

CONTENTS OF A SECURITY PLAN:-1] POLICY :-

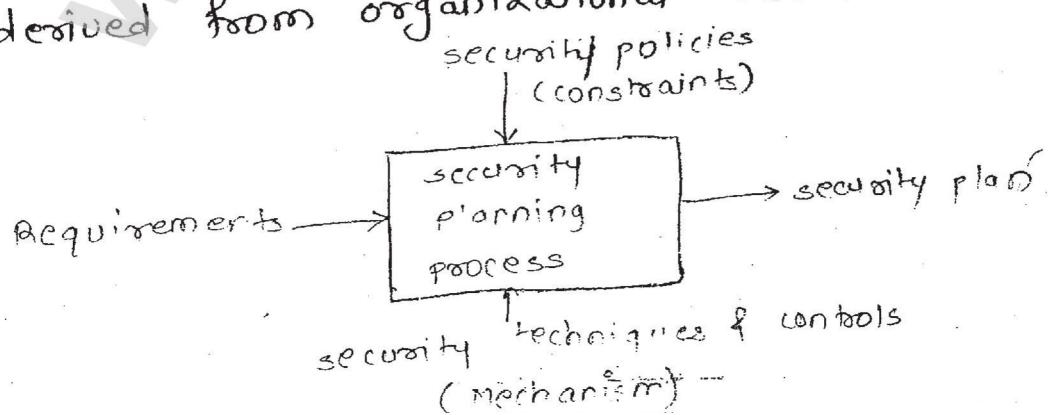
- must state the organisation's policy...
- indicates the goals of a computer security.
- willingness of the people involved in work.
- policy statement must answer to :-
 - i) Who should be allowed access ?
 - ii) To what system should access be allowed ?
 - iii) What types of access should each user be allowed.
- policy should specify the following :-
 - i) The organization's goals & commitment.
 - ii) Responsibility for security.

2] CURRENT SECURITY STATUS :-

- defines the limits of responsibility.
- describes status of security at the time of the plan.
- describes which assets are to be protected & who is responsible to protect them.
- defines the boundaries of responsibility.
- should clarify who provides the security.

3] REQUIREMENTS :-

- derived from organizational needs.



- Basic reasons & needs for new security level should be clearly defined.
- Requirement should have following characteristics
 - i) correctness :- are the requirements understandable
 - ii) consistency :- Are there any conflicts?
 - iii) completeness :- Are all possible situations addressed

4] TIMETABLE:-

- shows how & when the elements of the plan will be performed.
- describes how the security requirements will be implemented.
- specify the order in which the controls are to be implemented.
- gives milestones.
- contains schedule for periodic review.

5] ACCOUNTABILITY:-

- Describes who is responsible for each activity.
- Responsibility of roles should be given to different users.

6] RECOMMENDED CONTROLS:-

- maps controls to the weaknesses identified in the policy & requirements.
- The ways for fulfilling requirements should be stated

7] CONTINUING ATTENTION:-

- specifies a structure for periodically updating the plan.

RISK ANALYSIS :-

1] A risk can be distinguish from other project events in following concept :-

- A loss associated with an event :-
 - The event must generate a negative effect.
 - lost time, lost money, lost understanding, low quality. This loss is called the risk impact.
- The likelihood that the event will occur :-
 - There is probability of occurrence associated with each risk.
 - It can be measured in 0 (impossible) to 1 (certain).
 - When the risk probability is 1, problem is there.
- The degree to which we can change the outcome :-
 - Risk control involves a set of actions to reduce or eliminate the risk.

2] The strategies for risk reduction are as follows:-

- Avoiding the risk :-
 - by changing requirements for security.
 - by changing system characteristics.
- Transferring the risk :-
 - allocate the risk to other systems, people, organization
- Assuming the risk :-
 - by accepting it, controlling it with available resources if it occurs.

$$\text{Risk leverage} = \frac{\text{(risk exposure before reduction)} - \text{(risk exposure after reduction)}}{\text{cost of risk reduction}}$$

STEPS IN RISK ANALYSIS:-

1] IDENTIFY ASSETS:-

Hardware :- processors, boards, keyboards monitors, terminals, tape drives, printers, disks.

software :- source program, object program, system programs, utility programs.

Data :- data used during execution, stored data on various media, printed data.

people :- skills needed to run the computing system or specific programs.

documentation :- on programs, hardware, systems.

supplies :- papers, forms, laser cartridges, magnetic media

2] DETERMINE VULNERABILITIES:-

- This step requires imagination.

- We want to predict what damage occurs to assets & from what sources.

- We enhance our imaginative skills to find the nature of vulnerability.

- We want to use an organized approach.

3] ESTIMATE LIKELIHOOD OF EXPLOITATION:-

4] compute expected loss

5] survey & select new controls

6] Project savings.

TWO-Phase update:-

- A problem is failure of computing system before completion of transaction.

Update technique:-

- first phase is called intent phase
- in which DBMS gathers all the info such as data, open files, lock out other users & calculate final answers.
- makes no changes to database.
- it is repeatable no of times.
- takes no permanent action.
- last event of first phase is committing.
- committing involves writing of commit flag.
- After committing DBMS makes permanent changes. called as second phase.
- update activities of phase two can be repeated.

Redundancy:-

- for some important data, redundancy maintained.
- for eg:- like check bits.

www.ErForum.Net to maintain consistency in data.

Recovery:-

- DBMS provides log based recovery method
- In case of failure, database is reloaded from backup copy & changes are applied from the audit log.

Monitor:-

- unit of DBMS which is responsible for structural integrity.
- for eg:- monitor rejects numeric value for alphabetic characters.

Range comparison:-

- ensures value is written within acceptable range or not.
- ensures internal consistency of a database

State constraints:-

- describes the condition of entire database
- eg:- commit flag.
- set when commit phase starts & cleared when it ends.

Transition constraints:-

- describes conditions before changes can be applied to database.