AVERTIUM

CHECKLIST

The Ultimate Incident Response Plan Checklist

AVERTIUM. SHOW NO WEAKNESS™

The Ultimate Incident Response Plan Checklist

A security incident can lead to significant breaches of your network and data that could impact your organization for hours, days, or even months.

A rigorously developed relevant incident response (IR) plan that considers potential impact to all aspects of your business in their current and future states will prepare you to quickly mobilize around minimizing the impacts of a breach.

Here is the ultimate checklist for creating a rigorous, relevant and responsive IR plan to empower you to build a show-no-weakness approach to cybersecurity.

- 01 ☑ Perform a risk assessment to locate and document where your organization keeps its crucial data assets and prioritize security issues to address.
- 02 ☐ Designate your computer security incident response team (CSIRT), being sure to include departments company-wide. Notify parties of their role in the event of an incident.
- 03 ☐ Determine internal and external stakeholders and define and communicate to them what their roles and responsibilities will be.
- 04 ☐ Avoid the mistake of using a free downloadable fill-in-the-blank plan, opting in instead to employ customizable incident response planning tools that identify your company's unique needs.
- 05 ☐ Engage regularly with internal parties to keep data security top-of-mind at all levels of the organization and to set the stage for communication in the event of an incident.
- 06 ☐ Form a plan for communicating transparently with external parties that clearly states the degree to which they've been affected, if at all. Include a crisis communication plan to proactively detail how to work with the media.

07 ☐ Train with your IR team, practicing through various situations through table-top exercises and penetration tests to identify and address gaps.

08 ☐ Prevention is your best line of defense: Implement processes and technology to ward off as much as possible, including training your users to report suspicious or anomalous activities and testing their knowledge regularly.

09 ☐ Stay vigilant to detect incidents by using security information and event management (SIEM) technology to constantly log and monitor systems activity.

10 ☐ In the event you detect an attack, immediately activate the incident response plan by alerting the CSIRT and internal stakeholders to the confirmed incident and communicating with third parties and possibly customers.

11 ☐ Simultaneously with #10, apply containment strategies such as quarantining one or multiple devices, performing network segmentation or taking devices offline, and/or reimaging devices when appropriate.

12 ☐ Eradicate all traces of the security incident including removing the attack from the network, deleting malware and disabling breached user account.

13 ☐ Identify, document and mitigate all vulnerabilities that were exploited. Use this to assist in responding to future attacks and developing a plan of action to stop events from happening again.

14 ☐ Restore normal operations, being careful to minimize disruption by clearly defining the order of recovery for systems and processes. Apply lessons learned now to get your systems and business operations running again in a way that reduces the threat of another breach.

15 ☐ **Identify, document and mitigate all vulnerabilities that were exploited. Use this to assist in responding to future attacks and developing a plan of action to stop events from happening again.**

Getting the Help You Need

Many businesses lack the resources to dedicate to developing, testing and organizing an effective incident response plan. Partnering with an outside consulting firm that has experience with different types of breaches across many industries can provide peace of mind in knowing you have a plan to deal with unexpected security incidents.

Working with experienced professionals can take the burden of preparation off you, and make a complex undertaking simple.

About Avertium

Avertium, one of the largest cybersecurity services providers to the mid-to-enterprise market, is redefining the landscape with its distinctive show-no-weakness approach. Forged out of three award-winning cybersecurity services companies, each with a unique perspective on the security landscape, Avertium brings enterprise-level security to the many mid-sized and larger organizations that don't have access to comprehensive, specialized protection. More than 1,200 organizations in industries ranging from financial services and manufacturing, to technology and healthcare benefit from Avertium's managed security, consulting and compliance services delivered with more rigor, more relevance, and more responsiveness. The company's dual security operations centers are located in Arizona and Tennessee.

Avertium. Show No Weakness.™

AVERTIUM

+1 (877)-707-7997
hello@avertium.com
www.avertium.com