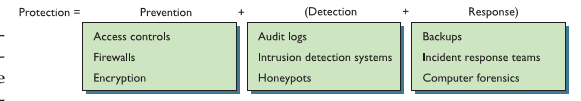
**Week 1. Notes**





* **Administrative**
  + Controls that determine the way people act, including policies, procedures, and guidance
* **Technical**
  + Controls implemented in operating systems, software, and security appliances
* **Physical**
  + Controls such as alarms, gateways, and locks that deter access to premises and hardware

**Steps of Security Control**

* **Preventive**
  + Physically or logically restricts unauthorized access
* **Deterrent**
  + May not physically or logically prevent access, but psychologically discourages an attacker from attempting an intrusion
* **Detective**
  + May not prevent or deter access, but it will identify and record any attempted or successful intrusion
* **Corrective**
  + Responds to and fixes an incident and may also prevent its reoccurrence
* **Compensating**
  + Does not prevent the attack but restores the function of the system through some other means

**Defense mechanism**

* Layered security
  + Force an intruder to bypass more than one security control to achieve action on objectives
  + Reduce attack surface
  + Increase resiliency
* Control diversity
  + Provision different classes and types of controls
  + Mix technical, administrative, and physical controls
  + Deploy controls to prevent, deter, detect, correct, and compensate
* Vendor diversity
  + Use more than one supplier

Although multiple defenses may be necessary to withstand an attack

Five fundamental security principles:

* + - Protecting systems by layering
    - Limiting
    - Diversity
    - Obscurity
    - Simplicity

**Assets we protect:**

* Tangible
* Intangible
* Employees
* Market value
* Liabilities

**CIA Triad**

* Confidentiality
* Integrity
* Availability

(Non-repudiation

**Vulnerability, Threat & Risk**

* NIST (National Institute of Standards and Technology) and FIPS (Federal Information Processing Standards)
* Vulnerability - a weakness that could be triggered accidentally or exploited intentionally to cause a security breach
* Threat
  + The potential for a threat agent or threat actor to "exercise" a vulnerability
  + The path or tool used by the threat actor can be referred to as the threat vector
* Risk - the likelihood and impact (or consequence) of a actor exercising a vulnerability
* Control - a system or procedure put in place to mitigate risk

**Threat Actors**

* Organized crime
* Nation state / Advanced Persistent Threat (APT)
* Hacktivists
* Competitors

**Definitions:**

* **Asset**
  + Something that has a value
* **Threat**
  + An event or object that may defeat the security measures in place and result in a loss
* **Threat agent**
  + A person or thing that has the power to carry out a threat
* **Phishing** = fake bait
* **Snooping** = casual observation or fake e-mail
* **Eavesdropping** = nosey
* **Monitor** = watch
* **Toolkits** = a set of software tools
* **Backdoor** = gain access to a computer program bypassing security mechanisms

**Types of Attackers**

* The types of people behind computer attacks are generally divided into several categories
* Hackers
* Crackers/Spies
* script kiddies
* Employees
* Cybercriminals
* Cyberterrorists