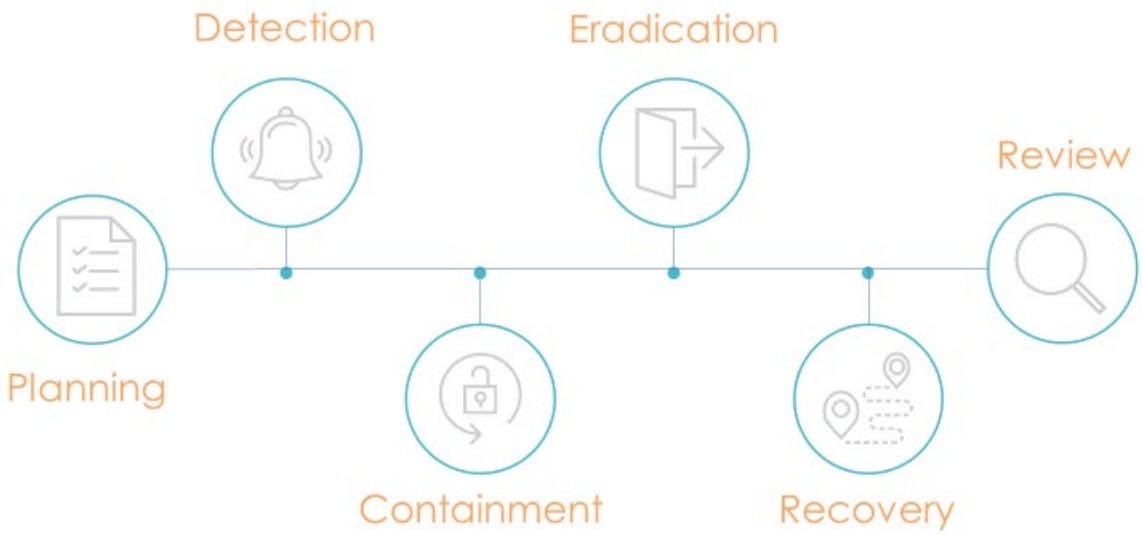
Incident Response Design Workshop

About the Workshop

INCIDENT RESPONSE, CYBERSECURITY

This post provides an approach for designing your incident response capability. Use this as your starting point for developing and maturing your incident response capability. Understand your incident response phases. The six proposed phases of the incident response process are:



For more about incident response (IR) management and preparedness read the National Institute of Standards Guide SP 800-61 Rev 2 published in August 2012. For more about incident response team guidance read the Blue Team Handbook: Incident Response Edition.

Our recommended approach is to conduct a workshop to review each of the six phases. Let's examine each phase in greater depth and highlight the items that you need to address in your own incident response planning.

1. Planning

Time spent planning reduces risk and increases the effectiveness of your approach and work efforts. Do not under-resource the planning phase! Preparing for incidents is the foundation for protecting your business and data. If you are in Aerospace and Defense, Construction, or any other industry, preparation will improve your incident response performance by lowering expended resources, improving activity effectiveness and coordination, and enhancing the quality of work during times of crisis. This phase includes:

Policy Development

Your policy is a written statement of high-level objectives and requirements for how possible incidents will be addressed. Your policy should define the purpose of having incident response capability, explain event types and escalation classes, and define key activities and roles in responding to incidents.

Plan

Your plan is a detailed step-by-step handbook for how the incident response process works. The plan should detail how you will address any given incident type and the escalation procedures you will apply.

Team Formation

Selecting the right team and roles in advance can be the difference between muddling through the process or doing it effectively. As a minimum, include the following:

- Legal Counsel – coordinates the plan and incident response.
  Having the team members report to and through an attorney will protect your organization since the plan and results of an investigation and/or incident response together with the recommended remediation will be protected from disclosure to outsiders by attorney-client privilege and work product doctrine.
- Incident Response Manager – coordinates and directs the technical effort.
- Information Security Officer (ISO) – performs as the deputy to the Legal Counsel and handles the administrative internal coordination and notification (when necessary) to external entities (Clients, DoD, law enforcement, etc.)
- Technical Analysts – investigates the incident (internal and external).
- Identify whether IT infrastructure engineers or security analysts are needed to perform the detailed analysis to determine what happened or is happening.
- External Technical Resources – fills other gaps in your team.
  Identify external resources that may be needed and contact or pre-arrange with them to be available when needed.

In addition to your core team, you will interact with Management and Leadership (for resources and funding), Human Resources (if employees are involved), Strategic Communications (Public Relations), and/or Internal Corporate Legal Counsel.

Activity and Workflow

Defining activities, establishing workflows, and assigning responsibility are crucial to developing, testing, and using your incident response capability. A visual, such as a graphic depiction of the workflow, will show all of your response steps and how you will work through them from the triggering incident through resolution and ultimately closure.

Training and Testing

Train your staff and incident response teams regarding their roles and responsibilities in the event of data breach. Test different incident response event types in advance through table-top testing.

Sample questions to ask:

- Network Time Protocol (NTP): Make sure you have NTP enabled on all devices that can use it. You especially want to ensure that everything on your network to be set to the same time and not off. (For example: make sure Windows Clients are synced with Active Directory, switches and routers use the same NTP server).
- Establish Central Logging capability: Ensure that you have some kind of storage device that can handle all your logs. Utilizing syslog is key because of its filtering options. Windows Event Logs will need this option so that certain events aren't sent over that are not relevant to incident response.
- Asset Inventory: Having an updated list of all your assets will greatly improve an IR team's response and outcome.

    - Have your policies and plans been developed and approved by management?
    - Have workflows been included in the planning documentation?
    - Do you have an incident team established and has the team been trained and participated in plan testing?
    - Has the incident response policy been communicated to staff and subcontractors?
    - Do you have an NTP server?
    - What device are you using to store your central logs?
    - Do you know what devices you have on your network?
    - Does your plan comply with all current applicable rules, standards, and regulations?

- Planning step exit criteria: This is a continuous event in many companies as each new system and updates to existing systems are being prepared for incident response.

2. Detection (or Identification)

Security Incidents come in all shapes and sizes. Being able to detect them and have an approach for dealing with them requires people and technology working side by side to determine if you have been breached.

Speed is of the essence, and incident response expectations have moved from fairly laissez-faire questions such as, "Do you have an incident response capability?" to "Do you have a documented capability?" to "Can you respond in 30 days?" to "Can you respond in 72 hours?" to "Can you respond in 24 hours… 8 hours… or even less?" The enhanced expectations require you to have the capability to detect that something occurred, are made aware of it, and take action in that time period. Oh, how times have changed.

Leverage your understanding of your business by having up-to date-architecture and threat models so that you can draw upon these resources. Include legal counsel in the investigation and reporting of the incident. This can protect the organization's interests from third-party discovery and encourage full and honest reporting.

Sample questions to ask:

- Did an event take place? What was it?
- Who discovered it?
- What was discovered?
- Where was it discovered?
- When did the event take place?
- Why did it take place?
- How is the business impacted?
- How pervasive is the breach/compromise?
- Are there signs of exfiltration?
- Do we watch and learn? If so, how long? Or do we pull the plug?
- What is the needed uptime or business impact if these systems need to be taken down?

Detection step exit criteria: If the assessment process has made a confirmation that this is indeed an incident then activate the IR process.

3. Containment

We often run into cases where the information around an incident no longer exists because the organization moved quickly to delete it. However, containment is both a strategy to limit the impact of an incident and to preserve enough information to prevent it from occurring again.

Preservation may also be required by law. You should consult with legal counsel to know your obligations in this regard. In addition, if you have insurance, you should comply with all notice obligations to be certain your insurance policy offers maximum coverage for the types of incidents to which you might be vulnerable.

Different incidents will have different containment strategies. For example, if there is a breach on an endpoint, you will disconnect the device and examine it offline. You can then examine the issue (i.e. like a ransomware attack) using forensic software. Then you can wipe and re-image the device.

However, there are attacks that may cause greater harm when a device (such as a host) is disconnected from a network. Those incidents need to be dealt with differently.

It is critical to consider the types of threats and your containment options. Your options may be based on where the attack takes place and what data it is putting at risk (short term and long term).

Sample questions to ask:

- What is the type of breach you have? Examples: DoS or DDoS, Data loss, Ransomware, Website Defacement, or Internal Employee.
- What has been done (i.e. did some person or system take action that you need to know/understand)?
- What needs to be done to contain the breach now and moving forward in the longer term?
- Can you operate the business while you are mitigating the breach? Are disaster recovery/backup procedures in place?
- Can you safely separate the breached environment / contain it?
- What environment will you have to set up the containment environment?
- Initial data collection: what to gather early?
- Does immediate isolation need to be started on the device?

Containment step exit criteria: The attacker can no longer attack the network and the affected systems are identified.

4. Eradication

After putting a containment strategy in place, you will take steps to fully investigate and eliminate the cause of the data breach. You will collect information and conduct root cause analysis.

You will make decisions on what are sufficient steps or technical measures you will take to eliminate the causes of the attack. You are striving to eliminate it completely or to an acceptable level.

Sample questions to ask:

- How will you eradicate the vulnerability you are facing?
- What system changes (hardening, patching, other configuration activities) will need to be implemented?
- Are user accounts affected?
- What vulnerability scans/tools will use to validate the eradication process?
- Will you implement changes at once, will you have work around in the short term, will you require significant investment to implement new solutions?
- Will you need to wipe and re-image systems?
- Has the environment been hardened to reduce a potential recurrence?
- What are your preservation obligations and where should they be maintained?

Eradication step exit criteria: The IR team and the business are confident that network and systems are configured to eliminate a repeat occurrence.

5. Recovery

Recovery is the process of restoring you affected systems back to "normal" operating status. The process starts when the eradication step is complete. You should take your time to do this right. The old adage, go slow to go fast, is the basic principle here. This requires prioritizing recovery activities and not trying to do too much at once and not meeting your recovery objectives.

Sample questions to ask:

- Have systems been patched and hardened (to a standard)?
- Can the system be restored from a trusted back-up?
- How will you know that systems are clean and fully operational?
- Have the systems been tested, has data been validated, and when can systems be returned to production?
- How long will you continue to monitor the systems for abnormal behaviors?
- What abnormalities will you look for?
- What reporting obligations do you have to regulators and/or customers?
- If there are reporting obligations, who should be the messenger and how should the message be delivered?
- Any sign of repeat events?
- Are you implementing monitoring to check for repeat events?

Recovery step exit criteria: No evidence of repeat events, unusual activity or incidents.

Do you have the right tools or procedures to make sure a similar attack will not take place? (Example Tools: Security Incident & Event Management (SIEM), Endpoint Detection and Response (EDR), behavioral threat analytics, file integrity monitoring, security configuration monitoring, next generation data intrusion detection/protection, privileged access management).

6. After Action Review

Once the incident response team has completed the investigation, hold an after-action review with all the team members. The purpose of the review is to discuss what you have learned from investigating the data breach. We call this a "Hot Wash".

The hot wash will review the entire event and response from beginning to end. Examine what worked well and where the team and process ran into challenges. Document everything.

All team members should be part of this hot wash. Each will bring a unique perspective. It is critical to take the individual perspectives and integrate them through discussion to reach a common understanding of what you learned from the investigation. Document everything and use this information for improving the next iteration of your Incident Response Plan.

Sample questions to ask:

- What changes need to be made to the security?
- What changes need to be made to the incident response process?
- How should employees be trained differently?
- What weakness did the breach exploit?
- Was there human error or a system error?
- Do you have an actionable plan to prevent this type of breach event from happening again?
- How likely or unlikely is that claims will be made against the customer?
- How great is the legal exposure to the organization?
- Is management satisfied the incident is closed?

After Action Review Exit Criteria: Management is satisfied the incident is closed.

After the Workshop

Begin documentation as you prepare and conduct the workshop. Following the workshop, continue the documentation process. All of your documentation efforts form your inputs to the Planning and Preparation phase.

This six-step process gets codified through an incident response policy and managed through an incident response plan. Be sure that you have both.

In addition, you need to be sure you can follow your own process. You do this by testing and training. Test the policy and the plan by conducting drills. They will not replace the experience of a real incident, but they will greatly improve your preparation.

Keep preparing. Keep testing. Keep learning. Keep improving.