SOPHOS
Cybersecurity delivered.

Incident Response Guide

The 10 steps to creating an effective cyber incident response plan

"Before anything else, preparation is the key to success."
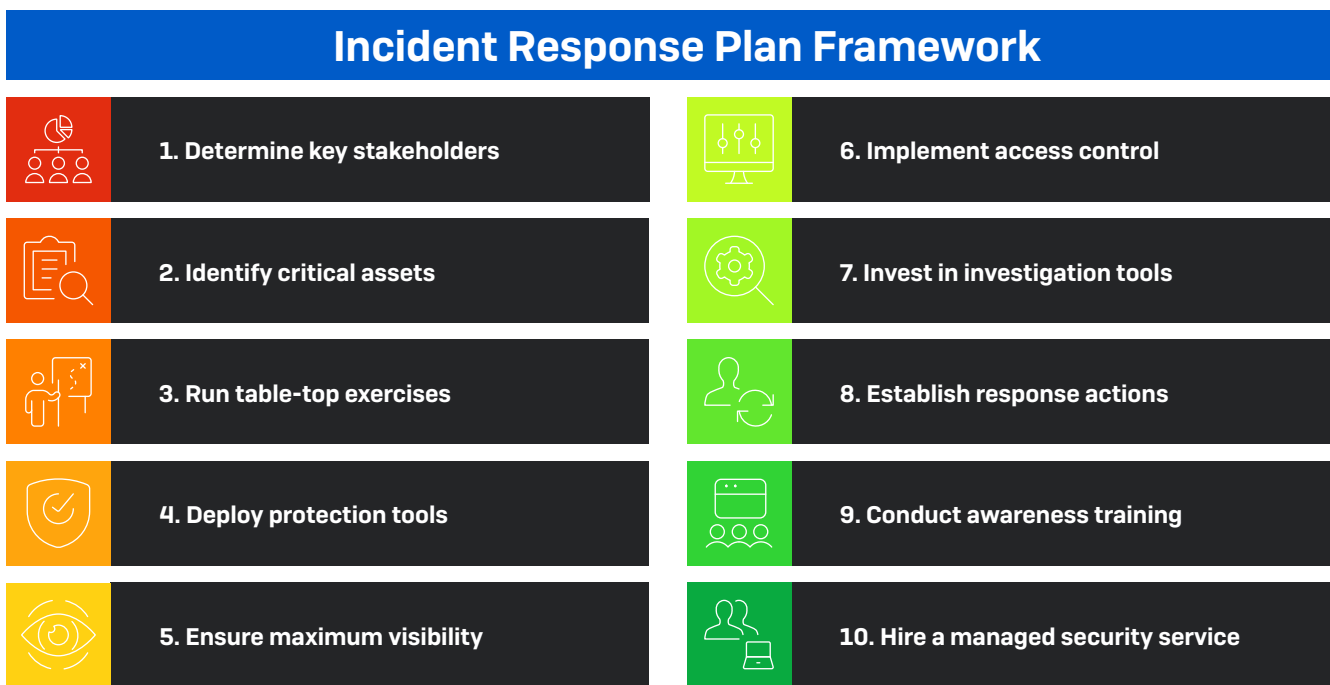
Alexander Graham Bell

What is the best way to avoid having a cyberattack turn into a full breach? Prepare in advance.

After experiencing a breach, organizations often realize they could have avoided a lot of cost, pain, and disruption if only they'd had an effective incident response plan in place.

This guide is intended to help you define the framework for cybersecurity incident response planning that gives you the best chance at thwarting an adversary. These recommendations are based on the real-world experiences of the Sophos Managed Detection and Response and Sophos Rapid Response teams, who have tens of thousands of hours of experience when it comes to dealing with cyberattacks.

Cybersecurity incident response plan

There are 10 main steps to an effective incident response plan.

Incident Response Plan Framework

1. Determine key stakeholders	6. Implement access control
2. Identify critical assets	7. Invest in investigation tools
3. Run table-top exercises	8. Establish response actions
4. Deploy protection tools	9. Conduct awareness training
5. Ensure maximum visibility	10. Hire a managed security service

1. Determine key stakeholders

Properly planning for a potential incident is not the sole responsibility of your security team. In fact, an incident will likely impact almost every department in your organization, especially if the incident turns into a full-scale breach. To properly coordinate a response, you must first determine who should be involved. This often includes representation from senior management, security, IT, legal, and public relations.

Knowing who should be at the table and involved in your organization's planning exercises is something that should be determined in advance. Additionally, a method of communication needs to be established to ensure a quick response. This should take into account the possibility that your normal channels of communication (i.e. corporate email) may be impacted by an incident.

2. Identify critical assets

To determine the scope and impact of an attack, your organization first needs to identify its highest priority assets. Mapping out your highest priority assets will not only help you determine your protection strategy but will make it much easier to determine the scope and impact of an attack. Additionally, by identifying these in advance, your incident response team will be able to focus on the most critical assets during an attack, minimizing disruption to the business.

3. Run tabletop exercises

Incident response is like many other disciplines – practice makes perfect. While it is difficult to fully replicate the intense pressure your team will experience during a potential breach, practice exercises ensure a more tightly coordinated and effective response when a real situation occurs. It is important to not only run technical tabletop exercises (often as part of a red team drill), but also broader exercises that include the various business stakeholders previously identified.

Tabletop exercises should test your organizational responses to a variety of potential incident response scenarios. Each of these scenarios might also include stakeholders beyond the immediate technical team. Your organization should determine in advance who needs to be informed when an attack is detected, even if was successfully defended.

Common incident response scenarios include:

‣ **Active adversary detected within your network**: In these scenarios, it is critical that the response team determines how an attacker was able to infiltrate your environment, what tools and techniques they used, what was targeted, and if they have established persistence. This information will help determine the proper course of action to neutralize the attack.

 While it might seem obvious that you would immediately eject the adversary from the environment, some security teams choose to wait and observe the attacker to gain important intelligence in order to determine what they are trying to achieve and what methods they are using to achieve them.

‣ **Successful data breach**: If a successful data breach is detected, your team should be able to determine what was exfiltrated and how. This will then inform the proper response, including the potential need to consider the impact on compliance and regulatory policies, if customers need to be contacted, and potential legal or law enforcement involvement.

‣ **Successful ransomware attack**: If critical data and systems are encrypted, your team should follow a plan to recover such losses as quickly as possible. This should include a process to restore systems from backups. To ensure the attack won't be repeated as soon as you're back online, the team should investigate if the adversary's access has been cut off. Additionally, your broader organization should determine if it would be willing to pay a ransom in extreme situations and, if so, how much it would be willing to spend.

‣ **High-priority system compromised**: When a high-priority system is compromised, your organization may not be able to conduct business normally. In addition to all the steps needed as part of an incident response plan, your organization also needs to consider establishing a business recovery plan to ensure minimal disruption in a scenario such as this.

4. Deploy protection tools

The best way to deal with an incident is to protect against it in the first place. Ensure your organization has the appropriate endpoint, network, server, cloud, mobile, and email protection available.

5. Ensure you have maximum visibility

Without the proper visibility into what is happening during an attack, your organization will struggle to respond appropriately. Before an attack occurs, IT and security teams should ensure they have the ability to understand the scope and impact of an attack, including determining adversary entry points and points of persistence. Proper visibility includes collecting log data, with a focus on endpoint and network data. Since many attacks take days or weeks to discover, it is important that you have historical data going back for days or weeks (even months) to investigate. Additionally, ensure such data is backed up so it can be accessed during an active incident.

6. Implement access control

Attackers can leverage weak access control to infiltrate your organization's defenses and escalate privileges. Regularly ensure that you have the proper controls in place to establish access control. This includes, but is not limited to, deploying multi-factor authentication, limiting admin privileges to as few accounts as possible (following the Principle of Least Privilege), changing default passwords, and reducing the amount of access points you need to monitor.

7. Invest in investigation tools

In addition to ensuring you have the necessary visibility, your organization should invest in tools that provide necessary context during an investigation.

Some of the most common tools used for incident response include endpoint detection and response (EDR) or extended detection and response (XDR), which allow you to hunt across your environment to detect indicators of compromise (IOCs) and indicators of attack (IOA). EDR tools help analysts pinpoint which assets have been compromised, which in turn helps determine the impact and scope of an attack. The more data that is collected – from the endpoints and beyond – the more context is available during investigation. Having broader visibility will allow your team to not only determine what the attackers targeted but how they gained entry into the environment and if they still have the ability to access it again.

In addition to EDR tools, advanced security teams might also deploy a security orchestration, automation, and response (SOAR) solution that aids in response workflows.

8. Establish response actions

Detecting an attack is only part of the process. In order to properly respond to an attack, your IT and security teams need to ensure they have the ability to conduct a wide range of remedial actions to disrupt and neutralize an attacker. Response actions include, but are not limited to:

- ‣ Isolating affected hosts
- ‣ Blocking malicious files, processes, and programs
- ‣ Blocking command and control (C2) and malicious website activity
- ‣ Freezing compromised accounts and cutting off access to attackers
- ‣ Cleaning up adversary artifacts and tools
- ‣ Closing entry points and areas of persistence leveraged by attackers (internal and third-party)
- ‣ Adjusting configurations (threat policies, enabling endpoint security and EDR on unprotected devices, adjusting exclusions, etc.)
- ‣ Restoring impacted assets via offline backups

9. Conduct awareness training

While no training program will ever be 100% effective against a determined adversary, education programs (i.e. phishing awareness) help reduce your risk level and limit the number of alerts your team needs to respond to. Using tools to simulate phishing attacks provides a safe way for your staff to experience (and potentially fall victim to) a phish, enrolling those that fail into training, as well as identifying risky user groups who may require additional training.

10. Hire a managed security service

Many organizations are not equipped to handle incidents on their own. Swift and effective response requires experienced security operators. To ensure you can properly respond, consider working with an outside resource such as a managed detection and response (MDR) provider.

MDR providers offer 24/7 threat hunting, investigation, and incident response delivered as a managed service. MDR services not only help your organization respond to incidents before they become breaches but also work to reduce the likelihood of an incident in the first place. MDR services are becoming very popular: according to Gartner*, by 2025, 50% of organizations will be using MDR services (this is up from less than 5% in 2019).

Data forensic incident response (DFIR) services are occasionally also retained after an incident to collect evidence to support a legal or insurance claim.

Summary

When a cybersecurity incident strikes, time is of the essence. Having a well-prepared, well-understood response plan that all key parties can immediately put into action will dramatically reduce the impact of an attack on your organization.

How Sophos can help

Sophos Managed Detection and Response (MDR) service

Sophos Managed Detection and Response (MDR) provides 24/7 threat hunting, detection, and response capabilities delivered by an expert team as a fully-managed service. Going beyond simply notifying you of attacks or suspicious behaviors, the Sophos MDR team takes targeted actions on your behalf to neutralize even the most sophisticated and complex threats.

The Sophos MDR team of threat hunters and response experts:

‣ Proactively hunts for and validates potential threats and incidents

‣ Uses all available information to determine the scope and severity of threats

‣ Applies the appropriate business context for valid threats

‣ Initiates actions to remotely disrupt, contain, and neutralize threats

‣ Provides actionable advice for addressing the root causes of recurring incidents

Learn more at www.sophos.com/mdr

Sophos Rapid Response service

Delivered by an expert team of incident responders, Sophos Rapid Response provides lightning-fast assistance with identification and neutralization of active threats against organizations. Onboarding starts within hours, and most customers are triaged within 48 hours. The service is available for both existing Sophos customers as well as non-Sophos customers.

The Sophos Rapid Response team of remote incident responders, threat analysts, and threat hunters:

‣ Quickly takes action to triage, contain, and neutralize active threats

‣ Ejects adversaries from your estate to prevent further damage to your assets

‣ Performs ongoing 24/7 monitoring and response to enhance your protection

‣ Recommends real-time preventative actions to address the root cause of an attack

‣ Provides a detailed post-incident threat summary that describes the investigation

Learn more at www.sophos.com/rapidresponse

Sophos XDR

Sophos XDR is the industry's only XDR solution that synchronizes native endpoint, server, firewall, email, cloud and M365 security. Get a holistic view of your organization's environment with the richest data set and deep analysis for threat detection, investigation and response for both dedicated SOC teams and IT admins.

Learn more and try it for free at www.sophos.com/xdr

* Gartner, Market Guide for Managed Detection and Response Services, 26 August 2020, Analysts: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneiderd

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS