CYBALT

Importance Of An Incident Response Plan

Cybalt Inc. Suite #510, 2701,
North Dallas Parkway, Plano, TX

discover@cybalt.com

What are the Key Risks of Digital Transformation?

First, let's define an Incident Response:

It is a process for organizations to identify, prioritize, contain and eradicate cyberattacks. The goal of incident response is to ensure that organizations are aware of significant security incidents, and act quickly to stop the attacker, minimize damage caused, and prevent follow-on attacks or similar incidents in the future.

Why you need an Incident Response Plan:

Cyberattacks, including high profile ransomware attacks, have significantly impacted thousands of organizations of all sizes and in all industries. The attackers do not discriminate, they exploit targets who have lax security controls or prey on vulnerable users through phishing attacks. This could include a small industrial distribution company or a mid-size healthcare clinic. The commonality of any cyberattack is business disruption or financial leverage, forcing an organization to pay the cybercriminal or risk having exfiltrated data published on the dark web. No organization having sensitive data or negatively impacted by a business disruption is too small or too secure to be hit by a breach.

Without an incident response plan, your IT security and management teams will be scrambling to understand and respond, and under intense pressure, missteps are often made. Depending on the type of information exposed and the size of the breach, you may be legally required to notify not only those affected but also government agencies or other industry organizations. Not having an Incident Response Plan in place will potentially create legal action and fines.

Certain states, such as California with their Consumer Protection Act (CCPA), mandates strict data privacy regulations that require an Incident Response Plan. There are also security frameworks in place that require an Incident Response Plan. For example, an ISO 27001 Certification requires an Incident Response Plan. Annex A has a specific requirement for an information security incident response plan.

Ultimately, whether your business is big or small, in any industry (private, non-profit or public sector), and regardless of mindset that you don't feel you are a target for a cyberattack, you need to have an Incident Response Plan in place. Cyberattacks are indiscriminate and a Plan will prepare you to respond efficiently, effectively and accelerate the recovery process, not to mention the legal mandates of having a plan.

How do you write an Incident Response Plan:

There are numerous cybersecurity consulting firms that have built templates and provide consultative services around the Incident Response planning process. A search will uncover plans that are five-step, six-step and even a ten-step methodology. Writing an Incident Response Plan does not have to be complicated, but follow a defined path that is inclusive of relevant components.

One of the cybersecurity industry bodies - The National Institute of Standards and Technology (NIST) – has published a comprehensive guide to writing an Incident Response Plan titled: Computer Security Incident Handling Guide. The Guide overviews three core areas:

1. **Organizing an Incident Response capability within your organization**
2. **Handling an Incident**
3. **Coordination and sharing of information with outside organizations**

In addition to NIST, the SANS Institute also has published an Incident Response template. Both non-profit bodies offer a comprehensive, yet straightforward approach to creating an Incident Response Plan. Effective IR Plans can be written by in-house cybersecurity or IT resources. It is not required to use outside consultative services. The only requirement will be time, access to specific internal documentation and access to key constituents within the organization, including executive management, legal, financial, human resources, marketing/PR and the IT staff.

If the organization is severely resource constrained, then outside help may be warranted. Another reason for outside guidance would be an expert review of a recently completed IR Plan - a second set of eyes can be helpful to spot potential holes or provide further Plan refinement.

Using NIST's guide, let's briefly summarize each of the Guide elements:

1. Organizing an Incident Response Capability Within Your Organization

From the NIST Guide:

Organizing an effective computer security incident response capability involves several major decisions and actions:

One of the first considerations should be to create an organization-specific definition of the term "incident" so that the scope of the term is clear.

The organization should decide what services the incident response team should provide, consider which team structures and models can provide those services, and select and implement one or more incident response teams.

Incident response plan, policy, and procedure creation is an important part of establishing a team, so that incident response is performed effectively, efficiently, and consistently, and so that the team is empowered to do what needs to be done. The plan, policies, and procedures should reflect the team's interactions with other teams within the organization as well as with outside parties, such as law enforcement, the media, and other incident response organizations.

From NIST, the illustration below includes the key outside parties an organization must coordinate with as part of the planning process and during an actual event.

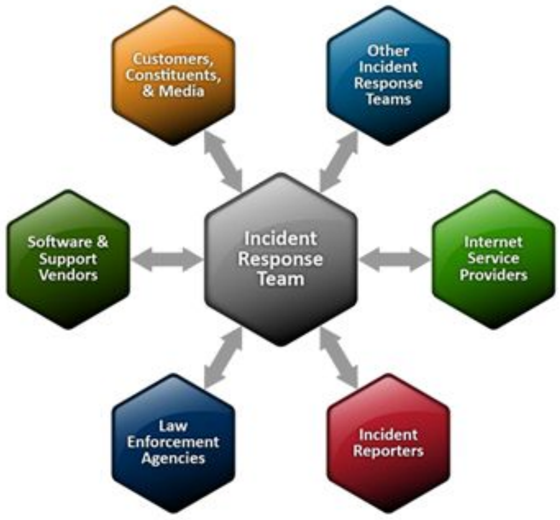
Customers, Constituents, & Media
Other Incident Response Teams
Software & Support Vendors
Incident Response Team
Internet Service Providers
Law Enforcement Agencies
Incident Reporters

Figure 2-1. Communications with Outside Parties

2. Handling an Incident

The core to your Incident Plan is the documentation on how to handle an incident. Although the NIST approach is 'only' four steps, every step is equally important and serves an important role in the entire Incident Response process. Below is the NIST Incident Response Lifecycle.

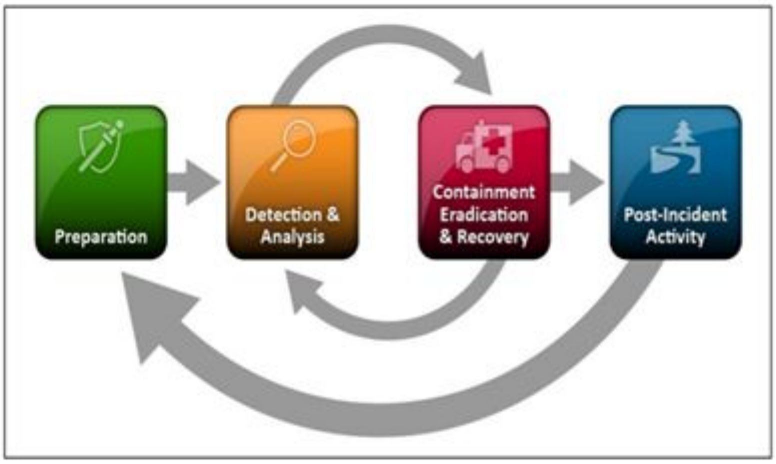

Figure 3-1. Incident Response Life Cycle

Here is an overview of each step in the handling of an incident:

i) **Preparation:** This initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, residual risk will inevitably persist after controls are implemented.

From NIST: “Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs.”

NIST’s preparation section provides basic advice on preparing to handle incidents and on preventing incidents.

ii) **Detection and Analysis:** Detection of security breaches is critical to alert the organization whenever incidents occur. In keeping with the severity of the incident, the organization can mitigate the impact of the incident by containing it and ultimately recovering from it (see next section).

From NIST: “Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors. Different types of incidents merit different response strategies.”

NIST lists various attack vectors but are not intended to provide definitive classification for incidents; rather, they simply list common methods of attack, which can be used as a basis for defining more specific handling procedures.

iii) **Containment, Eradication, and Recovery:** During this phase, activity often cycles back to detection and analysis—for example, to see if additional hosts are infected by malware while eradicating a malware incident.

From NIST: “Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident.

Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly. Containment strategies vary based on the type of incident. For example, the strategy for containing an email-borne malware infection is quite different from that of a network-based DDoS attack. Organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision-making."

iv) Post-incident Activity: Another way of saying it: "Lessons Learned." After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents.

From NIST: "One of the most important parts of incident response is also the most often omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. Holding a "lessons learned" meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself. Multiple incidents can be covered in a single lessons learned meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident."

SANS suggests this general format for the incident report:

- When was the problem first detected and by whom
- The scope of the incident
- How it was contained and eradicated
- Worked performed during recovery
- Areas where the CIRT teams were effective
- Areas that need improvement

3. Coordination and Sharing of Information With Outside Organizations

From NIST: "The nature of contemporary threats and attacks makes it more important than ever for organizations to work together during incident response. Organizations should ensure that they effectively coordinate portions of their incident response activities with appropriate partners. The most important aspect of incident response coordination is information sharing, where different organizations share threat, attack, and vulnerability information with each other so that each organization's knowledge benefits the other. Incident information sharing is frequently mutually beneficial because the same threats and attacks often affect multiple organizations simultaneously.

As mentioned in Section 1, coordinating and sharing information with partner organizations can strengthen the organization's ability to effectively respond to IT incidents.

For example, if an organization identifies some behavior on its network that seems suspicious and sends information about the event to a set of trusted partners, someone else in that network may have already seen similar behavior and be able to respond with additional details about the suspicious activity, including signatures, other indicators to look for, or suggested remediation actions. Collaboration with the trusted partner can enable an organization to respond to the incident more quickly and efficiently than an organization operating in isolation."

Some final words:

An Incident Response Plan should be reviewed annually at a minimum. Organizations change through M&A activity or organic growth. Technology quickly evolves. Cyber Attackers frequently leverage new techniques. New industry guidelines may necessitate complying with new policies. The organization's workforce will change, requiring ongoing communication. Global political, healthcare and environmental events will impact your plan. All of these factors will impact your Plan, not only content but the frequency of revisions.

In order to 'battle test' an IR Plan, it is recommended that organizations consider conducting an IR 'tabletop' exercise which simulates a cyber 'event' such as a ransomware attack. Tabletops are a great way to identify potential gaps in the Plan – whether they be internal communications, lack of clear guidance, gaps in expectations with the cybersecurity insurance carrier or outside legal counsel. A myriad of small 'things' will arise in a tabletop exercise. At this stage, they can be easily rectified before a real event occurs. Ultimately, the tabletop exercise will give you (and executive management) the confidence that you are ready, as best as possible, when that inevitable cyberattack does occur.