Cybersecurity Best Practices

INCIDENT RESPONSE PLAN

FBI CYBER

Cybersecurity best practices include having a written incident response plan. The development of an incident response plan can improve decision making, limit damage, and expedite remediation. An effective incident response plan addresses incident detection, analysis, containment, workarounds or fixes, prevention, logging of events, preservation of evidence, and post-incident review.

Creating and practicing a plan to respond to incidents on your network is just as important as preventing the incidents. If you can design and execute a thoughtful response, you may be able to mitigate damage, and may even avoid an incident altogether as work done in support of creating an incident response plan also likely strengthens your organization’s cybersecurity posture.

Creating an Incident Response Plan

Before you create an incident response plan, identify what is at risk. Ask yourself:

- What are the most crucial operations of your company that could be affected by a cyberattack?
- How could a successful cyberattack impact your company?

Varying functions and company information might be of different urgency or value to different companies. Knowing what really matters to your company’s ability to function will be critical in designing the best way to respond to an attack.

Identify an incident response team.

There are three main components to an incident response plan: technical, legal, and managerial. As part of your plan, designate specific, skilled people who are best positioned to cover those functions. Ask yourself:

- What information does each component need?
- What should you expect from each component?
- What’s the chain of command?
- To whom does the team report?
- Who has the authority to make judgment calls as to when the company’s computer networks will be taken down, quarantined, or put back online?

Identify a means for communication.

After identifying an incident response team, find a way for the team members to communicate that does not rely on potentially compromised systems. If your incident response team talks on channels where the attacker is listening, you’ve created more problems.

Develop a playbook to address the most likely incidents. Various types of incidents might require different kinds of responses, depending on which systems are affected and to what extent. Each response should include these elements:

- Who to notify in the company
- What information to collect
- When and how to contact law enforcement
- How to preserve evidence
- Whether other potential victims should be warned
- Which facts a decision-maker will use to decide how to treat affected systems

Your plan should cover these basic steps:

1. Assess the attack and potential damage
2. Contain the attack to prevent additional damage
3. Collect information about the attack to inform decision-makers, law enforcement and other victims
4. Notify your internal command chain and outside partners to address all aspects of the attack, especially to remediate any damage.

Consider adding the FBI as part of your incident response plan.

The FBI encourages companies to develop a relationship with their local FBI field office prior to a cyber incident. Cyber-trained special agents, computer scientists, and intelligence analysts in FBI field offices can provide local expertise and are available for deployment to victim sites immediately upon notice of an incident. While the FBI does not provide remediation services, FBI investigators will work alongside the 3rd party entity designated by a company that is part of its incident response plan. Contacting the FBI helps us to collect evidence to discover who the attackers are, where and how they operate, and how we may disrupt them and impose consequences most impactful against them. Additionally, our involvement allows us to warn others by sharing threat indicators so long as doing so is beneficial and does not jeopardize ongoing investigations.

Ensure your legal, technical, and management experts approve of your incident response plan.

Once the incident response plan is approved, ensure your response team regularly reviews and practices the plan. You can ask for guidance to fine-tune your plan from Private IT/security partners who may be involved in your incident response.

Drafting an incident response plan can be intimidating. There are several free resources online, including a guide published by the Department of Justice (https://www.justice.gov/criminal-ccips/file/1096971/download).

Stay ahead of the threat by anticipating how you will respond in the event of an attack. Creating an incident response time will save you time and money if you are hit, and will minimize damage as you work to restore your systems.