Incident Response

Policies

Policies are formal statements about organizational intent. In short, they explain why an organization wishes to operate in a certain way, and they define things like the purpose or objective of an activity or program.

Well-written incident response policies will include important components of the IR process.

They will identify the team and the authority that the team operates under.

They will also require the creation and maintenance of incident handling and response procedures and practices, and they may define the overall IR process used by the organization.

A policy is a high-level statement of management intent that is used to convey the organization's expectations and direction for a topic.

Standards will then point to a policy for their authority, while providing specific guidance about what should be done.

Procedures are then used to implement standards or to guide how a task is done.

Policies tend to be slow to change, whereas standards change more frequently, and procedures and guidelines may be updated frequently

Retention Policies

A retention policy determines how long you keep data and how it will be disposed of.

The reason why it's important to incident responders is because it may determine how long the organization keeps incident data, how long logs will be available, and what data is likely to have been retained and thus may have been exposed if a system or data store is compromised or exposed.

Incident Response Plan

Can include several subplans to handle various stages of the response process.

Individual plans may also be managed or run by different teams.

Regardless of the structure of the plan, they need to be regularly reviewed and tested.

Important Factors/Items

Communication plans
List roles, such as who should communicate with the press or media, who will handle specific stakeholders...

Stakeholder management plans
Related to communication plans

Focus on groups and individuals who have an interest or role in the systems, organizations, or services that are impacted by an incident.

Business continuity (BC) plans
Focus on keeping an organizational functional when misfortune or incidents occur.

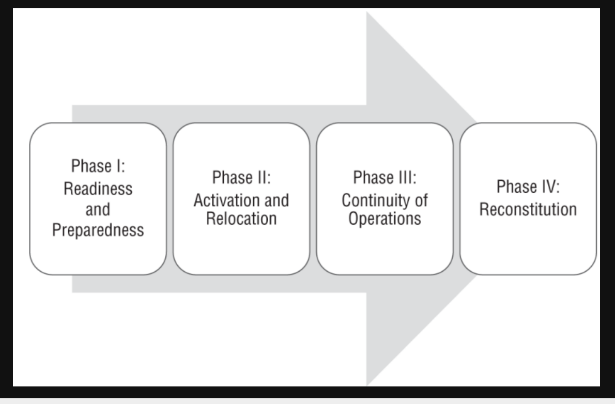
Disaster recovery (DR) plans
Define the processes and procedures that an organization will take when a disaster occurs.

A DR plan focuses on restoration or continuation of services despite a disaster.

COOP

A federally sponsored program in the United States that is part of the national continuity program.

COOP defines the requirements that government agencies need to meet to ensure that continuity of operations can be ensured.



Phase I: Readiness and Preparedness
Phase II: Activation and Relocation
Phase III: Continuity of Operations
Phase IV: Reconstitution

Exercises

Tabletop:
Talk through processes
Resembles a brainstorming session

The team thinks of a scenario and discuss the issues and potential improvements in their response and IR plan

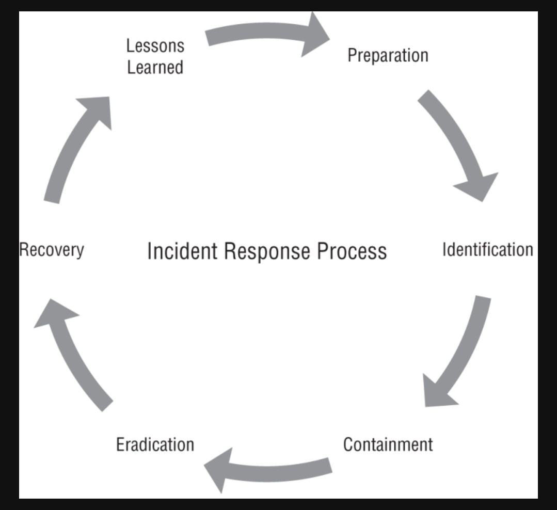
Walk-through:
Take a team through an incident step by step

Excellent way to ensure that teams respond as they should without the overhead of a full simulation

Simulations
Can be done on full scale or just parts or specific departments

All members involved must know that they are engaged in an exercise so that no actions are taken outside of the exercise environment

The 6 steps for incident response



The 6 steps for incident response

Preparation:
In this phase tools, processes, and procedures to respond to an incident are built and set in place (ie. training an incident response team, conducting exercises, documenting...)

Identification:
In this phase, events are reviewed to be able to identify incidents (ie. log analysis, monitoring tools, etc..)

Containment:
This phase starts once an incident is identified, in this phase, the incident response team needs to contain the incident to prevent further issues or damage.

Eradication:
This phase involves removing the artifacts associated with the incident (In many cases, that will involve rebuilding or restoring systems and applications from backups rather than simply removing tools from a system since proving that a system has been fully cleaned can be very difficult.)

An artifact of an incident is a domain, URL, IP address or a file affected in the incident.

Recovery:
At the heart of this phase is restoration to normal. That may mean bringing systems or services back online or other actions that are part of a return to operations. It also involves implementing fixes to ensure that whatever security weakness that allowed the incident to occur has been remediated.

Lessons Learned:
These are important to ensure that organizations improve and do not make the same mistakes again. (They may be as simple as patching systems or as complex as needing to redesign permission structures and operational procedures.)

Incidents: individual organizations may define them differently, in general an incident is a violation of the organization's policies and procedures or security practices.

Events: are an observable occurrence, which means that there are many events, few of which are likely to be incidents.

The Team

A member of management or organizational leadership. This individual will be responsible for making decisions for the team.

Information security staff members are I (the core of the team) as they will bring the specialized IR and analysis skills needed for the process.

The team will need technical experts such as systems administrators, developers, or others from disciplines throughout the organization. (It varies based on the incident, not all the technical experts might be needed for all incidents.

Communications and public relations staff, they are important to help make sure that internal and external communications are handled well.

Legal and human relations (HR) staff, they maybe involved in some, but not all, incidents.

Law enforcement, only when specific issues or attacks require their involvement.

Regardless of the specific composition of your organization's team, you will also need to ensure that team members have proper training.

Incident Response

Incident response is the process by which an organization handles a data breach or a cyber attack.

Although organizations may use slightly different labels or steps and the number of steps may vary, the basic concepts remain the same.

Policies

A policy is a high-level statement of management intent that is used to convey the organization's expectations and direction for a topic.

Standards will then point to a policy for their authority, while providing specific guidance about what should be done.

Procedures are then used to implement standards or to guide how a task is done.

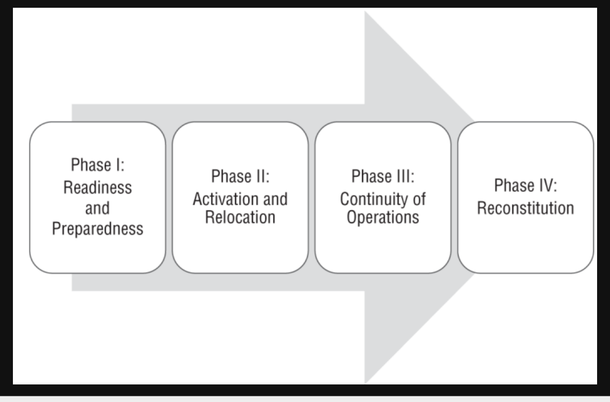
Policies tend to be slow to change, whereas standards change more frequently, and procedures and guidelines may be updated frequently

- Policies are formal statements about organizational intent. In short, they explain why an organization wishes to operate in a certain way, and they define things like the purpose or objective of an activity or program.
- Well-written incident response policies will include important components of the IR process.

  They will identify the team and the authority that the team operates under.

  They will also require the creation and maintenance of incident handling and response procedures and practices, and they may define the overall IR process used by the organization.
- Retention Policies
  - A retention policy determines how long you keep data and how it will be disposed of.
  - The reason why it's important to incident responders is because it may determine how long the organization keeps incident data, how long logs will be available, and what data is likely to have been retained and thus may have been exposed if a system or data store is compromised or exposed.

COOP

- A federally sponsored program in the United States that is part of the national continuity program.
- COOP defines the requirements that government agencies need to meet to ensure that continuity of operations can be ensured.
- 
Phase I: Readiness and Preparedness
Phase II: Activation and Relocation
Phase III: Continuity of Operations
Phase IV: Reconstitution

Incident Response Plan

- Can include several subplans to handle various stages of the response process.
- Individual plans may also be managed or run by different teams.
- Regardless of the structure of the plan, they need to be regularly reviewed and tested.
- Important Factors/Items
  - Communication plans
    List roles, such as who should communicate with the press or media, who will handle specific stakeholders...
  - Stakeholder management plans
    Related to communication plans

    Focus on groups and individuals who have an interest or role in the systems, organizations, or services that are impacted by an incident.
  - Business continuity (BC) plans
    Focus on keeping an organizational functional when misfortune or incidents occur.
  - Disaster recovery (DR) plans
    Define the processes and procedures that an organization will take when a disaster occurs.

    A DR plan focuses on restoration or continuation of services despite a disaster.

Exercises

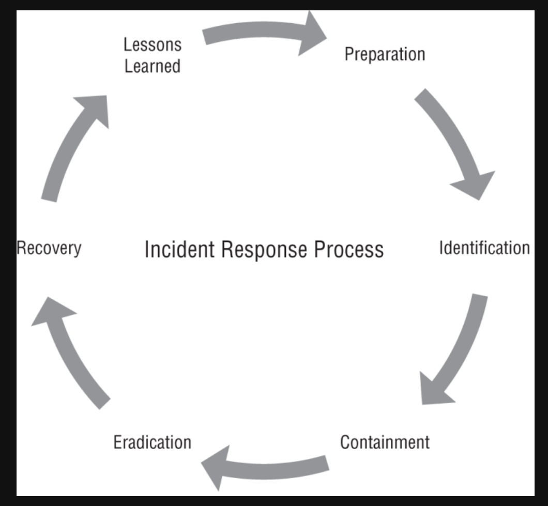
- Tabletop:
  Talk through processes
  Resembles a brainstorming session

  The team thinks of a scenario and discuss the issues and potential improvements in their response and IR plan
- Walk-through:
  Take a team through an incident step by step

  Excellent way to ensure that teams respond as they should without the overhead of a full simulation
- Simulations
  Can be done on full scale or just parts or specific departments

  All members involved must know that they are engaged in an exercise so that no actions are taken outside of the exercise environment

The 6 steps for incident response



The 6 steps for incident response

- Preparation:
  In this phase tools, processes, and procedures to respond to an incident are built and set in place (ie. training an incident response team, conducting exercises, documenting...)
- Identification:
  In this phase, events are reviewed to be able to identify incidents (ie. log analysis, monitoring tools, etc..)
- Containment:
  This phase starts once an incident is identified, in this phase, the incident response team needs to contain the incident to prevent further issues or damage.
- Eradication:
  This phase involves removing the artifacts associated with the incident (In many cases, that will involve rebuilding or restoring systems and applications from backups rather than simply removing tools from a system since proving that a system has been fully cleaned can be very difficult.)
  - An artifact of an incident is a domain, URL, IP address or a file affected in the incident.
- Recovery:
  At the heart of this phase is restoration to normal. That may mean bringing systems or services back online or other actions that are part of a return to operations. It also involves implementing fixes to ensure that whatever security weakness that allowed the incident to occur has been remediated.
- Lessons Learned:
  These are important to ensure that organizations improve and do not make the same mistakes again. (They may be as simple as patching systems or as complex as needing to redesign permission structures and operational procedures.)

Incidents: individual organizations may define them differently, in general an incident is a violation of the organization's policies and procedures or security practices.

Events: are an observable occurrence, which means that there are many events, few of which are likely to be incidents.

The Team

- A member of management or organizational leadership. This individual will be responsible for making decisions for the team.
- Information security staff members are l (the core of the team) as they will bring the specialized IR and analysis skills needed for the process.
- The team will need technical experts such as systems administrators, developers, or others from disciplines throughout the organization. (It varies based on the incident, not all the technical experts might be needed for all incidents.
- Communications and public relations staff, they are important to help make sure that internal and external communications are handled well.
- Legal and human relations (HR) staff, they maybe involved in some, but not all, incidents.
- Law enforcement, only when specific issues or attacks require their involvement.

Regardless of the specific composition of your organization's team, you will also need to ensure that team members have proper training.