``````````````````````````````````````````````````````````CH2````````````````````````````````````````````````````````

**Information is an asset اصلwhich, like other important business assets, has value to an organization and consequently needs to be suitably protected.**

**Computer Systems Security protection of computing and network communication**

**The evolution of computer networks has made the sharing of information ever more common.**

**A typical security policy might be hierarchical and apply differently depending**.

**Information can be created, stored electronically or magnetically, printed, or written on paper**.

**Security is the state of being safe and free from danger**.

**Information security is concerned in protecting valuable information and the systems that handle these information against any threats.**

**Security Policy is a document that states in writing how a company plans to protect the company's physical and information technology assets.**

**Security Policy is a critical document that helps to describe how an organization should manage risk, control access to key assets and resources, and establish procedures, and practices to keep its premises safe and secure.**

**A security policy defines the rules that regulate how an organization manages and protects its information and computing resources to achieve security objectives.**

**A security policy is often considered to be a 'living document', meaning that the document is never finished, but is continuously updated as technology and employee requirements change.**

**Building a Security Policy**

**PHASE 1: Asset inventory(list) and elaboration**

**PHASE 2:  IT Security audit / inventory**

**PHASE 3: Employee policy inventory**

**PHASE 4: Physical security audit**

**PHASE 5: Risk Assessment and protection**

**PHASE 6: Set protection level.**

**PHASE 7: Test protection level.**

**PHASE 8: Establish Backup, recovery.**

**PHASE 9: Document Security policy**

**PHASE 10: Review security policy**
``````````````````````````````````````````````````````````

**Security is not something we buy, it is something we do [T]**

**Security should be monitored 24x7 hours per week[T]**

**Experience teaches us that what works well for one organization may not precisely fit another [T]**

**It is extremely difficult to develop a unique policy for each organization[T]**

**````````````````````````````````````````````````````````````````CH3``````````````````````````````````````````````````````````**

**Key Points for a Good Policy**

**The security policy must be Understandable.**

**The security policy must be Realistic.**

**The security policy must be Consistent.**

**The security policy must be enforceable.**

**The security policy must be documented and distributed.**

**A successful security policy needs to be flexible.**

**A successful security policy must be reviewed.**

**Security training involves providing members of the organization with detailed information and hands-on instruction designed to prepare them to perform their duties securely.**

**One of the least frequently implemented, but the most beneficial programs is the security awareness program.**

**Why do we need a security policy?**

**could face damage to or loss of critical assets.**

**It is better to learn from others' mistakes instead of your own.**

**helps create a “security culture”.**

**Effects of security breaches**

**Reputation loss**

**Financial loss.**

**Loss of customer**

**LOSS OF GOODWILL**

**The board and management of the organization are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information.**

**Employee education about security is a key ingredient in enforcing successful and usable security policies [T]**

**The more valuable the assets that must be secured[T]**

**Management of information security can develop customized in-house training or outsource the training program[T]**

**One of the least frequently implemented, but the most beneficial programs is the security awareness program [T]**

**If the program is not actively implemented, employees begin to 'tune out', and the risk of employee accidents and failures increases[T]**

**All employees of the organization are required to conform with this policy[T]**

**This policy will be reviewed when necessary and at least yearly[T]**

**"A formal Hardware Inventory of all equipment is to be maintained and kept up-to-date at all times"[T]**

**````````````````````````````````````````````````````````````````````````````CH4``````````````````````````````````````````````````````````````````**

**Risk is a possible that a given threat will exploit vulnerabilities of an asset or a group.**

**Risk means the chance that someone or something will be harmed by the hazard**

**Risk includes the following three elements:**

**Asset: the entity requiring protection.**

**Threat: is a a potential violation of security .**

**Vulnerability: a deficiency creating the hazard**

**The Security Risk Assessment is:**

**A tool to identify organizational assets need to be protected.**

**Security Risk Assessment Approaches**

**baseline**

**informal**

**formal**

**combined**

**Baseline Approach**

1. **Use "industry best practice**
2. **Easy**

3. Cheap
4. may give too much or too little security.
5. implement safeguards.
6. suitable for small organizations

Formal Approach

1. Costly
2. Slow
3. may be a legal requirement to use.
4. suitable for large organizations

Combined Approach better use of time and money resources

Risk Assessment Process

Identify assets.

Identify threats.

Identify vulnerabilities.

Determine harm.

The Security Domain is defined by physical and logical perimeter boundaries.

Tangible Assets (which is of value to the organization):

Buildings

Employees

Intangible Assets

thinker property

Goodwill

Types of threats

Natural Threats

Accidental Threats

Intentional Threats

Probability Frequency in which threat will exploit vulnerability independent of harm.

Probability of each asset/threat/vulnerability combination should be quantified.

Harm of each asset/threat/vulnerability combination should be quantified.

Harm is the Impact if threat exploits vulnerability independent of probability.

Four basic strategies are used to control the risks that result from vulnerabilities

Apply safeguards (avoidance)

Transfer the risk (transference)

Reduce the impact (mitigation)

Inform themselves of all of the consequences and accept the risk without control or mitigation (acceptance)

Avoidance attempts to prevent the exploitation of the vulnerability.

Transference is the control approach that attempts to shift the risk to other assets, other processes, or other organizations.

Mitigation attempts to reduce the impact of exploitation through planning and preparation.

Three types of plans:

DRP

BCP

IRP

Acceptance of risk is doing nothing to close a vulnerability and to accept the outcome of its exploitation.

Risk management is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to assure the confidentiality, integrity, and availability of all the components in the organization's information systems.

The Security Domain includes assets that are by definition controllable[T]

Informal Approach suitable for small to medium sized orgs[T]

The Security Risk Assessment is a process to quantify hazards based upon probability and harm[T]

The Security Risk Assessment is a means to justify risk management strategies and allocation of assets[T]

Risk can never be eliminated [T]

Assets may have multiple threats and vulnerabilities[T]

When risks from information security threats are creating a competitive disadvantage[T]