Unit-3

Introduction to Security Measures

→ Why security is considered as major focus for an organization?

(i) Surveys proves that organization having proper security measures are able to protect their assets and generate better revenue than organizations with no proper measures taken

→ Challenges related to 'information security':-

(1) Physical security

(2) Threat of stealing information

(3) Destruction

(4) Disaster

etc.

Note : In order to cope-up with the security Challenges proper planning or streategy need to be made

→ How to proceed for secure Information System Development?

Secure Information System development can be proceeded by integrating risk analysis and management activities at the start of System Development Lifecycle (SDLC), which should get continued till the end of the development. This include : (1) Planning, (2) acquisition, (3) Buiding and ~~de~~ (4) Deployment of security.

→ What all phases are there in the conceptual view of SDLC

(1) Initiation
(2) Development/Acquisition
(3) Implementation/Assessment
(4) Operation/Maintenance
(5) Disposal

→ What all components are used to depict ~~in~~ each of the phases of ~~dev~~ SDLC?

(1) Control Gates : List the objectives to be met after the completion of intended phase, on which each of the activities is required to be validated

(2) Output ~~box~~ : In order to meet given objectives of the phase certain activities are performed. Those activities comes out with certain outputs regarded as ~~mile~~ different milestones of reaching the objectives listed through control gates.

(3) Activity Box : Shows the the activity to have required output. to meet objectives of the intended phase. If somehow required outputs are not comming after ~~the~~ performing the required activity then intended or all preceding activities may get revisited for having the desired output in meet specified objectives.

(4) Synchronization: is the arrowed circle to depict or the show space for revisiting related activities to have desired output

(5) Interdependencies: Shows the order in which activities are performed along with their concerned output as arrow.

→ List of primary security considrations in disposal phase

(1) Building and executing a plan for the disposal or transition of obsolete systems

(2) Archiving the important information to support up-comming system

(3) Cleaning of storage media and other supporting components

(4) Disposing of hardware and s/w components.

→ List of objectives for final phase of SDLC as part of it's control gate:

(1) Reviewing the closure of the system

(2) Reviewing the security of ~~system~~ closure

(3) Should take the consent of board that controls the change management process.

→ List of issues for secure application development

(1) Less trained/skilled developers

(2) Less educational focus on secure development

(3) Technical problems in finding right information for making secure application development strategies.

(4) Traditionlly security becomes part of focus in the last phase of development

(5) Compilers, interpreters and programming being unable to utilize system resources in the best way possible.

→ Why common framework of development is required?

(1) To reduce development time.

(2) " " " complexity

(3) " " " errors

(4) " increase " accuracy

→ What are the benefits of using common framework?

Ans → page 114

→ What are the factor should get included in the common framework of development

(1) Foundation

(2) Principles

(3) Design Guidelines

→ List out the design guidelines and it's benefits & :-

(1) Validating input

(2) Handling exception

(3) Applying cryptography

(4) Using random numbers

→ How Information Security Governance and Risk Management can be performed?

(1) Senior managers being assigned the responsibility of managing risk.

(2) Executives should get involved in recognizing and understanding the risk which can harm the organization or it's,assets in any aspects

(3) Risk tolerance should get established

(4) Risk management program should get implemented by involving all levels of employees.

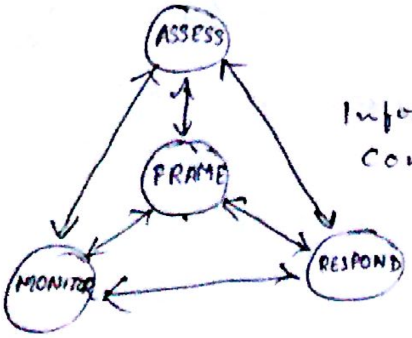
→ What are the activities involved in risk management process?

(1) Framing : About sensing the threat and informing all the related parties who perform required activities to control or avert the possible damage

(2) ~~Assing~~ Assessing: It is about analyzing the risk and related measures in order to keep them in synchronized stage.

(3) Monitoring: It helps in providing or setting required guidelines for acquiring security in best possible manner by monitoring all the activities happening inside the organization.

(4) Responding: It is about taking or performing the action to nutralize the adverse affect of any unwanted event.



Information and communications Flows shown with arrow

→ How to achive Secure System Design?

By following the given concepts :-

(1) <u>Layering</u> : Arranging H/w and S/w in logical order such that H/w will be kept at bottom layer. On the top of it layers of S/w will get arranged.

2. <u>Abstraction</u> : As per the predefined policy of an organization only required set of activities will get exposed to the users of it. Thus this will help in hiding non essential details from the users.

3. <u>Security Domain</u> : helps in defining access levels so that hiearchy of accessibility can be maintained.

4, The ring model : consist of 4 layers starting from 0-3 for layering CPU hardware and software

(4) <u>Open and closed system</u> : is about the liberty of incorporating H/w and S/w from one or multiple vendors. Closed system does not provide such liberty of incorporating both from multiple vendor.

→ What are the primrary threat for physical security?

(1) Physical access exposure to human being

(2) Physical access exposure to natural disasters

→ What machanisms are there to have physical security?

(1) Physical access control

(2) Electronic and visual surveillance systems

→ What measures should be taken for securing backups?

(1) Assigning responsibility, authority and accountability

(2) Assessing risk

(3) Developing data protection process

(4) Communicating processes to concerned persons

(5) Excuting and testing process

→