DataCrest

Start Somewhere Series:

Incident Response Planning

CONTENT

What is Start Somewhere?

The Start Somewhere Series is an informational guide that breaks down complex topics into digestible building blocks and takeaways ensuring that you, as the reader, can take small steps to execute changes within your organization for timely results. Our point of view is simple - begin somewhere, evolve the topic, and iterate over time. Our key focus is for organizations that do not have an incident management and response plan in place and who do not know where to begin. Our goal is to provide information that will enable you to take preparatory steps and build your security program.

About the Author

Ben Thomas is the Chief Technology and Information Security Officer for DataCrest, an insurtech. Ben has over 25+ years of professional experience in the management and delivery of business and technology solutions that spans strategy and management consulting, technology strategy, application development, managed cloud services, enterprise systems, customer relationship management, and strategic global outsourcing.

Introduction

Incident response (IR) planning is something every organization needs to prioritize, but is often overlooked and outdated in the event that an incident occurs. IR planning should be a pragmatic and proactive approach to preparing your organization for security threats. **It is not a question of "if" a security incident or data breach happens, but "when", and how to respond.** Even with the best security teams and practices in place, a security incident will happen, and it will test the strength of the organization from leadership to your employees. The initial step to successfully respond to the incident is how an organization prepares for the inevitable. An incident can be minor, like accidentally sending personal identifiable information to a co-worker, or major, like the global impact of the log4J vulnerability that rocked the software industry in January 2022.

With the exponential rise of Cybersecurity attacks and new threat actors, Cybersecurity programs can be potentially impacted by the weakest link. IR planning is designed to identify, contain, and control security events to minimize both the impact and downtime while simultaneously protecting your brand, reputation, data, and revenue. The more prepared you are, the better you are able to respond to a Cybersecurity incident. This document outlines the key aspects of incident management and response so, let's start somewhere.

What is an Incident Response Plan?

The incident response (IR) plan, often referred to as an incident management and response plan, is a living document that should be comprehensive, communicated, continually reexamined for adjustments dependent on the organization's needs. As depicted in Figure 1, the second and third phases of the incident response lifecycle work cyclically to detect, analyze, eradicate, and recover prior to post-incident activities. The plan of action in each of these phases will be repeated until the incident is completely eradicated and recovered from. In order to be effective, the IR plan needs to be exercised and updated periodically throughout the year. Training all employees on the most important aspects of the IR plan and conducting regular tabletop exercises with IT, security, and leadership on different security incident scenarios is extremely beneficial for organizations because security extends down to the individual level. There are six steps of incident management and response as described in the National Institute of Standards and Technology.

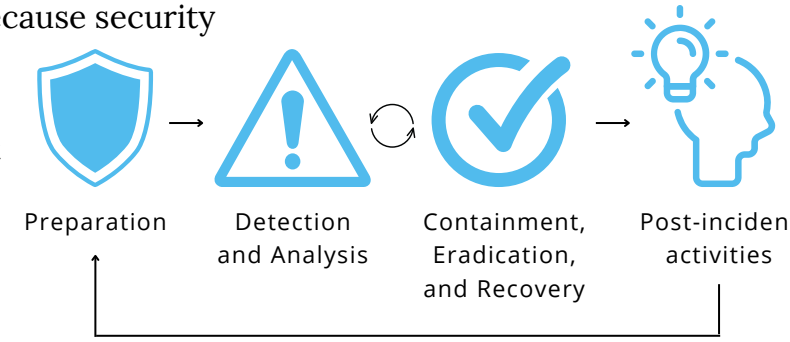

Figure 1. Incident Response Lifecycle

Preparation

This is, by far, the most important step in the process to be adhered by the organization. The faster your organization can detect and respond to security incidents, the less likely they will have a significant impact on your critical technology assets, data, brand, and revenue loss will occur. Downloading a free incident response plan template can help jumpstart and provide guidance on the preparation process. **The IR plan should be easy to read and understand for both technical and non-technical audiences, be broken down into digestible steps with clear communication channels, and outline critical actions throughout the process.**

Steps to Take

- Create an initial IR plan using a template that can be customized as the plan matures over time, growth, and annual reassessment.
- Establish an Incident Response Team (IRT) and identify clear roles and responsibilities within your organization. Key stakeholders include leadership, IT, HR, legal, public relations, etc.
  - If you don't have security expertise or skills within your IRT, prepare to work with a security vendor to assist with security incidents.
  - Line up vendors to supplement your team (e.g., a cyber forensics team has the skills and tools necessary to investigate a cyber attack and trace it back to its origin).
- Establish a clear communication channel for employees to report an incident.
- Identify your critical technology assets and data through a risk assessment test (based on impact matrix) conducted internally by your team or by a third-party security or compliance vendor.
- Conduct a baseline audit against your Information Security Policies. Test your security controls quarterly to document evidence against your controls (e.g., rotating passwords every 90 days, conducting a vulnerability scan, and remediating once a quarter).
- Implement proactive tools to create a proactive detection strategy (e.g., IDPS, File Monitoring, SEIM).
- Coordinate tabletop security incident scenario exercises throughout the year.
  - Common scenarios and attack vectors include web, attrition (DDOS brute force), email compromise, impersonation (rogue wi-fi, spoofing), improper usage, and loss or theft of equipment.
- Conduct IR training for all employees that includes information on who to contact and escalate to, what to record and document, and location of critical documents (e.g., emergency phone numbers, IR process workflow, chain of command).

Detection and Analysis

DataCrest

This phase, according to NIST, can be the most challenging for organizations: detection of the first signs of an attack, reported either by a monitoring system or an individual employee. The IR team will investigate the signs of a potential security incident, determine whether an incident has occurred, and identify the type, extent, and magnitude of the problem. They should take time to perform a thorough analysis resulting in informed response and remediation strategies.

Many organizations fail to spend enough time on detection and analysis, immediately moving into containment and eradication. Not spending enough time in this phase can result in a misdiagnosis of the threat or inaccurate assessment of the magnitude of impacted systems. **Taking the time needed to analyze the incident, rule out false positives, and determine the source is recommended before time and money is spent on containment and eradication.** There are many different types of incidents and ways to analyze them. Some possible methods of detection and analysis include, but are not limited to:

- The IR Team should adhere to the IR process and capture data (e.g., who, what, when, and where via documented interviews, screen capture, attach logs etc.).
- Systematically maintain all evidence and artifacts to be collected as part of your incident report.
- Analyze events including network, application and system logs, IDPS, SIEMS, AV, anti-spam software, file integrity monitoring, and notifications from a security operating center (SOC).
- Prioritize the incident based on functional impact, sensitivity of information, magnitude of loss, and estimated time.
- Determine if sensitive data has been compromised and assess the potential risk to your business and/or clients.
- Consider bringing in required talent to help with analysis (e.g., forensics team or security operations team).
- Research known vulnerabilities through the NVD or CVE databases.
- Use incident notification to notify appropriate individuals to fulfill their roles in the IR process.
- Review contracts and compliance regulations on security incident notifications with customers and vendors.
    - Many customers have a 24-72 hour security incident and data breach notification.

Containment, Eradication, and Recovery

DataCrest

Containment

The goal of containment is to prevent the widespread, damaging impact of a security incident. Various containment strategies include decision-making: an essential part of containment (e.g., shut down a system, disconnect from a network, disable certain functions). These decisions are easier to make when predetermined scenarios and procedures for containment are in place. The containment strategy selected will depend on the level of damage caused, the upkeep of the business's critical services, and the duration of the solution (temporary vs permanent). In the containment process, it is necessary to determine whether to direct the threat to a sandboxed environment or let the threat persist so you can observe the actions taken to identify the source.

Eradication

After an incident is identified and contained, eradication removes the threat. Take necessary eradication steps including patching vulnerabilities, removing files, or restoring systems from clean backups. Some examples of eradication include deleting unknown files and malware, disabling breached user accounts, and mitigating all vulnerabilities that were exploited.

Recovery

Recovery focuses on returning to normal operations. **Following thorough investigation and analysis of identified threats, employing containment activities to breached systems, applications, networks, data will isolate and prevent them from causing widespread damage.** Recovery may involve actions like restoring systems from clean backups, adding or replacing hardware or software, rebuilding systems from scratch, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, access control lists). Listed below are key actions taken during this phase.

- Employing containment activities, following thorough investigation and analysis of identified threats, to breached systems, applications, networks, and data to isolate and prevent them from causing widespread damage.
- Research known vulnerabilities through the NVD or CVE databases.
- Determine if sensitive data has been compromised and assess the potential risk to your business.
- Systematically maintain all evidence and artifacts to be collected as part of your incident report.
- Take necessary eradication steps including patching vulnerabilities, removing files, or restoring systems from clean backups.
- Ensure notifications to internal and external parties are reviewed with legal, HR and leadership teams.

Closure (Post-Incident Activities)

The post-incident activities phase focuses on lessons learned and uses retrospective analysis to determine what steps of IR process could be improved or refined. Post-incident activities involve team member review of people, process, and technologies involved in performing the IR process. Post-incident activities are often overlooked following recovery from an incident due to time and resource constraint. **This phase is crucial in maturing your incident management and response plan to effectively update methods of preparation.**

Critical Questions

- Did we engage the right people?
  - Were they engaged at the right time?
  - Is training or outsourcing needed (e.g., talent, skill sets, legal, HR, business)?
- Did we communicate effectively upstream and downstream?
  - Where was communication ineffective?
  - How and where can the communication channel be refined?
- How effectively did we work with our third-party providers and vice versa?
  - Was their service level agreement (SLA) met?
  - Were our third-party providers engaged at the right time?
- Did we complete the IR process?
  - What information was missed?
  - How long did the IR process take to complete?
  - What tabletop exercises can we run to improve areas of the IR process?
- In what ways was evidence collection successful?
  - What areas of evidence collection could be improved?
  - What specific details were missed?
- Do we now have the right tools, technologies, and processes in place to prevent this type of incident from happening again?

There are many frameworks for incident management and response to choose from and tailor to your organization's needs. They all outline a similar path and no framework is superior to another. Figure 2 (below) details a selection of available frameworks.

SANS	ISO/IEC	ISACA	NIST phase equivalent
Preparation	Plan and Prepare	Planning and Preparation	Preparation
Identification	Detection and Reporting	Detection, Triage, and Investigation	Detection and Analysis
Containment	Assessment and Decision	Containment, Analysis, Tracking, and Recovery	Containment, Eradication, and Recovery
Eradication Recovery	Responses		
Lessons Learned	Lessons Learned	Post-incident Assessment Incident Closure	Post-incident Activity

Figure 2. Various IR Processes

Final Thoughts

The incident response (IR) plan, referred to as an incident management and response plan, is a living document that should be comprehensive, communicated, continually reexamined for adjustments dependent on the organization's needs. IR planning is designed to identify security events, contain and control threats, and minimize impact and downtime while protecting your brand, reputation, data, and revenue. The more prepared you are, the better you are able to respond to a cybersecurity incident.

There are various IR frameworks available for free download, start somewhere by selecting one and tailoring it to your organization's needs. **For more information, reach out to DataCrest, we would be happy to walk you through the process in greater detail.**

Glossary

Chain of Command - an organizational structure that documents how each member of a company reports to one another (e.g., top of the chart would be the founder, owner, or CEO, people who report to them would appear directly below, etc.).

Communication Channel - the way information flows between stakeholders in a structured plan of communication (e.g., what groups or people need to be notified and who is working the incident).

Functional Impact - the measure of the effect of an incident on the day-to-day business functions of an organization.

Impact Matrix - a method of prioritizing incidents based on their magnitude (the extent of an incident and the potential damage it can cause) and urgency (how quickly a resolution is required).

Sandboxed Environment - an isolated virtual machine in which potentially unsafe software code can execute without affecting network resources or local applications.