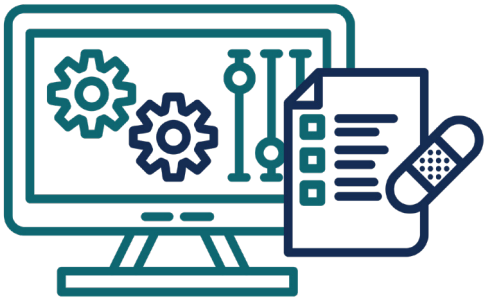
Key Steps To Include in Your Incident Response Plan

PONDURANCE



Cyberattacks are constantly evolving. Organizations must have an incident response (IR) plan in place to respond to cyberattacks, reduce the impact on business operations, and get back to normal operations. The key steps should revolve around the life cycle of an attack. We outline the key steps to include in your IR plan below:

Preparation

Collecting key information, assembling your key stakeholders, assigning roles and responsibilities, and documenting the process to create a formal cybersecurity policy are essential for the team to effectively respond to threats.

- [ ] Understand and identify what type of information your company manages. This will give you a baseline of where security efforts must be focused, including any data management regulations that could be violated (HIPAA, GDPR, CPRA, etc.).
- [ ] Assess your security team and determine if your internal security operations center (SOC) has enough analysts to monitor, detect, and respond to threats on a 24/7 basis. This can gauge whether you have enough staff on hand or need to implement a managed detection and response (MDR) service to help fill the gaps, mitigate blind spots in your security posture, and provide log activity of your digital landscape.
- [ ] Develop a list of essential logs, inventory all digital assets, and establish who in IT and the SOC will receive clear and actionable alerts to execute a review of these items.
- [ ] Identify who your key stakeholders are, such as employees in human resources, IT, SOC, legal, customer success, and marketing. Upon assembling your IR team, assign roles and responsibilities for all relevant stakeholders.
- [ ] Establish the location of all company backups, including privileged credentials, passwords, and SSH keys. These should be stored in an off-site centralized vault.
- [ ] Make a list of contacts such as vendors, partners, cyber insurance providers, and law enforcement that must be notified in the event of an incident.

Identification

When every minute counts, it is essential to have a strong security team and security tools to monitor and detect malicious activity throughout your network, endpoints, logs, and cloud on a 24/7 basis.

- [ ] Understand and determine what type of security tools your internal SOC will leverage to detect threats (i.e., endpoint detection and response, network sensors, logs, and cloud).
- [ ] Perform a vulnerability assessment to identify weaknesses that need to be patched in your digital landscape.
- [ ] Consider leveraging an MDR provider if you lack the number of staff required to implement 24/7 monitoring.
- [ ] Ensure you are keeping security and activity logs for legal purposes.
- [ ] Document who will lead the team if a breach occurs and who they should contact.

pondurance.com
500 N. Meridian St., Suite 500, Indianapolis, IN 46204

PONDURANCE

Containment and Eradication

Responding to security incidents can take many forms such as triaging alerts and containing the threat by isolating or shutting down the infected systems to prevent further spread to your network. In addition, leveraging your SOC to actively hunt for these threats is critical to detecting the location of malicious files, backdoors, and other types of threats that can lead to a security incident.

- [ ] Immediately contain systems, networks, servers, databases, and devices to minimize any potential widespread damage.
- [ ] Determine if any sensitive information was breached or data loss occurred.
- [ ] Update any firewalls and network security to capture any evidence that can be used for post-breach investigations.
- [ ] Preserve all evidence that can further analyze the origin, impact, and intention behind the attack.
- [ ] Keep a log of the incident and response, such as the date, time, location, and extent of the damage. This is critical to identifying whether the attack was deployed externally, internally, or possibly from a misconfiguration or human error. Also, it is vital to document those on your team who discovered and reported the incident.

Response

All hands on deck are required when communicating the incident externally and with other internal departments.

- [ ] Work with your marketing team to draft external communications (public statements) on how you are dealing with mitigating the incident. This time is especially critical because disclosing an attack too late can negatively affect the reputation of the business and impact customer trust.
- [ ] Engage with your legal team and examine any compliance or regulatory risks to determine potential violations.
- [ ] Contact law enforcement and any other required government agencies.
- [ ] Communicate with your internal team and coach them on discussing the matter with customers who contact the organization.

Recovery

Reviewing and reporting on what happened, what was the root cause, and what could have been improved in the IR plan can reduce the time and likelihood of another incident.

- [ ] Gather logs, memory dumps, audits, network traffic reports, and disk images to perform a post-incident investigation.
- [ ] Patch and mitigate the entry point to ensure the attacker cannot regain access.
- [ ] Perform a root cause analysis to determine the attacker's steps used to gain access to your systems to improve security controls.
- [ ] Perform a companywide vulnerability analysis to ensure all vulnerabilities have been addressed.
- [ ] Restore systems to the preincident state.
- [ ] Implement security awareness training among your staff and provide insight into how human error and password management are essential.
- [ ] Keep all stakeholders informed about any of the latest updates to the IR plan.

Learn more about the importance of an incident response plan and how it can help your organization our eBook ***Incident Response Planning.***

pondurance.com
500 N. Meridian St., Suite 500, Indianapolis, IN 46204