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]

CH5

Information asset classification helps to specify the protection levels required for each information asset throughout its lifecycle.

Factors that affect the classification:

- **Value to the organization.**
- **Age.**
- **regulations govern protection.**

Information can be classified into:

- **Confidential**
- **Secret**
- **Top Secret**
- **Unclassified**

Policy should describe how data be protected.

Information asset classification is critical to ensure assets have a level of protection.

As the originator, or recipient, of sensitive documents you must:

- **Mark the document(s)**
- **Ensure documents are processed and stored.**
- **Remove or change the level of protection.**
- **Distribute the information.**

two main security categories

- **Classified**
  - **Top Secret**
  - **Secret**
  - **Confidential**
- **Protected**
  - **Protected C**
  - **Protected B**
  - **Protected A**

The "Unclassified" information is not protected [T]

You need to mark sensitive information at the time it is created or collected [T]

When marking you need to include

- **The sensitivity level (CAPS) ;**
- **The date of creation**

Top-Secret documents require a copy number [T]

MARKING SENSITIVE DOCUMENTS

- **Mark sensitive information**
- **Mark all material used.**

- **Indicate who may, or may not, have access.**
- **Must indicate the highest level of sensitivity.**

You should clearly record on the surface of electronic media, the following information:

- **Name of the organization**
- **Highest level of protection**
- **Subject of the documents**

Declassification: removal of sensitivity rating

Downgrading: reducing level of sensitivity rating

Protected information will lose its sensitivity

- **Over time**
- **Occurrence of specific events**

The classification to downgrade to upon a certain date [T]

Marked with highest classification when not stored[T]

``**CH6**``

Physical security is as important as logical security[T]

The **physical security policies** cover the elements involved in:

- Choosing a secure site
- Providing and securing internal support systems
- environmental and safety measures

Physical Threats fall into many categories:

- Natural environmental threats (e.g., floods, earthquakes and tornados).
- Supply system threats (e.g., power failures, and communication interruptions).
- Manmade threats (e.g., explosions).
- Politically motivated threats (e.g., strikes اضرابات).

Safety deals with the protection of life and assets against fires, natural disasters

Security addresses vandalismتخريب, theft, and attacks by individuals.

Physical Security Layers

- Protection
- Detection
- Delaying
- Assessment
- Response
``

Crime Prevention Through Environmental Design (CPTED) has three main strategies:

- Natural Access Control.
- Natural Monitoring.
- Regional (domestic) Reinforcement.

Natural Access Control The **guidance of people entering** and leaving a space by the placement of doors, fences, lighting, and landscaping.

Natural Monitoring Is the use and placement of physical environmental features, personnel walkways, and activity areas in ways that **maximize visibility.**

Regional Reinforcement Creates physical designs that **highlight the company's area** of influence to give legitimate owners a sense of ownership.

Issues with selecting a facility site:

- Visibility
- Accessibility
- Natural Threats

Using "mantraps" to protect sensitive areas.

A Mantrap is a small room with two doors.

"Fail safe:" if a power failure occurs, the door defaults to being **unlocked** (fire exits, lefts).

"Fail secure:" if a power failure occurs, the door defaults to being **locked** (safe boxes).

Environmental Issues:

- Temperature
- Positive Drains

"Closed Loop:" the air within the building is reused after it has been properly filtered, instead of bringing outside air in.

Positive Pressurization: when an employee opens a door, the air goes out and outside area does not come in.

"Fire Prevention:" includes **training employees** on how to react, supplying the right equipment, enabling fire suppression supply, proper storage of combustible elements.

"Fire Detection:" includes **alarms**, manual detection pull boxes, automatic detection systems with sensors, etc.

"Fire Suppression:" is the use of a **suppression** agent to put out a fire.

Types of Fire:

1. Liquid
2. Electrical
3. Kitchens

Types of Fire Detectors

- Smoker
- heat

Different types of suppression اطفاء-مكافحةagents

- Soda
- Water

``**CH7**``

Security is about regulating access to assets[T]

Software security is about managing these risks[T]

Software provides functionality comes with certain risks [T]

Owners Want to maximize the availability of the information assets and countermeasures vulnerabilities to reduce risks.

Attackers Want to make use of vulnerabilities to increase risks and threatens assets.

Confidentiality unauthorized users cannot read information.

Integrity unauthorized users cannot alter information.

Availability authorized users can always access information.

Non-repudiation for accountability authorized users cannot deny actions.

How to Realize Security Objectives?

- Authentication
- Authorization
- Auditing
- Action

Prevention measures to stop breaches of security goals.

Detection measures to detect breaches of security goals.

Reaction measures to recover assets, repair damage, and persecute offenders.

Good prevention **does not make** detection & reaction superfluous [T]

Countermeasures can lead to **new vulnerabilities**.

The **Witty worm** is a computer worm that attacks the firewall.

Example Security Technologies

- Cryptography
- Access-control
- Language-based security
``

Applications are built on top of "infrastructure" consisting of:

- Operating system
- Programming language

security/risk/requirements analysis

- stakeholders
- Brainstorm
- Rank threats

Example Techniques to Mitigate Threats

- Spoofing
- Tampering
- Information Disclosure
- Denial of Service

Examples of Software Security Policies

- Only administrators are allowed to install new software.
- Do not open messages from unknown sources.
- Keep antivirus up-to-date.

``**CH8**``

Types of Networks

LANs

WANs

VPNs

Attributes of an Effective Security Matrix

Easy to use.

Flexible.

The Network Security Policy

- Classify systems.
- Assign risk factors.
- Assign policy administration.

What We Are Trying to Protect

- End user resources.
- Network resources.
- Server resources.

Network Security Threats

- Spoofing
- Denial-of-Service (DOS)
``

- Viruses

Security Services

- Confidentiality
- Integrity
- Availability

Authentication methods

- Proving what you know
- Showing what you have

Authentication Techniques

- Password
- One time password
- Biometric

Brute-force attack Repeated access attempts

Dictionary attack Customized version of brute-force attack

Access Control List

- Discretionary مرنaccess control
- Mandatory access control
- Role-based access control

Execution Control List

- Sandboxing.

A **sandbox** is a security mechanism for separating running programs.

Sandboxing is used to test unverified programs from unverified third parties [T]

Antivirus is a computer software used to prevent, detect and remove malicious software like computer.

Antivirus must be installed on servers and user hosts, and permanently enabled [T]

Firewalls log the Internet activity and limit network host exposure [T]

Types of Firewalls

- Packet-filter firewalls:
    - Examine data flowing back and forth between a trusted network and the Internet.
- Gateway servers:
    - Firewalls that filter traffic based on the application requested.
- Proxy server firewalls
    - Firewalls that communicate with the Internet on the private network's behalf.

A proxy server is a server (a computer system or an application) that acts as an intermediary for requests.

Proxy Servers Advantage:

- Authentication
- Caching
- Speed

Passive auditing: automatic saving activities with user and time.

Active auditing: in addition to saving activities, it provides the real-time capability.

Availability is provided using extra resources:

- RAID
- UPS

The Network OSI Reference Model

- Physical layer
- Data link layer
- Network layer
- Transport layer
- Session layer
- Presentation layer
- Application layer

``CH9``

The Internet is a global system of interconnected computer networks.

***network of networks* that consists of millions of private, public, academic, business, and government networks of local to global scope.**

The Internet carries an extensive range of information resources and services.

Threats to the Internet

1. **Virus.**
2. **Worm.**
3. **Spam.**
4. **Trojan horse.**
5. **Phishing**
6. **Key**
7. **Logger**

Virus: a program that attaches itself to files and is spread when they are transferred or executed.

Worm: self-replicating program that proactively spreads itself.
``

Trojan horse: a program that appears legitimate but is in fact malicious.

Malicious Software Goals:

- **Key logging**
- **Hidden mail server**
- **Machine takeover.**
- **Destroying Information.**

Data communications requirements:

- **Keep data secure.**
- **Keep data private.**

Securing the Internet

- **Proxy**
- **Firewall**
- **Password**
- **Antivirus**

Proxy servers

- **All internet traffic routed via proxy server.**
- **Can filter content.**
- **Can cache content.**

Disaster recovery plan: Preparation of proactive arrangements for restoring computer processing operations and data files if operations are halted or files are damaged by major destruction.

1. Hardware loss:

- **Use Extra (Spare) Resources.**

2. Software loss:

- **make backups of program files.**

3. Data loss (Major costs and time):

- **Reassemble records: Customer information, accounting data, and Design information.**

4. Human Loss (Unrecoverable Loss):

- **Hiring and Training more Staff.**

What Can Cause Data Loss?

- ❖ **Incorrect software use**
- ❖ **Input data incorrectly**
- ❖ **Software may harm data.**
- ❖ **Virus infection.**

Methods of Backup:

- **Full backup**
- **Differential backup**
- **Incremental backup**

types of Backup Media:

- **Diskette / Hard disk**
- **USB Flash Memory**
- **CD-R / CR-RW / DVD**

Examples of Internet Security Policies

- **No games installing extraneous software.**
- **No shopping installing extraneous software.**
- **Keep your emails clean.**
- **Keep your computer updated.**

Penalties

- **You can lose network.**
- **Termination is possible.**