Incident Response and Preparedness Guide

Cybersecurity incidents can occur in any organization, even with stringent preventive measures. The risk makes incident response essential to any organization's information technology (IT) program. Incident response reduces the harm that incidents cause. It also produces information that you can use to prevent or handle similar incidents in the future.

This guide provides incident response recommendations and best practices. This information comes from the National Institute of Standards and Technology (NIST), the SysAdmin, Audit, Network, and Security (SANS) Institute, and IBM cybersecurity experts. You can use the guide as a quick reference to help develop your organization's incident response plan or conduct incident response yourself.

This guide summarizes considerations for each step of incident response outlined by NIST:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity

Table of Contents

1. Preparation

Preparation involves creating an incident response policy and plan, ensuring all needed resources are available, and preventing incidents to increase the organization's stability and reduce the number of incidents.

1.1. Incident response policy

Your incident response team should have a policy determining how you will respond to an incident. The policy should cover the following content:

- **Incident response team**
- **Roles and responsibilities** of incident response team members
- **Means, tools, and resources** that the team will use to identify and recover compromised data
- **Policy testing**, including the persons responsible for performing testing
- **Action plan** for carrying out your incident response plan from start to finish

1.2. Means, tools, and resources

When describing the means, tools, and resources that your team will use to identify and recover compromised data, include the following types of information:

1.2.1. Incident handler communications and facilities

- **Contact information** for team members and other relevant parties in and outside the organization, such as system owner, human resources (HR), public affairs, legal department, and law enforcement
- **On-call information** for incidents that occur during off hours
- **Incident reporting mechanisms** such as phone numbers, email addresses, online forms, and secure instant messaging systems.
- **Issue tracking system** for tracking an incident's information and status

- **Smartphones** that team members carry with them at all times in case an incident occurs
- **Encryption software** that team members use to communicate with themselves, other employees, and outside parties
- **War room** in which all parties can meet and communicate
- **Secure storage facility** in which the team stores evidence and other relevant assets

1.2.2. Incident analysis hardware and software

- **Digital forensic workstations or backup devices** to help incident handlers collect and analyze data
- **Laptops** for all team members to perform activities related to incident response
- **Spare workstations, servers, and networking equipment**, or the virtual machine equivalents of those.
- **Blank removable media** such as CDs, external hard drives, or flash drives
- **Portable printer** for printing logs or other evidence
- **Packet sniffers and protocol analyzers** for monitoring and examining network traffic
- **Digital forensic software** for analyzing disk images
- **Removable media** that contain trusted versions of programs that the team uses to collect evidence
- **Evidence-gathering accessories** such as notebooks, cameras, audio recorders, forms, evidence bags, and evidence tape.

1.2.3. Incident analysis resources

- **Port lists**, including lists of commonly used ports and trojan ports
- **Documentation** for all relevant software, including OSs, applications, protocols, intrusion detection systems (IDSs), and antimalware software
- **Network diagrams and lists of critical assets**

- **Current baselines** of the network and organization for services, software, and other offerings so that the team can compare baseline activity with the activity during and after the incident
- **Cryptographic hashes** of important files for efficient analysis, verification, and eradication

1.3. Incident prevention

Preparation also involves preventing incidents to increase the organization's stability and reduce the number of incidents. Prevention isn't necessarily the incident response team's job, but the team has a personal stake in decreasing the number of incidents. The more overwhelmed the team, the lower its response rate and quality.

The following examples demonstrate some of the topics on which incident response teams can advise others in the organization to help prevent incidents:

- **Risk assessment**, including periodic risk assessments that help parties identify the risks that combinations of threats and vulnerabilities present
- **Host security**, ensuring that each device is sufficiently hardened, adheres to strict access control lists (ACLs), and undergoes continuous monitoring
- **Network security**, ensuring that the perimeter is set up to reject any activity not explicitly allowed
- **Malware prevention**, deploying antimalware software throughout the organization
- **User awareness and training**, ensuring that users know about cybersecurity policies and procedures and any updates to those

1.4. Preparation checklist

The SANS Institute recommends answering the following questions to help ensure that you are prepared for an incident:

- Are all members aware of the organization's security policies?
- Do all incident response team members know whom to contact if an incident occurs?

- Do all incident responders have access to journals and access to incident response toolkits to complete all parts of the response?
- Do all members regularly participate in drills to practice the incident response process and improve proficiency?

2. Detection and Analysis

Incident response begins when you detect an incident, and then analyze it to determine its severity and the next steps to take.

2.1. Precursors and indicators

Detecting an incident requires detecting its signs, which come in two types:

- A **precursor** is a sign that an incident may occur in the future, such as a web server log entry showing the use of a port scanner.
- An **indicator** is a sign that an incident might have occurred or is occurring now, such as an antimalware program alert indicating that a trojan has infected a device.

Incident response teams may prevent incidents if they detect precursors in time. Unfortunately, precursors are much less common than indicators.

Typically, precursors and indicators come from one of the following sources:

- **Alerts**, such as from intrusion detection or prevention systems (IDSs or IPSs), security information and event management (SIEM) software, and antimalware applications
- **Logs** from network flows, network device logs, or application, service, or operating system logs
- **Publicly available information**, such as from the news or the National Vulnerability Database (NVD)
- **People** within or outside your organization

2.2. Incident documentation

Once an incident response team member suspects an incident has occurred, start documenting it. A thorough ticket will not only help you handle the current incident but future incidents that occur.

2.2.1. Ticket information

Ensure that your issue-tracking system requires the following information:

- **Status** of the incident
- **Summary** of the incident
- **Indicators related to the incident**
- **Other incidents related to this incident**, if any
- **Actions that incident handlers have taken** regarding this incident
- **Chain of custody**, if applicable
- **Impact assessment related to the incident**
- **Contact information for other involved parties**, such as system owners or administrators
- **List of evidence collected during the investigation**
- **Comments from all the incident handlers**
- **Next steps to take**, such as updating the software or rebuilding the server

2.2.2. Chain of custody

The **chain of custody** is a process in which you document the evidence lifecycle. You record information including but not limited to the following details:

- Date, time, and duration that each person handled the evidence
- Actions that the person performed, such as copying and analyzing evidence and verifying the copy's integrity compared to the original
- Location in which you store the evidence when not in use

2.3. Impact assessment and prioritization

Instead of handling incidents in the order of detection, prioritize them by their functional, informational, and recoverability impacts using the following criteria from NIST.

2.3.1. Functional impact categories

Category	Definition

None	No effect on the organization's ability to provide services to all users.
Low	Minimal effect; the organization can still provide all critical services but has lost efficiency.
Medium	The organization has lost the ability to provide a critical service to a subset of users.
High	The organization can no longer provide some critical services to any users.

2.3.2. Information impact categories

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised.
Privacy breach	Sensitive personally identifiable information (PII) of parties such as taxpayers, employees, or beneficiaries was accessed and exfiltrated.
Proprietary breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated.
Integrity loss	Sensitive or propriety information was changed or deleted.

2.3.3. Recoverability impact categories

Category	Definition
Regular	The time to recover is predictable with existing resources.
Supplemented	The time to recover is predictable with additional resources.
Extended	The time to recover is unpredictable, and additional resources and outside help are needed.
Not recoverable	Recovery is not possible, such as when sensitive data is exfiltrated and posted publicly; an investigation is required.

2.4. Notifications

After documenting the incident and determining its impact, the incident response team must alert relevant parties such as the following people:

- **Chief information officer (CIO)**
- **Local and head of information security**
- **Other incident response teams within the organization,** if there are different sites or countries
- **External incident response teams**, if appropriate
- **System owner**
- **HR**, if appropriate
- **Public affairs** if the incident could reach the media
- **Legal department**, if appropriate
- **Law enforcement**, if appropriate

2.5. Detection and analysis checklist

The SANS Institute recommends answering the following questions during detection and analysis:

- Where did the incident occur?
- Who reported or discovered the incident?
- How was the incident discovered?
- What other areas, if any, has the incident compromised, and when were they discovered?
- What is the scope of the impact?
- What is the business impact?
- Have you located the source of the incident, and if so, where, when, and what is it?

3. Containment, Eradication, and Recovery

NIST groups containment, eradication, and recovery into a single step; the requirements of one of these sub-steps can impact the requirements of the others.

3.1. Containment

Containment is a phase in which you limit the damage.

3.1.1. Containment strategy

The most appropriate containment strategy depends on the incident type, and NIST provides the following criteria for choosing the best strategy for the incident:

- **Potential damage to and theft of resources**
- **Need to preserve evidence**
- **Service availability**, such as how quickly you need to restore services
- **Time and resources required** to implement the strategy
- **Effectiveness of the strategy**, such as partial containment versus complete resolution
- **Duration of the solution**, such as a temporary one-week workaround versus a permanent solution

3.1.2. Forensics

To ensure all evidence is admissible in court, you must follow laws and regulations when gathering evidence. Follow these guidelines for digital forensics:

- **Capture a backup image, or clone, of the system as-is** before anyone changes it, and only work off that clone to avoid tampering with the original.
- **Gather evidence** from that backup image by working with the image in an environment.
- **Follow chain of custody protocols**.

3.2. Eradication and recovery

Eradication is the process of eliminating the threat from all affected devices. For example, eradication could involve reimaging devices, disabling services, and installing patches.

What you do in eradication impacts recovery. According to NIST, **recovery** is the process in which you "restore impacted systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents." In recovery, you take actions such as the following:

- Restoring partitions from backups
- Swapping out affected files for clean ones
- Updating passwords
- Patching and hardening systems

The appropriate actions to take in recovery depend on the incident, the systems, and the approach to eradication. You often must extensively test and monitor restored systems to ensure that the incident no longer impacts them. Testing and monitoring could take weeks to months, depending on the time needed to return the compromised systems to production. Typically, incident response teams perform eradication and recovery in phases to ensure they can prioritize the steps taken to restore systems securely and effectively.

3.3. Containment, eradication, and recovery checklist

The SANS Institute recommends answering the following questions during containment, eradication, and recovery.

3.3.1. Containment

- Can the problem be isolated?
- Are all affected systems isolated from non-affected systems?
- Have forensic copies of affected systems been created for further analysis?

3.3.2. Eradication

- Is eradication possible?
- Can the system be reimaged and then hardened with patches or other countermeasures to prevent or reduce the risk of attacks?
- Have all malware and other artifacts from the attack been removed and affected systems hardened against further attacks?

3.3.3. Recovery

- Have affected systems been patched and hardened against this and future attacks?
- What tools will be used to test, monitor, and verify that the systems being restored to production are not compromised by the same methods that caused the original incident?

4. Post-Incident Activity

A crucial component of incident response is what you do *after* resolving the incident. NIST recommends several actions to learn from this incident and prepare for other follow-up activities.

4.1. Lessons learned

Both NIST and SANS recommend holding a **lessons learned meeting**. This meeting is a retrospective discussion in which all involved parties explore what could have been done better at all stages of the response. From this discussion, you can discover ways to improve security and respond more effectively to future incidents.

NIST recommends that you answer the following questions:

- What happened exactly, and at what times?
- How well did staff and management deal with the incident? Were the documented procedures followed? Were the procedures adequate?
- What information was needed sooner?

- Did any steps or actions taken inhibit recovery?
- What would everyone do differently if a similar incident occurred?
- How could you improve information sharing with other organizations?
- What changes can prevent similar incidents in the future?
- What precursors or indicators should you watch for to detect similar events?
- What other resources do you need to detect, analyze, and mitigate future incidents?

4.2. Other post-incident activities

Consider a few additional post-incident activities appropriate for the situation.

- **Create an incident response report**. This report should include a detailed timeline of events, an estimate of the incident's financial damage, and other relevant information. The report can serve as a reference for responding to similar incidents and as a crucial document in subsequent legal proceedings.
- **Use the data that you've collected.** You can collect data on response times, impacted data, total response time, and total recovery time, to name a few examples. You can measure every step that you take. With the data, you must determine the most valuable metrics for your organization and then analyze those to identify trends over time given similar incidents.
- **Ensure you have a proper evidence retention policy**. You must store, archive, and handle all data and forensic evidence such that they are usable in a court of law at any given time. This time could be months, even years, after the incident. And remember to follow the chain of custody to ensure that you properly document evidence handling.
- **Review all incident documentation**. This documentation includes everything from your incident response plan, such as incident handling, ticketing, and chain of custody. Address any gaps that you uncover.

4.3. Post-incident activity checklist

The SANS Institute recommends answering the following questions after you have resolved the incident:

- Is all needed incident documentation complete, including the incident response report?
- Does the incident response report answer who, what, when, where, why, and how for each step of incident response?
- Can you hold a lessons learned meeting within two weeks of the incident's resolution?
- In the lessons learned meeting, did you review the response with all involved parties and identify ways to improve future incident responses?

5. Additional Resources

This guide summarizes the basics of incident response and should work well as a quick reference. For more guidance, consult the following resources:

- Computer Security Incident Handling Guide – the NIST document from which much of this guide's content derives
- Incident Handler's Handbook – a SANS document that also provides helpful guidance on incident response, including the checklists referenced in this guide
- Documentation is to Incident Response as an Air Tank is to Scuba Diving – a SANS document that details documentation's impact on incident response
- Empowering Incident Response via Automation – a SANS document that explores automation's benefits and challenges for incident response
- A Practical Example of Incident Response to a Network Based Attack – a SANS case study of a response to a network-based threat