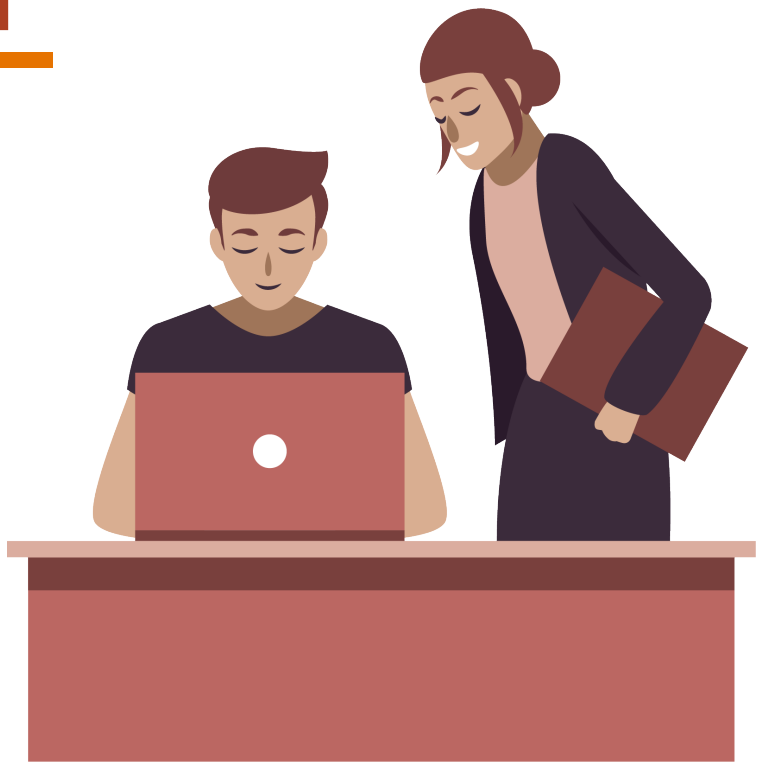
SecurityAwarenessNews

the security awareness newsletter for security aware people

Responding to Incidents

Behind the Scenes of Incident Response



Picture this:

You've poured your heart and soul into building a thriving family business. Through years of dedication, you've grown from a small team to over 100 dedicated employees, earning a stellar reputation from loyal customers in the process.

Now, imagine one morning you learn that **cybercriminals have breached your network and locked up your systems.** Your operations grind to a halt, and customers are calling because they can't access services. You're facing a financial downfall, and your reputation is at stake.

What do you do next?

That question is why organizations have an incident response plan. It provides a comprehensive strategy to help detect, respond to, and recover from security events and other incidents. Think of it as an emergency plan with step-by-step guidelines, similar to how most buildings have predefined evacuation routes.

While different organizations will have different approaches to how they build their plan, here's a common framework:

- **Preparation –** compile a list of assets and identify risks to those assets.
- **Detection –** discover and analyze the security incident.
- **Containment, eradication, and recovery –** contain the incident, remove the threat, and restore affected assets.
- **Post-incident analysis –** determine how the incident occurred and take measures to reduce the probability of similar incidents in the future.

Your family business could use this framework to quickly assess your situation, mitigate damages, and restore operations. While the main goal is to avoid incidents, in today's landscape of frequent cyberattacks and other threats, the unexpected can happen at any time. Incident response plans address that concern with actionable strategies.

And your part in this is essential. An organization's incident response plan won't work unless employees report incidents as soon as they notice them. Your role, therefore, is to stay alert and report anything suspicious immediately per your organization's protocols.

That simple process is a key part of protecting data, assets, and most importantly, people.

Why Timely Action Matters

There's no doubt that matters of security require timeliness, especially when incidents occur. **Quick action can lead to quick solutions.** That's why reporting suspicious activity immediately is so important. To get a better idea of this, let's review an example of timely reporting in action.

The Incident

Imagine a traditional office setting for a large organization. An employee in the marketing department receives an email from human resources. The subject states, "Urgent: Action Required for Payroll Update." It asks the employee to click a link and verify their login details to access the payroll portal.

The Detection

While the email does appear to come from human resources, the sender's email address looks slightly unusual, and the tone of the message seems a bit too demanding. The employee feels a sense of alarm but quickly grows suspicious.

The Report

Rather than simply deleting the email, the employee immediately reports it using their organization's designated phish alert button. This informs the security team of a potential phishing attack, which is a malicious attempt designed to lure people into making bad decisions.

The Response

The security team is able to quickly analyze the message and determines that it is, indeed, malicious. They then use automated security tools to instantly remove that same malicious email from every other employee's inbox across the entire organization.

The Outcome

Had the email been ignored or gone unreported, others might have fallen for the scam. Instead, thanks to someone's quick action, the phishing attack was neutralized before it could cause any harm.

This example illustrates how a simple, immediate report protects everyone. So remember: **Don't wait. Don't assume. Always act — even if something seems minor.**

Proactive Security

While incident response plans are vital, organizations hope they never have to use them. **You can help by taking a few proactive steps that represent the fundamentals of security awareness.**

Learn To Recognize Warning Signs of Attacks

Cyberthreats, like phishing scams, are constantly evolving, but many still rely on common tricks. They often feature warning signs such as threatening language, urgent requests, and unrealistic promises or scenarios. Stay alert for those signs, and use extreme caution when opening links or attachments.

Avoid Making Assumptions

It's easy to assume an email is legitimate or that someone is who they claim to be, but scammers rely on these assumptions. Always approach unusual requests with skepticism, especially if they involve confidential information. If a situation seems off, verify through alternative and trusted channels.

Use Strong, Unique Passphrases for Every Account

A passphrase is a way of creating passwords that are long, hard to guess, but easy for you to remember. A good way to do this is by using obscure quotes from your favorite books, movies, or songs. Never use the same passphrase more than once. To make this easier, consider using a password manager (if your organization allows them). It's software that creates, stores, and syncs login credentials across multiple devices.

Practice Physical Security

Physical security is just as important as cybersecurity. Here are a few examples of what it includes:

- Locking workstations and devices when not in use
- Properly storing confidential documents
- Ensuring doors to secured areas remain closed
- Never allowing someone to borrow your keycards or badges

Always Follow Organizational Policies

Implementing strong policies is a fundamental part of incident response plans and an organization's collective security. By always following those policies, you help protect data, assets, and people. Conversely, circumventing or ignoring policies puts everyone at risk.

These proactive steps are simple and contribute to the shared responsibility of security awareness. Thanks for doing your part!