INCIDENT RESPONSE PLANNING

- Incident response planning covers the identification of, classification of, and response to an incident.
- What is incident? What is incident Response?
- An incident is an attack against an information asset that poses a clear threat to the confidentiality, integrity, or availability of information resources.
- If an action that threatens information occurs and is completed, the action is classified as an incident. an incident.

- Attacks are only classified as incidents if they have the following characteristics:
    1) . They are directed against information assets.
    2) . They have a realistic chance of success.
    3) . They could threaten the confidentiality, integrity, or availability of information resources.

Incident Response-IR

IR is therefore the set of activities taken to plan for, detect, and correct the impact of an incident on information assets.

- IR is more reactive than proactive.
- IR consists of the following FOUR phases:
    1. Planning
    2. Detection
    3. Reaction
    4. Recovery

Incident Planning

- Planning for incidents is the first step in the overall process of incident response planning.
- Planning for an incident requires a detailed understanding of the scenarios developed for

the BIA.

- With this information in hand, the planning team can develop a series of predefined responses that guide the organizations' incident response (IR) team and information security staff.
- This assumes TWO things

  The organization has an IR team and

  The organization can detect the incident.
- The IR team consists of those individuals who must be present to handle the systems and functional areas that can minimize the impact of an incident as it takes place.
- IR team verifies the threat, determines the appropriate response, ands co-ordinates the actions necessary to deal with the situation.

 # Format and Content

-The IR plan must be organized in such a way to support, rather than impede, quick and easy access to require information, such as to create a directory of incidents with tabbed sections for each incident.

-To respond to an incident, the responder simply opens the

binder, flips to the appropriate section, and follows the clearly outlined procedures for an assigned role.

 # Storage

- Where is the IR plan stored?
- Note that the information in the IR plan should be protected as sensitive information.
- If attackers gain knowledge of how a company responds to a particular incident, they can improve their chances of success in the attacks.
- The document could be stored adjacent to the administrator's workstation, or in a book case in the server room.

 # Testing

- A plan untested is not a useful plan
- " Train as you fight, and fight as you train"
- Even if an organization has what appears on paper to be an effective IR plan, the procedures that come from the plan has been practiced and tested.
- Testing can be done by the following FIVE strategies:

1. Check list: copies of the IR plan are distributed to each individual with a role to play during an actual incident. These individuals each review the plan and create a checklist of correct and incorrect components.

2. Structured walkthrough: in a walkthrough, each involved individual practices the steps he/she will take during an actual event.

This can consist of an "on the ground" walkthrough, in which everyone discusses hi/her actions at each particular location and juncture or it can be more of a "talk through" in which all involved individuals sit around a conference table and discuss in turn how they would act as the incident unfolded.

3. Simulation: Simulation of an incident where each involved individual works individually rather than in conference, simulating the performance of each task required to react to and recover from a simulated incident.

4. Parallel: This test is larger in scope and intensity. In the parallel test, individuals act as if an actual incident occurred, performing the required tasks and executing the necessary procedures.

5. Full interruption: It is the final; most comprehensive and realistic test is to react to an incident as if it were real.

In a full interruption, the individuals follow each and every procedure, including the interruption of service, restoration of data from backups, and notification of appropriate individuals.

Best sayings.

- The more you sweat in training, the less you bleed in combat.
- Training and preparation hurt.
- Lead from the front, not the rear.
- You don't have to like it, just do it.
- Keep it simple.
- Never assume
- You are paid for your results, not your methods.

Incident Detection

- Individuals sometimes notify system administrator, security administrator, or their managers of an unusual occurrence.
- This is most often a complaint to the help desk from one or more users about a technology service.
- These complaints are often collected by the help desk and can include reports such as "the system is acting unusual", " programs are slow", " my computer is acting weird", " data is not available".

 # Incident Indicators

- There are a number of occurrences that could signal the presence of an incident candidate. Donald Pipkin, an IT security expert identifies THREE categories of incident indicators:

  POSSIBLE,
  PROBABLE and
  DEFINITE

Possible Indicators

- **Presence of unfamiliar files.**

  If users report discovering files in their home directories or on their office computers , or administrators find files that do not seem to have been placed in a logical location or that were not created by an authorized user, the presence of these files may signal the occurrence of an incident.

- **Possible Indicators**

  Presence or execution of unknown program or process:

  If users or administrators detect unfamiliar programs running or processes executing on office machines or network servers, this could be an incident.

Probable Indicators

a) **Activities at unexpected times.**

If traffic levels on the organization's network exceed the measured baseline values, there is a probability that an incident is underway.

If systems are accessing drives, such as floppies, and CD –ROMS, when the end user is not using them, is an incident.

b) **Presence of new accounts**

Periodic review of user accounts can reveal an account that the administrator does not remember creating, or accounts that are not logged in the administrator's journal.

Even one unlogged new account is a candidate incident.

c) **Reported Attacks**

If users of the system report a suspected attack, there is a high probability that an incident is underway or has already occurred.

d) **Notification from IDS**

If the organization has installed host-based or network based intrusion detection system and if they are correctly configures, the notification from the IDS could indicate a strong likelihood that an incident is in progress.

Definite Indicators

Definite indicators are the activities which clearly signal that an incident is in progress or has occurred.

- USE OF DORMANT ACCOUNTS
  Many network servers maintain default accounts that came with the systems from the manufacturer. Although industry best practices indicate that these accounts should be changed or removed; some organizations ignore these practices by making the default accounts inactive.

- In addition, systems may have any number of accounts that are not actively used, such as those of previous employees, employees on extended vacation or sabbatical, or dummy accounts set up to support system testing.

- If any of these dormant accounts suddenly become active without a change in status for the underlying user, this indicates incident occurred.

CHANGE TO LOGS

The smart administrator backs up systems logs as well as systems data. As a part of a routine incident scan, these logs may be compared to the online version to determine if they have been modified .If they have been modified, and the systems administrator cannot determine explicitly that an authorized individual modified them, an incident has occurred.

PRESENCE OF HACKER TOOLS:

A number of hacker tools can be used periodically to scan internal computers and networks to determine what the hacker can see.

They are also used to support research into attack profiles

.

Incident Reaction

- Incident reaction consists of actions that guide the organization to stop the incident, mitigate the impact of the incident, and provide information for the recovery from the incident

- In reacting to the incident there are a number of actions that must occur quickly including:

- notification of key personnel
- assignment of tasks
- documentation of the incident

Notification of Key Personnel

- Most organizations maintain alert rosters for emergencies. An alert roster contains contact information for the individuals to be notified in an incident.
- Two ways to activate an alert roster:
  - A sequential roster is activated as a contact person calls each and every person on the roster.
  - A hierarchical roster is activated as the first person calls a few other people on the roster, who in turn call a few other people, and so on.

Documenting an Incident

- Documenting the event is important:
  - It is important to ensure that the event is recorded for the organization's records, to know what happened, and how it happened, and what actions were taken. The documentation should record the who, what, when, where, why, and how of the event.

Incident Recovery

- The first task is to identify the human resources needed and launch them into action.
- The full extent of the damage must be assessed.
- The organization repairs vulnerabilities, addresses any shortcomings in safeguards, and restores the data and services of the systems.