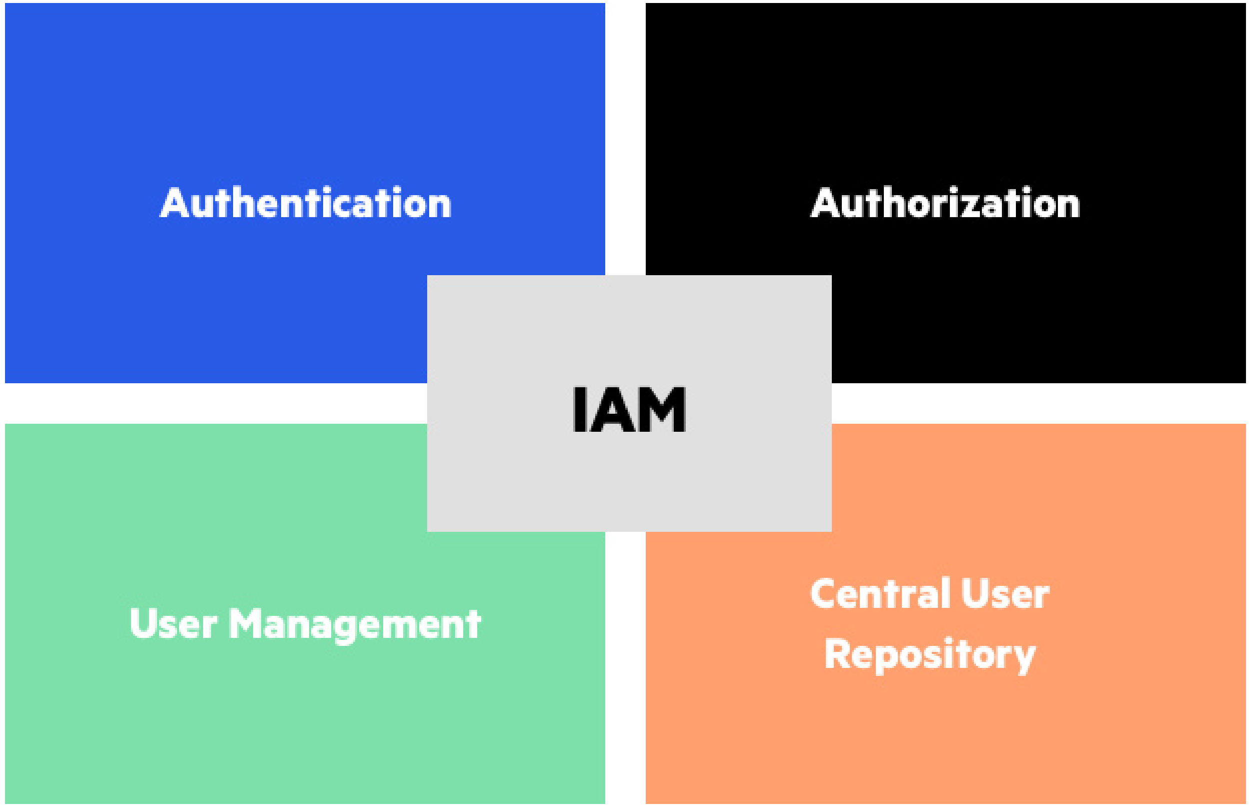
# IDENTITY AND ACCESS MANAGEMENT

WHO

can

ACCESS

WHAT



Authentication

Authorization

IAM

User Management

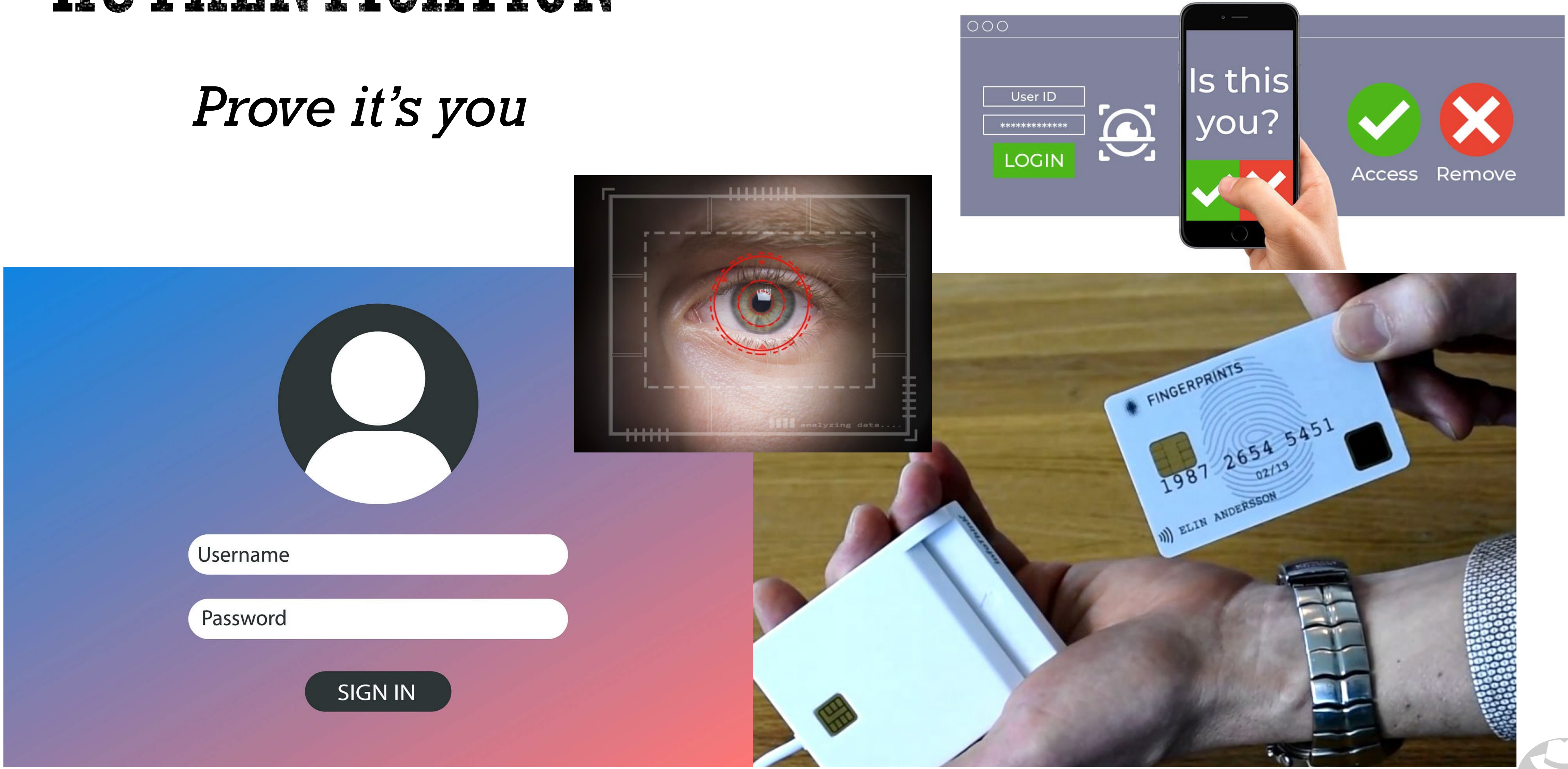
Central User Repository

# IDENTIFICATION

- The action or process of identifying someone
- Can include:
  - Your name, picture, username, ID number, employee number, SSN etc.
- Can also apply to non-human entities such as devices, applications, services
  - Anything that needs to make use of system or network resources

# AUTHENTICATION

*Prove it's you*



# AUTHENTICATION FACTORS

- Something you know
  - (PIN, password)
- Something you have
  - (smart card, certificate, authenticating app on a phone)
- Something you are
  - (fingerprint, iris scan, facial recognition)
- Something you do
  - (signature dynamics, typing dynamics)
- Somewhere you are
  - (geolocation)

Multi-factor authentication uses two or more factors
Not from the same category

# AUTHORIZATION

- What you are allowed to access/do
- Applied after successful authentication
- Permissions:
  - Applied to resources
- Rights / Privileges:
  - Assigned at the system level
- Authorization strategies:
  - Least privilege
    - Give the user the minimal level of access or permissions – just enough to do their job
  - Separation of Duties
    - AKA Segregation of duties
    - Prevent the conflict of interest
    - Reduce the risk of unauthorized access and fraudulent activity
    - Identify and mitigate control failures such as security breaches, information theft and circumvention of security controls

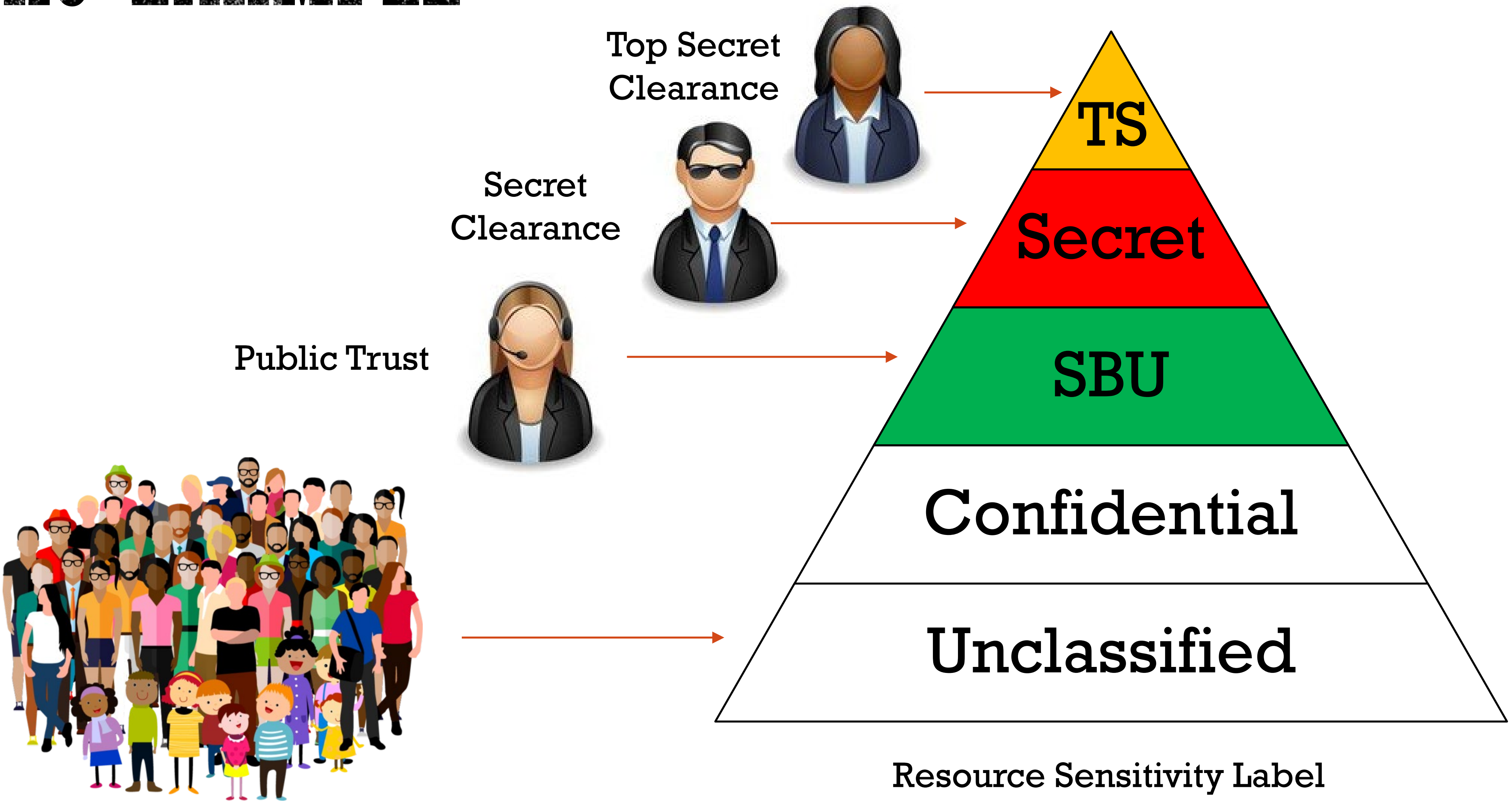
# ACCOUNTING

- Trace an action to an entity
- Prove who or what performed an action
- Log the action for:
  - Compliance
  - Auditing
  - Later reference

# MANDATORY ACCESS CONTROL (MAC)

- Every object is assigned a **sensitivity** label:
  - Unclassified, Confidential, Sensitive But Unclassified, Secret, Top Secret
- Subject receives a **clearance** level
  - Subject undergoes extensive investigation to determine if they are granted clearance
    - Public Trust
    - Secret
    - Top Secret
- Neither can be arbitrarily changed
- Subjects can access objects at or below their clearance level
- Top Secret access can also be compartmentalized
  - Based on need-to-know

# MAC EXAMPLE

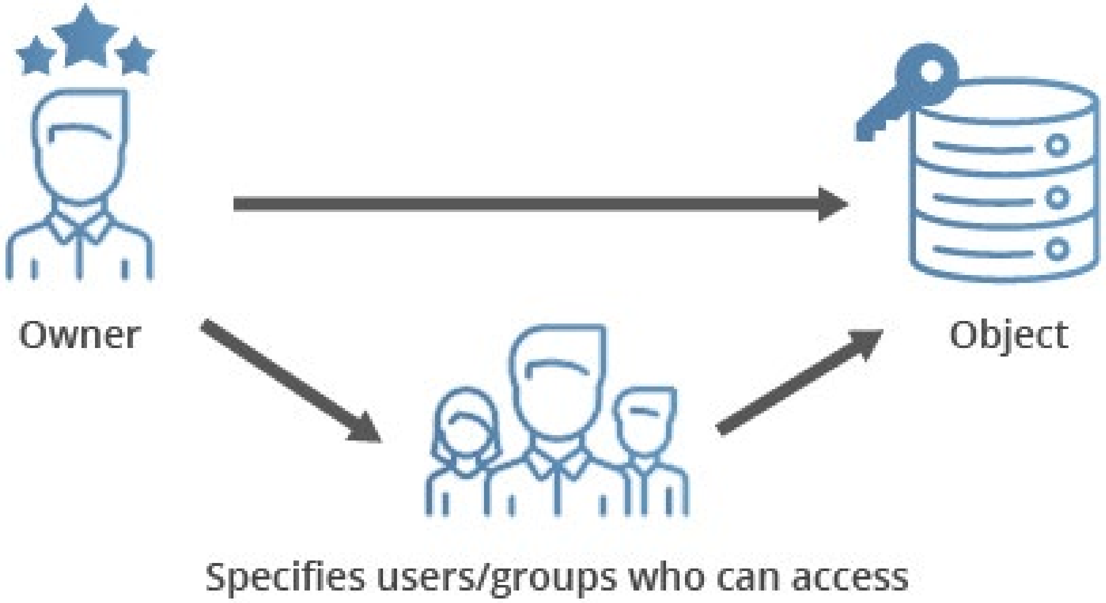


Resource Sensitivity Label

General Public

# DISCRETIONARY ACCESS CONTROL (DAC)

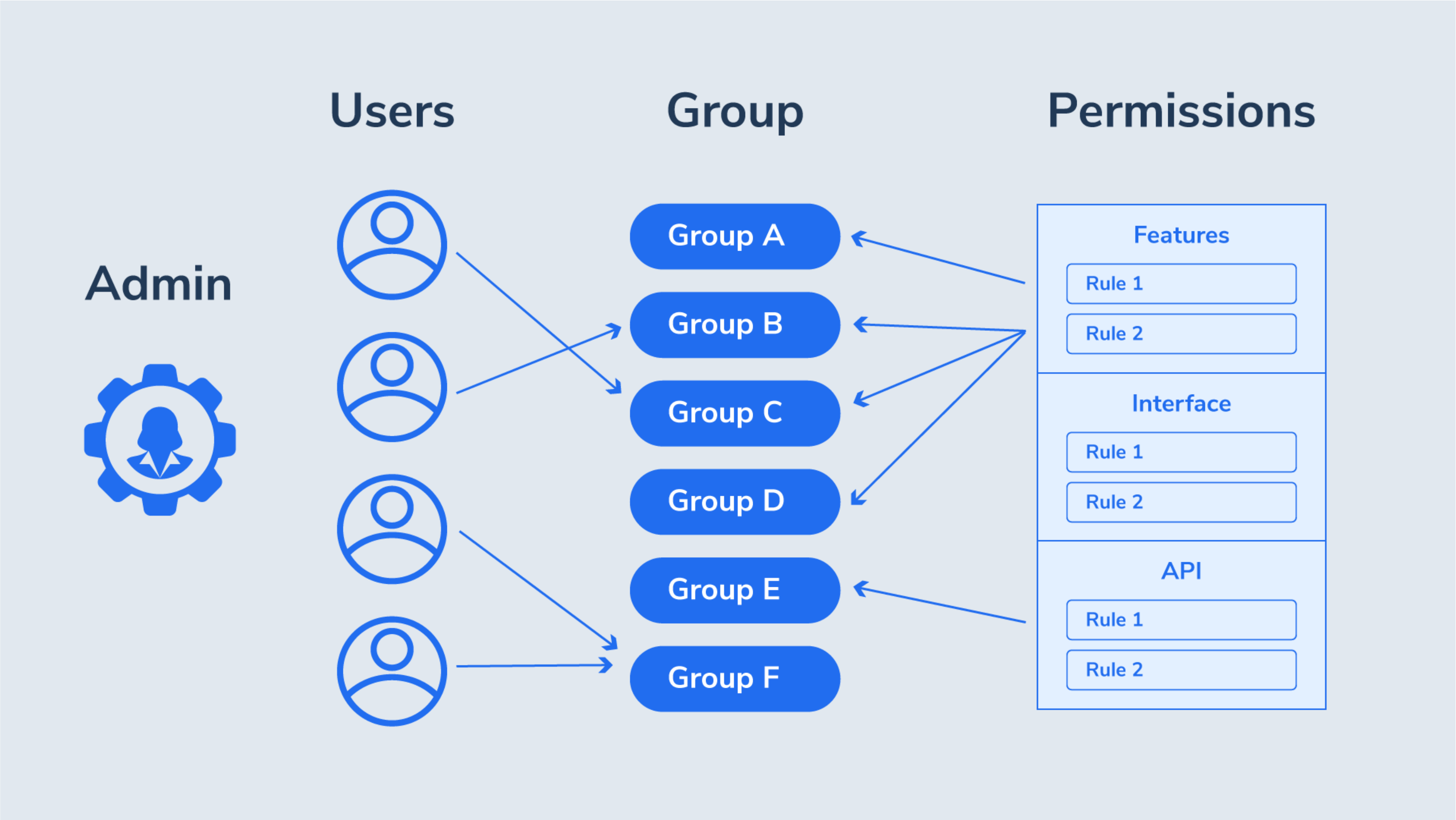
- Used in most operating systems
- Owner of the data defines access at their discretion
- Flexible but weak
- Examples of permissions
  - Read
  - Write
  - Execute
  - Delete
  - List
  - Take ownership



# ROLE-BASED ACCESS CONTROL (RBAC)

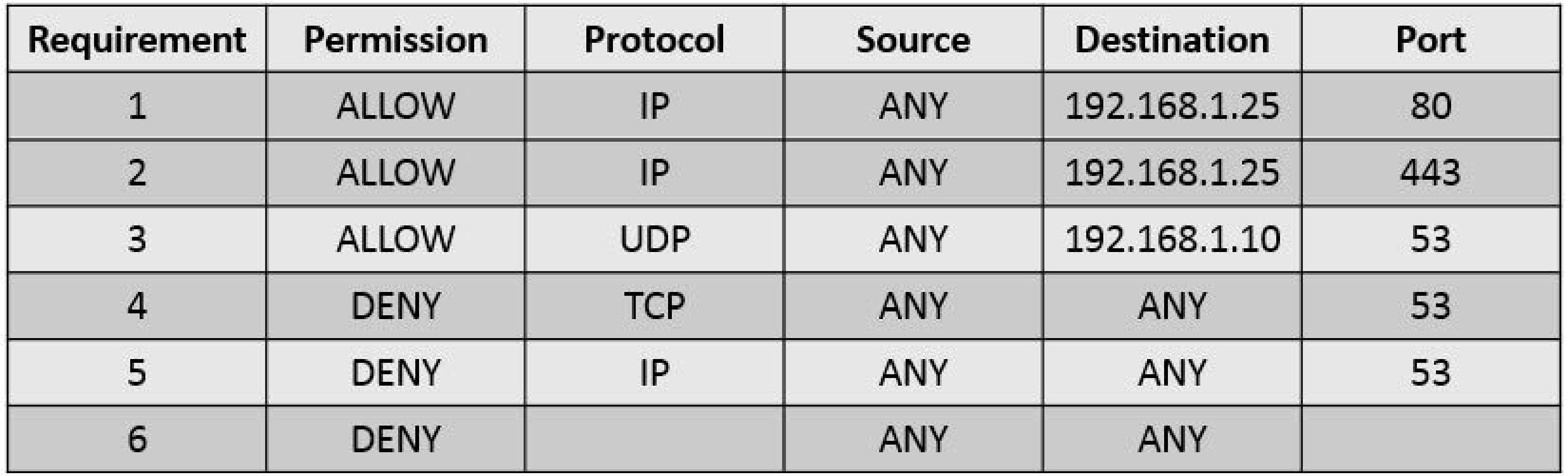
- Access to resources is defined by your role/job function in the organization
- Permissions are granted to the role, not individual users
- Users can be added to or removed from a role
- In Windows, groups are used to represent roles

# RBAC EXAMPLE



# RULE-BASED ACCESS CONTROL (RULEBAC)

- Access is granted or denied based on whether or not a rule is met
- Firewalls and packet-filtering routers use RuleBAC to permit or deny network packets



| Requirement | Permission | Protocol | Source | Destination | Port |
|---|---|---|---|---|---|
| 1 | ALLOW | IP | ANY | 192.168.1.25 | 80 |
| 2 | ALLOW | IP | ANY | 192.168.1.25 | 443 |
| 3 | ALLOW | UDP | ANY | 192.168.1.10 | 53 |
| 4 | DENY | TCP | ANY | ANY | 53 |
| 5 | DENY | IP | ANY | ANY | 53 |
| 6 | DENY |  | ANY | ANY |  |

# 1.2 CYBER KILL CHAIN

- Concepts
- Stages

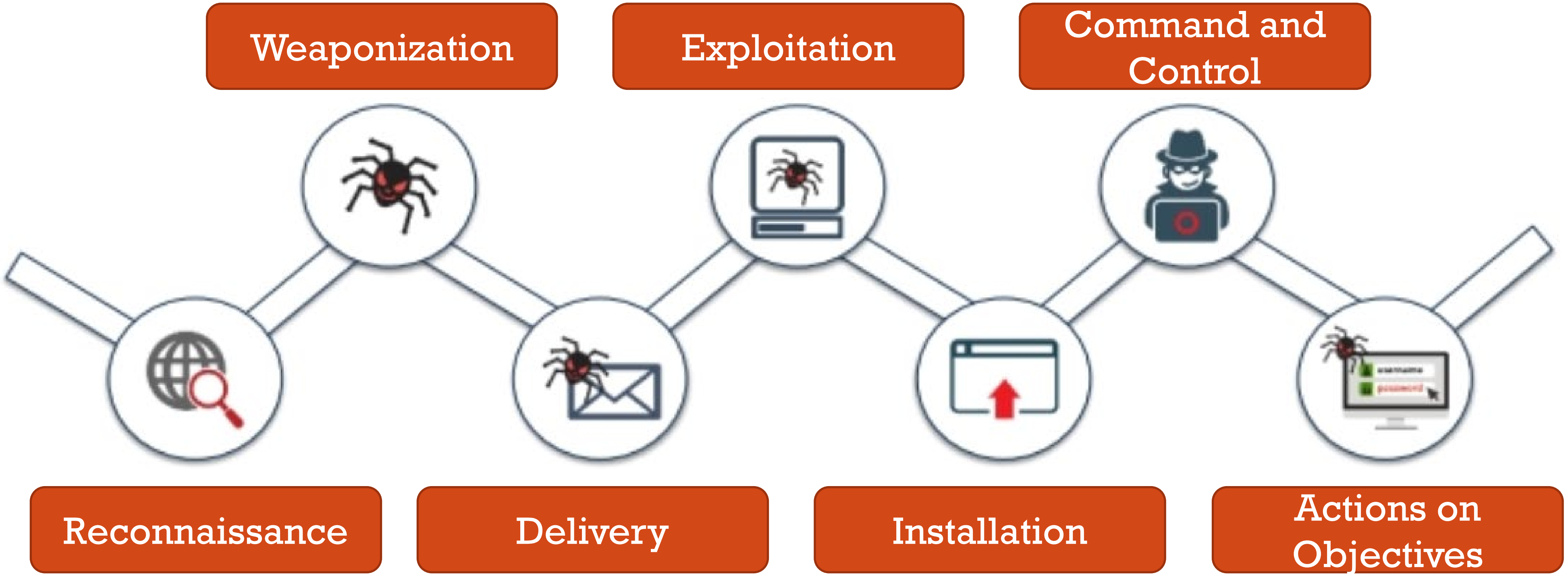
# THE CYBER KILL CHAIN

- AKA cyber-attack chain
- A security model that outlines the phases of a cyberattack
- Developed by Lockheed Martin
- Covers all the stages of a network breach
  - From early planning and spying to the hacker's final goal
- Understanding the stages of an attack enables companies to plan the tactics for preventing and detecting malicious intruders
- Helps prepare for all common online threats, including:
  - Ransomware attacks
  - Network breaches
  - Data theft
  - Advanced persistent threats (APTs)

# ORIGIN OF THE CYBER KILL CHAIN

- The term *"kill chain"* originates from the military
- The original concept defined the structure of a military operation and included:
  - Target identification
  - Force dispatch to target
  - Order to attack the target
  - Destruction of the target

# CYBER KILL CHAIN STAGES



Note: Depending on the vulnerability and exploit used, some of these stages can happen in rapid succession

# 1. RECONNAISSANCE

- Gather data on the target
- Probe for weak points
- Two kinds:
  - Passive
  - Active

# 1. PASSIVE RECONNAISSANCE

- Footprinting - open source intelligence activity
- The attacker searches for information without interacting with the targ
- The victim has no way of knowing or recording the attacker’s activity
- Gather employee email addresses and social media accounts for social engineering
- Focuses on establishing:
  - Who has access to a target system
  - A map of the target’s infrastructure (security tools, software, devices, target’s overall security posture)

# 1. ACTIVE RECONNAISSANCE

- Scanning
- The attacker interacts with the target to gain more information:
  - Open ports
  - Operating system and service versions
  - Applied policies
  - Firewall rules
  - Possible ways of bypassing the firewall

# 2. WEAPONIZATION

- Identify or develop a malicious deliverable for conducting the attack
- Exploit + back door

# 2. WEAPONIZATION COMMON APPROACHES

- Create a botnet
- Create an infected file such as a PDF or Office document, video or popular app
- Prepare a phishing email
- Prepare the server and landing page for a phishing campaign
- Stand up or compromise another machine to house malware
- Prepare a Metasploit "staging" computer for a shrink wrap attack
- Create a virus/worm for a zero-day attack
- Prepare a Raspberry PI to be physically planted at the target site
- Prepare malicious USB sticks

# 3. DELIVERY

- Send the weaponized bundle to the victim
- Examples:
  - Send phishing email
  - Scatter infected USB sticks in the parking lot
  - Physically plant a Raspberry PI on the network

# 4. EXPLOITATION

- Exploit the vulnerability by executing code on the target system
- Often starts with smaller malware called a “stager”, “dropper”, or “downloader”
  - This has a small payload that is easier to deliver
  - Sets up a communication channel to download the larger payload (“stage”)

# 5. INSTALLATION

- Install malware on the target system
  - “Stager” downloads the “stage”
- Download additional tools
- Hide presence from firewall and IDS
- Set up back door / remote access

# 6. COMMAND AND CONTROL

- Establish a connection back to the command and control server (C2)
- The malicious actor can now operate within the target environment and pivot or crawl laterally through the network
- The command and control channel is usually manual
- Requires the attacker to interact with the malware from the C2 server to carry out desired activities

# 7. ACTIONS ON OBJECTIVES

- Attacker takes specific actions to achieve their original objectives:
  - Data exfiltration
  - Espionage
  - Expanded presence in the target infrastructure

# 1.3 MITRE ATT&CK FRAMEWORK

- Overview
- Enterprise
- Mobile
- ICS

# WHAT IS THE MITRE ATT&CK FRAMEWORK?

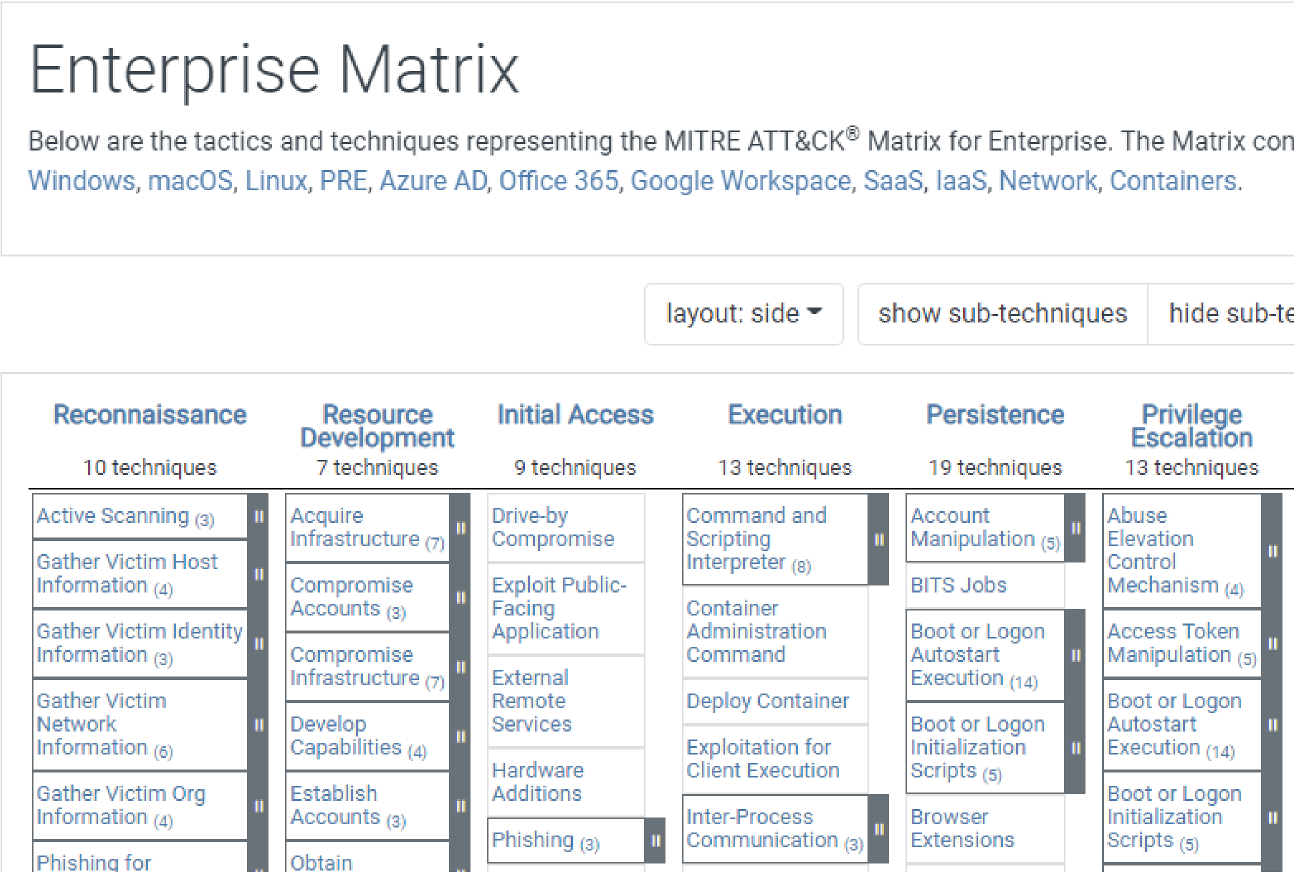
- A comprehensive matrix of tactics and techniques used by threat hunters, red teamers and defenders
- More comprehensive than Cyber Kill Chain
- Tracks cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle
- Indexes everything about an attack from both the attacker and defender sides
- Database is constantly being curated and updated
- Intended to be used as a tool to strengthen an organization’s security posture
- Helps identify attack types and define risk

# MITRE ATT&CK FRAMEWORK (CONT'D)

- Attack scenarios mapped by MITRE ATT&CK can be:
  - Replicated by red teams
  - Tested by blue teams
- Security operations teams can:
  - More easily deduce an adversary's motivation for individual actions
  - Understand how those actions relate to specific classes of defenses

# ATT&CK MATRICES

- ATT&CK for Enterprise
  - PRE
  - Windows
  - macOS
  - Linux
  - Cloud
  - Network
  - Containers
- ATT&CK for Mobile
  - Android
  - iOS
- ATT&CK for ICS



Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix con

Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation |
|---|---|---|---|---|---|
| 10 techniques | 7 techniques | 9 techniques | 13 techniques | 19 techniques | 13 techniques |
| Active Scanning (3) | Acquire Infrastructure (7) | Drive-by Compromise | Command and Scripting Interpreter (8) | Account Manipulation (5) | Abuse Elevation Control Mechanism (4) |
| Gather Victim Host Information (4) | Compromise Accounts (3) | Exploit Public-Facing Application | Container Administration Command | BITS Jobs | Access Token Manipulation (5) |
| Gather Victim Identity Information (3) | Compromise Infrastructure (7) | External Remote Services | Deploy Container | Boot or Logon Autostart Execution (14) | Boot or Logon Autostart Execution (14) |
| Gather Victim Network Information (6) | Develop Capabilities (4) | Hardware Additions | Exploitation for Client Execution | Boot or Logon Initialization Scripts (5) | Boot or Logon Initialization Scripts (5) |
| Gather Victim Org Information (4) | Establish Accounts (3) | Phishing (3) | Inter-Process Communication (3) | Browser Extensions | |
| Phishing for | Obtain | | | | |

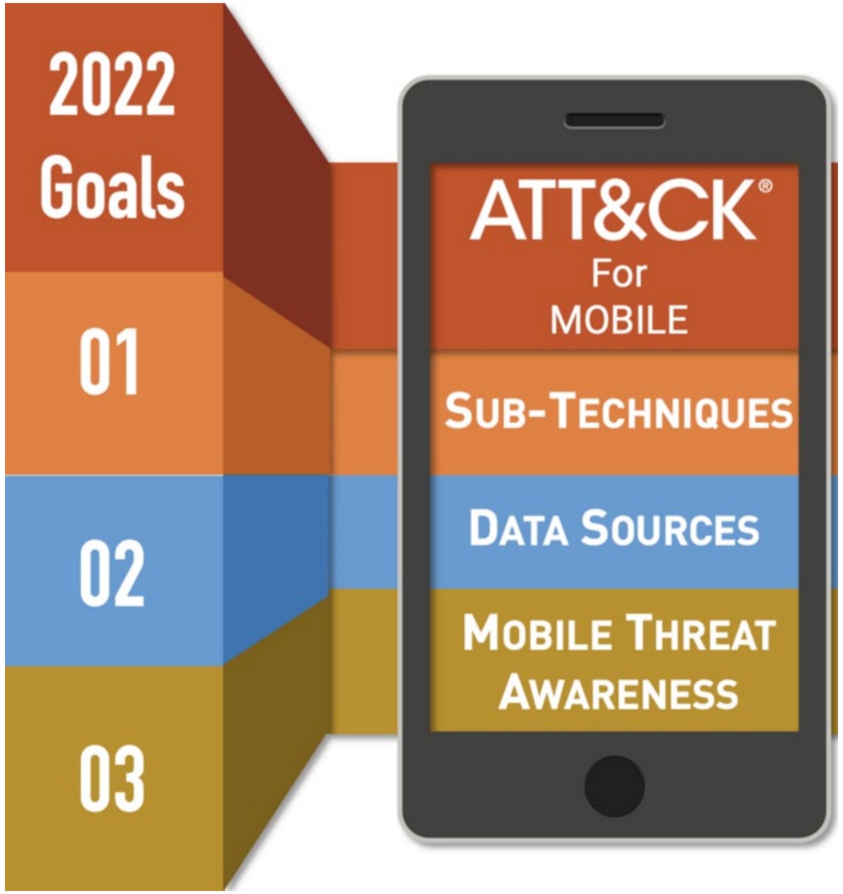
# ATT&CK FOR ENTERPRISE TACTICS CATEGORIES

- Reconnaissance
- Resource development
- Initial access
- Execution
- Persistence
- Privilege escalation
- Defense evasion
- Credential access
- Discovery
- Lateral movement
- Collection
- Command and Control
- Exfiltration
- Impact

MITRE ATT&CK currently identifies 188 attack techniques and 379 sub-techniques for enterprises

# ATT&CK FOR MOBILE CATEGORIES

- Same categories as Enterprise except no:
  - Reconnaissance
  - Resource development



# ATT&CK FOR ICS CATEGORIES

- Initial Access
- Execution
- Persistence
- Privilege escalation
- Evasion
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Inhibit Response Function
- Impair Process Control
- Impact

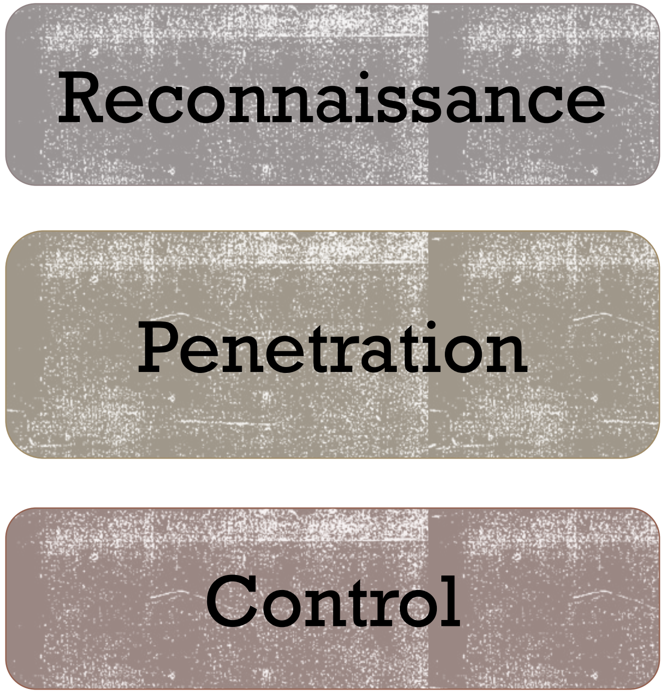
# 1.4 HACKING

- Concepts
- Terminology

# WHAT IS HACKING?

- Exploiting system vulnerabilities and compromising security to gain unauthorized access to system resources
- Modifying system or application features to achieve a goal
- Used to steal and redistribute intellectual property leading to business loss

# TRADITIONAL HACKING MODEL



Reconnaissance

OSINT
Footprinting
Scanning/Fingerprinting

Penetration

Active hacking
Delivering malware
Social engineering
Physical intrusion

Control

Planting backdoors
Instructing zombies
Covering tracks

# WHO IS A HACKER?

- Intelligent person with excellent computer and networking skills exploring a system or network
- Hobbyist testing vulnerabilities of systems and networks
- Consultant hired by an organization to improve network security
- Cyber criminal
- Anyone attempting to gain knowledge for legal or illegal purposes

# HACKER CLASSES / TYPES

| Hacker Class | Description |
|---|---|
| Black Hat | Performs malicious activities; cyber criminal |
| Grey Hat | Performs good or bad activities but do not have the permission of the organization they are hacking against |
| White Hat /<br>Ethical Hacker | Uses their skills to improve security by exposing vulnerabilities before malicious hackers |
| Script Kiddie / Skiddie | Unskilled individual; uses malicious scripts or programs developed by others to attack systems and deface websites |
| State-Sponsored Hacker | Hired by a government to perform attacks on other governments or high-profile targets |
| Hacktivist | Hacks for a cause or political agenda |
| Suicide Hacker | Not afraid of going jail or facing any sort of punishment;<br>they hack to get the job done |
| Cyber Terrorist | Motivated by religious/political beliefs to create fear or disruption |

# HACKER TYPE EXAMPLES

Black hat

Grey hat

White hat

Script kiddie

State sponsored Hacker

Hacktivist

# ADVANCED PERSISTENT THREAT (APT)

- APTs are external threats
- They seek to:
  - Quietly gain access to your system
  - Stay there undetected as long as possible
- They are usually sponsored by nation-states and well-funded
- They use multiple attack vectors (whatever they can) to gain access to sensitive data
- They are used for intelligence-gathering operations against government, military, and commercial networks
- There have recently been high-profile cases in the news of APTs exfiltrating and exposing corporate and government data

# APT EXAMPLES

- APT 27 – LuckyMouse
  - Chinese group that focuses on Asian/Pacific nations/Middle Eastern states
  - Targets aerospace, education, and government sectors
  - Uses existing tools such as PsExec, Mimikatz, ProcDump and others
- APT 28 – Fancy Bear
  - Russian cyber espionage group sponsored by the Russian Government
  - Associated with  the Russian military intelligence agency GRU
  - Targets NATO-aligned countries
  - Uses zero-day exploits, phishing and malware
- APT 35 – Charming Kitten
  - Iranian government cyber warfare group that uses phishing and social media
  - Developed a tool to steal data from well-known email providers such as Google, Yahoo, and Microsoft
  - Documented interference in US 2020 and 2022 elections
- APT 37 – Reaper
  - North Korean government hacking group
  - Mostly targets South Korean industries such as chemical, electronics, manufacturing, aerospace, automotive, and healthcare

# APT 37 EXAMPLE

- Took advantage of the Oct. 29 Itaewon crowd-crush tragedy, which killed more than 150 people
- Used social engineering to trick South Koreans into downloading malicious files

North Korean hackers exploit Itaewon tragedy to infiltrate South Korean targets

# INSIDER THREAT

- Trusted users who abuse/misuse the system
- Most insider threats are not intentionally malicious
  - Users cause accidental breaches
- Some insider threats are purposeful
  - Disgruntled employee
  - Corporate or government spy
  - Terminated employee or contractor whose access was not revoked upon termination

# 1.5 ETHICAL HACKING

- Understanding Ethical Hacking
- Ethical Hacker Skills
- Developing Technical Hacking Skills

# WHAT IS ETHICAL HACKING?

- The use of hacking to improve security
- An attempt to identify vulnerabilities before they are exploited by a bad actor
- Ethical hackers use the same tools, steps, and techniques as other hackers
  - However the intent is to protect, not damage

# WHY ETHICAL HACKING IS NECESSARY

- Keep ahead of unethical hackers
- Uncover and fix vulnerabilities before they are exploited by a bad actor
- Analyze and strengthen an organization's security posture
- The ethical hacker attempts to discover:
  - What an intruder can see
  - What an intruder can do
  - If any intrusions have already occurred
  - If systems are properly patched and protected
  - The amount of effort necessary to protect the system
  - If information security measures are in compliance with industry and legal standards

# ETHICAL HACKING VS PENETRATION TEST

- Ethical hacking the primary mechanism of a penetration test
  - The ethical hacker is part of the penetration testing team
- In a penetration test, an organization engages a team of cybersecurity experts
  - Actively attempt to exploit systems, infrastructure, and people
- Not to be confused with vulnerability scan
  - A vulnerability scan is one small part of a penetration test
  - It identifies systems that *might* be vulnerable to hacking
  - It does not attempt to actually exploit the vulnerable system

# TECHNICAL SKILLS OF AN ETHICAL HACKER

- In-depth knowledge of major operating environments, concepts, technologies and related hardware and software
- Should be a computer expert understanding technical domains
- Should be comfortable using the same tools and exploits that other hackers use
- Should have security knowledge and experience
- Should understand sophisticated attacks

# NON-TECHNICAL SKILLS OF AN ETHICAL HACKER

- Ability to learn and adapt new technologies quickly
- Strong work ethic
- Commitment to the organization’s security and policies
- Understanding of local, state, and federal laws and organizational compliance
- Ability to communicate concisely with the client
- Ability to explain that systems can never be fully secured
    - Security can always be improved
    - It is up to the organization to implement recommendations once vulnerabilities are discovered

# ETHICAL HACKING PROCESS

- The client hires you to find vulnerabilities in their network
- A contract will clearly specify the rules of engagement:
  - The start time
  - Which systems will be tested
  - Which systems will not be tested
  - If the test will include processes and people
    - Social engineering

# TESTING TYPES

- White box
  - The tester has complete visibility into the system they are testing
  - Allows the tester to be more thorough (need not "discover" the attack surface)
  - Used by in-house teams to test their own systems
  - Risk that teams already familiar with a system will overlook some vulnerabilities
- Grey box
  - The tester has some visibility into the system they are testing
- Black box
  - The tester has no visibility into the system they are testing
  - Most closely resembles actual attack
  - Used by third parties performing a security audit of the system
  - Requires the attacker to be creative

# DISCOVERING SENSITIVE INFORMATION

- If during your pentest you come across some really sensitive information:
  - An entire list of usernames and passwords
  - PII (personally identifiable) or PHI (personal health) information
  - The user's bank account and login info
- You should stop and notify the client's system administrator
  - You want to prevent any future possible damage
  - Let them deal with it

# DISCOVERING ILLEGAL ACTIVITY

- While conducting a routine security assessment, you might discover that the client is engaged in fraudulent or illegal activity
- Your first duty is to upholding the law
- You must immediately stop work and contact the proper authorities first
  - You can then consider whether or not to show your findings to the client's upper management
  - Be careful about showing the client what you have discovered
  - They might try to dispose of evidence before law enforcement arrives

# DISCOVERING EVIDENCE OF AN ACTUAL INTRUSION

- As you conduct your penetration test, you might discover evidence of actual hacking or compromise
- Examples:
  - Active malware/trojans/botnet/compromised machines
  - Unauthorized data exfiltration
  - Unexpected connections to the Internet
  - A production server with some of its log files deleted
  - A workstation that is scanning the internal network
  - Unusual network traffic
- You should stop what you are doing
  - Notify the client's trusted point of contact for guidance
  - The company's security team should investigate before you continue with your engagement

# USING HACKING TOOLS

- An ethical hacker must practice using the same tools and methods a black hat would use
  - You cannot be effective otherwise
- Using such tools will always carry an element of risk
  - They could potentially exploit vulnerabilities and damage the systems you are testing
- You must keep these risks in mind when performing your penetration test:
  - Avoid fragile systems
  - Perform potentially disruptive tests when they will have the least impact on the network and its users
  - Coordinate closely with your client counterparts to ensure a disaster recovery plan is in place to restore systems in case of accident
  - Communicate incidents with your counterparts so that DR can be implemented immediately

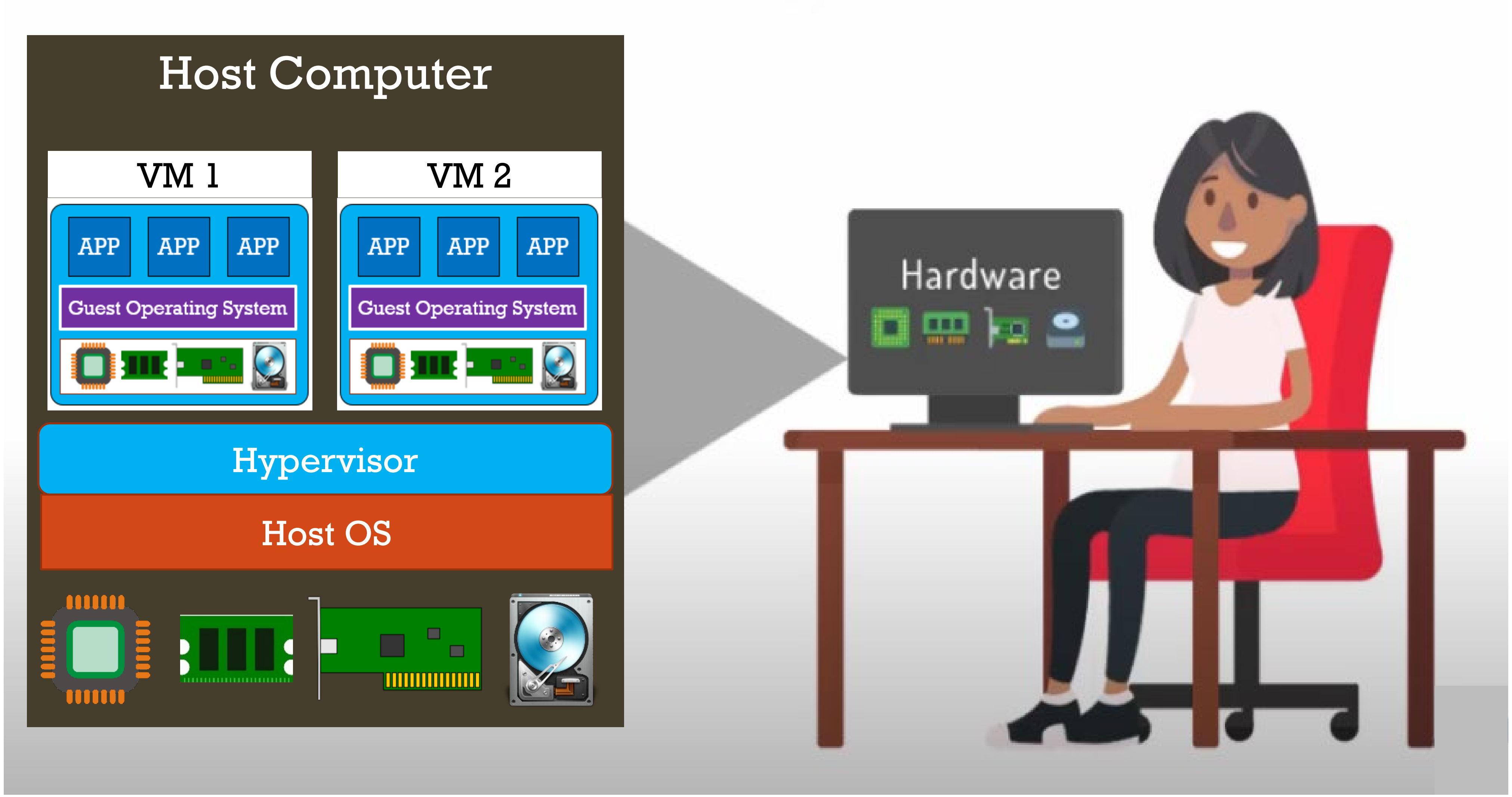
# DEVELOPING ETHICAL HACKING SKILLS

- Set up a practice lab hacking environment
- Keep the lab away from a production environment
- Install the various operating systems and tools that hackers use
- Download pre-configured "targets" that you can practice on:
    - DVWA / Mutillidae / Metasploitable 1, 2, or 3
    - OWASP Web Testing Environment / WebGoat
    - OWASP iGoat
    - OWASP Android Crackmes
    - bWAPP / Bee-Box
    - Kioptrix Levels 1 - 4
    - VMs from Vulnhub

# VIRTUALIZED PRACTICE ENVIRONMENT

- You can set up a single host computer to run several guest computers inside it
  - Rather than having multiple physical computers in your lab
- Virtual Machines (VMs):
  - Run an entire operating system as an app on your lab machine
  - Not a simulation
  - Standard practice in a corporate data center
  - Each VM has its own NIC, IP address, MAC address, CPU, RAM, disks, operating system, applications, etc.
    - On the network, the VM appears as any other host
    - VMs borrow the functionality of physical hardware but are kept separate
    - A "hypervisor"
    - You can have as many VMs as your host has hardware to support
  - Virtualization products: VMware, Virtual Box, Hyper-V, Bluestacks, Genymotion, iPadia

# VIRTUAL MACHINE EXAMPLE



# VIRTUALIZED CONTAINERS

- You can also run “containers” on your host machine
  - VM for one app only
  - The container directly uses the host OS and hardware
  - Very lightweight
- Container products: Docker, Kubernetes, Podman, ZeroVM

# RISKS OF VIRTUALIZATION

- Virtual environments are designed for functionality, rather than security
  - They were created to address the problem of wasted resources, physical space, and power consumption that physical devices have
- You must be very careful to limit the amount of host resources a VM or container is permitted to have
  - Consider disallowing the VM from interacting directly with the host or outside network
- A VM environment is an imperfect sandbox
  - Most implementations assume the VM will interact with the host and/or network
  - You must configure the level of isolation
  - There is always the risk that a malicious app running in the VM can escape the sandbox

# RISKS OF VIRTUALIZATION

- Virtual environments are designed for functionality, rather than security
  - They were created to address the problem of wasted resources, physical space, and power consumption that physical devices have
- You must be very careful to limit the amount of host resources a VM or container is permitted to have
  - Consider disallowing the VM from interacting directly with the host or outside network
- A VM environment is an imperfect sandbox
  - Most implementations assume the VM will interact with the host and/or network
  - You must configure the level of isolation
  - There is always the risk that a malicious app running in the VM can escape the sandbox

# RISKS OF VIRTUALIZATION (CONT'D)

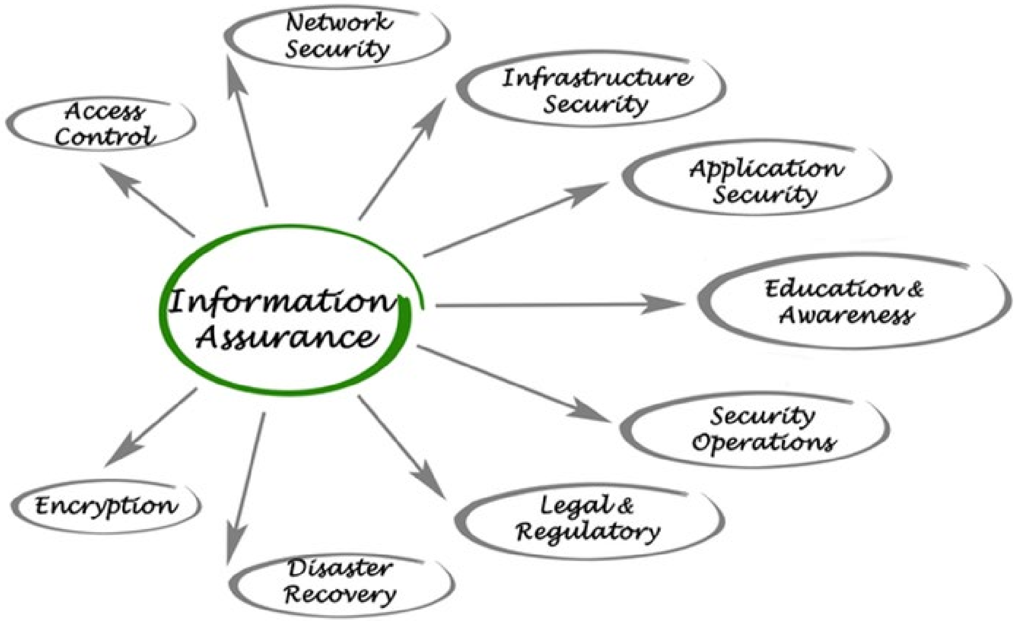
- Containerization is an even greater risk to the host
- A container uses the host OS and hardware
- An app inside of a container might consume too many host resources and "starve" the host of CPU, RAM or disk space

# 1.6 INFORMATION ASSURANCE

- IA
- Policies

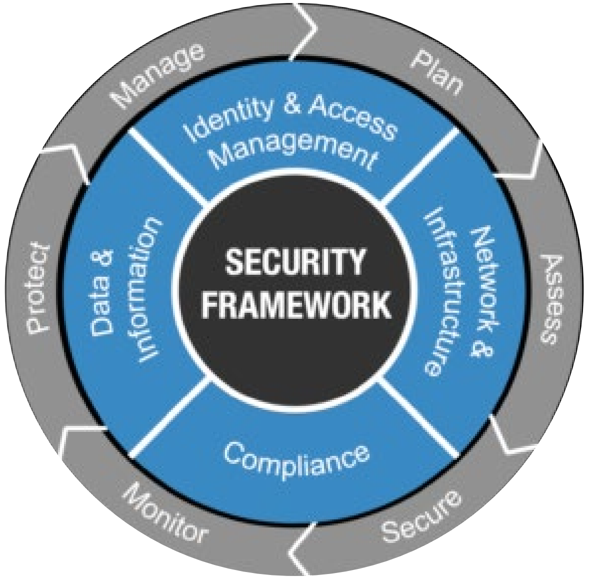
# WHAT IS INFORMATION ASSURANCE (IA)?

- The assurance that information and information systems maintain confidentiality, integrity, availability, and authenticity at all times
- IA is achieved by implementing a security architecture and management program



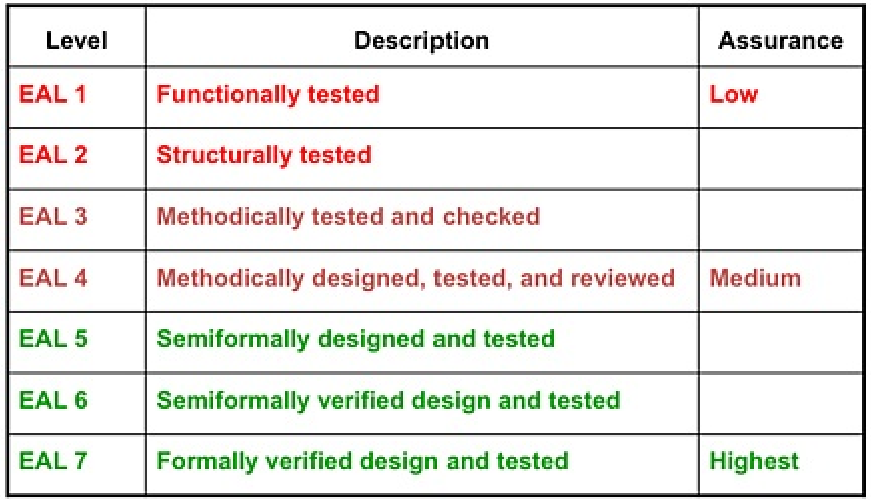
# INFORMATION SECURITY FRAMEWORK

- A series of documented processes
  - Used to define policies and procedures for the implementation and management of information security controls in an enterprise environment
- A blueprint for building an information security program to manage risk and reduce vulnerabilities
- Popular Frameworks:
  - PCI DSS
  - ISO 27001/27002
  - CIS Critical Security Controls
  - NIST Framework for Improving Critical Infrastructure
  - Sherwood Applied Security Business Architecture (SABSA)
  - Control Objectives for IT (COBIT)
  - TOGAF



# COMMON CRITERIA (CC)

- An international set of standardized guidelines and specifications
- Establishes a baseline level of confidence in the security functionality of IT products
  - Assigns an Evaluation Assurance Level to a specific product
- Ensures that certified products meet an agreed-upon security standard for government deployments



| Level | Description | Assurance |
|---|---|---|
| EAL 1 | Functionally tested | Low |
| EAL 2 | Structurally tested | |
| EAL 3 | Methodically tested and checked | |
| EAL 4 | Methodically designed, tested, and reviewed | Medium |
| EAL 5 | Semiformally designed and tested | |
| EAL 6 | Semiformally verified design and tested | |
| EAL 7 | Formally verified design and tested | Highest |

# ENTERPRISE INFORMATION SECURITY ARCHITECTURE (EISA)

- An organization adopts relevant industry/government frameworks to create their EISA
- The key elements of an EISA are:
  - **Business context**
    - Defines enterprise information use cases and their importance for reaching business goals
  - **Conceptual layer**
    - Provides the big picture, including the enterprise profile and risk attributes
  - **Logical layer**
    - Defines the logical paths between information, services, processes and application
  - **Implementation**
    - Defines how the EISA should be implemented
  - **Solutions**
    - Details the software, devices, processes and other components used to mitigate security vulnerabilities and maintain security for the future

# INFORMATION SECURITY MANAGEMENT PROGRAM

- Implementation of EISA into a program
- Designed to ensure the business operates in a state of reduced risk
- Encompasses all organizational and operational processes and participants relevant to information security
- ⚠ IA focuses on risk assessment and mitigation
- ⚠ InfoSec focuses on actually implementing security measures to safeguard systems

# SECURITY METRICS

- Metrics are a method of measuring something over time
- You can use metrics to show the effect of security improvements over time
- For example, you may wish to look at the number of unpatched and known vulnerabilities
- As this number decreases, your network would be considered to have improved security Reports and testing tools alone cannot show progress
- You must have measurable results using metrics
- Examples of security metrics:
  - Number of security incidents per month
  - Incident response time
  - Incident mitigation/repair time
  - Number of systems patched
  - Number of antivirus updates per month

# POLICIES, PROCEDURES, GUIDELINES

- Policies
  - High-level statements about protecting information
  - Business rules to safeguard CIA triad
  - Security Policies can be applied to Users, Systems, Partners, Networks, and Providers
- Procedures
  - Set of details steps to accomplish a goal
  - Instructions for implementation
- Guidelines
  - Advice on actions given a situation
  - Recommended, not mandatory

# INFORMATION SECURITY POLICIES

- Designed to ensure all users and networks within an organization meet minimum IT security and data protection security requirements
- Outlines expectations for employees and penalties for breaking policy
- Goals:
  - Maintain management and administration of network security
  - Protect computing resources
  - Avoid legal liabilities
  - Prevent waste of computing resources
  - Prevent unauthorized modification of data
  - Define user access rights
  - Protect confidential, proprietary information from theft, misuse, and unauthorized disclosure

# TYPES OF SECURITY POLICIES

- Promiscuous Policy
  - No restrictions
- Permissive Policy
  - Some restrictions but only on known attacks
- Prudent Policy
  - Maximum security
  - Blocks all services unless used by the organization
  - Typical in an unclassified government facility
- Paranoid Policy
  - Restricts everything
  - Little or no Internet connectivity
  - Typical in a classified government facility

# IMPLEMENTING AN INFORMATION SECURITY POLICY

- Implement the strictest policy that is practical for that environment
- Harden the network, devices, services, and apps at all levels
    - Implement multiple layers of security
    - Do not think that a strong perimeter or physical security alone will be enough to protect your network
- Two printed copies of the policy should be given to an employee as soon as they join the organization
- The employee should be asked to sign and return one copy
    - This should be safely filed by the company
- No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms

# COMMON SECURITY POLICIES

- User Account Policy
  - Defines the account creation process, authority, rights and responsibility of user accounts.
- Password Policy
  - Specifies password length, complexity, history, and reuse requirements
  - May specify different requirements for different user roles
- Acceptable Use Policy (AUP)
  - Governs employees’ use of company equipment and Internet services
  - Typically forbids the use of equipment to defraud, defame, or obtain illegal material
  - May also prohibit unauthorized hardware or software installation, actual or attempted hacking activity and intrusions (snooping)
  - May also specify limits of employees using company equipment for personal use

# COMMON SECURITY POLICIES (CONT'D)

- Wireless Security Policy
  - Specifies how staff, guests, vendors, partners, etc. may connect to and use the company's Wi-Fi
- Data Retention Policy
  - How long records, including emails, must be retained
  - How to safeguard stored records
- Access Control Policy
  - Defines the resources being protected and the rules that control access to them
- Remote Access Policy
  - Who can dial/VPN into the company network
  - When and how remote access is permitted
- Firewall Management Policy
  - Defines access, management and monitoring of firewalls in an organization.

# COMMON SECURITY POLICIES (CONT'D)

- Network Connection Policy
  - Defines who can install new resources on the network, approve the installation of new devices, document network changes etc.
- Information Protection Policy
  - This defines the sensitivity levels of information, who may have access, how it is stored and transmitted, and how it should be deleted from storage media etc.
- Special Access Policy
  - This defines the terms and conditions of granting special access to system resources.
- Email Security Policy
  - This policy is designed to govern the proper usage of corporate email.

# PRIVACY POLICIES IN THE WORKPLACE

- Employers have access to employees' personal information
  - Employees have no expectation of privacy except as required by law
- Rules for Workplace Privacy
  - Limit the amount of collected information (legal)
  - Tell employees about the information being collected and keep them informed of any potential collection, use, and disclosure of person information
  - Maintain accurate employee records
  - Provide employees access to their person information
  - Secure employees personal information
  - Monitoring employees' email or Internet activities without informing them could legally be an invasion of privacy

# HOW TO CREATE AND IMPLEMENT A SECURITY POLICY

1. Perform a Risk Assessment
2. Use proper types of organizational standards
3. Include senior management
4. Set penalties for violations
5. Create a finalized version
6. Ensure all staff understand and sign an agreement to abide by the policy
7. Enforce the policy at all levels, including top management and contractors
8. Train employees sufficiently and in accordance with their work role
9. Review and update regularly

# HR/LEGAL IMPLICATIONS OF SECURITY POLICY ENFORCEMENT

- Human Resources
  - Responsible for making employees aware of security policies
  - Security training for employees
  - Work with management to monitor policy implementation and violation
- Legal
  - Policies should be developed with consultation with legal experts
  - Additional attention to violation of employee rights must be considered

# SECURITY POLICY RISKS

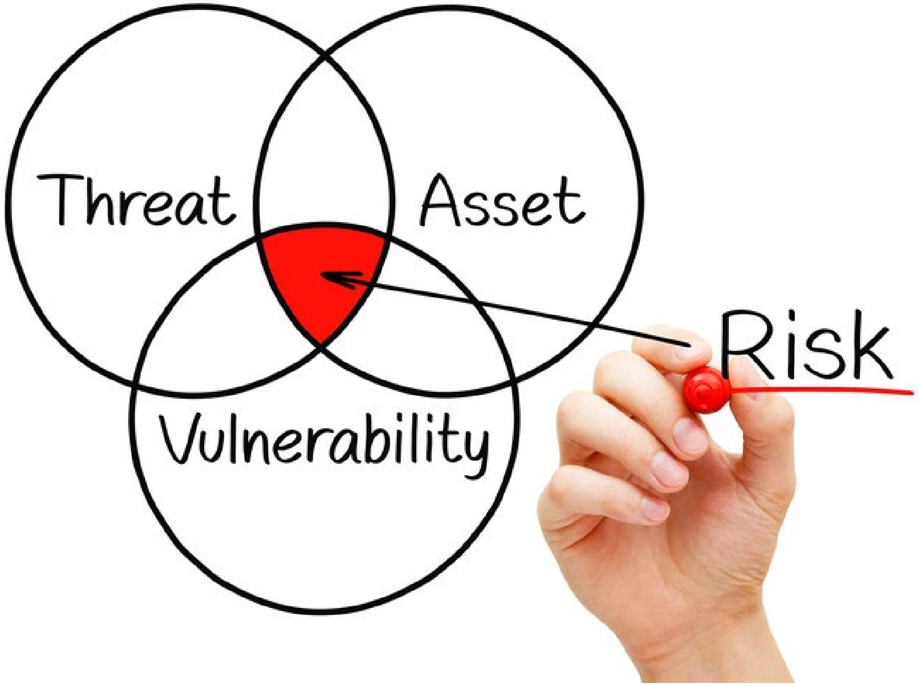
- Policies are at risk of:
  - Not being enforced
  - Not taken seriously
  - Being enforced sporadically or unevenly
  - Not being accepted/adopted by staff
  - Not being supported by upper management
- Security culture in the organization starts with top management
- Everyone including the CEO down to the new hires must comply with security policies
- If the executive management does not comply with the security policies and the consequences of non-compliance with the policy are not enforced, then mistrust and apathy toward compliance with the policy can affect your organization

# 1.7 RISK MANAGEMENT

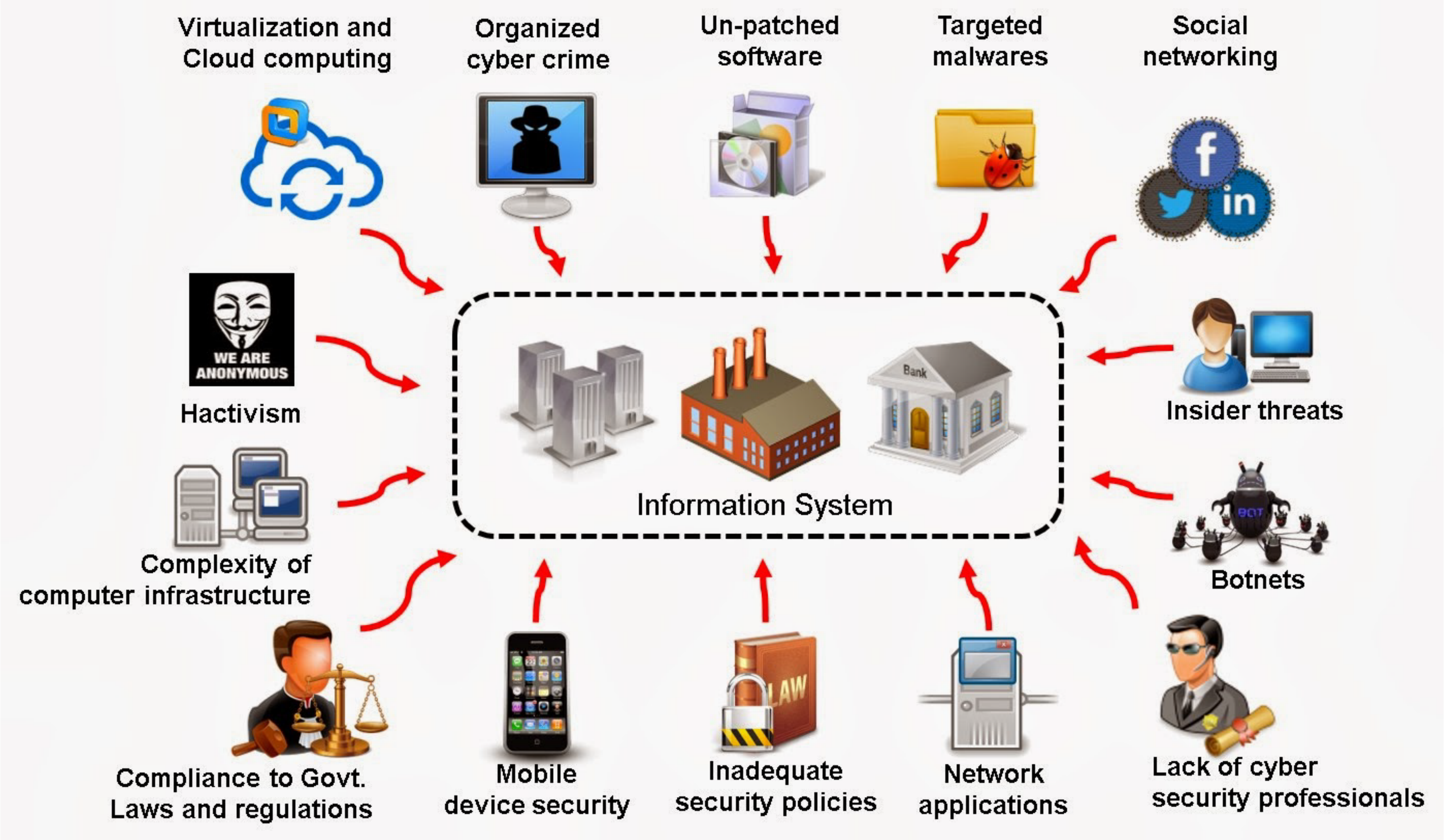
- Risk Management
- BIA
- Risk Assessments
- Risk Response

# WHAT IS RISK?

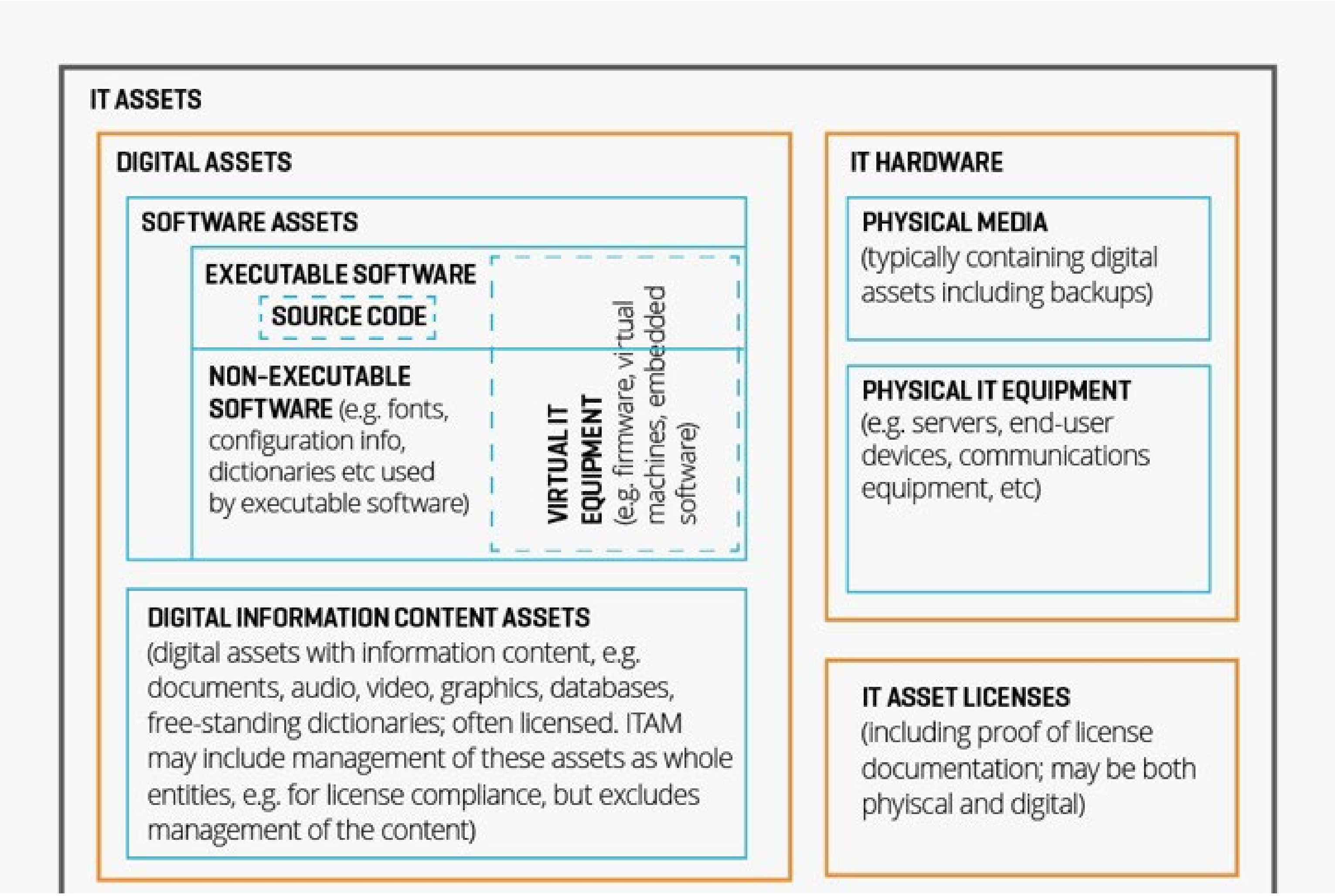
- The probability that a threat may actually materialize and cause damage



# WHAT ARE THE RISKS FOR EACH OF THESE?



# IT ASSETS



IT ASSETS

DIGITAL ASSETS

SOFTWARE ASSETS

EXECUTABLE SOFTWARE

SOURCE CODE

**NON-EXECUTABLE SOFTWARE** (e.g. fonts, configuration info, dictionaries etc used by executable software)

**VIRTUAL IT EQUIPMENT** (e.g. firmware, virtual machines, embedded software)

**DIGITAL INFORMATION CONTENT ASSETS** (digital assets with information content, e.g. documents, audio, video, graphics, databases, free-standing dictionaries; often licensed. ITAM may include management of these assets as whole entities, e.g. for license compliance, but excludes management of the content)

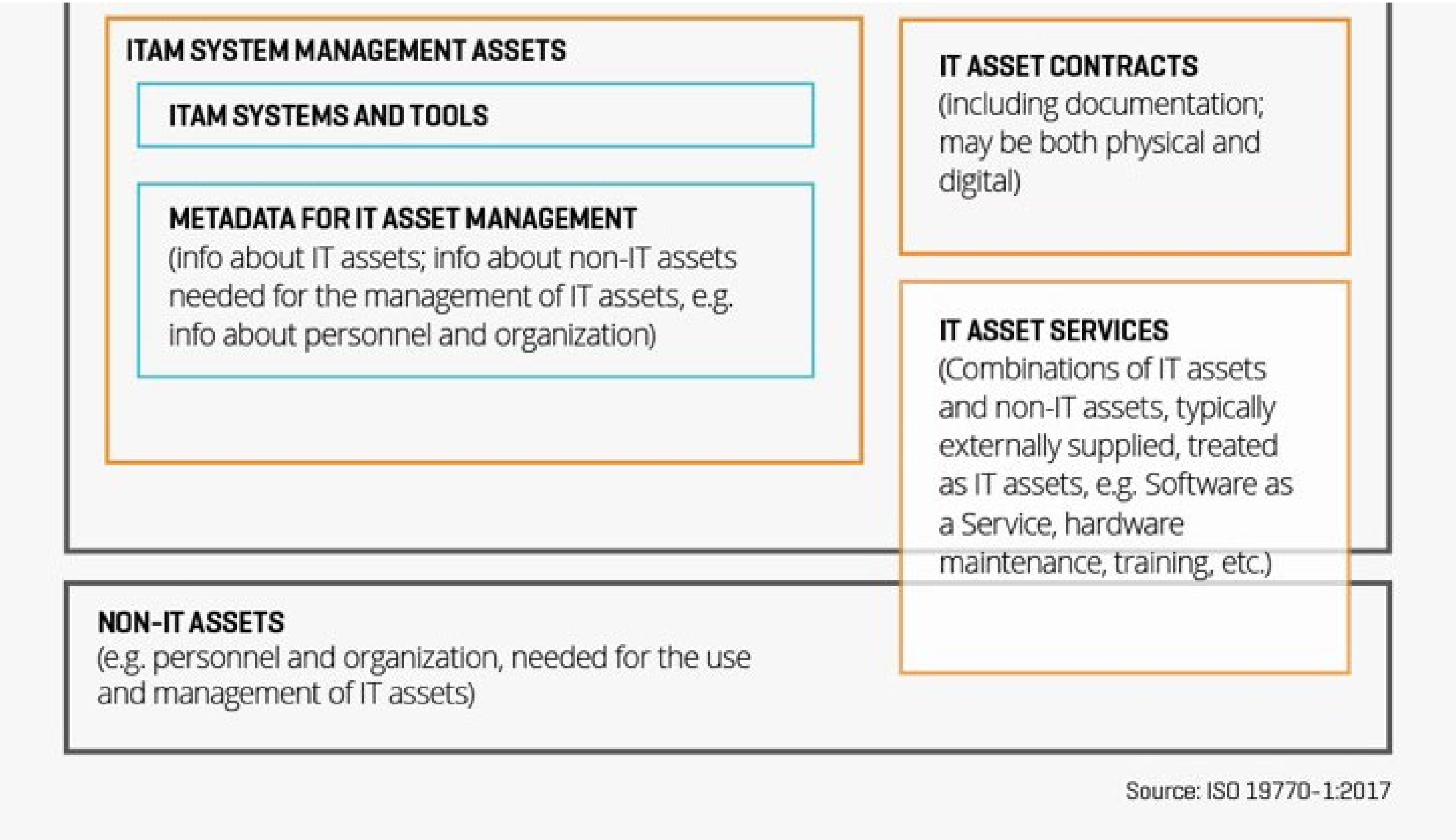
IT HARDWARE

**PHYSICAL MEDIA** (typically containing digital assets including backups)

**PHYSICAL IT EQUIPMENT** (e.g. servers, end-user devices, communications equipment, etc)

**IT ASSET LICENSES** (including proof of license documentation; may be both phyiscal and digital)

# IT ASSETS (CONT'D)



**ITAM SYSTEM MANAGEMENT ASSETS**

**ITAM SYSTEMS AND TOOLS**

**METADATA FOR IT ASSET MANAGEMENT**
(info about IT assets; info about non-IT assets needed for the management of IT assets, e.g. info about personnel and organization)

**IT ASSET CONTRACTS**
(including documentation; may be both physical and digital)

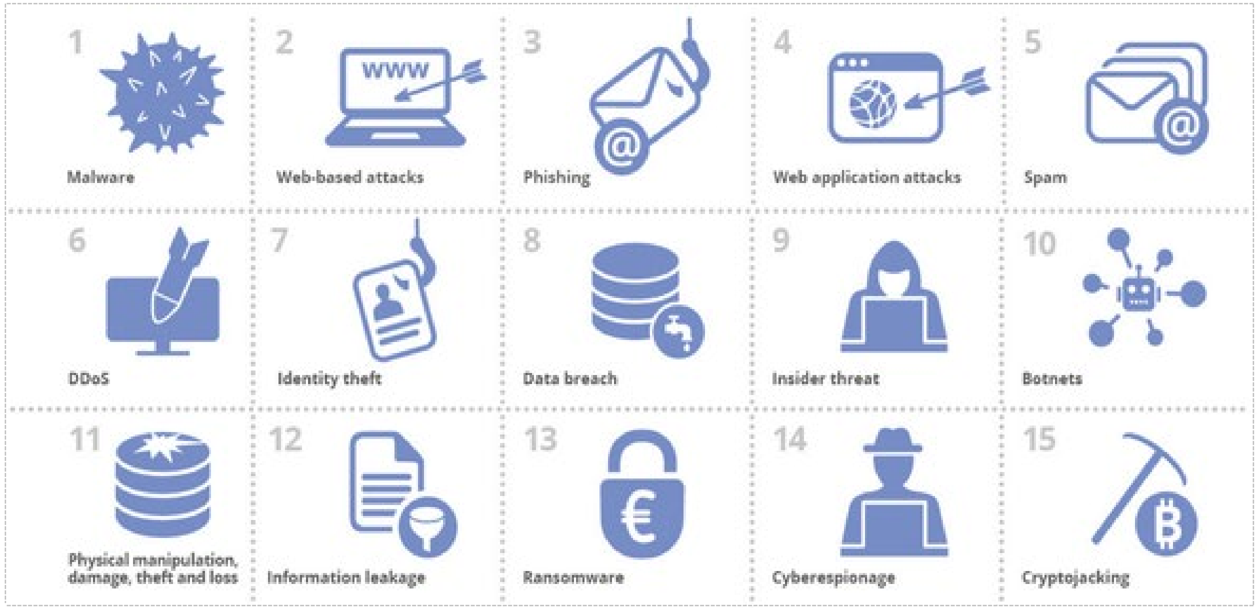
**IT ASSET SERVICES**
(Combinations of IT assets and non-IT assets, typically externally supplied, treated as IT assets, e.g. Software as a Service, hardware maintenance, training, etc.)

**NON-IT ASSETS**
(e.g. personnel and organization, needed for the use and management of IT assets)

Source: ISO 19770-1:2017

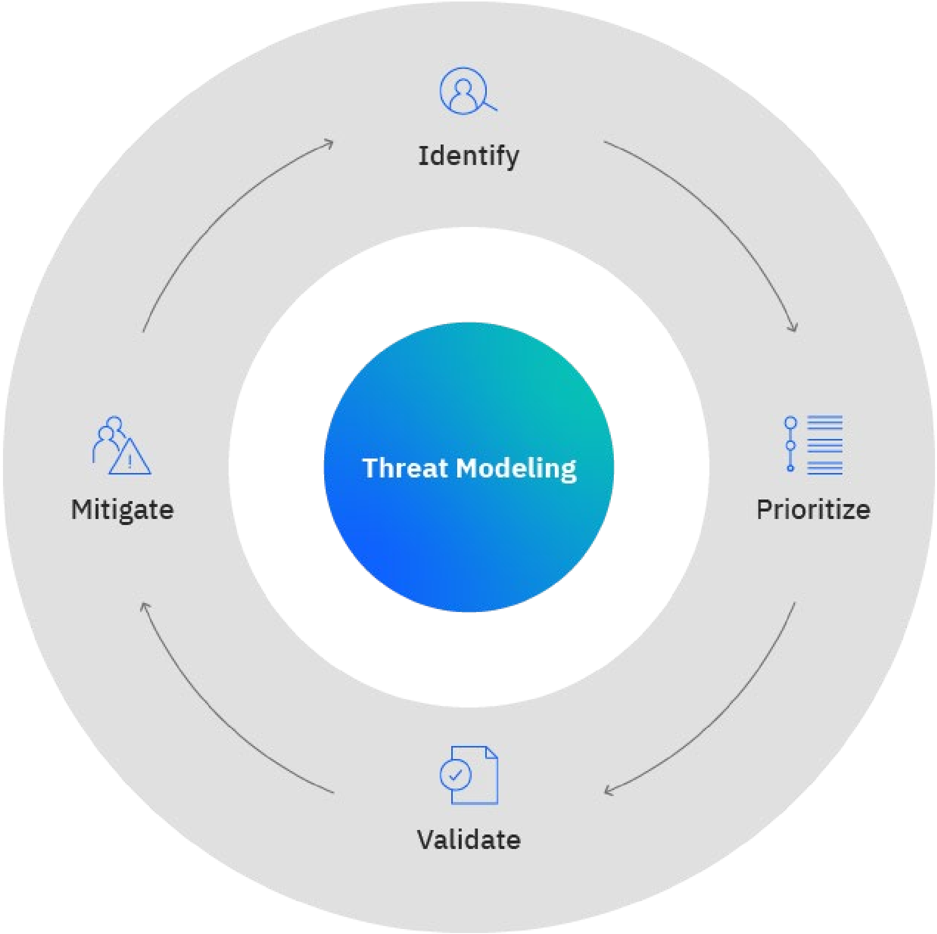
# THREATS

- Any circumstance or event with the potential to harm an information system
  - Unauthorized access, destruction, disclosure, data modification, and/or denial of service
- Threats arise from human actions and natural events
- Threats can be against people, processes, technology



# THREAT MODELING

- A structured process an organization undertakes to:
  - Identify all potential threats to the organization
    - Threats to people, processes, technology, infrastructure
  - Visualize how each threat could occur
  - Quantify and rank the impact of each threat
- The organization then uses this information to prioritize threats
- Assign resources to counter the threats

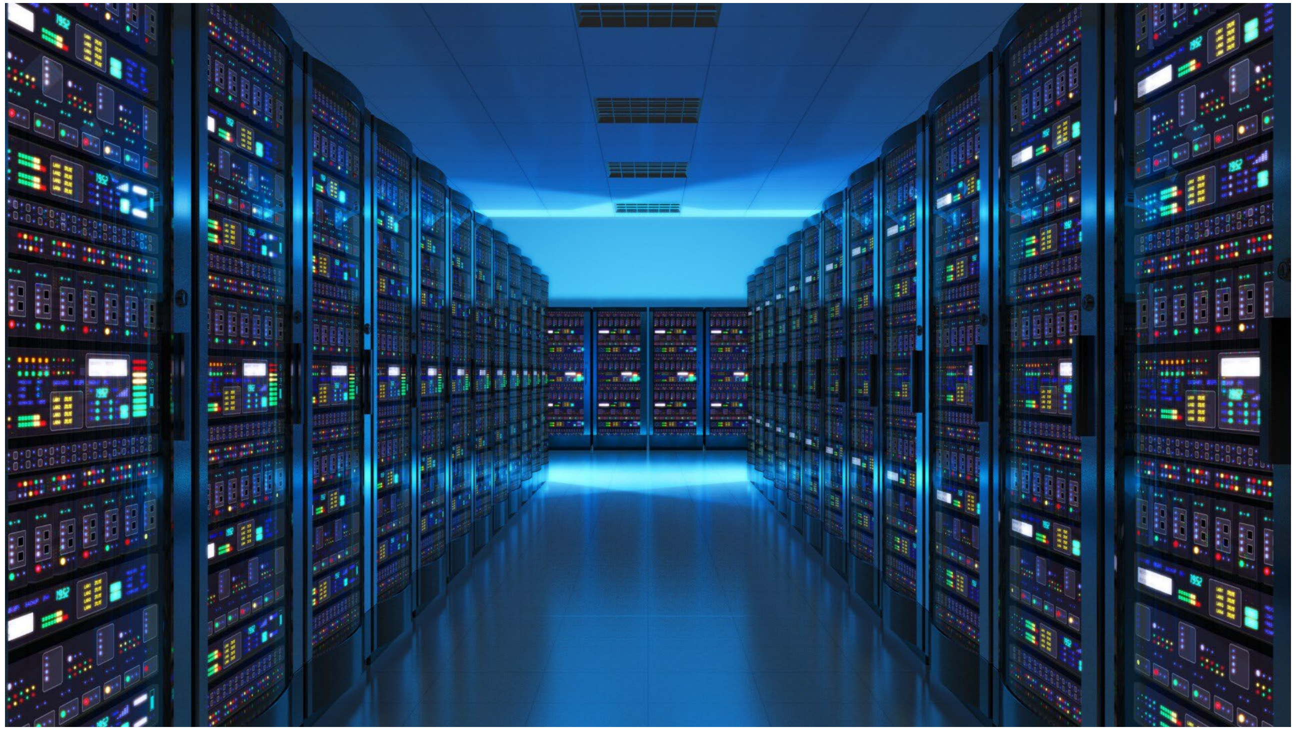


# NETWORK THREAT CATEGORIES

- Sniffing and eavesdropping
- DNS/ARP Poisoning
- MITM (Man-in-the-Middle Attack)
- DoS/DDoS
- Password-based attacks
- Firewall and IDS attack
- Session Hijacking

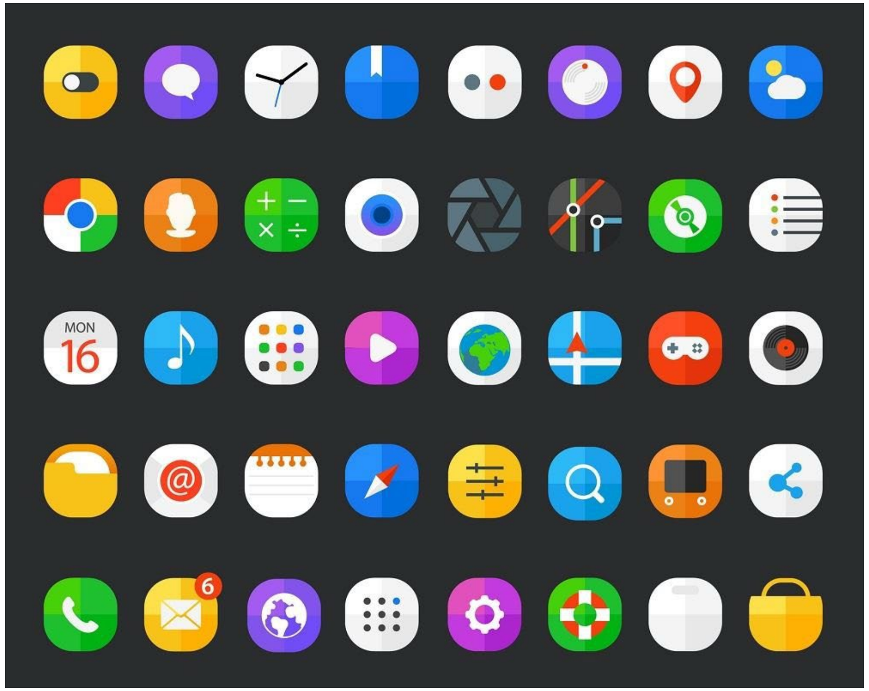
# HOST THREAT CATEGORIES

- Misconfiguration
- Default configuration
- Missing patches/updates
- Password cracking
- Malware attacks
- Scanning/Fingerprinting
- Arbitrary code execution
- Backdoor access
- Privilege Escalation



# APPLICATION THREAT CATEGORIES

- Injection Attacks
- Improper data/input validation
- Improper error handling
- Hidden-field manipulation
- Broken session management
- Cryptography issues
- SQL injection
- Buffer Overflow
- Information disclosure
- Security misconfigurations

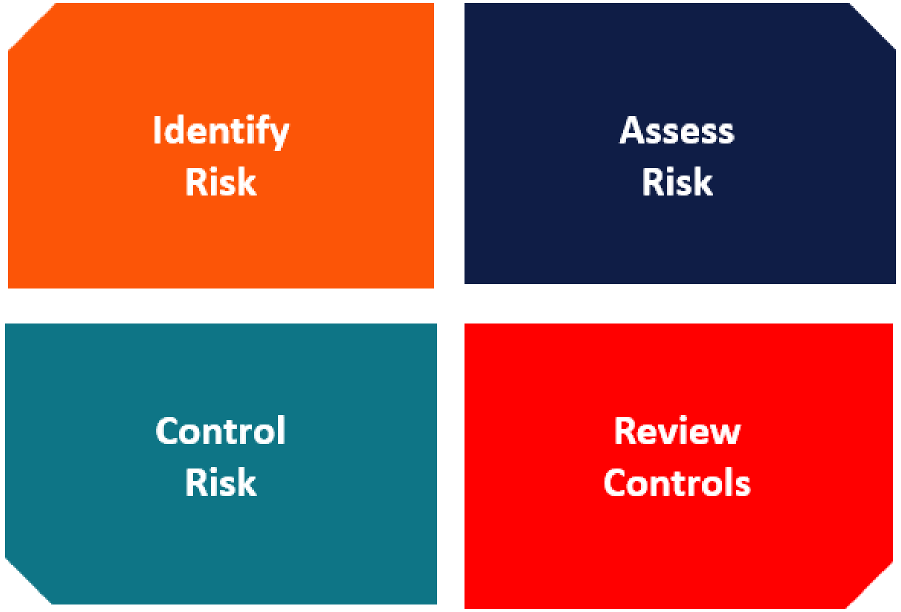


# SHRINK WRAP CODE ATTACK

- Takes advantage of a software bug present in the *original* version of a product
  - The vendor has released a patch
  - But the system administrator has not applied the patch
- Examples:
  - Default usernames and passwords (any system)
  - Windows 10 (v 1809 – 20h2) ReFS Remote Code Vulnerability CVE-2022-21963
  - Windows Server 2016 EternalBlue SMBv1 Arbitrary Code Execution
    - MS17-010 CVE-2017-0144
  - CentOS Web Panel File Inclusion/File Write Arbitrary Code Execution
    - CVE-2021-45466/7

# RISK MANAGEMENT

- The identification, evaluation, and prioritization of risks
- Followed by coordinated and economical application of resources
  - to minimize, monitor, and control probability or impact



Identify Risk

Assess Risk

Control Risk

Review Controls

# BUSINESS IMPACT ANALYSIS (BIA)

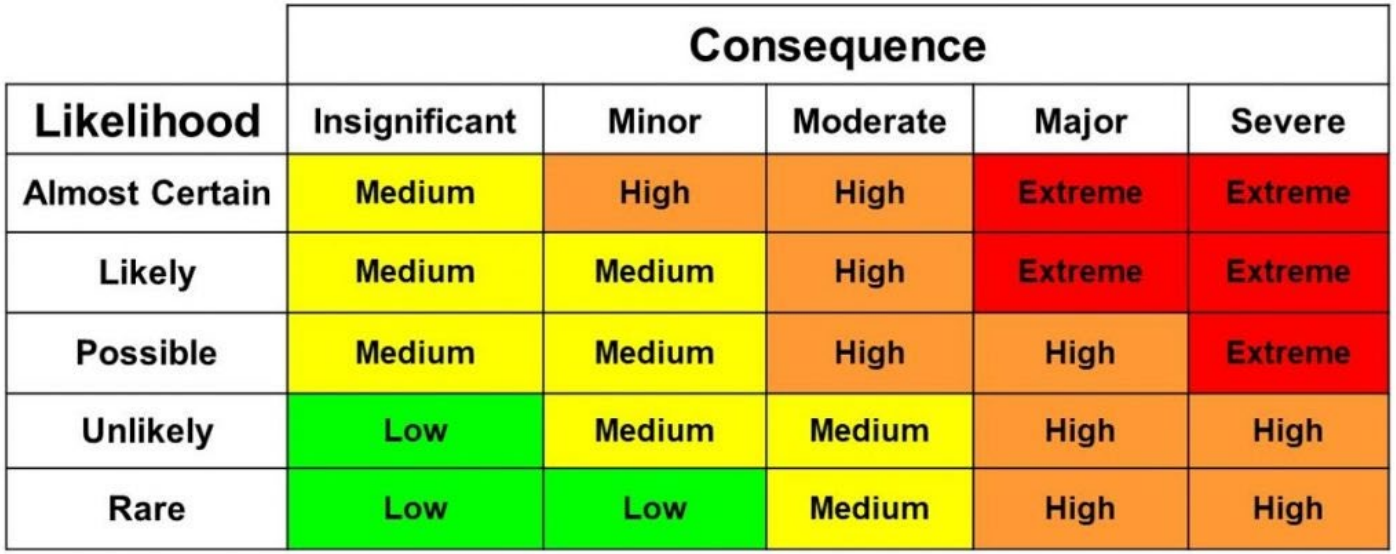
- The first step in risk assessment
- The process of determining the criticality of business activities and associated resource requirements
  - Used to ensure operational resilience and continuity of operations during and after a business disruption
- The BIA quantifies:
  - The impact of service delivery disruption
  - Risks to service delivery
  - Recovery time objectives (RTOs)
  - Recovery point objectives (RPOs)
- RTOs and RPOs are then used to develop strategies, solutions and business continuity/disaster recovery plans (BCP and DR)

# RISK ASSESSMENT

- The process of identifying security risks and assessing the threat they pose
- The ultimate purpose of IT risk assessment is to mitigate risks
  - to prevent security incidents and compliance failures
- An IT risk assessment starts with risk intelligence and threat analysis. You need to make three lists:
  - The IT assets in your organization and how much damage their loss or exposure would cause
  - The business processes that depend on those assets
  - The threat events that could impact those assets and how likely those events are
- Using the information from the risk assessment process, you can determine which threats are the most important to mitigate

# QUALITATIVE RISK ASSESSMENT

- Subjective assessment
- Assigns relative probability and impact to a risk
- Can be measured on various scales:
  - High, Medium, Low
  - 1 - 10



| | Consequence | | | | |
|---|---|---|---|---|---|
| **Likelihood** | Insignificant | Minor | Moderate | Major | Severe |
| Almost Certain | Medium | High | High | Extreme | Extreme |
| Likely | Medium | Medium | High | Extreme | Extreme |
| Possible | Medium | Medium | High | High | Extreme |
| Unlikely | Low | Medium | Medium | High | High |
| Rare | Low | Low | Medium | High | High |

# QUANTITATIVE RISK ASSESSMENT

- Objective assessment
- Assigns a monetary value to risk
- Uses a formula:

  SLE x ARO = ALE

  - Single Loss Expectancy (SLE) - how much one incident will cost
    - SLE = Asset Value (AV) x Exposure Factor (EF)
      - AV = How much revenue the asset brings in or the cost to replace it
      - EF = What percentage of the AV is lost if there is an incident
  - Annual Rate of Occurrence (ARO) - how often the incident is expected to happen over a year
    - If less than one year, can be amortized over several years
  - Annual Loss Expectancy (ALE) - how much this risk will cost us annually
- Allows you to more concretely justify priority and remediation expense
  - You can determine if a control is more expensive than an asset

# QUANTITATIVE RISK ASSESSMENT EXAMPLE

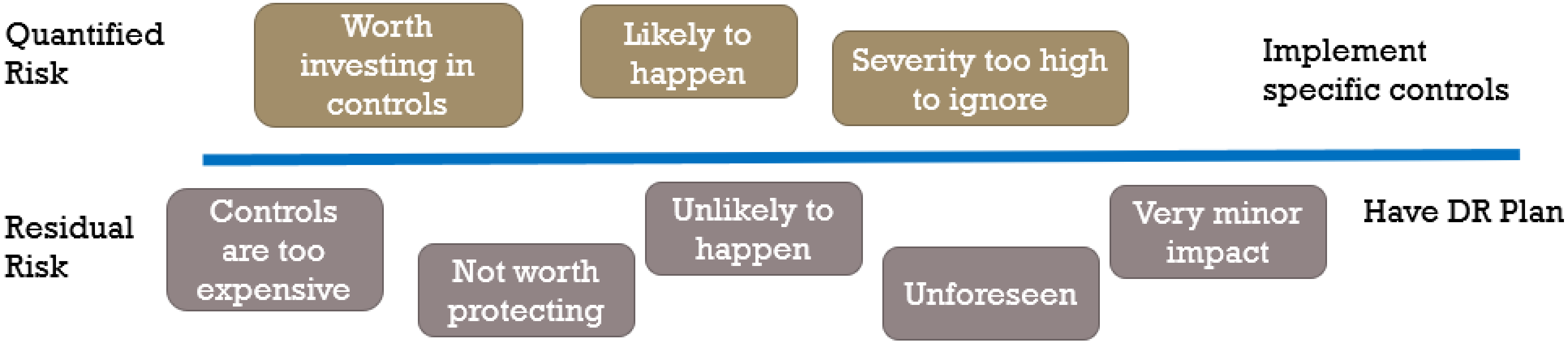
- A hard drive fails every three years
- The cost to buy a new hard drive is $300
- It will require 10 hours to restore the OS and software to the new hard disk
- It will require a further 4 hours to restore the database from the last backup to the new hard disk
- The recovery person earns $10/hour
- Calculate the SLE, ARO, and ALE
- Assume the EF = 1(100%)
- What is the closest approximate cost of this replacement and recovery operation per year?
- $146

# QUANTITATIVE RISK ASSESSMENT EXAMPLE

- A hard drive fails every three years - ARO = 0.34
- The cost to buy a new hard drive is $300
- It will require 10 hours to restore the OS and software to the new hard disk
- It will require a further 4 hours to restore the database from the last backup to the new hard disk
- Assume the EF = 1(100%)
- The recovery person earns $10/hour
  - SLE: $440
  - Hard cost (replace drive) = $300 + Soft cost (labor) = (10 + 4)hours x $10/hr = $140
- Calculate the SLE $440, ARO 1/3, and ALE 440/3 = ~$146.67
- What is the closest approximate cost of this replacement and recovery operation per year? Slightly more than $146.

# "THE LINE" AND RESIDUAL RISK

- All risks "above the line" are worth mitigating
  - Worth the time, effort and cost
- All risks "below the line" are not worth mitigating
  - Too costly, too unlikely to materialize
  - These risks are called "residual risk"
  - You can cover them all with a good backup/disaster recovery strategy or insurance



Quantified Risk

Worth investing in controls

Likely to happen

Severity too high to ignore

Implement specific controls

Residual Risk

Controls are too expensive

Not worth protecting

Unlikely to happen

Unforeseen

Very minor impact

Have DR Plan

# RISK RESPONSES

- Avoid
  - Stop doing the risky thing, get rid of the risky asset
- Mitigate
  - Reduce the impact in case something happens
- Transfer
  - Make someone else responsible, such as buy insurance
- Accept
  - Realize the risk could happen, but do nothing about it
- Reject
  - Deny that the risk even exists (very bad strategy)

# RISK RESPONSE EXAMPLE

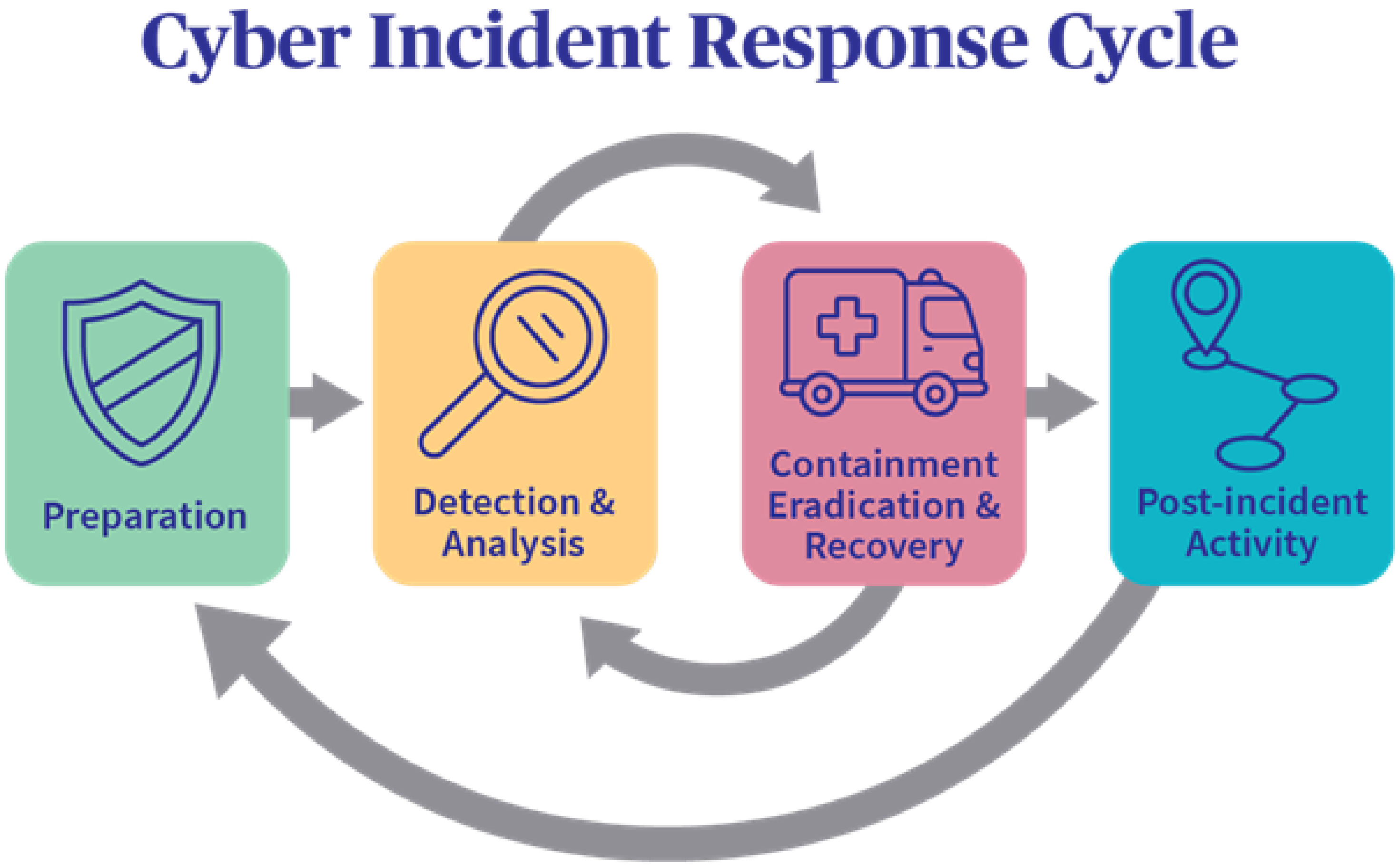
- An internet marketing company decided that they didn't want to follow the rules for GDPR because it would create too much work for them
- They wanted to buy insurance, but no insurance company would write them a policy to cover any fines received
- They considered how much the fines might be and decided to ignore the regulation and its requirements
- They chose to accept the risk

- Note: In this case, they tried to transfer the risk but couldn't
- They don't reject the risk - they realize it could happen - they're just not going to do anything about it - if they get caught, they're ok with paying the fine

# 1.8 INCIDENT MANAGEMENT

- Incident Response
- Incident Management
- Incident Response Team

# INCIDENT RESPONSE


Cyber Incident Response Cycle
Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-incident Activity

# INCIDENT MANAGEMENT

- **Incident**
  - An event that could lead to loss of, or disruption to, an organization's operations, services or functions
- **Incident management**
  - Processes to identify, analyze, prioritize, and resolve security incidents and prevent future incidents
  - The process of managing IT service disruptions and restoring services within agreed service level agreements (SLAs)

# INCIDENT MANAGEMENT PROCESS

- **Preparation:**
  - Select people, assign rules, define tools to handle the incident
- **Detection & Analysis:**
  - Determine an incident has occurred
  - (IDS, SIEM, AV, Someone makes a report, etc.)
- **Classification and Prioritization:**
  - Identify the severity and impact of the incident
  - Priority "P"
  - Severity "S"
  - Scale 1 (high) - 3 (low)
  - Example: P1S1 = Major disruption that is felt company-wide; top priority

# INCIDENT MANAGEMENT PROCESS (CONT'D)

- **Notification:**
  - Who and how to notify
  - Includes management, staff, partners, law enforcement/regulators, the news media, the public
- **Containment:**
  - Limit the damage
  - Isolate hosts and network segments
  - Contact system owners
- **Forensic Investigation:**
  - Investigate the root cause of the incident using forensic tools
  - System logs, real-time memory, network device logs, application logs, etc.

# INCIDENT MANAGEMENT PROCESS (CONT'D)

- **Eradication & Recovery:**
  - Remove the cause of incident
  - Patch if needed
  - Get systems back into production
  - Monitor affected systems
- **Post-incident Activities:**
  - Post mortem / lessons learned
  - Document what happened and why
  - Transfer knowledge
  - Improve controls to reduce future risk

# RESPONSIBILITIES OF THE INCIDENT RESPONSE TEAM

- Manage security issues using a proactive approach and responding effectively
- Develop and review processes and procedures
- Regularly review legal and regulatory requirements
- Provide a single point of contact for reporting security incidents
- Manage response to an incident
  - Make sure all procedures are followed properly to minimize and control damage
- Review controls and recommend steps update technology
- Identify and analyze the incident including impact
- Work with local law enforcement and government agencies, partners and suppliers

# INCIDENT HANDLING SCENARIO

- You just found out that an unauthorized data spillage is occurring on someone's computer.
  - It's not clear yet how this is happening
- You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down.
- What step in incident handling did you just complete?
- **Containment**

# 1.9 INFORMATION SECURITY LAWS AND STANDARDS

- Security Organizations
- Security Standards
- US Security Laws
- PCI-DSS
- OSSTMM
- GDPR

# SECURITY ORGANIZATIONS

- Cybersecurity & Infrastructure Security Agency (CISA)
  - An agency of the United States Department of Homeland Security (DHS)
  - Responsible for strengthening cybersecurity and infrastructure protection across all levels of government
- Computer Security Incident Response Team (CSIRT)
  - Privately held US organization
  - Provides 24x7 cybersecurity incident response to any user, company, government agency or organization
  - Single point of contact for reporting computer security incidents worldwide
- International Information System Security Certification Consortium (ISC)2
  - International nonprofit cybersecurity professional organization
  - Provides the CISSP certification

# SECURITY ORGANIZATIONS (CONT'D)

- ISACA
  - International professional association focused on IT governance
  - Published COBIT
  - Offers many certifications including CISA and CISM
- NIST (National Institute of Standards and Technology)
  - A physical sciences laboratory and non-regulatory agency of the United States Department of Commerce
  - Its mission is to promote American innovation and industrial competitiveness
  - NIST activities are organized into laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement

# SECURITY ORGANIZATIONS (CONT'D)

- SANS
  - A company that specializes in information security and cybersecurity training
  - Sponsors the Global Information Assurance Certification (GIAC)
- OWASP (Open Web Application Security Project)
  - A community effort that works to improve the security of software
  - Produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security

# INFORMATION SECURITY STANDARDS

| Law / Standard | Description |
|---|---|
| ISO 27002 AND 17799 | • Specifies the requirements for launching, instigating, keeping, and continually improving an organization's information security management system<br>• Also includes the requirements needed to assess and treat data security risks tailored to the organization's needs |
| ISO/IEC 27001:2013 | • Specifies requirements for establishing, implementing, maintaining, and improving a security management system for an organization |

# INFORMATION SECURITY STANDARDS (CONT'D)

| Law / Standard | Description |
|---|---|
| Information Technology Infrastructure Library (ITIL) | An operational framework that standardizes IT management procedures |
| Control Objectives for Information and Related Technology (COBIT) | A popular framework developed by ISACA to handle IT governance and management for any organization in any industry |
| Computer Security Incident Response Team (CSIRT) | Provides a single point of contact when reporting computer security incidents |
| Payment Card Industry Data Security Standard (PCI-DSS) | • Industry standard to protect cardholder information for debit, credit, prepaid, e-purse, ATM, and POS cards<br>• PCI-DSS applies to all entities involved in payment processing |

# PCI-DSS RECOMMENDATIONS

- Use encryption to protect all transmission of card holder data over any public network.
- Limit access to card holder data to as few individuals as possible.
- Use a firewall between the public network and the payment card data.

PCI-DSS is an industry standard, not a regulatory requirement.
It is voluntary, but widely adopted

# US GOVERNMENT SECURITY CONTROLS

- NIST Special Publication 800-53
  - Catalog of security and privacy controls for all U.S. federal information systems except those related to national security
- NIST SP 800-40
  - Patch and vulnerability management program framework
- Federal Information Security Modernization Act of 2014 (FISMA)
  - Update to the US Federal Government's cybersecurity practices

# US INFORMATION SECURITY LAWS

| Standard | Description |
|---|---|
| Health Insurance Portability and Accountability Act (HIPAA) | • Sets patient privacy standards<br>• Protects patients' health information from being disclosed without their consent or knowledge<br>• Protects medical records and health information shared between doctors, hospitals and insurance providers |
| Sarbanes Oxley Act (SOX) - 2002 | • Requires publicly traded companies to submit to independent audits and to properly disclose financial information<br>• Seeks to protect investors and the public |

# US INFORMATION SECURITY LAWS (CONT'D)

| Standard | Description |
|---|---|
| Digital Millennium Copyright Act (DMCA) | • Implements two 1996 treaties of the World Intellectual Property Organization<br>• Criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted work |
| Gramm-Leach-Bliley Act (GLBA) | • Protects the confidentiality and integrity of personal information that is collected by financial institutions |
| Federal Information Security Modernization Act (FISMA) | • Provides a comprehensive framework for guaranteeing effectiveness of information security controls for Federal operations and assets |

# US INFORMATION SECURITY LAWS (CONT'D)

| Law / Standard | Description |
|---|---|
| Federal Information Technology Acquisition Reform Act (FITARA) | • A 2013 bill that was intended to change the framework that determines how the US GOV purchases technology |
| Cybersecurity Information Sharing Act (CISA) 2015 | • Its objective is to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes<br>• The law allows the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies |

# US INFORMATION SECURITY LAWS (CONT'D)

| Law / Standard | Description |
|---|---|
| Cybersecurity Enhancement Act of 2014 | • Provides an ongoing, voluntary public-private partnership to:<br>• Improve cybersecurity<br>• Strengthen:<br>  • Cybersecurity research and development<br>  • Workforce development and education<br>  • Public awareness and preparedness |
| Federal Exchange Data Breach Notification Act of 2015: | • Requires a health insurance exchange to notify each individual whose personal information is known to have been acquired or accessed as a result of a breach of security<br>• Applies to any system maintained by the exchange<br>• Notification must happen as soon as possible but not later than 60 days after discovery of the breach |

# US INFORMATION SECURITY LAWS (CONT'D)

| Law / Standard | Description |
|---|---|
| National Cybersecurity Protection Advancement Act of 2015: | • This law amends the Homeland Security Act of 2002<br>• Allows the Department of Homeland Security's (DHS's) national cyber security and communications integration center (NCCIC) to include:<br>  • Tribal governments<br>  • Information sharing and analysis centers<br>  • Private entities<br>among its non-federal representatives |

# General Data Protection Regulation (GDPR)

- A regulation that requires businesses to ensure the protection of personal data and privacy of European citizens
- Includes:
  - Compliance, Privacy, Security, Control, Credibility
- It establishes one law across the continent
  - A single set of rules
  - Applies to any company doing business within EU member states

# 1.10 INTRODUCTION TO ETHICAL HACKING REVIEW

- Review

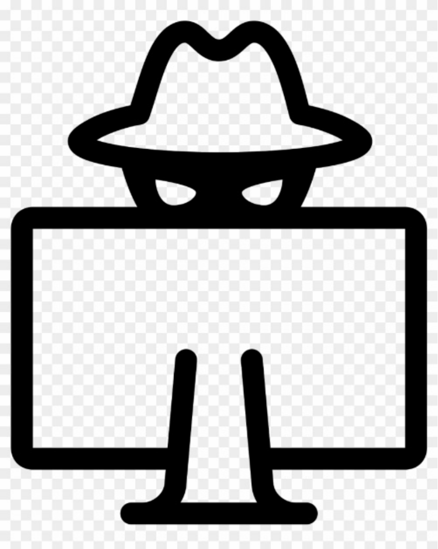
# INTRODUCTION TO ETHICAL HACKING REVIEW

- CIA is the foundation of all security
- Security should be applied in layers - Defense in Depth
- Hacking is the attempt to gain unauthorized access into a network or system
- There are many types of hackers, from malicious to ethical
- The Advanced Persistent Threat (APT) is sponsored by a nation-state and is the most dangerous

- Much of your damage will come from insider threats
  - Most are accidental and not intentionally malicious
- Ethical Hacking seeks to discover vulnerabilities before they are actually exploited
- Ethical hackers use the same tools as other hackers
- Ethical hackers need to have both technical and non-technical skills
- You can build a virtual lab to practice your hacking skills

# INTRODUCTION TO ETHICAL HACKING REVIEW

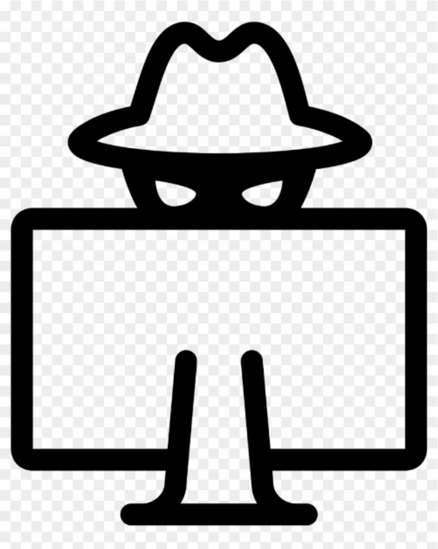
- The Cyber Kill Chain outlines all phases of an attack:
  - Reconnaissance
  - Weaponization
  - Delivery
  - Exploitation
  - Installation
  - Command and Control
  - Action on Objectives



- The MITRE ATT&CK Framework is a comprehensive matrix of tactics and techniques
- It helps identify attack types and define risk
- It has three attack matrices with categories and subcategories:
  - Enterprise
  - Mobile
  - IoT

# INTRODUCTION TO ETHICAL HACKING REVIEW

- Information Assurance implement a security architecture and management program to maintain CIA throughout the enterprise
- Policies are high-level mandatory business rules designed to safeguard information security
- Procedures are step-by-step task lists to achieve a specific security goal
- Guidelines are recommended best practices



- Risk management identifies, evaluates and prioritizes risk
  - It seeks to reduce risk by applying security controls
- A Qualitative Risk Assessment is subjective
  - It assigns relative probability and impact to a risk
- A Quantitative Risk Assessment is objective
  - It assigns a monetary value to a risk based on asset value, exposure factor, single loss expectancy, annual rate of occurrence, and annual loss expectancy

# INTRODUCTION TO ETHICAL HACKING REVIEW

- Risk response types are: avoid, mitigate, transfer, accept, and reject
- Incident management is a set of processes that identify, analyze, prioritize, and resolve security incidents and prevent future incidents
- There are numerous security organizations, laws and standards that the ethical hacker should be aware of