Kaseya®

EBOOK

HOW TO BUILD AN INCIDENT RESPONSE PLAN

A security breach is among an organization's biggest nightmares, often putting its reputation, revenue and customer trust at stake. In the last few years, the ever-growing frequency and scale of cyberattacks paint an alarming picture, with numerous organizations falling prey to threats like ransomware, business email compromise, spear phishing and other dangerous cyberattacks. These attacks often lead to severe consequences for organizations and the situation is only worsening. According to IBM, the average cost of a data breach increased by 2.6% from $4.24 million in 2021 to $4.35 million in 2022.

With a significant rise in cyberattacks and cybercriminals constantly on the prowl, organizations must not discount the possibility of falling prey to a cyber incident. It is paramount for every company to have a formal, tested incident response plan in place to minimize damage and get back to work quickly should an attack occur.

WHY DO ORGANIZATIONS NEED AN INCIDENT RESPONSE PLAN?

According to a recent IDC ransomware survey, one-third of companies worldwide have experienced a ransomware attack or breach that blocked access to their systems or data. Without a proper incident response plan, organizations are left in the lurch during a breach, which gives threat actors free reign to effect maximum damage on the victim organization. However, with a formal, tested incident response plan, organizations can define a breach, the roles and responsibilities of the response team, tools for managing a breach, steps to address a cyber incident, how the incident will be investigated and communicated and all the other requirements following a data breach.

Along with rapid restoration of normal operations and the reduction of financial damages, here are some other benefits of an incident response plan.

MINIMIZE REPUTATION DAMAGE

If a security breach is not handled carefully, it can be a PR nightmare. Organizations risk losing customer trust, which might diminish their customer base. According to the United States Securities and Exchange Commission (SEC) almost **60% of SMBs go out of business** within six months of a data breach or cyberattack. Even publicly traded organizations risk losing investor and shareholder confidence following a publicized data breach. For example, the share prices of companies like Equifax, Target, Yahoo! and Sony dipped significantly following a cyberattack on their systems.

FIND SECURITY GAPS BEFORE THEY ARE EXPLOITED

An incident response plan can prevent an organization from falling victim to a cyberattack. It helps them identify and close security gaps and increases cybersecurity awareness among employees, reducing cyberattacks due to human error. **IBM researchers announced** that only 39% of organizations with a formal, tested incident response plan experienced an incident as compared to 62% of those that didn't have a plan.

IMPROVE COMPLIANCE

Having an incident response plan is a universal best practice and is mandatory under many data privacy regulations, including the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA).

WHAT SECURITY SOLUTIONS HELP WITH INCIDENT RESPONSE?

While cyberattacks always come unannounced, some solutions play a crucial role in enabling organizations to quickly identify and address security threats. Here are a few solutions that strengthen an organization's security and also offer incident response benefits.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Effective access control is critical for preventing intrusions, giving security teams the required tools to effectively deal with an incident. Many solutions feature single sign-on (SSO), with access to networks and tools controlled for each user from individualized launchpads. Not only does this make it easy for techs to control access points, it also makes it easy to close them off and isolate a compromised user account.

ENDPOINT DETECTION AND RESPONSE (EDR)

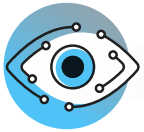
EDR solutions record and store activities and events taking place on endpoints and use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity and provide remediation suggestions to restore affected systems. An EDR tool augments an organization's incident detection, investigation and response capabilities, including incident data search and investigation alert triage, suspicious activity validation, threat hunting and malicious activity detection and containment.

SECURITY OPERATIONS CENTER (SOC)

A SOC is one of the most significant assets in incident response planning. A SOC gives responders the data they need to quickly mount an effective response, helping reduce the attackers' dwell time and damage. It also enables organizations to establish the metrics to measure the success of any incident response. A SOC can be maintained in-house, or an organization may opt to use a managed SOC. Using a managed SOC has many advantages for preventing and addressing cyberattacks. First and foremost, a managed SOC will be staffed by cybersecurity professionals who can provide threat analysis and expert help in the event of a cyberattack. With a managed SOC, SMBs can also perform vulnerability assessments to identify potential threats and address vulnerabilities.

BACKUP AND RECOVERY

A backup and recovery strategy is critical for helping organizations minimize the impact of downtime. A backup and recovery solution helps an organization recover data and IT resources, enabling it to quickly get back to work following a cybersecurity incident.



DARK WEB MONITORING

Cybercriminals often sell an organization's stolen data on dark web forums, which allows other perpetrators to launch a cyberattack on the organization. A dark web monitoring solution scans through billions of pages on the internet to find leaked or stolen information, such as compromised passwords, credentials, intellectual property and other sensitive data. Once the solution finds compromised data, it alerts the impacted organization, enabling it to devise remediation strategies.

SECURITY AWARENESS TRAINING

Most cyberattacks are caused by a human error with cybercriminals increasingly using social engineering techniques to trap an organization's employees. A security awareness training solution empowers an organization's employees to detect phishing lures easily and protect their organization from costly cyberattacks. Organizations that engage their employees in regular security awareness training have **70% fewer security incidents**.

EMAIL SECURITY

Since email is the primary communication channel for almost all organizations, cybercriminals look for vulnerabilities in an organization's email environment that they can exploit. Email security solutions monitor an organization's email traffic continually and rapidly detect and report any unusual and malicious emails that enter its network. This allows organizations to eliminate threats before they can inflict any harm.

BUILDING YOUR INCIDENT RESPONSE TEAM

The key to effective incident management is having the right people in the right roles. To accomplish this task, you need a Computer Security Incident Response Team (CSIRT) that can respond to incidents promptly and effectively.

An effective CSIRT requires a variety of professionals with the appropriate skill sets. The team should be able to handle all aspects of an incident and provide a broad range of expertise.

A CSIRT should include the following roles:

- **Management:** The management members include the upper-level management, such as C-suite execs, working across the organization. The management role is responsible for establishing incident response policy, budget and staffing. They are also responsible for coordinating incident response among various stakeholders, minimizing damage and reporting to appropriate authorities.
- **Technical lead:** The CSIRT technical lead is responsible for coordinating IT and security activities and making strategic decisions. They are accountable for the company's operations, incident response budget and strategic direction. They also report to upper-level management and render advice on security issues, current threats and issues related to meeting compliance standards.
- **Lead Investigator:** The lead investigator works with an extended team of security analysts and forensic investigators to investigate the occurrences during a security incident.
- **Communications:** The communications team members are responsible for managing communications within the CSIRT and organization as a whole to defuse the situation after a breach. They also ensure that stakeholders, clients and appropriate authorities are duly informed about an incident.
- **Legal:** The legal expert advises the organization about compliance and disclosure requirements and the types and scope of any potential legal implications the incident may have for the organization.

CREATE A DECISION MATRIX

Once the roles and responsibilities of the incident response team have been established, it is important to ensure it can respond quickly to any breach. To facilitate a quick response, organizations must create a high-level decision matrix. Here are some of the roles that make up an effective decision matrix:

THE NIST INCIDENT RESPONSE LIFECYCLE

The U.S. National Institute of Standards and Technology (NIST) has outlined a series of steps for cybersecurity incident response that are generally considered to be the industry standard. NIST advises that "Preventive measures based on risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore indispensable to rapidly detect breaches, minimize damages, mitigate the loopholes that cybercriminals exploited and restore IT services."

The NIST incident response lifecycle includes four main stages: Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-Incident Activity.

Source: NIST

EXPLORING THE FOUR STAGES OF AN INCIDENT RESPONSE

The National Institute of Standards and Technology (NIST) has set clear standards and practices for incident response and cybersecurity to help organizations stay prepared for an adverse event. These standards are categorized in four of the below mentioned stages.

Preparation: The preparation stage is the fundamental phase where incident response teams set strategies to help the organization stay prepared for an incident. This phase includes establishing and training an incident response team and acquiring the necessary tools and resources to prevent an incident from causing severe damages.

The preparation stage also emphasizes establishing mechanisms to limit the number of future incidents by selecting and implementing a set of controls. There are three key precautionary measures for securing networks, systems and applications.

Risk assessments: A periodic risk assessment of systems and applications can help organizations identify existing threats and vulnerabilities before cybercriminals exploit them. It also helps organizations identify critical resources, enabling their workforce to emphasize monitoring and response activities for those resources.

Malware detection: Every organization should have software deployed throughout their organization to detect and mitigate malware. For effective detection and prevention, malware protection solutions should monitor operating systems, endpoints, email servers and web proxies at a minimum.

User awareness and training: Having an incident response plan serves no purpose without educating every user about the policies and procedures regarding appropriate use of networks, systems and applications. With effective user awareness training, organizations can drastically minimize the number of security incidents.

Detection and analysis: While the preparation stage helps organizations limit the number of cyberattacks, some attacks still sneak past even the most stringent cyber defenses. The detection and analysis phase helps organizations identify the source of the incident, gauge the severity of the incident and alert the required parties to curb its impact.

According to the NIST, detecting and assessing incidents is one of the most challenging parts of incident response for organizations. This is because incidents can happen in a plethora of ways, and each incident merits a different response strategy. However, profiling networks and systems, studying normal behaviors, creating a log retention policy and maintaining a knowledge base of information can help make incident analysis easier and more effective.

Rapid detection and analysis is key after an incident has occurred. The team should rapidly perform an initial analysis to get a detailed insight into the incident's scope, such as knowledge about the affected networks, systems or applications, information about the cause and origin of the incident, and details about the perpetrators, the tools they use and their attack methods. An accurate initial analysis goes a long way in helping organizations in the containment stage.

Containment, eradication and recovery: Containment is a significant step to limit the damage of a cyberattack. Organizations should create different containment strategies for each incident type, with criteria documented clearly to facilitate decision making. For example, a phishing attack requires a different approach than a network-based DDoS attack.

Once the incident has been contained, you can work on eliminating components of the incident, such as removing malware and disabling breached user accounts, and identifying and mitigating all exploited vulnerabilities. Identifying all affected systems within the organization and disabling them to prevent future damage is essential.

In recovery, the incident response team works toward restoring normal operations. The team confirms that all the systems are functioning normally and remediates any existing vulnerabilities to prevent similar incidents. The recovery stage includes actions, such as restoring systems from backups, rebuilding systems, replacing affected files with clean versions, installing software patches, changing compromised passwords and tightening network perimeter security with additional measures.

Post-incident activity: Learning and improving after each incident is vital for incident response teams. After handling the incident, the organization should draft a detailed report about the cause and cost of the incident and steps to take to prevent future incidents.

Organizations should have subjective and objective data regarding each incident to limit the chances of the incident happening again and to identify ways of improving future incident response activity. The incident response team should collaborate regularly to learn about and fix any gaps in their cyber defense. An effective post-incident activity report must:

- Document the exact reason and time of the incident.
- Evaluate how well the staff and management dealt with the incident.
- Identify if proper procedures were followed by the staff.
- Indicate what information, if provided sooner, would have resulted in a better incident response.
- Note corrective steps to be taken to prevent similar incidents in the future.
- Cite what the staff and management should do differently if a similar incident occurs in the future.
- List additional tools or resources needed to detect, analyze and mitigate future incidents.

DETECT AND MITIGATE INCIDENTS WITH MANAGED SOC

With the growing number and sophistication of cyberattacks, organizations need round-the-clock security for timely and effective response to security threats or incidents. A security operations center (SOC) can help you detect and mitigate security gaps and breaches, providing tools and expertise that enables you to handle an incident response quickly. However, building a SOC is costly and complex and can be a daunting task.

You can boost your organization's cyber defense by choosing to partner with Kaseya's Managed SOC. With Managed SOC, your organization has access to the tools and help it needs to stop advanced cyberthreats from damaging your organization. Our world-class, white-labeled managed detection and response (MDR) solution is an innovative, affordable and effective way to power up your security.

An elite team of cybersecurity experts leverages our Threat Monitoring Platform to detect malicious and suspicious activity across three critical attack vectors – endpoint, network and cloud. **Plus, you'll have a team of security veterans available to you 24/7/365 to dive in immediately and work with your team when actionable threats are discovered.**

Benefits of Kaseya's Managed SOC

Continuous monitoring: Get round-the-clock protection with real-time advanced threat detection.

Breach detection: Thwart sophisticated and advanced threats that bypass traditional AV and perimeter security solutions.

Threat hunting: Focus on other pressing matters while an elite cybersecurity team proactively hunts for malicious activities.

SIEM-less log monitoring: Monitor, search, alert and report on the three attack pillars' (network, cloud and endpoint) log data spanning Windows and macOS, firewalls, network devices, Microsoft 365 and Azure AD without requiring heavy security event and incident management investment.

No hardware requirements: Eliminate the need for costly and complex on-premises hardware with our patent-pending, cloud-based technology.

Learn more about Managed SOC

About Kaseya

Kaseya is the leading provider of complete IT management solutions for managed service providers (MSPs) and midsized enterprises. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage and secure IT. Offered both on-premise and in the cloud, Kaseya solutions empower businesses to command all of IT centrally, easily manage remote and distributed environments, and automate across IT management functions. Kaseya solutions manage over 10 million endpoints worldwide.Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.