TWA
Risk Management
Fund

Incident Response Plan Creation and Testing

In today’s digital landscape, cyber threats are not a matter of if, but when. Organizations must be prepared to respond swiftly and effectively to security incidents to minimize damage, protect sensitive data, and maintain trust. A well-crafted Incident Response Plan (IRP) is the cornerstone of this preparedness.

What Is an Incident Response Plan?

An Incident Response Plan is a structured approach for detecting, responding to, and recovering from cybersecurity incidents. It outlines roles, responsibilities, procedures, and communication strategies to ensure a coordinated and efficient response.

Key Components of an Incident Response Plan

Preparation

- Define scope and objectives of the IRP.
- Build the incident response team (IRT) with clear roles.
- Establish communication protocols for internal and external stakeholders.
- Conduct training and simulations to build muscle memory.

Identification

- Use tools like SIEM, IDS/IPS, and endpoint protection.
- Define incident types and severity levels.
- Create a reporting mechanism for anomalies and suspicious activity.

Containment

- Short-term containment: Isolate affected systems.
- Long-term containment: Apply temporary fixes while maintaining operations.
- Preserve forensic evidence for investigation and legal purposes.

Eradication

- Identify and eliminate malware, unauthorized access, or vulnerabilities.
- Patch systems and update configurations.
- Validate system integrity before moving forward.
- Update the IRP based on findings.
- Share insights across teams to strengthen defenses.

Best Practices for a Successful IRP

- Keep it simple and actionable: Avoid jargon and ensure clarity.
- Test regularly: Run tabletop exercises and simulations.
- Integrate with business continuity plans.

- Ensure compliance with industry standards (e.g., NIST, ISO 27001, GDPR).

Plan Testing

Incident response plan testing is used to determine whether an incident response process is effective and identifies critical gaps. Testing helps to ensure all members of the team are aware of and familiar with their roles and responsibilities. Any gaps could cause issues if a real attack occurred. It is important to detect any vague or ineffective areas of the plan before the plan is ever used. We will discuss the Tabletop method for testing Incident Response Plans.

Tabletop Exercise

This is the most basic test of your incident response plan. All the key members of your Incident Team meet in a conference room and go over several breach scenarios. Members are asked to talk through their part of the response, as directed by the plan.

There is definite value from this approach. In most organizations, questions like the ones below, used in a Ransomware scenario, tend to highlight some holes, and generate some meaningful to-do items after the meeting.

- *How do you investigate and discover what was exfiltrated?*
- *How long will it take to recover data from backup(s)?*
- *What are the talking points for staff who get calls from customers?*
- *How will the multiple DDoS attacks be mitigated?*
- *What vendor agreements are in effect?*

A broad range of scenarios such as Ransomware, Business Email Compromise, and Cyber Extortion are encouraged to be looked at when testing.

Incident response capabilities *need* to be put to the test. It is important for ALL employees to understand their role in the cyber security of the organization. Responding to cyber incidents and breaches is an organization-wide effort, which is why clearly defining who needs to do what in your response plan is critical before you even begin to test it. An Incident Response Plan is not a static document—it's a living strategy that evolves with your organization and the threat landscape. By investing in a proactive and well-documented IRP, you empower your team to act decisively when it matters most.

The TWARMF Cyber Risk Services Advisor is currently scheduling Incident Response Plan Tabletop Testing visits for members. To get on the schedule, contact Lee Cain, Cyber Risk Services Advisor at 512-619-1437 or lee.cain@sedgwick.com.