ARTEMIS

Advanced Reactive Threat Elimination and Monitoring Integrated System

Computer Security Incident Handling Guide

Inspired by the recommendations of the National Institute of Standards and Technology

Sarang Shigwan

Atharva Kanawade

Table of Contents

List of Appendices

1. Introduction

1.1 Context

Cyber security relates to the confidentiality, availability and integrity of information and data that is processed, stored and communicated by electronic or similar means, and protecting it and associated systems from external or internal threat.

It is commonly recognized that cyber security involves the protection of critical information and ICT infrastructure, including supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS), through the alignment of people, processes and tools.

This document supports organization in managing contemporary cyber threats and incidents. The application of this document will support organization in reducing the scope, impact and severity of cyber incidents.

1.2 Purpose and Scope

This publication seeks to assist the organization in mitigating the risks from computer security incidents by providing practical guidelines on responding to incidents effectively and efficiently. It includes guidelines on establishing an effective incident response program, but the primary focus of the document is detecting, analyzing, prioritizing, and handling incidents.

1.3 Authority

This guideline has been prepared for use by XYZ agencies. It may be used by nongovernmental organizations or businesses on a voluntary basis and is a subject to copyright.

Not even the makers of this document can access any confidential information filled in the appendices.

1.4 Audience

This document has been created for computer security incident response teams (CSIRTs), system and network administrators, security staff, technical support staff, chief information security officers (CISOs), chief information officers (CIOs), computer security program managers, and others who are responsible for preparing for, or responding to security incidents of the organization.

2. Organizing a Computer Security Incident Response Capability

Organizing an effective computer security incident response capability (CSIRC) involves several major decisions and actions. One of the first considerations should be to create an organization-specific definition of the term “incident” so that the scope of the term is clear. The organization should decide what services the incident response team should provide, consider which team structures and models can provide those services, and select and implement one or more incident response teams. Incident response plan, policy, and procedure creation is an important part of establishing a team, so that incident response is performed effectively, efficiently, and consistently, and so that the team is empowered to do what needs to be done. The plan, policies, and procedures should reflect the team’s interactions with other teams within the organization as well as with outside parties, such as law enforcement, the media, and other incident response organizations. This section provides not only guidelines that should be helpful to organizations that are establishing incident response capabilities, but also advice on maintaining and enhancing existing capabilities.

2.1 What is a computer security incident?

A *computer security incident* is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

2.2 Need for Incident Response

Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur. The concept of computer security incident response has become widely accepted and implemented. One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response helps personnel to minimize loss or theft of information and disruption of services caused by incidents.

2.3 Incident Response Team Structure

An incident response team should be available for anyone who discovers or suspects that an incident involving the organization has occurred. One or more team members, depending on the magnitude of the incident and availability of personnel, will then handle the incident. The incident handlers analyze the incident data, determine the impact of the incident, and act appropriately to limit the damage and restore normal services. The incident response team's success depends on the participation and cooperation of individuals throughout the organization. This section identifies such individuals, discusses incident response team models, and provides advice on selecting an appropriate model.

2.3.1 Team Models

Possible structures for an incident response team include the following:

- **Central Incident Response Team.** A single incident response team handles incidents throughout the organization. This model is effective for small organizations and for organizations with minimal geographic diversity in terms of computing resources.
- **Distributed Incident Response Teams.** The organization has multiple incident response teams, each responsible for a particular logical or physical segment of the organization. This model is effective for large organizations (e.g., one team per division) and for organizations with major computing resources at distant locations (e.g., one team per geographic region, one team per major facility). However, the teams should be part of a single coordinated entity so that the incident response process is consistent across the organization and information is shared among teams. This is particularly important because multiple teams may see components of the same incident or may handle similar incidents.
- **Coordinating Team.** An incident response team provides advice to other teams without having authority over those teams—for example; a department wide team may assist individual agencies' teams. This model can be thought of as a CSIRT for CSIRTs.

Incident response teams can also use any of three staffing models:

- **Employees.** The organization performs all of its incident response work, with limited technical and administrative support from contractors.
- **Partially Outsourced.** The organization outsources portions of its incident response work. Although incident response duties can be divided among the organization and one or more outsourcers in many ways, a few arrangements have become commonplace:
- **Fully Outsourced.** The organization completely outsources its incident response work, typically to an onsite contractor. This model is most likely to be used when the organization needs a full-time, onsite incident response team but does not have enough available, qualified employees. It is assumed that the organization will have employees supervising and overseeing the outsourcer's work.

2.3.2 Team Model Selection

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

1. **The Need for 24/7 Availability.**
2. **Full-Time Versus Part-Time Team Members.**
3. **Employee Morale.**
4. **Cost.**
5. **Staff Expertise.**
6. **Current and Future Quality of Work.**
7. **Division of Responsibilities.**
8. **Sensitive Information Revealed to the Contractor.**
9. **Lack of Organization-Specific Knowledge.**
10. **Lack of Correlation.**
11. **Handling Incidents at Multiple Locations.**
12. **Maintaining Incident Response Skills In-House**

2.3.3 Incident Response Personnel

A single employee, with one or more designated alternates, should be in charge of incident response. In a fully outsourced model, this person oversees and evaluates the outsourcer's work. All other models generally have a team manager and one or more deputies 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, and ensuring that the team has the necessary personnel, resources, and skills. Managers should be technically adept and have excellent communication skills, particularly an ability to communicate to a range of audiences. Managers are ultimately responsible for ensuring that incident response activities are performed properly.

In addition to the team manager and deputy, some teams also have a technical lead—a person with strong technical skills and incident response experience who assumes oversight of and final responsibility for the quality of the team's technical work. The position of technical lead should not be confused with the position of incident lead. Larger teams often assign an incident lead as the primary POC for handling a specific incident; the incident lead is held accountable for the incident's handling. Depending on the size of the incident response team and the magnitude of the incident, the incident lead may not actually perform any actual incident handling, but rather coordinate the handlers' activities, gather information from the handlers, provide incident updates to other groups, and ensure that the team's needs are met.

Members of the incident response team should have excellent technical skills, such as system administration, network administration, programming, technical support, or intrusion detection. Every team member should have good problem solving skills and critical thinking abilities. It is not necessary for every team member to be a technical expert—to a large degree, practical and funding considerations will dictate this—but having at least one highly proficient person in each major area of technology (e.g., commonly attacked operating systems and applications) is a necessity. It may also be helpful to have some team members specialize in particular technical areas, such as network intrusion detection, malware analysis, or forensics. It is also often helpful to temporarily bring in technical specialists that aren't normally part of the team.

Incident response team members should have other skills in addition to technical expertise. Teamwork skills are of fundamental importance because cooperation and coordination are necessary for successful incident response. Every team member should also have good communication skills. Speaking skills are important because the team will interact with a wide variety of people, and writing skills are important when team members are preparing advisories and procedures. Although not everyone within a team needs to have strong writing and speaking skills, at least a few people within every team should possess them so the team can represent itself well in front of others.

2.3.4 Incident Response Team Services

The main focus of an incident response team is performing incident response, but it is fairly rare for a team to perform incident response only. The following are examples of other services a team might offer:

- **Intrusion Detection.** The first tier of an incident response team often assumes responsibility for intrusion detection.[17] The team generally benefits because it should be poised to analyze incidents more quickly and accurately, based on the knowledge it gains of intrusion detection technologies.
- **Advisory Distribution.** A team may issue advisories within the organization regarding new vulnerabilities and threats.[18] Automated methods should be used whenever appropriate to disseminate information; for example, the National Vulnerability Database (NVD) provides information via XML and RSS feeds when new vulnerabilities are added to it.[19] Advisories are often most necessary when new threats are emerging, such as a high-profile social or political event (e.g., celebrity wedding) that attackers are likely to leverage in their social engineering. Only one group within the organization should distribute computer security advisories to avoid duplicated effort and conflicting information.
- **Education and Awareness.** Education and awareness are resource multipliers—the more the users and technical staff know about detecting, reporting, and responding to incidents, the less drain there should be on the incident response team. This information can be communicated through many means: workshops, websites, newsletters, posters, and even stickers on monitors and laptops.
- **Information Sharing.** Incident response teams often participate in information sharing groups, such as ISACs or regional partnerships. Accordingly, incident response teams often manage the organization’s incident information sharing efforts, such as aggregating information related to incidents and effectively sharing that information with other organizations, as well as ensuring that pertinent information is shared within the enterprise.

3. Handling an incident

The incident response process has several phases. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, residual risk will inevitably persist after controls are implemented. Detection of security breaches is thus necessary to alert the organization whenever incidents occur. In keeping with the severity of the incident, the organization can mitigate the impact of the incident by containing it and ultimately recovering from it. During this phase, activity often cycles back to detection and analysis—for example, to see if additional hosts are infected by malware while eradicating a malware incident. After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents. This section describes the major phases of the incident response process—preparation, detection and analysis, containment, eradication and recovery, and post-incident activity—in detail.
Figure 3-1 illustrates the incident response life cycle.

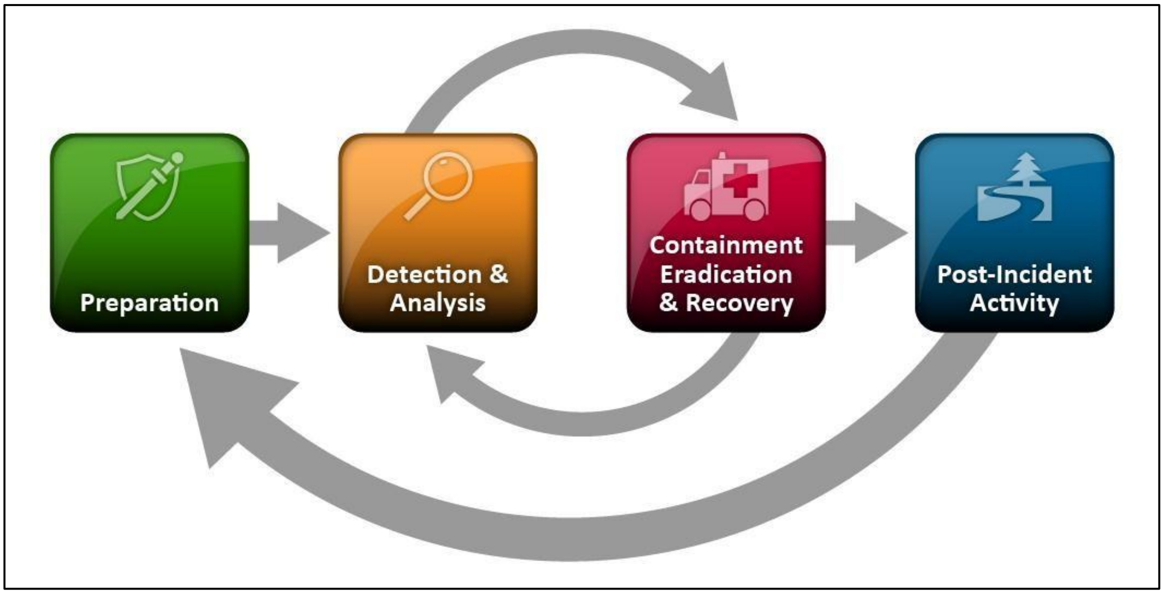

Figure 3-1. Incident Response Life Cycle

3.1 Preparation

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. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs. This section provides basic advice on preparing to handle incidents and on preventing incidents.

3.1.1 Preparing to Handle Incidents

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, email 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
- **Incident reporting mechanisms,** such as phone numbers, email addresses, online forms, and secure instant messaging systems that users can use to report suspected incidents; at least one mechanism should permit people to report incidents anonymously
- **Issue tracking system** for tracking incident information, status, etc.
- **Smartphones** to be carried by team members for off-hour support and onsite communications
- **Encryption software** to be used for communications among team members, within the organization and with external parties; for Federal agencies, software must use a FIPS-validated encryption algorithm[20]
- **War room** for central communication and coordination; if a permanent war room is not necessary or practical, 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:

- **Digital forensic workstations and/or backup devices** to create disk images, preserve log files, and save other relevant incident data
- **Laptops** for activities such as analyzing data, sniffing packets, and writing reports
- **Spare workstations, servers, and networking equipment, or the virtualized equivalents**, which may be used for many purposes, such as restoring backups and trying out malware
- **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
- **Digital forensic software** to analyze disk images
- **Removable media** 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 products
- **Network diagrams and lists of critical assets,** such as database servers
- **Current baselines** of expected network, system, and application activity
- **Cryptographic hashes** of critical files[22] to speed incident analysis, verification, and eradication

3.1.2 Preventing Incidents

Keeping the number of incidents reasonably low is very important to protect the business processes of the organization. If security controls are insufficient, higher volumes of incidents may occur, overwhelming the incident response team. This can lead to slow and incomplete responses, which translate to a larger negative business impact.

The following text, however, provides a brief overview of some of the main recommended practices for securing networks, systems, and applications:

- **Risk Assessments.** Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities. This should include understanding the applicable threats, including organization-specific threats. Each risk should be prioritized, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasize monitoring and response activities for those resources.
- **Host Security.** All hosts should be hardened appropriately using standard configurations. In addition to keeping each host properly patched, hosts should be configured to follow the principle of least privilege—granting users only the privileges necessary for performing their authorized tasks.
- **Network Security.** The network perimeter should be configured to deny all activity that is not expressly permitted. This includes securing all connection points, such as virtual private networks (VPNs) and dedicated connections to other organizations.
- **Malware Prevention.** Software to detect and stop malware should be deployed throughout the organization. Malware protection should be deployed at the host level (e.g., server and workstation operating systems), the application server level (e.g., email server, web proxies), and the application client level (e.g., email clients, instant messaging clients).
- **User Awareness and Training.** Users should be made aware of policies and procedures regarding appropriate use of networks, systems, and applications. Applicable lessons learned from previous incidents should also be shared with users so they can see how their actions could affect the organization. Improving user awareness regarding incidents should reduce the frequency of incidents.

3.2 Detection and Analysis

3.2.1 Attack Vectors

Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors. Different types of incidents merit different response strategies. The attack vectors listed below are not intended to provide definitive classification for incidents; rather, they simply list common methods of attack, which can be used as a basis for defining more specific handling procedures.

- **External/Removable Media:** An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive.
- **Attrition:** An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures).
- **Web:** An attack executed from a website or web-based application—for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.
- **Email:** An attack executed via an email message or attachment—for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.
- **Impersonation:** An attack involving replacement of something benign with something malicious—for example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
- **Improper Usage:** Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
- **Loss or Theft of Equipment:** The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token.
- **Other:** An attack that does not fit into any of the other categories.

3.2.2 Signs of an Incident

For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem. What makes this so challenging is a combination of three factors:

Common indicators of the attack include :

- Web server log entries that show the usage of a vulnerability scanner
- An announcement of a new exploit that targets a vulnerability of the organization's mail server
- A threat from a group stating that the group will attack the organization.
- While precursors are relatively rare, indicators are all too common. Too many types of indicators exist to exhaustively list them, but some examples are listed below:
- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against database server.
- Antivirus software alerts when it detects that a host is infected with malware.
- A system administrator sees a filename with unusual characters.
- A host records an auditing configuration change in its log.
- An application logs multiple failed login attempts from an unfamiliar remote system.
- An email administrator sees a large number of bounced emails with suspicious content.
- A network administrator notices an unusual deviation from typical network traffic flows.

3.2.3 Incident Analysis

Incident detection and analysis would be easy if every precursor or indicator were guaranteed to be accurate; unfortunately, this is not the case. For example, user-provided indicators such as a complaint of a server being unavailable are often incorrect. Intrusion detection systems may produce false positives— incorrect indicators. These examples demonstrate what makes incident detection and analysis so difficult: each indicator ideally should be evaluated to determine if it is legitimate. Making matters worse, the total number of indicators may be thousands or millions a day. Finding the real security incidents that occurred out of all the indicators can be a daunting task.

Performing the initial analysis and validation is challenging. The following are recommendations for making incident analysis easier and more effective:

- **Profile Networks and Systems.** *Profiling* is measuring the characteristics of expected activity so that changes to it can be more easily identified. Examples of profiling are running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. In practice, it is difficult to detect incidents accurately using most profiling techniques; organizations should use profiling as one of several detection and analysis techniques.

- **Understand Normal Behaviors.** Incident response team members should study networks, systems, and applications to understand what their normal behavior is so that abnormal behavior can be recognized more easily. No incident handler will have a comprehensive knowledge of all behavior throughout the environment, but handlers should know which experts could fill in the gaps. One way to gain this knowledge is through reviewing log entries and security alerts. This may be tedious if filtering is not used to condense the logs to a reasonable size. As handlers become more familiar with the logs and alerts, they should be able to focus on unexplained entries, which are usually more important to investigate. Conducting frequent log reviews should keep the knowledge fresh, and the analyst should be able to notice trends and changes over time. The reviews also give the analyst an indication of the reliability of each source.

- **Create a Log Retention Policy.** Information regarding an incident may be recorded in several places, such as firewall, IDPS, and application logs. Creating and implementing a log retention policy that specifies how long log data should be maintained may be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks. Another reason for retaining logs is that incidents may not be discovered until days, weeks, or even months later. The length of time to maintain log data is dependent on several factors, including the organization's data retention policies and the volume of data. See NIST SP 800-92, *Guide to Computer Security Log Management* for additional recommendations related to logging.[34]

- **Perform Event Correlation.** Evidence of an incident may be captured in several logs that each contain different types of data—a firewall log may have the source IP address that was used, whereas an application log may contain a username. A network IDPS may detect that an attack was launched against a particular host, but it may not know if the attack was successful. The analyst may need to examine the host's logs to determine that information. Correlating events among multiple indicator sources can be invaluable in validating whether a particular incident occurred.

- **Keep All Host Clocks Synchronized.** Protocols such as the Network Time Protocol (NTP) synchronize clocks among hosts.[35] Event correlation will be more complicated if the devices reporting events have inconsistent clock settings. From an evidentiary standpoint, it is preferable to have consistent timestamps in logs—for example, to have three logs that show an attack occurred at 12:07:01 a.m., rather than logs that list the attack as occurring at 12:07:01, 12:10:35, and 11:07:06.

- **Maintain and Use a Knowledge Base of Information.** The knowledge base should include information that handlers need for referencing quickly during incident analysis. Although it is possible to build a knowledge base with a complex structure, a simple approach can be effective. Text documents, spreadsheets, and relatively simple databases provide effective, flexible, and searchable mechanisms for sharing data among team members. The knowledge base should also contain a variety of information, including explanations of the significance and validity of precursors and indicators, such as IDPS alerts, operating system log entries, and application error codes.

- **Use Internet Search Engines for Research.** Internet search engines can help analysts find information on unusual activity. For example, an analyst may see some unusual connection attempts targeting TCP port 22912. Performing a search on the terms “TCP,” “port,” and “22912” may return some hits that contain logs of similar activity or even an explanation of the significance of the port number. Note that separate workstations should be used for research to minimize the risk to the organization from conducting these searches.

- **Run Packet Sniffers to Collect Additional Data.** Sometimes the indicators do not record enough detail to permit the handler to understand what is occurring. If an incident is occurring over a network, the fastest way to collect the necessary data may be to have a packet sniffer capture network traffic. Configuring the sniffer to record traffic that matches specified criteria should keep the volume of data manageable and minimize the inadvertent capture of other information. Because of privacy concerns, some organizations may require incident handlers to request and receive permission before using packet sniffers.

- **Filter the Data.** There is simply not enough time to review and analyze all the indicators; at minimum the most suspicious activity should be investigated. One effective strategy is to filter out categories of indicators that tend to be insignificant. Another filtering strategy is to show only the categories of indicators that are of the highest significance; however, this approach carries substantial risk because new malicious activity may not fall into one of the chosen indicator categories.

- **Seek Assistance from Others.** Occasionally, the team will be unable to determine the full cause and nature of an incident. If the team lacks sufficient information to contain and eradicate the incident, then it should consult with internal resources (e.g., information security staff) and external resources (e.g., US-CERT, other CSIRTs, contractors with incident response expertise). It is important to accurately determine the cause of each incident so that it can be fully contained and the exploited vulnerabilities can be mitigated to prevent similar incidents from occurring.

3.2.4 Incident Prioritization

Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, incidents can be prioritized by levels, such as the following:

Priority Level	**Description**	**Response Time**	**Action**
Critical(P1)	Incidents that cause severe business impact, affect critical systems, or involve sensitive data exposure	Immediate (15-30 minutes)	-Immediate executive notification -24/7 response team activation. - Potential system isolation - Consider external forensic support
High(P2)	Incidents with significant business impact, affecting multiple systems or departments	Within 1-2 hours	- Rapid containment - Escalate to security leads - Develop incident-specific strategy
Medium(P3)	Incidents with moderate business impact, affecting individual systems or limited scopeWithin 8	Within 8 hours	- Investigate during business hours - Document findings - Apply standard remediation - Monitor for escalation
Low(P4)	Incidents with minimal business impact, routine security events	Within 24-48 hours	- Standard operating procedures - Add to security metrics - Schedule remediation - Consider for training topics

3.2.5 Incident Notification

When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals so that all who need to be involved will play their roles. Incident response policies should include provisions concerning incident reporting—at a minimum, what must be reported to whom and at what times (e.g., initial notification, regular status updates). The exact reporting requirements vary among organizations, but parties that are typically notified include:

- CIO
- Head of information security
- Local information security officer
- Other incident response teams within the organization
- External incident response teams (if appropriate)
- System owner
- Human resources (for cases involving employees, such as harassment through email)
- 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; see Section 2.3.4.3)
- Law enforcement (if appropriate)
- During incident handling, the team may need to provide status updates to certain parties, even in some cases the entire organization. The team should plan and prepare several communication methods, including out-of-band methods (e.g., in person, paper), and select the methods that are appropriate for a particular incident. Possible communication methods include:
- Email
- Website (internal, external, or portal)
- 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; use the help desk's voice mail greeting)
- Paper (e.g., post notices on bulletin boards and doors, hand out notices at all entrance points).

3.3 Containment, Eradication, and Recovery

3.3.1 Choosing a Containment Strategy

Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly.

Criteria for determining the 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., partial containment, full containment)
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

3.3.2 Evidence Gathering and Handling

Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal proceedings.[42] In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved.[43] Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court.[44] In addition, evidence should be accounted for at all times; whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log should be kept for all evidence, including the following:

- Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses 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.

3.3.3 Identifying the Attacking Hosts

During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts. Although this information can be important, incident handlers should generally stay focused on containment, eradication, and recovery. Identifying an attacking host can be a time-consuming and futile process that can prevent a team from achieving its primary goal—minimizing the business impact. The following items describe the most commonly performed activities for attacking host identification:

- **Validating the Attacking Host's IP Address.** New incident handlers often focus on the attacking host's IP address. The handler may attempt to validate that the address was not spoofed by verifying connectivity to it; however, this simply indicates that a host at that address does or does not respond to the requests. A failure to respond does not mean the address is not real—for example, a host may be configured to ignore pings and traceroutes. Also, the attacker may have received a dynamic address that has already been reassigned to someone else.

- **Researching the Attacking Host through Search Engines.** Performing an Internet search using the apparent source IP address of an attack may lead to more information on the attack—for example, a mailing list message regarding a similar attack.

- **Using Incident Databases.** Several groups collect and consolidate incident data from various organizations into incident databases. This information sharing may take place in many forms, such as trackers and real-time blacklists. The organization can also check its own knowledge base or issue tracking system for related activity.

- **Monitoring Possible Attacker Communication Channels.** Incident handlers can monitor communication channels that may be used by an attacking host. For example, many bots use IRC as their primary means of communication. Also, attackers may congregate on certain IRC channels to brag about their compromises and share information. However, incident handlers should treat any such information that they acquire only as a potential lead, not as fact.

3.3.4 Eradication and Recovery

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities 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 rulesets, boundary router access control lists). Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.

3.4 Post-Incident Activity

3.4.1 Lessons Learned

One of the most important parts of incident response is also the most often omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. Holding a “lessons learned” meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself. Multiple incidents can be covered in a single lessons learned meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident. Questions to be answered in the meeting include:

3.4.2 Using Collected Incident Data

Lessons learned activities should produce a set of objective and subjective data regarding each incident. Over time, the collected incident data should be useful in several capacities. The data, particularly the total hours of involvement and the cost, may be used to justify additional funding of the incident response team. A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends. This data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls.

Possible metrics for incident-related data include:

- **Number of Incidents Handled.**
- **Time Per Incident.**
- **Objective analysis .**
- **Subjective Assessment of Each Incident**

3.4.3 Evidence Retention

Organizations should establish policy for how long evidence from an incident should be retained. Most organizations choose to retain all evidence for months or years after the incident ends. The following factors should be considered during the policy creation:

- **Prosecution.** If it is possible that the attacker will be prosecuted, evidence may need to be retained until all legal actions have been completed. In some cases, this may take several years. Furthermore, evidence that seems insignificant now may become more important in the future. For example, if an attacker is able to use knowledge gathered in one attack to perform a more severe attack later, evidence from the first attack may be key to explaining how the second attack was accomplished.

- **Data Retention.** Most organizations have data retention policies that state how long certain types of data may be kept. For example, an organization may state that email messages should be retained for only 180 days. If a disk image contains thousands of emails, the organization may not want the image to be kept for more than 180 days unless it is absolutely necessary.

- **Cost.** Original hardware (e.g., hard drives, compromised systems) that is stored as evidence, as well as hard drives and removable media that are used to hold disk images, are generally individually inexpensive. However, if an organization stores many such components for years, the cost can be substantial. The organization also must retain functional computers that can use the stored hardware and media.

3.4.4 Incident Handling Checklist

The checklist in Table 3-5 provides the major steps to be performed in the handling of an incident. Note that the actual steps performed may vary based on the type of incident and the nature of individual incidents. For example, if the handler knows exactly what has happened based on analysis of indicators (Step 1.1), there may be no need to perform Steps 1.2 or 1.3 to further research the activity. The checklist provides guidelines to handlers on the major steps that should be performed; it does not dictate the exact sequence of steps that should always be followed.

Table 3-5. Incident Handling Checklist

Action		Completed
Detection and Analysis		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

4. Coordination and Information Sharing

4.1 Coordination

An organization may need to interact with several types of external organizations in the course of conducting incident response activities. Examples of these organizations include other incident response teams, law enforcement agencies, Internet service providers, and constituents and customers. An organization's incident response team should plan its incident coordination with those parties before incidents occur to ensure that all parties know their roles and that effective line of communication are established. Organizations may find it challenging to build the relationships needed for coordination. Good places to start building a community include the industry sector that the organization belongs to and the geographic region where the organization operates. An organization's incident response team can try to form relationships with other teams (at the team-to-team level) within its own industry sector and region, or join established bodies within the industry sector that already facilitate information sharing. Another consideration for building relationships is that some relationships are mandatory and others voluntary; for example, team-to-coordinating team relationships are often mandatory, while team-to-team relationships are usually voluntary. Organizations pursue voluntary relationships because they fulfill mutual self- interests. Mandatory relationships are usually defined by a regulatory body within the industry or by another entity.

4.2 Information Sharing Techniques

Information sharing is a key element of enabling coordination across organizations. Even the smallest organizations need to be able to share incident information with peers and partners in order to deal with many incidents effectively. Organizations should perform such information sharing throughout the incident response life cycle and not wait until an incident has been fully resolved before sharing details of it with others. Section 4.3 discusses the types of incident information that organizations may or may not want to share with others.

This section focuses on techniques for information sharing. Section 4.2.1 looks at ad hoc methods, while Section 4.2.2 examines partially automated methods. Finally, Section 4.2.3 discusses security considerations related to information sharing.

4.2.1 Ad Hoc

Most incident information sharing has traditionally occurred through ad hoc methods, such as email, instant messaging clients, and phone. Ad hoc information sharing mechanisms normally rely on an individual employee’s connections with employees in incident response teams of partner organizations. The employee uses these connections to manually share information with peers and coordinate with them to construct strategies for responding to an incident. Depending on the size of the organization, these ad hoc techniques may be the most cost-effective way of sharing information with partner organizations.

4.2.2 Partially Automated

Organizations should attempt to automate as much of the information sharing process as possible to make cross-organizational coordination efficient and cost effective. In reality, it will not be possible to fully automate the sharing of all incident information, nor will it be desirable due to security and trust considerations. Organizations should attempt to achieve a balance of automated information sharing overlaid with human-centric processes for managing the information flow.

When engineering automated information sharing solutions, organizations should first consider what types of information they will communicate with partners. The organization may want to construct a formal data dictionary enumerating all entities and relationships between entities that they will wish to share. Once the organization understands the types of information they will share, it is necessary to construct formal, machine-processable models to capture this information.

4.2.3 Security Considerations

There are several security considerations that incident response teams should consider when planning their information sharing. One is being able to designate who can see which pieces of incident information (e.g., protection of sensitive information). It may also be necessary to perform data sanitization or scrubbing to remove sensitive pieces of data from the incident information without disturbing the information on precursors, indicators, and other technical information. The incident response team should also ensure that the necessary measures are taken to protect information shared with the team by other organizations.

4.3 Granular Information Sharing

Organizations need to balance the benefits of information sharing with the drawbacks of sharing sensitive information, ideally sharing the necessary information and only the necessary information with the appropriate parties. Organizations can think of their incident information as being comprised of two types of information: business impact and technical. Business impact information is often shared in the context of a team-to-coordinating-team relationship as defined in Section 4.1.1, while technical information is often shared within all three types of coordination relationships. This section discusses both types of information and provides recommendations for performing granular information sharing.

4.3.1 Business Impact Information

Business impact information involves how the incident is affecting the organization in terms of mission impact, financial impact, etc. Such information, at least at a summary level, is often reported to higher level coordinating incident response teams to communicate an estimate of the damage caused by the incident. Business impact information is only useful for reporting to organizations that have some interest in ensuring the mission of the organization experiencing the incident. In many cases, incident response teams should avoid sharing business impact information with outside organizations unless there is a clear value proposition or formal reporting requirements.

4.3.2. Technical Information

There are many different types of technical indicators signifying the occurrence of an incident within an organization. These indicators originate from the variety of technical information associated with incidents, such as the hostnames and IP addresses of attacking hosts, samples of malware, precursors and indicators of similar incidents, and types of vulnerabilities exploited in an incident. Section 3.2.2 provides an overview of how organizations should collect and utilize these indicators to help identify an incident that is in progress. In addition, Section 3.2.3 provides a listing of common sources of incident indicator data. Technical indicator data is useful when it allows an organization to identify an actual incident. However, not all indicator data received from external sources will pertain to the organization receiving it. In some cases, this external data will generate false positives within the receiving organization's network and may cause resources to be spent on nonexistent problems.

Appendix A. **Situation update** (template)

DATE OF ENTRY:	**TIME OF ENTRY:**	**AUTHOR:**
DATE AND TIME INCIDENT DETECTED		
CURRENT STATUS	New / In Progress / Resolved	
INCIDENT TYPE		
INCIDENT CLASSIFICATION	Incident / Significant Incident / Emergency	
SCOPE – list the affected affected networks, systems and/or applications; highlight any change to scope since the previous log entry		
IMPACT – list the affected stakeholder(s); highlight any change in impact since the previous log entry		
SEVERITY – outline the impact of the incident on the stakeholder(s); highlight any change to severity since the previous log entry		
NOTIICATIONS ACTIONED/PENDING		
ADDITIONAL NOTES		
CONTACT DETAILS FOR INCIDENT MANAGER		
DATE AND TIME OF NEXT UPDATE		

Appendix B. **Resolution action plan** (template)

DATE AND TIME	**CATEGORY** (Contain / Eradicate / Recover / Communications)	**ACTION**	**ACTION OWNER**	**STATUS** (Unallocated / In Progress / Closed)

Appendix C. **Evidence register** (template)

DATE, TIME AND LOCATION OF COLLECTION	**COLLECTED BY** (name, title, contact and phone number)	**ITEM DETAILS** (quantity, serial number, model number, hostname, media access control (mac) address, and ip addresses)	**STORAGE LOCATION AND LABEL NUMBER**	**ACCESS –** date, time, person and rationale for access after collection

Appendix D. **Assets and key contacts** (template)

SITE INFORMATION

IP SUBNET	
DHCP SCOPE	
CORE ROUTER IP	
DNS SERVERS (INTERNAL) / LOGS & LOCATIONS	
DNS NAME / LOGS & LOCATION	
SECONDARY DNS NAME (EXTERNAL)	

INTERNET CONNECTION / COMMUNICATIONS

INTERNET SERVICE PROVIDERS IP & CONNECTION DETAILS	
NETWORK PROVIDER IP & CONNECTION DETAILS	
VOIP / PABX PHONE SYSTEM DETAILS IPs & NUMBER RANGE	
FIXED LINE SERVICES & HARDWARE	
3G/4G MOBILE DATA SERVICES & HARDWARE	
SATELLITE PHONE SERVICES & HARDWARE	
SINGLE POINT OF FAILURE ANALYSIS – COMMUNICATIONS INFRASTRUCTURE	

FIREWALL & SECURITY

FIREWALL SOFTWARE / HARDWARE	
WIRED NETWORK	
WIRELESS NETWORK	
SINGLE POINT OF FAILURE – FIREWALL INFRASTRUCTURE	

SITE REMOTE ACCESS

REMOTE ACCESS METHODS / LOGS & LOCATIONS	
SINGLE POINT OF FAILURE ANALYSIS – REMOTE ACCESS INFRASTRUCTURE	

WIRED NETWORK SWITCH INFRASTRUCTURE

HARDWARE / FIRMWARE / LOGS & LOCATIONS	
SINGLE POINT OF FAILURE ANALYSIS	

WIRELESS NETWORK SWITCH INFRASTRUCTURE

HARDWARE / FIRMWARE / LOGS & LOCATIONS	
SINGLE POINT OF FAILURE ANALYSIS	

INDUSTRIAL CONTROL SYSTEMS / SCADA INFRASTRUCTURE

SCADA PLC RTU HARDWARE / FIRMWARE / LOGS & LOCATIONS	
AUTHENTICATION METHODS & CONTROLS	
FUNCTIONAL ANALYSIS	
PROCESS FLOW DIAGRAM	
CONFIGURATION BACKUP SCHEDULE / LOCATIONS	
ALERT / ALARM SYSTEMS & THRESHOLDS	
SINGLE POINT OF FAILURE ANALYSIS	

DATA BACKUP

BACKUP SOFTWARE	
BACKUP LOCATION & RESTORATION TIMEFRAMES	
DATA RETENTION REQUIREMENTS	

DISASTER RECOVERY PLAN

IDENTIFIED HIGH AVAILABILITY? (YES / NO)	
REQUIRED UP TIME (%)	

REQUIRED RETURN TO OPERATION (Hrs)	

REDUNDANT POWER SUPPLY / UPS INFRASTRUCTURE

UPS HARDWARE / LOCATION	
BATTERY CAPACITY / RUN TIME	
CONNECTED DEVICES	

REDUNDANT POWER SUPPLY / GENERATOR INFRASTRUCTURE

GENERATOR HARDWARE / LOCATION	
FIXED OR PORTABLE	
CAPACITY (KVA)	
FUEL TYPE / CAPACITY (L)	
FUEL CONSUMPTION (L/Hr)	
ON SITE FUEL STORAGE (L) & LOCATIONS	
FUEL SUPPLY ARRANGEMENTS / AGREEMENTS	
DOCUMENTED FAIL OVER / RESTORATION OF SERVICES.	

ADMINISTRATION SYSTEMS (Supporting ICT systems)

WEB PROXY SERVER DETAILS / LOGS & LOCATIONS	
DOMAIN CONTROLLER DETAILS / LOGS & LOCATIONS	
WEB SERVER DETAILS / LOGS & LOCATIONS	
SERVER ENVIRONMENT OPERATING SYSTEM DETAILS / LOGS & LOCATIONS	
VIRTUAL SERVER HOST ENVIRONMENT DETAILS / LOGS & LOCATIONS	

EMAIL SYSTEMS

EMAIL SERVER DETAILS / LOGS & LOCATIONS	

DATABASE SYSTEMS

SERVER DETAILS / LOGS & LOCATIONS	
PRODUCTION DATABASE DETAILS / LOGS & LOCATIONS	
TEST DATABASE DETAILS / LOGS & LOCATIONS	

CLOUD SERVICE PROVIDERS

HOSTED SERVICE PROVIDERS & SLAs	

STAFF DESKTOP / LAPTOP / TABLET SYSTEMS

CLIENT ENVIRONMENT OS / LOGS & LOCATIONS	
CLIENT HARDWARE MANUFACTURER / MODEL	

Appendix E - Glossary

- **Baselining:** Monitoring resources to determine typical utilization patterns so that significant deviations can be detected.
- **Computer Security Incident:** See “incident.”
- **Computer Security Incident Response Team (CSIRT):** A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).
- **Event:** Any observable occurrence in a network or system.
- **False Positive:** An alert that incorrectly indicates that malicious activity is occurring.
- **Incident:** A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
- **Incident Handling:** The mitigation of violations of security policies and recommended practices.
- **Incident Response:** See “incident handling.”
- **Indicator:** A sign that an incident may have occurred or may be currently occurring.
- **Intrusion Detection and Prevention System (IDPS)**: Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.
- **Malware:** A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.
- **Precursor:** A sign that an attacker may be preparing to cause an incident.
- **Profiling:** Measuring the characteristics of expected activity so that changes to it can be more easily identified.
- **Signature:** A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.
- **Social Engineering:** An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.
- **Threat:** The potential source of an adverse event.
- **Vulnerability:** A weakness in a system, application, or network that is subject to exploitation or misuse.