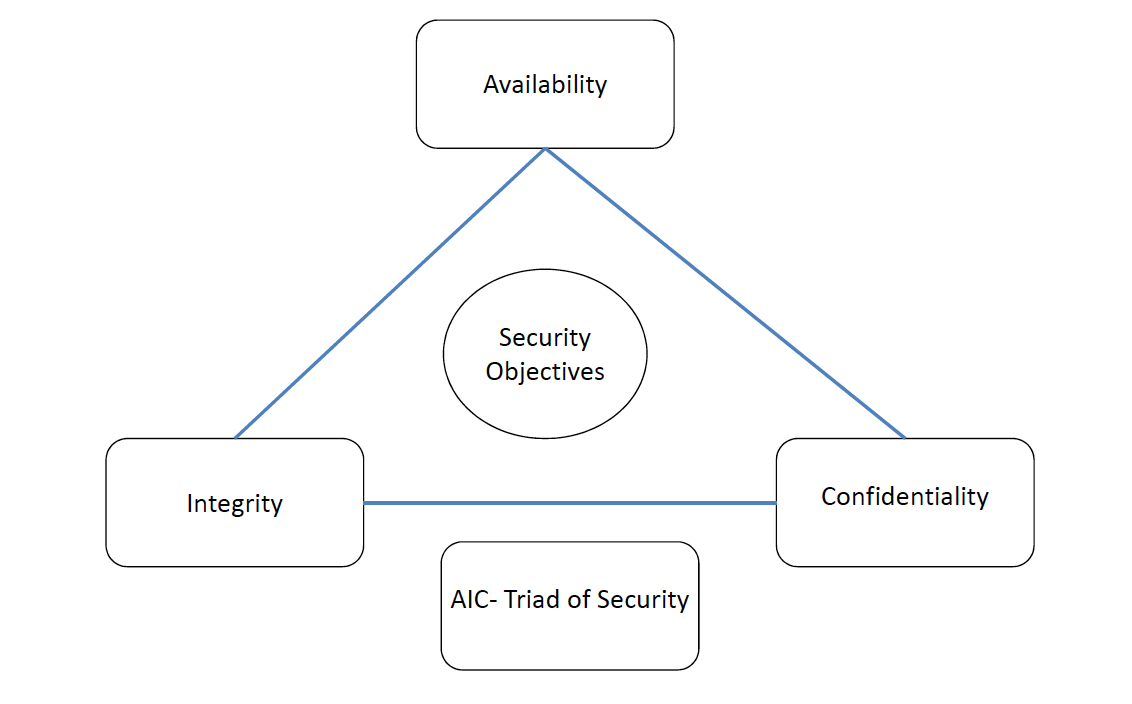
WEEK 1



**Availability** Protection ensures **reliability** and **timely** **access** to **data** and **resources** to **authorised** **individuals.**

**Integrity** Is upheld when the **assurance** of the **accuracy** and **reliability** of **information** and **systems** is **provided** and any **unauthorised** **modification** is **prevented**.

**Confidentiality** Ensures that the **necessary** **level** **of** **secrecy** is **enforced** at **each** **junction** of data **processing** and **prevents** **unauthorised** **disclosure**.

This **level** of **confidentiality** should **prevail** while **data** **resides** on **systems** and **devices** **within** the **network**, as it is **transmitted**, and **once** it **reaches** its **destination**.

Controls to Counter Cyber Attack

**Availability**

* Redundant array of inexpensive disks (***RAID***)
* Clustering
* Load balancing
* Redundant data and power lines
* Software and data backups

**Integrity**

* Hashing (data integrity)
* Configuration management (*system integrity*)
* Change control (*process integrity*)

**Confidentiality**

* Encryption for data at rest (*whole disk, database encryption*)
* Encryption for data in transit (*IPSec, SSL, PPTP, SSH*)
* Access control (*physical and technical*)

**Vulnerability** A lack of a **countermeasure** or a **weakness** in a **countermeasure** that is **in** **place**.

**Threat** A threat is **any** **potential** **danger** that is **associated** with the **exploitation** of a **vulnerability**.

**Threat** (*for business*) The threat is that **someone**, or **something**, will **identify** a **specific** **vulnerability** and **use** it **against** the **company** or **individual**.

**Threat Agent** The **entity** that **takes** **advantages** of a **vulnerability** is referred to as a **threat** **agent**.

**Risk** A risk is the **likelihood** of a **threat** **agent** **exploiting** a **vulnerability** and the **corresponding** **business** **impact**.

**Exposure** An exposure is an **instance** of **being** **exposed** to **losses**.

**Control** A **control**, or **countermeasure**, is put into place to **mitigate** the **potential** **risk**.

A **countermeasure** may be a **software** **configuration**, a **hardware** **device**, or a **procedure** that **eliminates** a **vulnerability** or that **reduces** the **likelihood** a **threat** **agent** will be able to **exploit** a **vulnerability**.