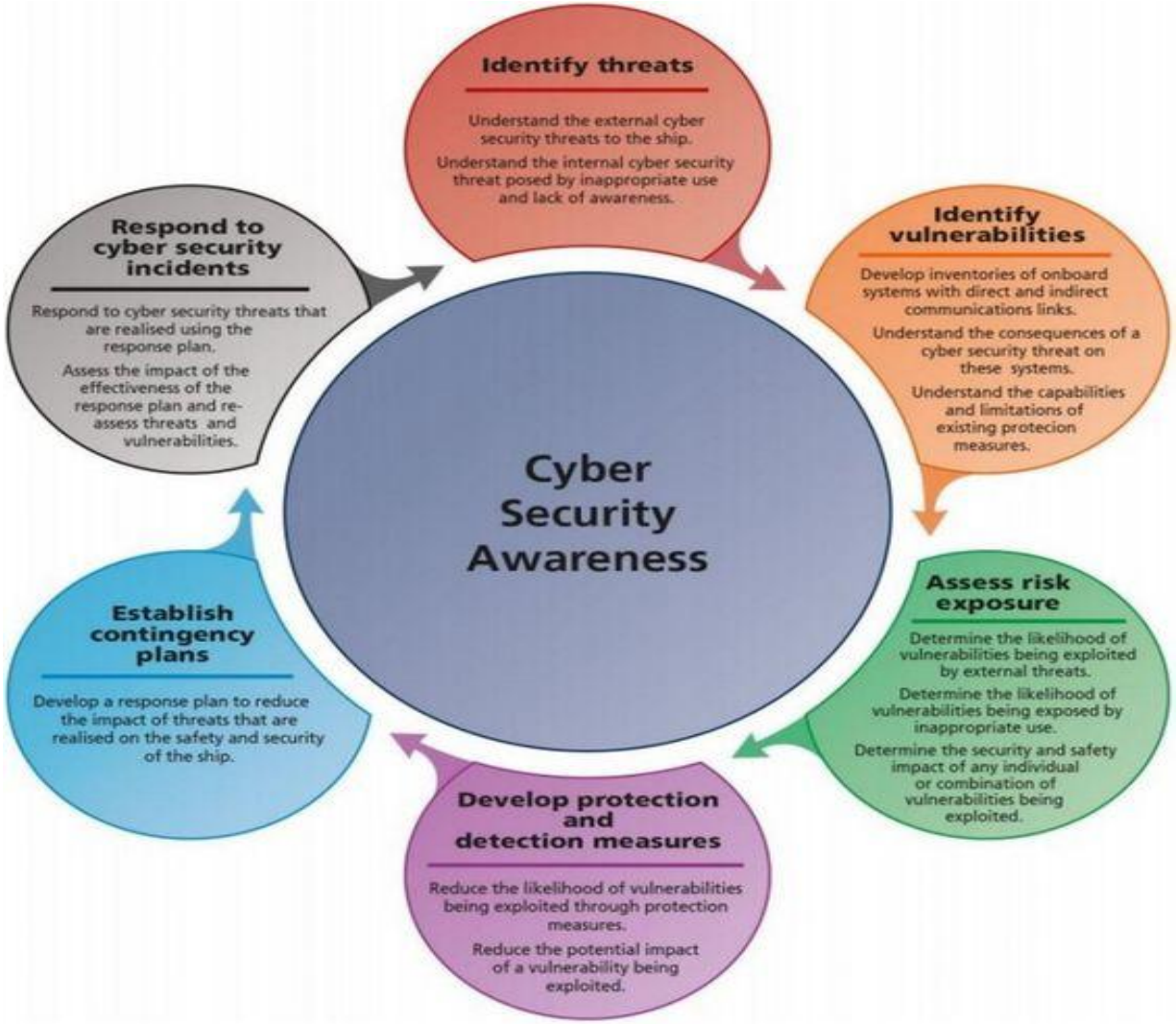
Lets check your understanding of Information Security

What Is Information Security?

- The protection of the assets of a computer system
  - Hardware
  - Software
  - Data

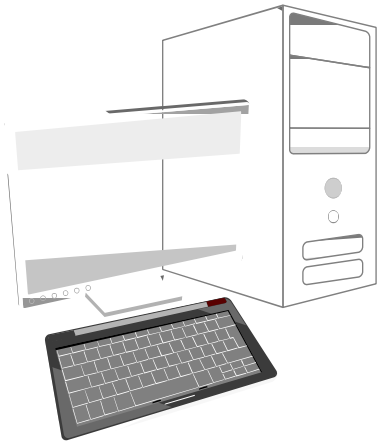


Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

Values of Assets



Off the shelf;
easily replaceable

Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)

Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

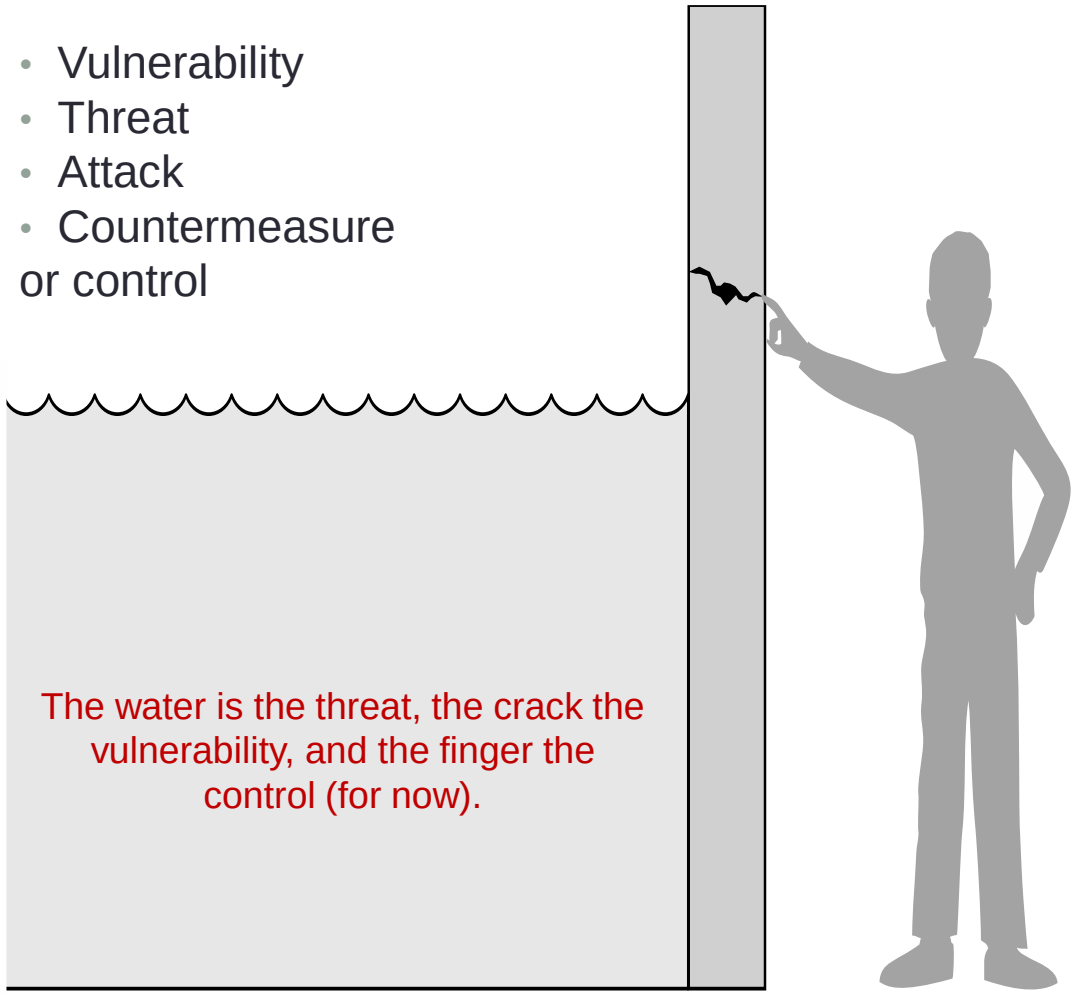
- Individual applications

Unique; irreplaceable

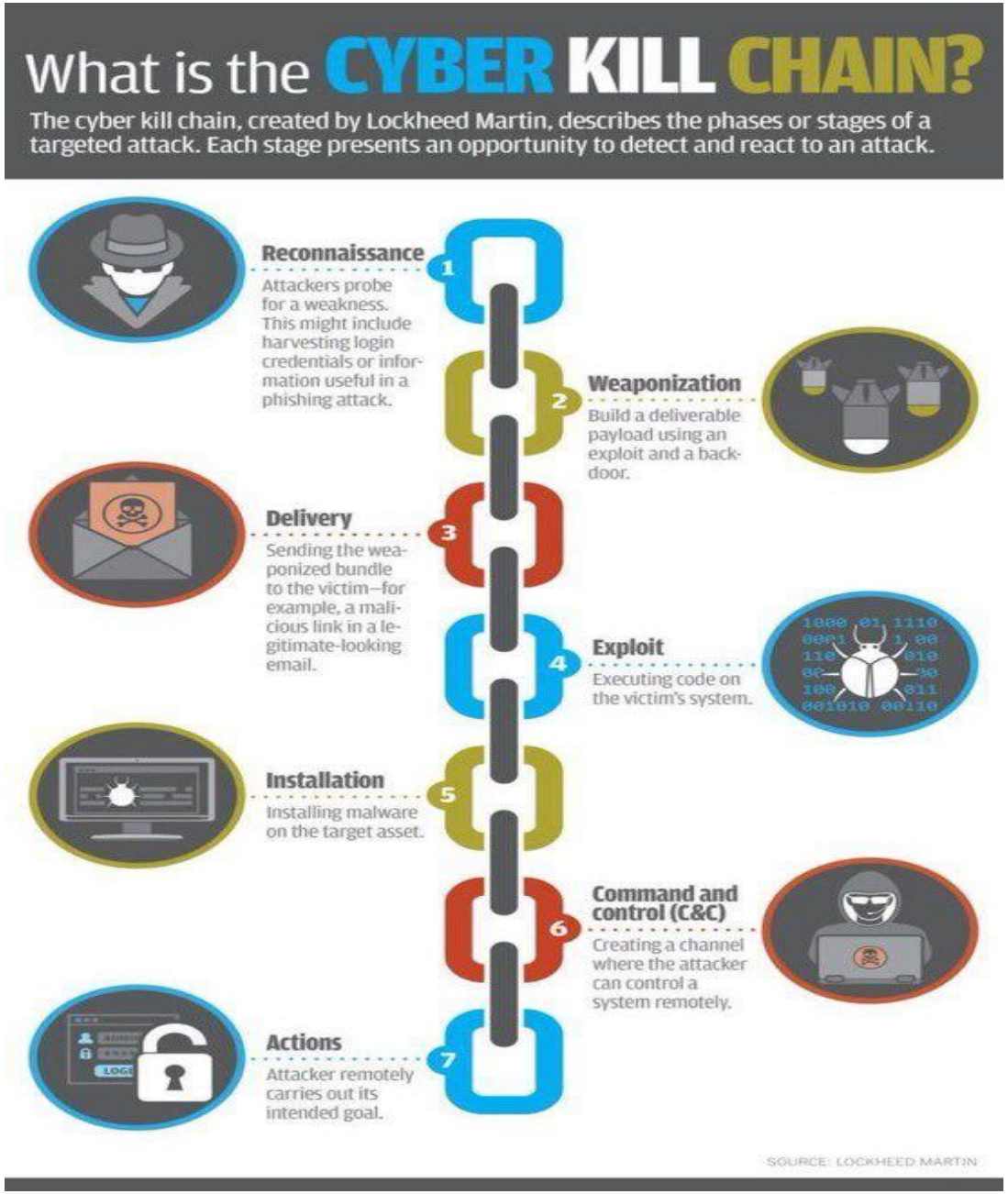
Threat & Vulnerability

- Vulnerability
- Threat
- Attack
- Countermeasure

or control



The water is the threat, the crack the vulnerability, and the finger the control (for now).



The National Institute of Standards and technology (NIST) Computer Security Handbook defines the term Computer Security as:

"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources" (includes hardware, software, firmware, information/data, and telecommunications).

Confidentiality

- preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity

- guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity

Availability

- ensuring timely and reliable access to and use of information

The CIA Triad

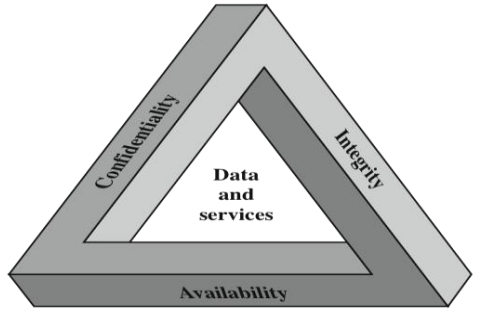


Figure 1.1 The Security Requirements Triad

Confidentiality

- It ensures that computer-related assets are accessed only by authorized parties
- Access means reading, viewing, printing, or simply knowing that a particular asset exists
- It is sometimes also called secrecy or privacy

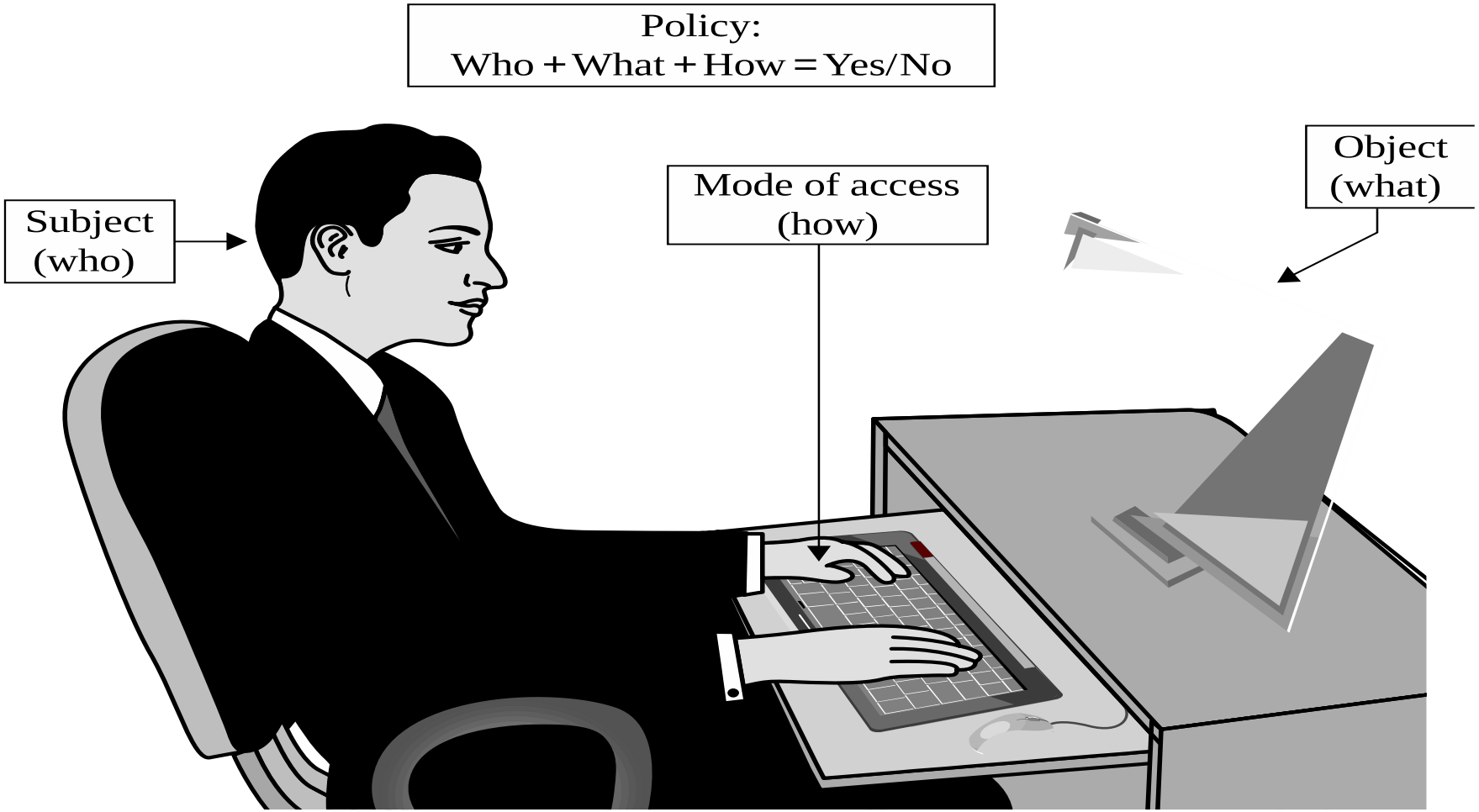
Integrity

- It means that assets can be modified only by authorized parties only in authorized ways.
- The integrity of an item is preserved if it is:
  - Precise, accurate, unmodified, modified only in acceptable ways, modified by authorized people, modified by authorized processes, consistent, meaningful and usable.

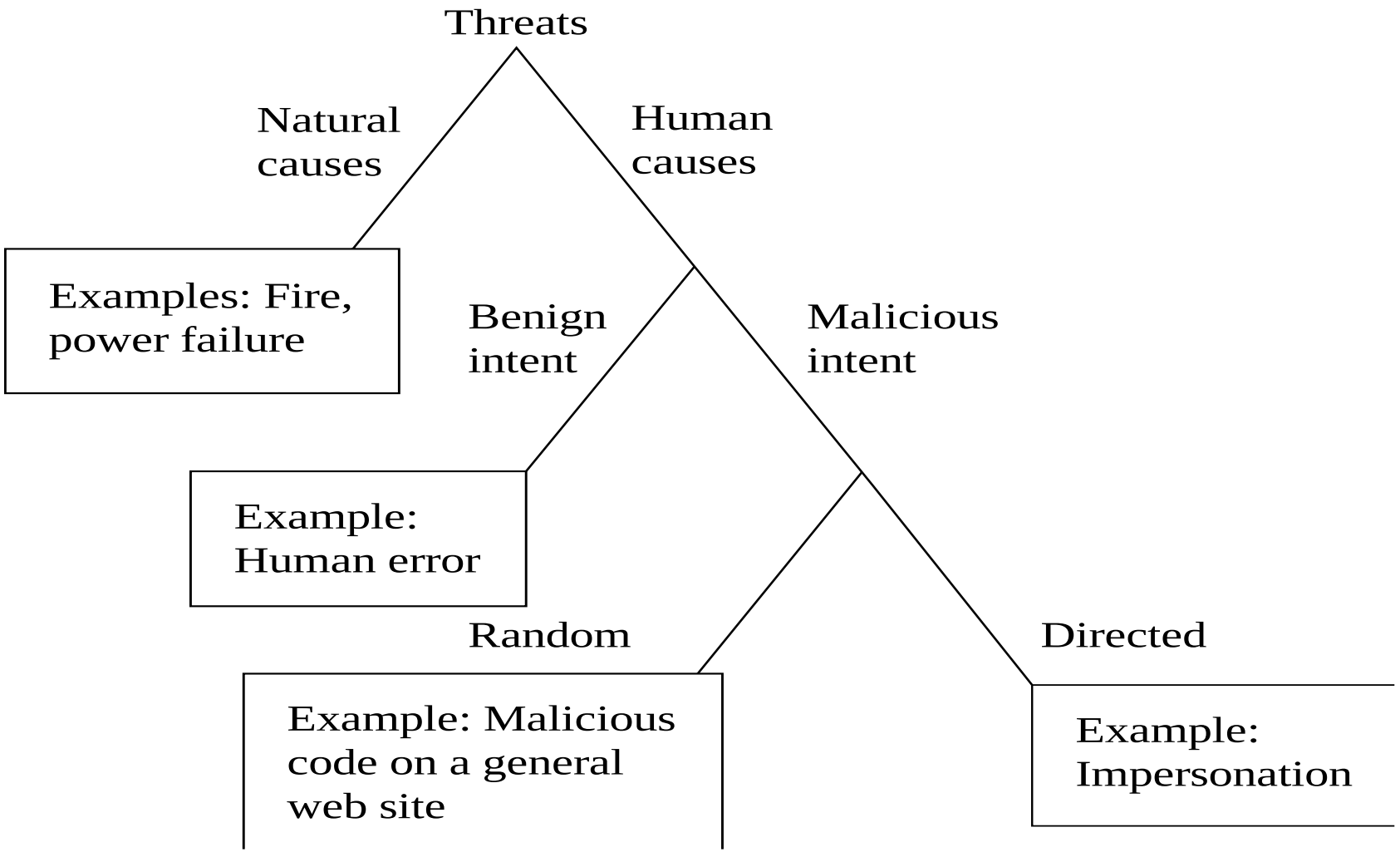
Availability

- It applies to both data and data processing
- A data item, service or system is available if
  - There is a timely response to our request
  - Fair to all i.e. some requesters are not favored over others
  - Fault tolerant
  - There is controlled concurrency, deadlock management, and exclusive access as required

Access Control



Types of Threats

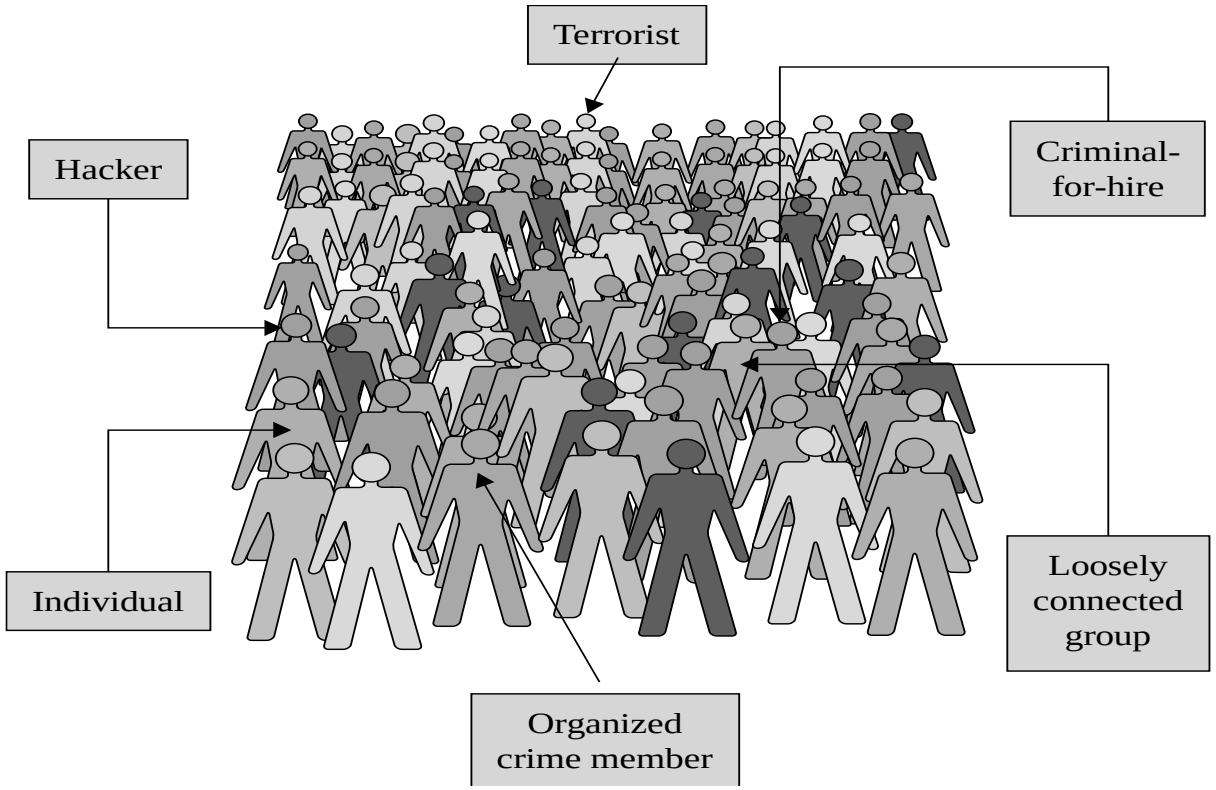


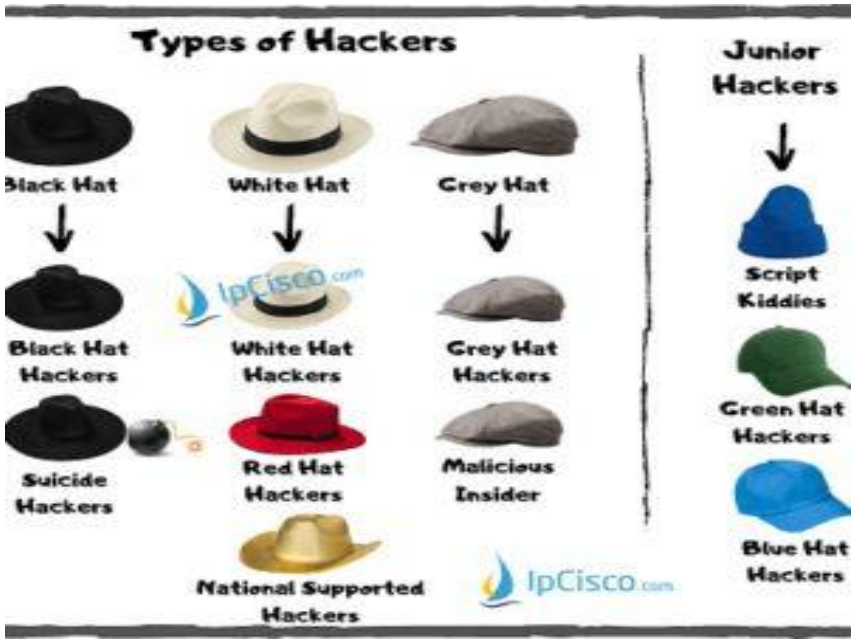
Advanced Persistent Threat (APT)

- Organized
- Directed
- Well financed
- Patient
- Silent

APT is a special type of threat that has only been taken seriously by the broad security community over the past decade. In general, security experts believe that no one who becomes a high-priority target can truly be safe from APT.

Types of Attackers

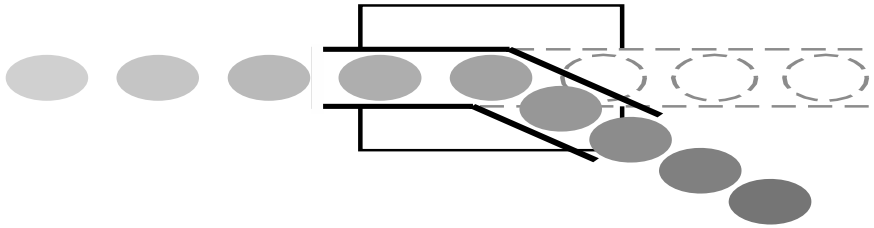




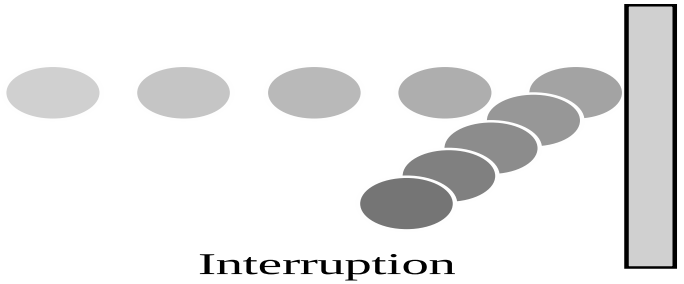
Each of these attacker types is associated with a different set of resources, capabilities & motivations.

Understanding the different types will help later in considering threats.

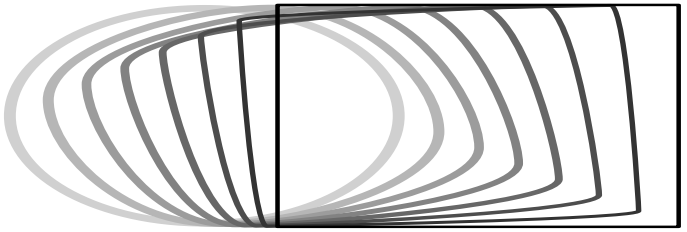
Types of Harm



Interception



Interruption



Modification

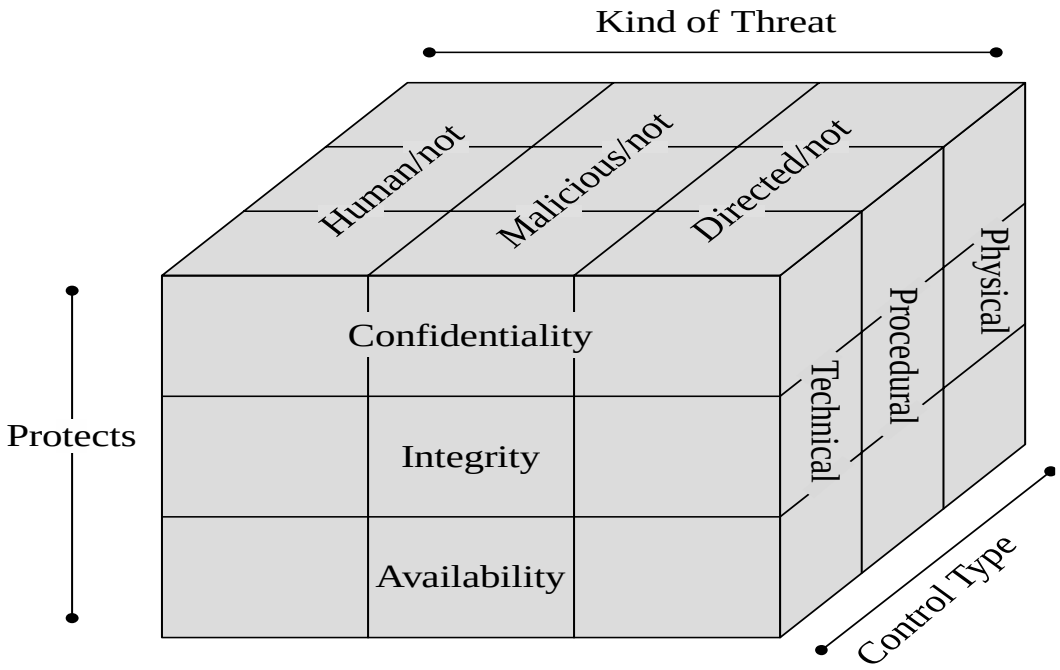
Fabrication

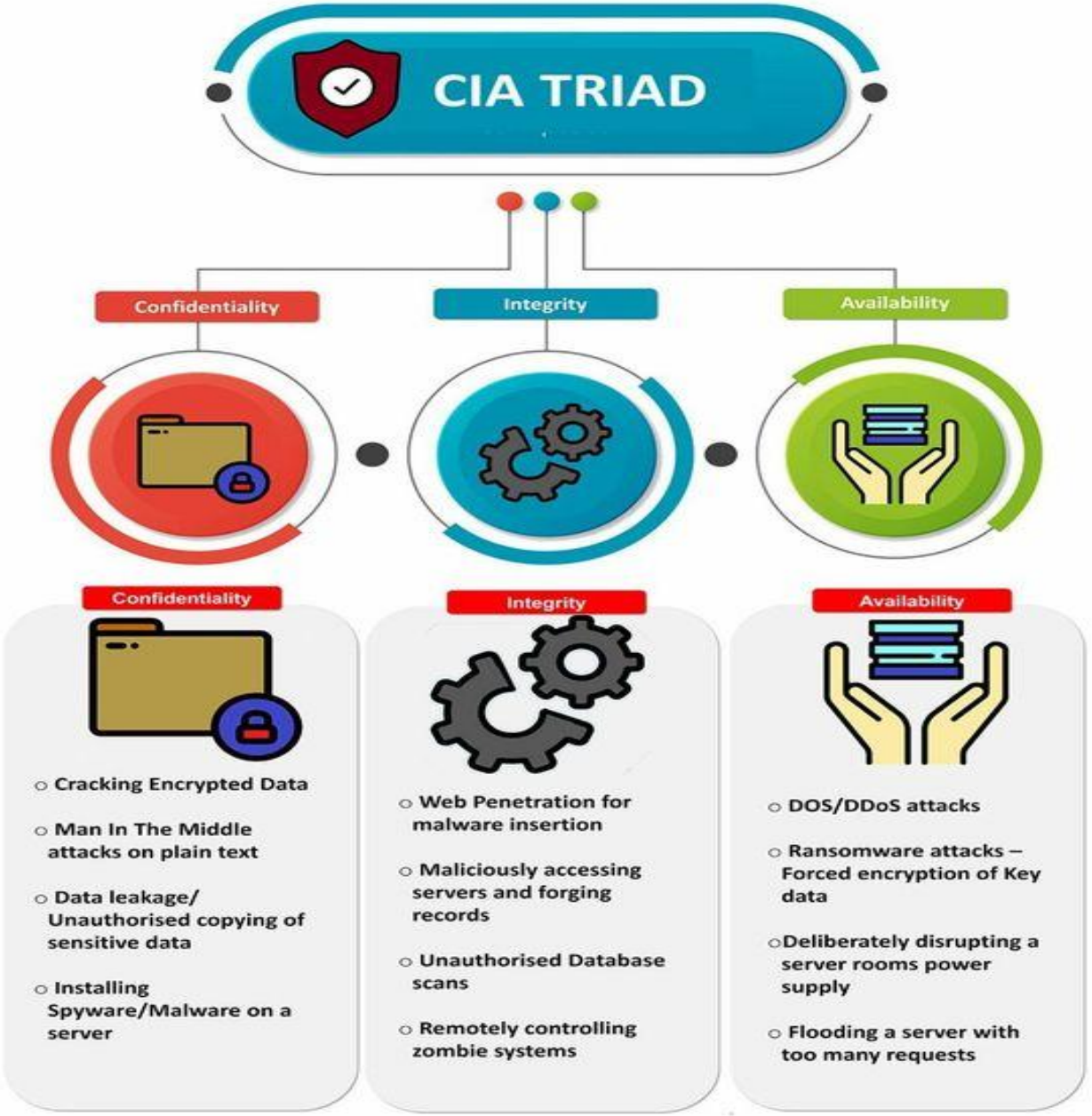
These are the primary types of harm against system data and functions. Understanding these possibilities is important to considering threat and risk.

Security Attacks

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

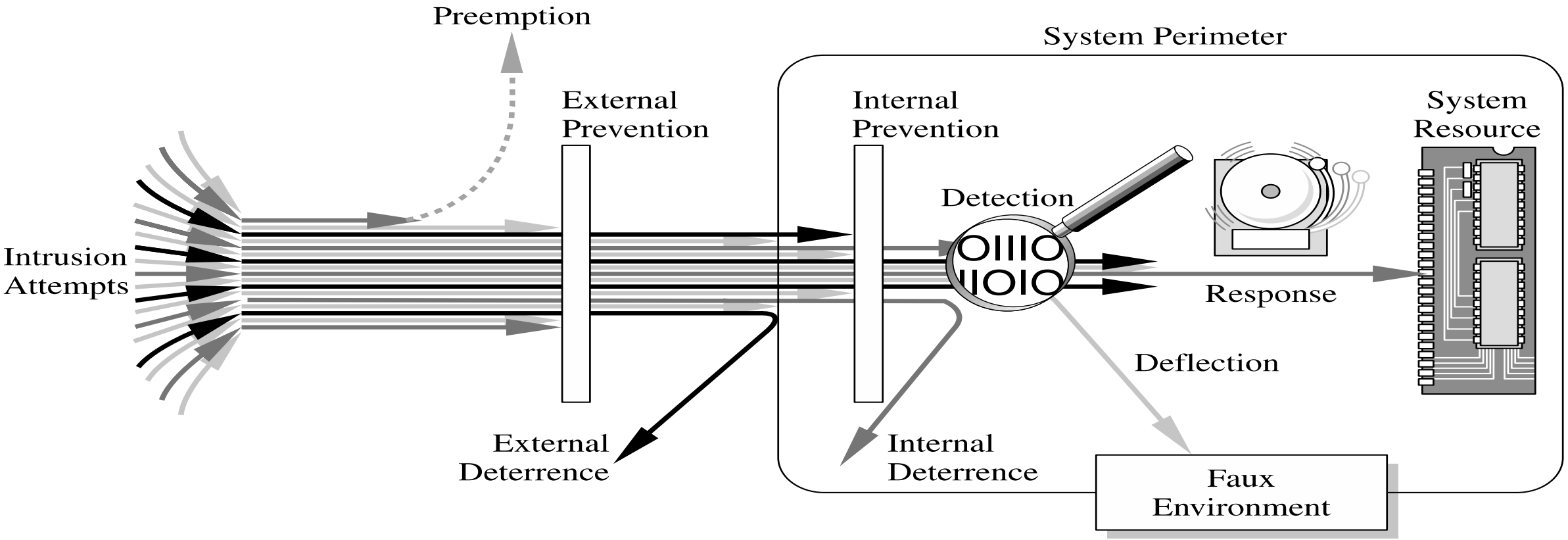
Controls/Countermeasures





- The three dimensions by which a control can be categorized.
- Thinking about controls in this way enables you to easily map the controls against the threats they help address.

Different Types of Controls



In this simple representation of a networked system, it is easy to see all the touch points where controls can be placed, as well as some different types of controls, including deterrence, deflection, response, prevention, and preemption.

Method, Opportunity and Motive

- Method : the skills, knowledge, tools and other things with which to be able to pull off the attack
- Opportunity : the time and access to accomplish the attack
- Motive : a reason to want to perform this attack against this system

DENY ANY OF THESE THREE THINGS AND

ATTACKS WILL NOT OCCUR

Method, Opportunity and Motive

Methods of Defense

- *Prevent it*, by blocking the attack or closing the vulnerability
- *Deter it*, by making attack harder if not impossible
- *Deflect it*, by making another target more attractive
- *Mitigate it*, by making its impact less severe
- *Detect it*, either as it happens or some time after the fact
- *Recover* from its effects

Methods of Defense

- Controls
  - Encryption
  - Hardware Controls
    - Hardware/smart card implementations of encryption
    - Locks or cables limiting access
    - Devices to verify users' identity
    - Firewalls
    - Intrusion detection systems
  - Software Controls
    - Internal program controls,
    - OS and Network system controls
    - Independent control program (anti virus, passwords etc.)
    - Development control
  - Policies and Procedures
  - Physical Controls

Effectiveness of Controls

- Awareness of Problem
  - Highlighting Need of security
- Likelihood of Use
  - They must be efficient, easy to use, and appropriate
- Overlapping Controls
  - Use several different controls, layered defense
- Periodic reviews
  - Judging the effectiveness of control is an ongoing task

Others Exposed Assets

- Networks
  - Network's lack of physical proximity
  - Use of insecure, shared media
  - Inability to identify remote users positively
- Access
  - Computer time
  - Malicious access
  - Denial of service to legitimate user
- Key People

Security checklist

Anti-SQL-injection protection

SSL and OpenSSL up to date

Passwords hashed with salt

Multi-factor authentication on the back-office

AES encryption on sensitive data

Preventing the PM from sending the whole unencrypted database by email

CommitStrip.com

HOW TO MAKE YOUR NETWORK SECURE

THE BASICS

EFFECTIVE CYBER SECURITY STARTS WITH A SECURE NETWORK.

Help make your network secure by developing and implementing some simple policies and response

CONTROL ACCESS

Control who can access your network – and what they can do in it.

- Do you know who is accessing your network?

PREVENT MALICIOUS CONTENT

Use malware-checking and scanning services to evaluate where files come from. They will also check incoming and outgoing data from external sources (the 'perimeter'), such as mobile devices, as well as your own internal protection.

- Do you use malwareand antivirus protection at your perimeter, as well as on the devices in your offices?

RUN REGULAR SCANS TO CHECK VULNERABILITY

Regularly run automatic scanning tools on your networked devices. Use the findings to resolve or manage any vulnerability identified.

- Do you perform vulnerability assessments to check your systems and networks?

SECURE WIRELESS ACCESS

Secure your wireless access points, only allowing known devices to connect to your Wi-Fi services.

- Have you installed security scanning tools to detect and locate unauthorised or cloned ('spoof') wireless access points?

MONITOR YOUR NETWORKS

Use network detection and prevention tools and make sure they are correctly installed by someone qualified.

- Is your network configured to deny traffic as a default?

SEGREGATE YOUR NETWORKS

Identify, group together and then isolate systems that are critical to your business – and apply the appropriate network security controls to them.

- Are your essential services as protected as possible, even if other parts of the network become compromised?

IS YOUR NETWORK CONFIGURED TO DENY TRAFFIC AS A DEFAULT? USE FIREWALLS

Use firewalls to create a buffer zone between the internet – and any other networks you don't trust – and your business's internal networks.

- Do you back up your firewall configurations regularly? Would you be able to detect any unauthorised change to your configurations?