SENG 460

Practice of Information Security and Privacy

Security In General

Fundamental Principles of Security

- **CIA Triad:**
  - **Confidentiality** ensures that data is protected from unauthorized disclosure.
  - **Integrity** ensures that data is accurate and reliable.
  - **Availability** ensures that data is accessible when and where it is needed.

    A balanced security approach should be implemented to ensure that all three facets are considered when security controls are implemented.

Common Security Terms/Definitions

- **Vulnerability:** An absence or weakness of a countermeasure that is in place.

- **Threat:** Any potential danger that is associated with the exploitation of a vulnerability.

- **Threat agents:** The entity that carries out the threat.

- **Risk:** The probability that a threat agent will exploit a vulnerability and the impact if the threat is carried out.

- **Exposure:** An instance of being exposed to losses.

- **Control/Countermeasure/Safeguard:** A control or mechanism that reduces the potential risk.

Common Security Control Types and Functionalities

- **Control types:** Administrative, technical, and physical
- **Control functionalities**
  - **Deterrent** Discourage a potential attacker
  - **Preventive** Stop an incident from occurring
  - **Corrective** Fix items after an incident has occurred
  - **Recovery** Restore necessary components to return to normal operations
  - **Detective** Identify an incident's activities after it took place
  - **Compensating** Alternative control that provides similar protection as the original control

Defense-in-depth Implementation of multiple controls so that successful penetration and compromise is more difficult to attain.