Computer Security Incident Handling Guide

NIST 800 – 61 Excerpts

Incident response capability required to:

1. Rapidly detect incidents
2. Minimize loss and destruction
3. Mitigate exploited weaknesses
4. Restore computing services.

Establishing a successful incident response capability requires planning and resources. Includes:

- Continual threat monitoring
- Establishing clear procedures for assessing the current and potential business impact of incidents
- Building relationships and establishing suitable means of communication with:
    - Internal and external groups

Five specific incident types

1. Denial of Service (DoS)
2. Malicious Code
3. Unauthorized Access
4. Inappropriate Usage
5. Multiple Component

By law, Federal agencies must report incidents to the Federal Computer Incident Response Center (FedCIRC) office within DHS.

- Federal Information Security Management Act (FISMA, 2002) required Federal agencies to establish incident response capabilities.
- Each Federal civilian agency must:
    - Designate a FedCIRC primary and secondary point of contact (POC)
    - Report all incidents
    - Internally document corrective actions and their impact.

Establishing an incident response capability includes:

- Creating incident response policy
- Developing incident handling and reporting procedures
- Setting guidelines for communicating with outside parties
- Selecting a team structure and staffing model
- Establishing relationships between the incident response team and other groups
    - Internal (e.g., legal department)
    - External (e.g., law enforcement agencies)
- Determining services that incident response team should provide
- Staffing and training incident response team.

Effectively securing networks, systems, and applications, organizations should reduce incident frequency.

- Preventing problems is less costly than reacting to them.

Organizations should document guidelines for interactions with other organizations during incidents. Outside organizations may include:

- Other incident response teams
- Law enforcement
- The media
- Vendors
- External victims

Throughout the organization, the importance of incident detection and analysis should be emphasized.

Organizations should create written guidelines for prioritizing incidents. Incidents can be prioritized based on:

- Criticality of the affected resources (e.g., public Web server, user workstation)
- Current and potential technical effect of the incident (e.g., root compromise, data destruction).

Organizations should decide how the incident response team should react under various circumstances

- A Service Level Agreement (SLA) documents appropriate actions and maximum response times.

To gain value from incidents, organizations should employ the lessons learned process.

During large-scale incidents, organizations should strive to maintain situational awareness.

Key to maintaining situational awareness is preparing for large-scale incidents, including:

- Establishing, documenting, maintaining, and exercising on-hours and off-hours contact and notification mechanisms for various individuals and groups
- Planning and documenting guidelines for the prioritization of incident response actions based on business impact.
- Preparing one or more individuals to act as incident leads who are responsible for gathering information from the incident handlers and other parties, and distributing relevant information to the parties that need it.
- Practicing the handling of large-scale incidents through regular exercises and simulations

A necessary enterprise task is to create an organization-specific definition of the term "incident" that has a clear scope.

- In a system or network, an event is any observable occurrence.
- Adverse events are events with a negative consequence, such as:

    - System crashes
    - Network packet floods
    - Unauthorized use of system privileges
    - Defacement of a web page
    - Execution of malicious code that destroys data.
- An incident can be thought of as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Incident examples:
- Denial of Service
- Malicious Code
- Unauthorized Access
- Inappropriate Usage

Incident response capability benefits
- Responding to incidents systematically with appropriate steps
- Helping personnel to recover quickly and efficiently from security incidents, minimizing loss or theft of information, and disruption of services
- Using information gained during incident handling to better prepare for future incidents and to provide stronger protection for systems and data
- Dealing properly with legal issues that may arise during incidents.

Policy governing incident response is highly individualized. However, most policies include the same key elements:
- Statement of management commitment
- Policy purpose and objectives
- Policy scope (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and their consequences within the context of the organization
- Organizational structure and delineation of roles, responsibilities, and levels of authority;
    - Should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, and the requirements for reporting certain types of incidents
    - Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms.

Procedures should be based on incident response policy.
- Standard operating procedures (SOPs)
    - A delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team.
- SOPs should be comprehensive and detailed.

Figure 2.1

Figure 2-1. Incident-Related Communications With Outside Parties

Conduct training sessions on interacting with the media regarding incidents, which should include

- The importance of not revealing sensitive information which could assist other would-be attackers
- The positive aspects of communicating important information to the public fully and effectively.
- Establish procedures to brief media contacts on the issues and sensitivities regarding a particular incident before discussing it with the media.
- Hold mock interviews and press conferences during incident handling exercises.

Examples questions:

- Who attacked you?
- When did it start?
- How did they do the attack?
- How widespread is this incident?
- Did this happen because you have poor security practices?
- What steps are you taking to determine what happened?
- What is the impact of this incident?
- What is the estimated monetary cost of this incident?

Available law enforcement:

- Federal Bureau of Investigation [FBI]
- U.S. Secret Service
- District attorney
- State law enforcement
- Local (e.g., county) law enforcement.

Before an incident occurs, the incident response team should become acquainted with law enforcement concerning:

- Conditions under which incidents should be reported
- How the reporting should be performed
- What evidence should be collected
- How evidence should be collected.

Law enforcement should be contacted through designated individuals in a manner consistent with the requirements of the law and the organization's procedures.

By Law, each Federal agency must designate a primary and secondary FedCIRC POC, report all incidents, and internally document corrective actions and their impact.

If an organization does not have its own CSIRT to contact, it can report incidents to other organizations, including—

- Information Analysis Infrastructure Protection (IAIP - DHS)
- CERT® Coordination Center (CERT®/CC).
- Information Sharing and Analysis Centers (ISAC).
    - Purpose of each ISAC is to share important computer security-related information among its members.

Other Outside Parties including

- Organization's ISP.
- Owners of Attacking Addresses.

Handlers should be cautious if they are unfamiliar with the external organization because the owner of the address space could be the attacker or an associate of the attacker.

Software Vendors.
Under some circumstances, incident handlers may consult a software vendor about suspicious activity.

Other Incident Response Teams.
Groups such as the Forum of Incident Response and Security Teams (FIRST)

Affected External Parties.
An incident may affect external parties directly; for example, an outside organization may contact the agency and claim that one of the agency's users is attacking it.

Team Models
Incident response team structure models fall into one of three categories:

Central Incident Response Team.	A single incident response team handles incidents throughout the organization. Effective for small organizations and for

	large organizations with minimal geographic diversity.
Distributed Incident Response Teams.	The organization has multiple incident response teams, each responsible for handling incidents for a particular logical or physical segment of the organization. Effective for large organizations (e.g., one team per division) and for organizations with major computing resources at distant.
Coordinating Team.	An incident response team provides guidance and advice to other teams without having authority over those teams—for example, a department wide team may assist individual agencies' teams.

Three Incident response team staffing models

1. Employees.
2. Partially Outsourced.
3. Outsourced managed security services provider (MSSP)

Some organizations perform basic incident response work in-house and call on contractors to assist with handling incidents, particularly those that are more serious or widespread.

The services most often performed by the contractors are computer forensics, advanced incident analysis, incident containment and eradication, and vulnerability mitigation.

Team Model Selection

When selecting appropriate structure and staffing models for an incident response team, organizations should consider:

- The Need for 24/7 Availability.
- Full-Time Versus Part-Time Team Members.
- Employee Morale.

Cost.

A major factor, especially if employees are required to be onsite 24/7.

Staff Expertise.

Outsourcers may possess deeper knowledge of intrusion detection, vulnerabilities, exploits, and other aspects of security than employees of the organization.

Organizational Structures.

If an organization has three departments that function independently, incident response may be more effective if each department has its own incident response team. The main organization can host a centralized incident response entity that facilitates standard practices and communications among the teams.

Division of Responsibilities.
It is important to decide the point at which the outsourcer hands off the incident response to the organization.

Sensitive Information Revealed to the Contractor.
Dividing incident response responsibilities and restricting access to sensitive information can limit this.

Lack of Organization-Specific Knowledge.
Accurate analysis and prioritization of incidents are dependent on specific knowledge of the organization's environment.

- Lack of organization-specific knowledge can also be a problem when incident response is not outsourced.

Lack of Correlation.
Correlation among multiple data sources is very important.

- If the intrusion detection system records an attempted attack against a Web server, but the outsourcer has no access to the Web logs, it may be unable to determine whether the attack was successful.
- To be efficient, the outsourcer will require administrative privileges to critical systems and security device logs remotely over a secure channel.
- Will increase administration costs, introduce additional access entry points, and increase the risk of unauthorized disclosure of sensitive information.

Handling Incidents at Multiple Locations.
Effective incident response work often requires a physical presence at the organization's facilities.

Maintaining Incident Response Skills In House.
Organizations that completely outsource incident response should strive to maintain basic incident response skills in house.

- The organization should be prepared to perform its own incident handling if the outsourcer is unable to act.
- The organization's technical staff must also be able to understand the significance, technical implications, and impact of the outsourcer's recommendations.

Incident Response Personnel
Regardless of which incident response model an organization chooses, a single employee should be in charge of incident response.

In a fully outsourced model, this person is responsible for overseeing and evaluating the outsourcer's work.

In all other models, this responsibility is generally achieved by having a team manager and a deputy team manager who assumes authority in the absence of the team manager.

The managers typically perform a variety of tasks, including:

- Acting as a liaison with upper management and other teams and organizations
- Defusing crisis situations
- Ensuring that the team has the necessary personnel, resources, and skills.

Team managers should be able to maintain positive working relationships with other groups, even under high pressure.

Incident Lead
Technical Lead

Critical technical skills include

- system administration
- network administration
- programming
- technical support
- intrusion detection.
- good problem solving skills.

Not necessary for every team member to be a technical expert.

- But it should have at least one highly proficient person in each major area of technology

In addition to technical expertise, Incident response team members should have other skills.

- Teamwork skills.
- Good communication skills.
- Speaking skills.
- Writing skills.

Dependencies Within Organizations
Every incident response team relies on the expertise, judgment, and abilities of others, including

- Management.
- Information Security.
- Telecommunications.
- IT Support.
- Legal Department.
- Public Affairs and Media Relations.
- Human Resources.

- Business Continuity Planning
- Physical Security and Facilities Management.

2.5 Incident Response Team Services
Rare for a team to only perform incident response. Additional services that an incident response team might offer include:
- Advisory Distribution.
- Vulnerability Assessment.
- Intrusion Detection.
- Education and Awareness.
- Technology Watch.
- Patch Management.

Recommendations
o Establish a formal incident response capability.
o Create an incident response policy and use it as the basis for incident response procedures.
o Establish policies and procedures regarding incident-related information sharing.
o Provide pertinent information on incidents to the appropriate incident reporting organization.
o
Federal civilian agencies are required to report incidents to FedCIRC; other organizations can contact other incident reporting organizations.

Critical technical skills include system administration, network administration, programming, technical support, and intrusion detection.

Teamwork and communications skills are also needed for effective incident handling.
o Identify other groups within the organization that may need to participate in incident handling.
Including management, information security, IT support, legal, public affairs, and facilities management.
o Determine which services the team should offer.

Examples include distributing security advisories, performing vulnerability assessments, educating users on security, and monitoring intrusion detection sensors.

Unit 3 Incident Response

Figure 3-1. Incident Response Life Cycle

Major phases of the incident response process:
1. Preparation
2. Detection and analysis
3. Containment/eradication/recovery
4. Post-incident activity.

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.

Acquired	Tool / Resource
	Incident Handler Communications and Facilities
	Contact information for team members and others within and outside the organization (primary and backup contacts), such as law enforcement and other incident response teams; information may include phone numbers, e-mail addresses, public encryption keys (in accordance with the encryption software described below), and instructions for verifying the contact's identity
	On-call information for other teams within the organization, including escalation information (see Section 3.2.6 for more information about escalation)
	Incident reporting mechanisms, such as phone numbers, e-mail addresses, and online forms that users can use to report suspected incidents; at least one mechanism should permit people to report incidents anonymously
	Pagers or cell phones to be carried by team members for off-hour support, onsite communications
	Encryption software to be used for communications among team members, within the organization and with external parties; software must use a Federal Information Processing Standards (FIPS) 140-2 validated encryption algorithm[31]
	War room for central communication and coordination; if a permanent war room is not necessary, the team should create a procedure for procuring a temporary war room when needed
	Secure storage facility for securing evidence and other sensitive materials
	Incident Analysis Hardware and Software

	Incident Analysis Hardware and Software
	Computer forensic workstations[32] **and/or backup devices** to create disk images, preserve log files, and save other relevant incident data
	Laptops, which provide easily portable workstations for activities such as analyzing data, sniffing packets, and writing reports
	Spare workstations, servers, and networking equipment, which may be used for many purposes, such as restoring backups and trying out malicious code; if the team cannot justify the expense of additional equipment, perhaps equipment in an existing test lab could be used, or a virtual lab could be established using operating system (OS) emulation software
	Blank media, such as floppy diskettes, CD-Rs, and DVD-Rs
	Easily portable printer to print copies of log files and other evidence from non-networked systems
	Packet sniffers and protocol analyzers to capture and analyze network traffic that may contain evidence of an incident
	Computer forensic software to analyze disk images for evidence of an incident
	Floppies and CDs with trusted versions of programs to be used to gather evidence from systems
	Evidence gathering accessories, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions

	Incident Analysis Resources
	Port lists, including commonly used ports and Trojan horse ports
	Documentation for OSs, applications, protocols, and intrusion detection and antivirus signatures
	Network diagrams and lists of critical assets, such as Web, e-mail, and File Transfer Protocol (FTP) servers
	Baselines of expected network, system and application activity
	Cryptographic hashes of critical files[33] to speed the analysis, verification, and eradication of incidents

Acquired	Tool / Resource
	Incident Mitigation Software
	Media, including OS boot disks and CD-ROMs, OS media, and application media
	Security patches from OS and application vendors
	Backup images of OS, applications, and data stored on secondary media

A jump kit is a portable bag or case that contains materials that an incident handler may need during an offsite investigation.

Each jump kit typically includes a laptop, loaded with appropriate software (e.g., packet sniffers, computer forensics). Other important materials include backup devices, blank media, basic networking equipment and cables, and operating system and application media and patches.

Preventing Incidents
Keeping the number of incidents low is critical.
Conduct periodic risk assessments of systems and applications.
- Determine what risks are posed by combinations of threats and vulnerabilities.

Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasize monitoring and response activities for those resources.

A brief overview of some of the main recommended practices for securing networks, systems, and applications:

- Patch Management.
- Host Security.
- Network Security.
- Malicious Code Prevention.
- User Awareness and Training.

Primary Incident Categories

Denial of Service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity that infects a host
Unauthorized Access	A person gains logical or physical access without permission to a network, system, application, data, or other resource
Inappropriate Usage	A person violates acceptable computing use policies
Multiple Component	A single incident that encompasses two or more incidents.

Signs of an Incident

A challenging attribute of the incident response process is … determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem

Challenging combination of three factors:

1. Incidents may be detected many different ways, with varying levels of detail and fidelity.
2. The high volume of potential signs of incidents.
3. The deep, specialized technical knowledge and extensive experience are necessary for proper and efficient analysis of incident-related data.

Signs of an incident fall into one of two categories:

1. Indications
2. Precursors.

A precursor is a sign that an incident may occur in the future. An indication is a sign that an incident may have occurred or may be occurring now.

Indications examples

Network intrusion detection sensor alerts when a buffer overflow attempt occurs against an FTP server.

Antivirus software alerts when it detects that a host is infected with a worm.
Web server crashes.
Users complain of slow access to hosts on the Internet.
System administrator sees a filename with unusual characters.
User calls the help desk to report a threatening email message.
Host records an auditing configuration change in its log.
Application logs multiple failed login attempts from an unfamiliar remote system.
Email administrator sees a large number of bounced emails with suspicious content. The network administrator notices an unusual deviation from typical network traffic flows.

Precursor Examples

Web server log entries that show the usage of a Web vulnerability scanner
An announcement of a new exploit that targets a vulnerability of the organization's mail server
A threat from a hacktivist group stating that the group will attack the organization.

Sources of Precursors and Indications

Precursors and indications are identified using many different sources. Most commonly software alerts, logs, publicly available information, and people.

Table 3-2. Common Sources of Precursors and Indications

Precursor or Indication Source	Description
Computer Security Software Alerts	
Network-based, host-based, wireless, and network behavior analysis IDPSs	IDPS products are designed to identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use a set of attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces *false positives*—alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources. The four different IDPSs each have different information gathering, logging, detection, and prevention capabilities.[44] In most environments, multiple types of IDPS should be implemented.

Precursor or Indication Source	Description
Antivirus, antispyware, and antispam software,	Antivirus and antispyware software are designed to detect various forms of malicious code and prevent them from infecting hosts. When antivirus or antispyware software detects malicious code, it typically generates alerts. Current antivirus and antispyware products are effective at detecting and eradicating or isolating malicious code if their signatures are kept up to date. This updating task can be overwhelming in large organizations. One way of addressing it is to configure centralized antivirus and antispyware software to push signature updates to individual hosts, rather than rely on hosts to be configured to pull updates. Because detection varies among products, some organizations use products from multiple vendors to provide better coverage and higher accuracy. Antivirus software should be deployed in at least two levels: at the network perimeter (e.g., firewalls, email servers) and at the host level (e.g., workstations, file servers, client software). Antispyware software should be used if the antivirus software does not have sufficiently robust spyware detection capabilities; if used, antispyware software should be deployed in the same levels as antivirus software. Antispam software is used to detect spam and prevent it from reaching users' mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts.
File integrity checking software	Incidents may cause changes to important files; file integrity checking software can detect such changes. It works by using a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected.
Third-party monitoring service	Some organizations pay a third party to monitor their publicly accessible services, such as Web, Domain Name System (DNS) and FTP servers. The third party automatically attempts to access each service every *x* minutes. If the service cannot be accessed, the third party alerts the organization using the methods specified by the organization, such as phone calls, pages, and emails. Some monitoring services can also detect and alert on changes in certain resources—for example, a Web page. Although a monitoring service is mainly useful from an operational standpoint, it can also provide an indication of a DoS attack or server compromise.
Logs	
Operating system, service and application logs	Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs. Logs can provide a wealth of information, such as which accounts were accessed and what actions were performed. Additionally, logs can assist in event aggregation to determine the number of hosts scanned in one occurrence. Unfortunately, in many incidents, the logs contain no evidence because logging was either disabled or configured improperly on the host. To facilitate effective incident handling, organizations should require a baseline level of logging on all systems, and a higher baseline level of logging on critical systems. All systems should have auditing turned on and should log audit events, particularly administrative-level activity. All systems should be checked periodically to verify that logging is functioning properly and adheres to the logging standards. Additionally, logs should be properly rotated and stored. While stored, log file integrity checking should be conducted to ensure the logs have not been accessed and changed. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated to indicate an incident. There are various types of centralized logging software, such as syslog, security event and information software, and host-based IDPS.[47] Section 3.2.4 discusses the value of performing centralized logging.

Precursor or Indication Source	Description
Network device logs	Logs from network devices such as firewalls and routers are not typically used as a primary source of precursors or indications. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying trends (e.g., a significantly increased number of attempts to access a particular port) and in correlating events detected by other devices.
Publicly Available Information	
Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in the detection and analysis of new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities.[46] Several organizations, such as US-CERT[47], CERT®/CC, IAIP,[48] and the Department of Energy's Computer Incident Advisory Capability (CIAC),[49] periodically provide threat update information through briefings, Web postings, and mailing lists.
Information on incidents at other organizations	Reports of incidents that have occurred at other organizations can provide a wealth of information. There are Web sites and mailing lists where incident response teams and security professionals can share information regarding reconnaissance and attacks that they have seen. In addition, some organizations acquire, consolidate, and analyze logs and intrusion detection alerts from many other organizations.[50]
People	
People from within the organization	Users, system administrators, network administrators, security staff, and others from within the organization may report signs of incidents. It is important to validate all such reports. Not only do users generally lack the knowledge to determine if an incident is occurring, but also even the best-trained technical experts make mistakes. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered.
People from other organizations	Although few reports of incidents will originate from people at other organizations, they should be taken seriously. A classic example is an attacker who identifies a serious vulnerability in a system and either informs the organization directly or publicly announces the issue. Another possibility is that the organization might be contacted by an external party claiming someone at the organization is attacking it. External users may also report other indications, such as a defaced Web page or an unavailable service. Other incident response teams also may report incidents. It is important to have mechanisms in place for external parties to report indications and for trained staff to monitor those mechanisms carefully; this may be as simple as setting up a phone number and email address, configured to forward messages to the help desk.

Incident Analysis
Separating the few real security incidents that occurred out of all the indications can be daunting.

Even if an indicator has occurred it may be necessary to collaborate with other technical and information security personnel to make a decision.
- In many instances, a situation should be handled the same way regardless of whether it is security related.

In incident handling, detection may be the most difficult task. Incident handlers are responsible for analyzing ambiguous, contradictory, and incomplete symptoms to determine what has happened.

Best remedy
Build a team of highly experienced and proficient staff members who can analyze the precursors and indications effectively and efficiently and take appropriate actions.

When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine:

- Incident's scope
- Who or what originated the incident;
- How the incident is occurring..

Recommendations for making incident analysis easier and more effective:
- Profile Networks and Systems.
- Understand Normal Behaviors.
- Use Centralized Logging and Create a Log Retention Policy.
- Perform Event Correlation.
- Keep All Host Clocks Synchronized.
- Maintain and Use a Knowledge Base of Information.
- Use Internet Search Engines for Research.
- Run Packet Sniffers to Collect Additional Data.
- Consider Filtering the Data.
- Consider Experience as Being Irreplaceable.
- Create a Diagnosis Matrix for Less Experienced Staff.
- Seek Assistance From Others.

Table 3-3. Excerpt of a Sample Diagnosis Matrix

Symptom	Denial of Service	Malicious Code	Unauthorized Access	Inappropriate Usage
Files, critical, access attempts	Low	Medium	High	Low
Files, inappropriate content	Low	Medium	Low	High
Host crashes	Medium	Medium	Medium	Low
Port scans, incoming, unusual	High	Low	Medium	Low
Port scans, outgoing, unusual	Low	High	Medium	Low
Utilization, bandwidth, high	High	Medium	Low	Medium
Utilization, email, high	Medium	High	Medium	Medium

Incident Documentation

As soon as an incident response team suspects that an incident is occurring or has occurred, it needs to start recording all facts.
- Every step taken from the time the incident was detected to its final resolution should be documented and time stamped.
- Every document regarding the incident should be dated and signed by the incident handler.

The Incident database, should contain the following
- Current incident status
- Incident summary
- All actions taken by incident handlers
- Contact information for other involved parties
- List of evidence gathered
- Incident handlers comments

- Next steps to be taken

Incident Prioritization
Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process.

Current and Potential Technical Effect of the Incident.
Criticality of the Affected Resources.

The team should prioritize the response to each incident based on its estimate of the business impact caused by the incident.

Table 3-4. Effect Rating Definitions

Value	Rating	Definition
0.00	None	No effect on a single agency, multiple agencies, or critical infrastructure
0.10	Minimal	Negligible effect on a single agency
0.25	Low	Moderate effect on a single agency
0.50	Medium	Severe effect on a single agency or negligible effect on multiple agencies or critical infrastructure
0.75	High	Moderate effect on multiple agencies or critical infrastructure
1.00	Critical	Severe effect on multiple agencies or critical infrastructure

Table 3-5. Criticality Rating Definitions

Value	Rating	Definition
0.10	Minimal	Non-critical system (e.g., employee workstations), systems, or infrastructure
0.25	Low	System or systems that support a single agency's mission (e.g., DNS servers, domain controllers), but are not mission critical
0.50	Medium	System or systems that are mission critical (e.g., payroll system, root DNS server) to a single agency
0.75	High	System or systems that support multiple agencies or sectors of the critical infrastructure
1.00	Critical	System or systems that are mission critical to multiple agencies or critical infrastructure

Table 3-7. Sample Incident Response SLA Matrix

Current Impact or Likely Future Impact of the Incident	Criticality of Resources Currently Impacted or Likely To Be Impacted by the Incident		
	High (e.g., Internet Connectivity, Public Web Servers, Firewalls, Customer Data)	Medium (e.g., System Administrator Workstations, File and Print Servers, XYZ Application Data)	Low (e.g., User Workstations)
Root-level access	15 minutes	30 minutes	1 hour
Unauthorized data modification	15 minutes	30 minutes	2 hours
Unauthorized access to sensitive data	15 minutes	1 hour	1 hour
Unauthorized user-level access	30 minutes	2 hours	4 hours
Services unavailable	30 minutes	2 hours	4 hours
Annoyance[61]	30 minutes	Local IT staff	Local IT staff

Matrix approach encourages organizations to consider carefully how the incident response team should react under various circumstances.

Organizations should also establish an escalation process for those instances when the team does not respond to an incident within the designated time.

Incident Notification
When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals within the organization and, occasionally, other organizations.

Incident response policies should include provisions concerning incident reporting—at a minimum, what must be reported to whom and at what times.
The exact reporting requirements vary among agencies, parties typically notified include

- CIO
- Head of information security
- Local information security officer
- Other incident response teams within the organization
- System owner
- Human resources (for cases involving employees, such as email harassment)
- Public affairs (for incidents that may generate publicity)
- Legal department (for incidents with potential legal ramifications)
- US-CERT (required for Federal agencies and systems operated on behalf of the Federal government)

During the handling of an incident, the team may need to notify certain parties frequently of the incident's current status.
o Some cases, such as a major malicious code infection, may require the sending of organization wide updates.

Team should select the methods that are appropriate for a particular incident.
Possible communication methods include

- Email
- Web site (Intranet-based)
- Telephone calls
- In person (e.g., daily briefings)
- Voice mailbox greeting (e.g., set up a separate voice mailbox for incident updates, and update the greeting message to reflect the current incident status)
- Paper (e.g., post notices on bulletin boards and doors, hand out notices at all entrance points).

Containment, Eradication, and Recovery

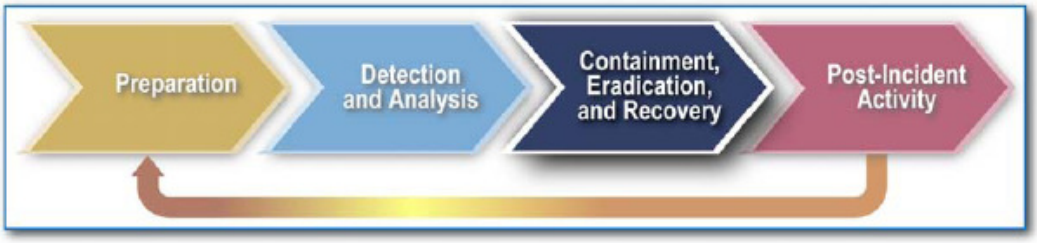

Figure 3-3. Incident Response Life Cycle (Containment, Eradication, and Recovery)

When an incident has been detected and analyzed, it is important to contain.

Decision-making
- Essential part of containment is (e.g., shut down a system, disconnect it from a wired or wireless network, disconnect its modem cable, …).

Containment strategies vary depending on the type of incident.
- Organizations should create separate containment strategies for each major type of incident.

Criteria for determining appropriate strategy include
- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (e.g., network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g., partially contains the incident, fully contains the incident)
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

In certain cases, some organizations delay incident containment so that they can monitor attacker's activity.

> Do not assume that because a host has been disconnected from the network, further damage to the host has been prevented.

Evidence Gathering and Handling

Although the primary reason for gathering evidence during an incident is to resolve the incident, evidence may also be needed for legal proceedings.

Evidence should be collected according to procedures that meet all applicable laws and regulations, … that it should be admissible in court.

Evidence should be accounted for at all times; a detailed evidence log should be kept, including:

- Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) address, and IP address of a computer)
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation
- Time and date (including time zone) of each occurrence of evidence handling
- Locations where the evidence was stored.

Forensics for standard computers

Before copying the files from the affected host, it is often desirable to capture volatile information … such as current network connections, processes, login sessions, open files, network interface configurations, and the contents of memory.

A well-trained and careful incident handler should issue only the minimum commands needed for acquiring the dynamic evidence without inadvertently altering other evidence.

- A single poorly chosen command can irrevocably destroy evidence;
- Running commands from the affected host is dangerous because they may have been altered or replaced.

Incident handlers should use write-protected removable media that contains trusted commands and all dependent files so that all necessary commands can be run without using the affected host's commands.

After acquiring volatile data, an incident handler with computer forensics training should immediately make a full disk image to sanitized write-protectable or write-once media. A disk image preserves all data on the disk, including deleted files and file fragments.

Obtaining a disk image is superior to a standard file system backup for computer forensic purposes. For the analysis process, such as:

- Identifying and recovering file fragments and hidden and deleted files and directories from any location (e.g., used space, free space, slack space)
- Examining file structures, headers, and other characteristics to determine what type of data each file contains, instead of relying on file extensions (e.g., .doc, .jpg, .mp3)
- Displaying contents of all graphics files
- Performing complex searches
- Graphically displaying the acquired drive's directory structure
- Generating reports.

During evidence acquisition, it is often prudent to acquire copies of supporting log files from other resources

Many incident handlers create a message digest for log files and other digital evidence;

Identifying the Attacker
During incident handling, system owners and others typically want to identify the attacker. Although this information can be important, particularly if the organization wants to prosecute the attacker, incident handlers should stay focused on containment, eradication, and recovery.

Identifying the attacker can be a time-consuming and futile process that can prevent a team from achieving its primary goal—minimizing the business impact.

Most common attacker identification activities

- Validating Attacker's IP Address.
- Scanning Attacker's System.
- Researching Attacker Through Search Engines.
- Using Incident Databases.
- Monitoring Possible Attacker Communication Channels.

Eradication and Recovery
After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malicious code and disabling breached user accounts.

For some incidents, eradication is either not necessary or is performed during recovery. In recovery, administrators restore systems to normal operation and (if applicable) harden systems to prevent similar incidents.

Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rule sets, boundary router access control lists).

Post-Incident Activity
Lessons Learned
One of the most important parts of incident response: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned.

Questions to be answered in the lessons learned include

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?

- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Using Collected Incident Data Lessons learned activities should produce a set of objective and subjective data regarding each incident.

Absolute numbers are not informative—understanding how they represent threats to the business processes of the organization is what matters.

Possible metrics for incident-related data include
- Number of Incidents Handled.
- Time Per Incident.
- Objective Assessment of Each Incident.
- Subjective Assessment of Each Incident.

At a minimum, an incident response audit should evaluate the following items against applicable regulations, policies, and generally accepted practices:
- Incident response policies, plans, and procedures
- Tools and resources
- Team model and structure
- Incident handler training and education
- Incident documentation and reports
- The measures of success discussed earlier in this section.