Summary Module 1

Terminology

Threat – Something that potentially could cause harm.

Harm – Something that cause damage.

Vulnerability – Something that can be exploited or used to cause harm.

Control – Something that can be used to control a vulnerability and thus a threat.

Characterization of security - CIA Triad

Confidentiality – Only authorized people and systems can access protected data.

Integrity – If the integrity of an item is preserved, we may mean that the item is precise, accurate, unmodified, modified only in acceptable ways, modified only by authorized people, modified only by authorized processes, consistent, internally consistent, meaningful and usable.

Availability – An item in considered available if the item is present in a usable form, has enough capacity to meet the service’s needs, making clear progress, and, if in wait mode, it has a bounded waiting time, it is complete in an acceptable period of time.

Examples of more fields:

* Authentication
* Nonrepudability

Characterization of harm

Interception – Compromises confidentiality

Interruption – Compromises availability

Modification – Compromises integrity

Fabrication – Compromises integrity

Counter measurement types in information security – Matrix

*Protects*

* Confidentiality
* Integrity
* Availability

*Kind of threat*

* Human / Not human
* Malicious / Not malicious
* Directed / Not directed

*Control type*

* Technical
* Procedural
* Physical

Characterization of threat

*Threats*

* Natural Causes (Fire, power failure)
* Human causes
  + Benign intent (Human error)
  + Malicious intent
    - Random (Malicious code on a general website)
    - Directed (Impersonation)

Characterization of attackers

* Terrorist
* Hacker
* Individual
* Criminal-for-hire
* Loosely connected group
* Organized crime member

Malicious attacker criteria

* Method
* Opportunity
* Motive

All those criteria must be fulfilled.

Characteristics of Control and Counter measurement

* Prevent (Blocking it)
* Deter (Making it harder)
* Deflect (Making another target more attractive)
* Mitigate (Making the impact less severe)
* Detect (Find the problem during or after)
* Recover (Go to a state not effecting)