PONDURANCE

Incident Response Planning

pondurance.com

Introduction

Ransomware attacks are at an all-time high. These attacks more than doubled from last year, with ransomware being one of the top three attacks leveraged by bad actors.[1] Moreover, ransomware groups are finding new techniques to extort more funds than ever from healthcare, government, manufacturing, education, and private sectors worldwide. It is safe to say that one of the primary lessons learned from high-profile cyberattacks in 2020 is that incident response (IR) planning and preparation can help organizations identify, prevent, and respond to business disruptions and avoid millions in losses.

After reading this guide, you will have a clear understanding of the importance of an IR plan. This guide covers why you need a comprehensive IR plan and provides a strategic outline for defending against cyberattacks, responding in the event of an incident, and mitigating threats.

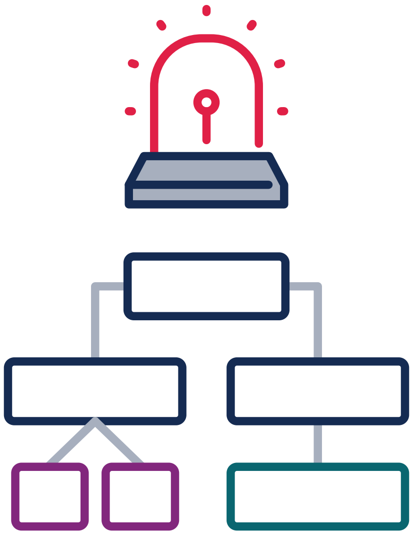
What Is an Incident Response Plan, and Why Is It Important?

An IR plan is a set of instructions designed to help prepare your organization for adverse events, including cyberattacks. Cyberattacks can have damaging effects on an organization in multiple ways and across various facets of the business.

IS YOUR ORGANIZATION PREPARED TO RESPOND TO A CYBERATTACK?

Whether you are creating an IR plan through a third party or on your own, the goals remain the same. A standard list to consider from the NIST 800-61 provides a baseline on how to handle various incidents[2]:

- Create an IR policy and plan.
- Develop policies and procedures for performing incident handling as well as reporting.
- Set guidelines for communicating with external parties and key stakeholders regarding incidents.
- Staff and train the IR team.
- Determine what services the IR team should provide.



Additionally, organizations that experience a cyberattack must be prepared to comply with the legal obligations, especially to individuals affected by the incident, state attorney generals, and other regulatory bodies, depending on the type of data your organization manages. In the event of an attack, the aftermath can be hectic. Organizations are pressed to answer critical questions such as:

- What information or data was accessed?
- When was the information accessed?
- Who gained access?
- Can you quickly mitigate this threat?
- How do we prevent these attacks in the future?

Creating an Incident Response Plan

There are three key components to keep top of mind when outlining your IR plan:

PROPER INVENTORY

Organizations that handle sensitive information such as personal identifiable information, financial data, and corporate information tend to be prime targets for cyberattacks. Therefore, when it comes to securing digital assets (computers, servers, cloud storage, user credentials, etc.), it is critical to understand what technology is being managed to ensure there is a proper inventory of what could be deemed as a vulnerable entry point as well as keeping an inventory of where sensitive data resides. Taking the proper inventory of your digital assets could help you prioritize security efforts to defend against attackers and know what data could be exposed.

ONGOING REVIEW

Ideally, your IR plan should be reviewed and audited continually. In addition, key stakeholders should be involved in the planning and execution process of the IR plan to ensure they are prepared for a cybersecurity incident.

TRAINING

Training different areas of the organization, such as human resources, legal, finance, employee communications, public relations, suppliers, partners, and customer service, and preparing them for different attack scenarios can make a tremendous difference.

Your IR plan should be reviewed and audited
CONTINUALLY.

Ransomware attacks can cost an organization upward of
$4.4 million
per incident.[3]

PONDURANCE

Essential Steps to Include in Your IR Plan

In developing an IR plan, key steps should revolve around the life cycle of an attack. An IR Plan highlights important details that identified stakeholders are aware of pre-breach, during an attack, and post-incident. Reviewing your IR plan and frequently updating it is key to improving IT and cybersecurity hygiene to better protect your organization from evolving cyber threats.

PREPARATION

Preparation is the first phase of IR planning, and it is the most crucial. The initial phase involves establishing and training an IR team and acquiring the necessary tools and resources. Understand and identify what type of information your organization manages. This will give you a baseline and set priorities of where security efforts must be focused, including any data management regulations that could be violated (HIPAA, GDPR, CPRA, etc.).

- Assess your security team and determine if your internal security operations center (SOC) has enough analysts to monitor, detect, and respond to threats on a 24/7 basis. This can gauge whether you have enough staff on hand or need to implement a managed detection and response (MDR) service to help fill the gaps, mitigate blind spots in your security posture, and provide log activity of your digital landscape.
- Develop a list of essential logs, inventory all digital assets, and establish who in IT and the SOC will receive clear and actionable alerts to execute a review of these items.
- Identify your key stakeholders, such as employees from human resources, IT, SOC, legal, customer success, and marketing. Upon assembling your IR team, assign roles and responsibilities for all relevant stakeholders.
- Document who will lead the team if a breach occurs and who they should contact.
- Establish the location of all company backups, including privileged credentials, passwords, and sensitive keys. These should be stored in an off-site centralized vault.
- Make a list of contacts such as vendors, partners, cyber insurance providers, and law enforcement that should be notified in the event of an incident.
- Perform a vulnerability assessment to identify weaknesses that need to be patched in your digital landscape.

STEP 2

IDENTIFICATION

The identification phase of your IR plan involves detecting and analyzing threats as soon as possible. When every minute counts, it is essential to have a strong security team and security tools to monitor and detect malicious activity throughout your network, endpoints, logs, and cloud on a 24/7 basis.

The identification phase is critical in your IR plan. Bad actors such as ransomware groups can go from entry to total encryption with your system within an hour. Some common entry methods are 1) email attachments or links 2) legitimate credentials that were stolen 3) exposed remote desktop protocol (RDP) services or unpatched remote access devices.

If an alert is triggered, your SOC team should review the security event for false positives and quickly triage the incident to determine the severity, type, and potential danger.

- Leveraging security tools such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), File Integrity Monitoring (FIM), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Antivirus (AV), and other log sources will be valuable in assisting your internal security team or IR team in detecting threats.
- Gather logs, memory dumps, audits, network traffic reports, and disk images to perform a post-incident investigation.
- Consider leveraging an MDR provider if you lack the staff or the security expertise to maintain and implement 24/7 monitoring.
- Ensure you are keeping security and activity logs for legal purposes.
- Develop step-by-step instructions for handling various incidents and attack types.

In 2020, the average time to identify a breach was

207 days

and

73 days

to contain one.[2]

CONTAINMENT AND ERADICATION

The containment phase of your IR plan includes stopping the incident, preserving evidence, collecting critical information, and reducing the impact on business operations. Responding to security incidents can take many forms, such as triaging alerts and containing the threat by isolating or shutting down the infected systems to prevent further spread to your network.

In addition, leveraging your SOC to hunt for these threats actively is critical to detecting the location of malicious files, backdoors, and other types of vulnerabilities that can lead to a security incident.

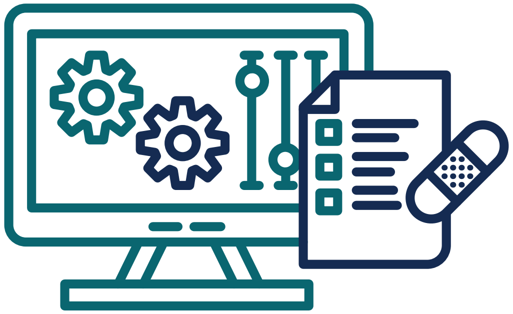
- Immediately contain systems, networks, servers, databases, and devices to minimize any potential widespread damage.
- Determine if any sensitive information was breached or data loss occurred.
- Upgrade any legacy firewalls and network security as they capture very simple netflow logs. A next-generation firewall (NGFW) can provide much more in-depth information, such as deep packet inspection and an intrusion prevention system.
- Preserve all evidence that can further analyze the origin, impact, and intention behind the attack.
- Keep a log of the incident and response, such as the date, time, location, and extent of the damage. This is critical to identifying whether the attack was deployed externally, internally, or possibly from a misconfiguration or human error. Also, it is vital to document those on your team who discovered and reported the incident.
- Patch and mitigate the entry point to ensure the attacker cannot regain access.

STEP 4

RESPONSE

The response phase of your IR plan involves your entire list of key stakeholders. This phase involves all hands on deck because this is where the crux of your IR plan comes into play when communicating the incident externally and with other internal departments.

- Work with your communications team to draft external communications (public statements) on how you mitigate the incident. This time is especially critical because disclosing an attack too late can negatively affect the reputation of the business and impact customer trust.
- Engage with your legal team and examine any compliance or regulatory risks to determine potential violations.
- Contact law enforcement and any other required government agencies.
- Communicate with your internal team and coach them on discussing the matter with customers who may have questions.
- Perform a root cause analysis to determine the attacker's steps to gain access to your systems to improve security controls.
- Perform companywide vulnerability analysis to ensure all vulnerabilities have been addressed.



RECOVERY

The recovery phase of your IR plan involves returning operations to normal and conducting a post-breach investigation. Reviewing and reporting on what happened, the root cause, and what could have been improved in the IR plan can reduce the time and likelihood of another incident.

- Restore systems to the pre-incident state.
- Implement security awareness training among your staff and provide insight into how human error and password management are essential.
- Discuss how well your IR plan performed.
- Update your IR plan based on what improvements should be made.
- Keep all stakeholders informed about any of the latest updates to the IR plan.

Conclusion

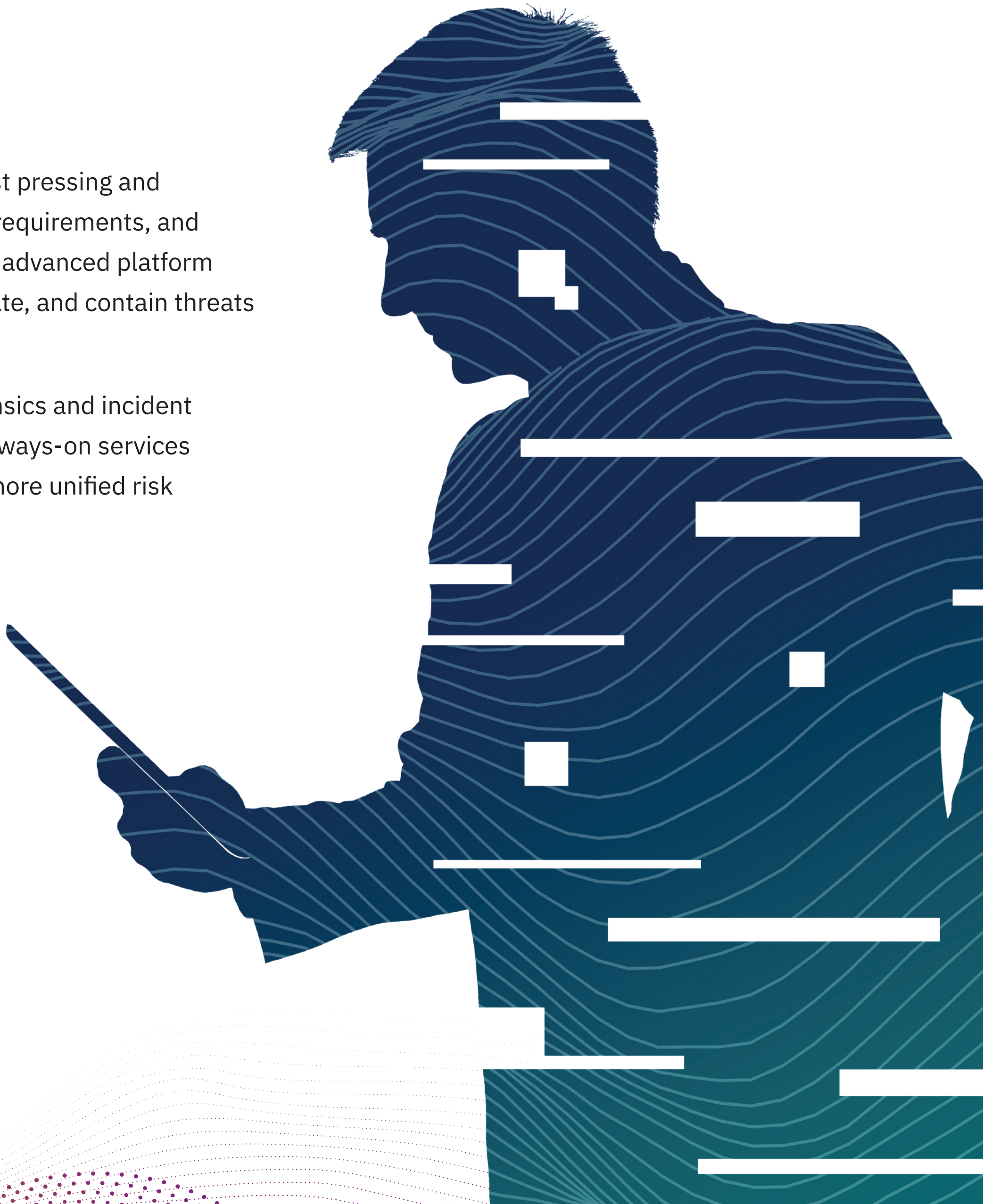
As cyberattacks continue to evolve, there is always going to be a need for an IR plan. Understanding why an IR plan is essential and knowing what steps you need to take are critical to improving your cybersecurity posture. Whether you create your IR plan or use a third party, it is never a one-and-done process. Instead, it takes repetition and fine-tuning among your key stakeholders, including live scenarios, to ensure your IR plan can keep pace with today’s and tomorrow’s cyber threats.

The shortage of cybersecurity talent and the cost to retain talent in today’s cybersecurity landscape can make it challenging to create and execute your IR plan relying only on internal stakeholders. Security technology is expensive and difficult to manage, which is why many organizations are turning to MDR providers as a critical piece to an IR plan due to the ability to expand visibility across the enterprise and have a team always ready to help remediate and stop threats before they become much more significant issues.

For organizations that need more guidance on planning for cybersecurity incidents, Pondurance delivers IR services and guides organizations every step of the way. With Pondurance as your cybersecurity IR partner, you are better prepared to mitigate threats successfully. Our team of experts is armed with leading technologies to respond to and eliminate even the most sophisticated cyberattacks that threaten technical operations within your healthcare organization.

PONDURANCE

About Pondurance



Pondurance delivers world-class MDR services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

Visit **www.pondurance.com** for more information.

Sources:

1. Data Breach Investigations Report, Verizon, May 13, 2021.
2. Computer Security Incident Handling Guide, NIST, August, 2012.
3. Cost of a Data Breach Report 2021, IBM, July 28, 2021.