Security (quality or state of being secure from danger)

Discuss

The higher the security, the higher ore controls you need to put in place.(monitoring, encryption, password0

Trades off between protection and privacy.

These slow processes and reduce ease of use.

Confidentiality: Prevents unauthorized disclosure

Integrity: Prevents unauthorized modification

Availalbility: Ensures access

Possesion: Control about who holds data

Authenticiry: Verify sources

Utility: usefulness of data

XTICS of information

* Timeliness
* Accuracy
* Utiity
* Confidentilaity
* Integrity

Information system consists, hardware and software, data, people, procedures and network necssary to use inforation as resource that is being uses in an organization

COMPONENTS OF Information system.

* Data
* People
* Hardware
* Software
* Network

**Threats**: Anything that has potential to cause damage or harm to people.

**Vulnerabilities** an existing weaknessin organization that can be exploit by a threat.

**Controls** is a technique that can be remove or reduce vulnerabilities

TYPES OF THREAT

* Interception
* Interruption
* Modification

**Controls methods of defense**

* Encryption
* Policies
* Software and hardware controls
* Physical controls.

**Risk** is a likelihood that something bad will happen.

**RISK MANAGEMENT PROCESS**

Identify assets

Identify threats

Asess vulnerabilities

Assess risk

Mitigate risk

**Mitigate risk**

* Physical (gates,fences, doors, cameras )
* Logical(passwords, encryption, firewalls)
* Admnistrative( laws,policies, procedures,regulations)

**INCIDENT RESPOND PLAN**

The incident response process, at a high level, consists of:

* Preparation
* Detection and analysis
* Containment
* Eradication
* Recovery
* Post incident activity

As we increase the level of security, we usually decrease the level of productivity. Discuss

but this would be expensive, slow down transactions causing delays, and could upset our customers who don’t trust the technology.

SLIDES 2

* **Identification** is the claim of what someone or some thing is.
* **Authentication** establishes whether this claim is true.

**Factors of identification**

**The different factors are**

* something you know (password)
* something you are (Iris scan, fingerprints, etc)
* something you have (swipe card)
* something you do (gait (walking) recognition), and
* the place you are (at a specific terminal).

SLIDES 3

* **Authorization** allows us to specify where the party should be allowed or denied access
* **Access Control** enables us to manage this access at a more granular level.

ACCESS CONTROL

When we look at access controls, we have four basics tasks we might want to carry out:

* Allowing access
* Denying access
* Limiting access, and
* Revoking access.

SLIDES 4

**Cryptography** is the science of keeping information secure

**Encryption** referring to the transformation of unencrypted data, called **plaintext** or **cleartext**, into its encrypted form, called **ciphertext**.

**Decryption** is the process of recovering the plaintext message from the **ciphertext**.

The **plaintext** and **ciphertext** may also be generically referred to as the **message**.

**SYMMETRIC**

**Symmetric key cryptography**, also known as **private key cryptography**, utilizes a single key for both **encryption of the plaintext** and **decryption of the ciphertext**.

The key itself must be shared between the **sender** and the **receiver**, and this process, known as **key exchange.**

**ASSYMETRIC**

**Asymmetric key cryptography**, also known as **public key** **cryptography**, utilizes **two keys:** a **public key** and a **private key.**

The **public key** is used **to encrypt data sent** from the **sender** to the **receiver** and is shared with everyone.

**Private keys** are used to **decrypt data** that arrives at the r**eceiving end** and are very carefully guarded by the receiver.