Standard Operating Procedure

for

Incident Coordination

Prepared by: Melissa A. Grohman | 832-372-5719

1.0 Introduction

1.1 Authority

This document is the result of research of publicly available documentation and consultation with experts. It is not intended to be conclusive or authoritative, only to map out the process, as understood by the writer, for coordinating computer security incident responses.

1.2 Purpose and Scope

The purpose of this document is to describe in writing the process an incident coordinator follows to ensure full-circle management of incident responses. It is not intended to delve into the procedures at each point of the process, which are covered by their own process documents and standard operating procedures.

1.3 Document Structure

This document will be structured to reflect its adherence to the process outlined in the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide.[1] Other resources used significantly in this document will be referenced in footnotes where relevant.

1.4 Assumptions

For the purpose of this document, it is assumed that robust standard operating procedures (SOPs) exist to cover the detailed processes and procedures required for the containment, eradication, and recovery phases of incident handling. The procedures used in these processes depend heavily on the incident type and to some extent, its priority. As with the NIST, this process assumes operation from an "overview" perspective.

In addition, it is understood that while the incident coordination process is presented sequentially in this and external governing documents, the phases run concurrently and cyclically. Therefore, phase instructions might seem redundant or contradictory.

2.0 Organizing for the Coordination Process

2.1 Education and Training

The incident coordinator should have a comprehensive understanding of the incident response process adequate to ensure that no critical steps or activities in the process are overlooked. The coordinator must be extremely organized and disciplined and must be able to communicate clearly and effectively at all levels of the organization. In addition, the coordinator must receive organizational training sufficient to

[1] NIST 800-61, Rev. 2, *Computer Security Incident Handling Guide*, http://dx.doi.org/10.6028/NIST.SP.800-61r2

understand how the broad, internal processes interact at the corporate level. Finally, the incident coordinator should be able to validate escalated alerts with very high reliability.

2.2 Authority for Actions

Because the coordinator will drive the response process, an amount of authority must be conferred on her/him to ensure timely and thorough response from all members of all teams.

2.3 Tools and Communication

The coordinator should have an up-to-date roster of all Incident Response Team (IRT) members and an understanding of each member's context and role in the organization. This ensures efficient communication during incidents. In addition, the coordinator should have access to a simple database in which to document alerts, resolutions, and actions taken at each step (e.g., Incident Management System [IMS]).

2.4 Process Inputs and Suppliers

All alerts and detections are first reviewed by the Security Operations Center (SOC). Those that are considered an incident or are at risk of becoming an incident are escalated to the IRT, the first point of contact for which is the Incident Coordinator.

3.0 Incident Coordination

3.1 Preparation

Preparation is a constant state. Being prepared for an incident at any moment assumes that communication plans are in place; an IMS is in use; and correct policies and procedures are in place both to govern the incident handling process and to ensure that security best practices are understood and implemented company-wide. In addition, the overall incident response process must be well-documented and understood throughout the security organization.

3.1.1 Communication

Adequate preparation requires a thorough communication plan. It has a documented internal interaction matrix (whom to call and when) that includes all contact information for team members. It includes a basic guideline for when to involve legal and investigative forensics teams during an incident. It requires a communication plan specific to each major incident, including a plan for status updates to incident targets.

3.1.2 Incident Documentation

Aside from the documentation created by incident responders throughout the process, the organization should have a "master" repository that permanently houses records of investigations. These records and team reports will be used to generate lessons learned and the final incident report.

3.1.3 Policies

Policies should be in place within the security organization to streamline the investigation process. These include regularly profiling use patterns to understand the baseline of normal behavior, performing risk assessments, and maintaining a network diagram and lists of critical assets.

In addition, the company must implement organization-wide security policies for prevention, such as training on major attack vectors to increase awareness and for profiling, such as log retention policies.

3.2 Detection and Analysis

3.2.1 Incident Alert and Confirmation

The incident coordination process is initiated with an incoming alert from the SOC, which has responsibility to review and classify alerts from all sources, including intrusion detection systems (IDSs) and security appliances. After review, these alerts are classified as either an event or an accident, according to Table 1, *Categories of Events (0, 3, 5, 6, 8, and 9) and Incidents (1, 2, 4, and 7)*. Alerts categorized as incidents are escalated to the IRT.

When the incident coordinator receives an escalation from the SOC, he or she begins by evaluating the validity of the escalation. This allows the coordinator to shield the IRT from unnecessary escalations in order for the team to maintain its prioritized workload.

Table 1: Categories of Events (0, 3, 5, 6, 8, and 9) and Incidents (1, 2, 4, and 7). [2]

Category	Description
0	Training and Exercises (Event): Operations performed for training purposes and support to Combatant Command/Service/Agency/Field Activity (CC/S/A/FA) exercises.
1	Root-Level Intrusion (Incident): Privileged access, often referred to as administrative or root access, provides unrestricted access to an IS. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If this IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
2	User-Level Intrusion (Incident): Unauthorized non-privileged access to an IS. Non-privileged access, often referred to as user-level access, provides restricted access to the IS based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
3	Unsuccessful Activity Attempt (Event): Deliberate attempts to gain unauthorized access to an IS that are defeated by normal defensive mechanisms. Attacker fails to gain access to the IS (i.e., attacker attempts valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Note the above CAT 3 explanation does not cover the “run-of-the-mill” virus that is defeated/deleted by AV software. “Run-of-the-mill” viruses that are defeated/deleted by AV software are not reportable events or incidents and should not be annotated in the Joint Information Management System (JIMS).
4	Denial of Service (Incident): Activity that denies, degrades, or disrupts normal functionality of an IS or DoD information

[2] Air Force Instruction (AFI) 17-203, *Cyber Incident Handling*, Table 1.1.

	network.
5	Non-Complianc Activity (Event): Activity that potentially exposes ISs or networks to increased risk as a result of the action or inaction of authorized users. This includes administrative and user actions such as failure to apply security patches, connections across security domains, installation of vulnerable applications, and other breaches of existing AF or DoD policy.
6	Reconnaissance (Event): Activity that seeks to gather information used to characterize ISs, applications, DoD information networks, and users that may be useful in formulating an attack. This includes activity such as mapping DoD information networks, IS devices and applications, interconnectivity, and their users or reporting structure. This activity does not directly result in a compromise.
7	Malicious Logic (Incident): Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This only includes malicious code that does not provide remote interactive control of the compromised IS. Malicious code that has allowed interactive access should be categorized as Category 1 or Category 2 incidents, not Category 7. Interactive active access may include automated tools that establish an open channel of communications to and/or from an IS. Unless otherwise directed, only those computers that were infected will be reported as a Category 7 incident.
8	Investigating (Event): Events that are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing, further review. No event will be closed out as a Category 8. Category 8 will be recategorized to appropriate Category 1-7 or 9 prior to closure.
9	Explained Anomaly (Event): Suspicious events that, after further investigation, are determined to be non-malicious activity and do not fit the criteria for any other categories. This includes events such as system malfunctions and false alarms. When reporting these events, clearly specify the reason for which it cannot be otherwise categorized.

3.2.2 Incident Alert Validation

In order to perform incident validation, the coordinator must understand the most common attack vectors, recognize major incident indicators, and be capable of reviewing and understanding the major sources of those indicators.

Major attack vectors are outlined in detail in NIST 600-81, Rev. 2, *Computer Security Incident Handling Guide,* Section 3.2.1, Attack Vectors. In addition to those outlined in the referenced document, coordinators should be familiar with and understand the following attacks:

- **Drive-by download:** Drive-by downloads are a form of social engineering. Usually, a compromised website will notify the user that a certain plug-in or application (such as Java) is missing, and content cannot be displayed without downloading and installing it.
- **Watering hole (online):** An attacker finds online locations where a target company's employees are known to congregate and share information online, then creates a look-alike, similarly named site designed to steal information from users who accidentally enter the look-alike web address.
- **Credential phishing:** Websites that attackers create to mimic legitimate websites (much like a watering hole attack) where the goal is to steal user information, especially user credentials that provide access to the network.
- **Fake technical support:** A site is created to look like an internal error page (similar web address, corporate template applied) with a phone number to call for technical support. Users who call the number reach the attacker rather than technical support, who then mines the user for information.

NIST 600-81, Rev. 2 distinguishes between precursors and indicators. Because precursors would be tracked by threat intelligence or malware analysis organizations, this document will focus on indicators:

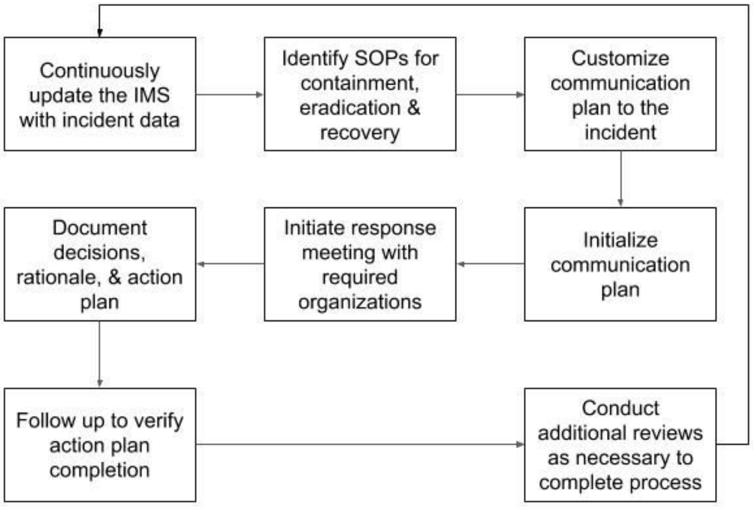
"signs that an incident may (*sic*) have occurred or may (*sic*) be underway."[3] The coordinator evaluates the escalated alert, looking for information such as:

- **Headers:** Look for evidence of spoofing and source information (for e-mails and web traffic)
- **Attachments:** Determine whether the attachment is an executable
- **Log entries:** Look for OS, service, network device, and application logs and evaluate access attempts, configuration changes, etc.
- **Network flows:** Evaluate communication sessions between the hosts in question in the alert to look for unusual activity.

With this basic information gathered, the coordinator must correlate across data types gathered to determine the validity of the escalated alert. This is a judgment call, and it should not be made in a vacuum. The incident coordinator should call on the expertise of security analysts in the organization for final confirmation when uncertain.

If the alert is deemed to be a valid incident, the coordinator initiates the formal incident coordination process as follows:

1. Update the IMS to indicate the incident type and priority
2. Identify the appropriate SOPs to user for the containment, eradication, and recovery phases
3. Customize communication plan for the incident in question
4. Initiate communication plan
5. Initiate meeting with all required organizations
6. Document decisions, rationale, and forward action plan to resolve the incident
7. Follow up with responsible parties to document action closure
8. Continuously update IMS
9. Initiate additional meetings as necessary to ensure completion of the incident response process.


Continuously update the IMS with incident data
Identify SOPs for containment, eradication & recovery
Customize communication plan to the incident
Initialize communication plan
Initiate response meeting with required organizations
Document decisions, rationale, & action plan
Follow up to verify action plan completion
Conduct additional reviews as necessary to complete process

[3] NIST 600-81 Rev. 2, *Computer Security Incident Handling Guide*. Section 3.2.2, "Signs of an Incident."

3.2.3 Incident Prioritization

Incidents shall be prioritized in accordance with NIST 800-61, Rev. 2, section 3.2.6, Incident Prioritization. This method considers the functional and informational impacts of the incident in conjunction with its recoverability. The referenced document provides rating tables for each component of the priority assignment.

The final priority assigned will require the coordinator to proactively assess the incident's priority relative to all open incidents to ensure that the highest priority incidents are resolved first.

3.2.4 Incident Notification

As a part of the preparation phase of incident handling, a communication plan should already exist. The coordinator uses this plan to tailor a communication plan for each major incident. The tailored plan addresses:

- Internal organizations to be involved and level of detail to be provided
- External organizations to be involved and level of detail to be provided
- Management
- The need (or lack thereof) for the legal discovery team's involvement
- The need (or lack thereof) for law enforcement
- System owner(s)
- Human resources
- Public affairs
- Method of communication for each

3.3 Containment

3.3.1 Containment Process

Specific actions to be taken during the containment phase are dependent on the incident type and severity; therefore, they cannot be fully addressed in a high-level process document. Instead, the coordinator refers to SOPs for the type of incident in question, and ensures that procedure is followed.

There are three high-level components of the containment phase: short-term containment, system backup, and long-term containment.[4]

3.3.2 Major Containment Components

Short-term containment seeks to limit damage to systems and the organization as quickly as possible. It is not intended to resolve the incident, only to ensure that the organization is as protected as possible while the security team investigates and resolves the issue.

System backup likely has been completed during the information gathering phase, but if it has not been completed, it should be done at this point. Required information includes:

- Forensic image of RAM

[4] Kral, Patrick. SANS Institute InfoSec Reading Room, *Incident Handler's Handbook*, Section 4, "Containment."

- A copy of the NTFS Master File Table (MFT)
- A copy of the user profile
- All event logs (in order to build a timeline)

Finally, long-term containment seeks to allow the user or system to return to normal operations during the investigation.

3.4 Eradication and Recovery

The eradication and recovery phases focus on restoring systems and devices to eliminate the components of the incident. In order to do this, the incident team should refer to applicable SOPs. At a minimum, the team should identify all affected hosts within the organization, remediate the incident, and restore systems to normal operations. Specific actions might include (but certainly aren't limited to):

- Restoring systems from clean backups
- Rebuilding systems from scratch
- Replacing compromised files with "clean" versions
- Installing patches
- Changing passwords
- Tightening network perimeter security
- Heightening system logging or network monitoring

Recovery and restoration activities should be verified as effective and complete, and all systems should be tested before placing them back into operation and production. During these steps, copious documentation should point to lessons learned and long term configuration, policy, and process changes to prevent, to the extent possible, a recurrence of the incident.

3.5 Lessons Learned and Continuous Improvement

3.5.1 Lessons Learned

The lessons learned process begins with the findings of the IRT during the information and analysis, containment, eradication, and recovery phases of the incident response process. The incident coordinator collects and documents these findings throughout the process. Many of them, such as the development of new IDS signatures will be implemented long before the formal lessons learned review.

The formal review addresses changes already implemented and their immediate effectiveness; changes proposed or in development; and the need for changes not already identified. These reviews might result in a long-term action plan; the changes needed might not be within the authority of the security team. In general, in addition to the changes identified during the response, the review should address the following (not all-inclusive) list:

- How well did staff and management perform in dealing with the incident? Were procedures followed? If not, why, and what changes need to be made?
- What information was needed sooner?
- Were any of the actions taken detrimental to the overall recovery?
- What would staff and management change if it happened again?
- Was information sharing with other organizations adequate? Why or why not?

- What corrective actions are necessary to prevent similar incidents?
- Were there precursors that security can watch for in the future?
- Are additional tools or resources needed to detect, analyze, and mitigate future incidents?
- What is the quantifiable monetary damage from the incident (addressed in the cost of response and the cost of any loss of data or customer)[5]

Following the formal review, the coordinator works with the IRT to develop a formal report on the incident. The report should cover, at a minimum:

- A timeline of the incident, including time of discovery and detection method
- The scope of the incident: impacted systems and organization, costs incurred
- How it was contained and eradicated
- Work performed during recovery
- Areas of effectiveness and areas for improvement[6]
- Formal, prioritized recommendations from the lessons learned review

3.5.2 Continuous Process Improvement

The primary function of the lessons learned phase is to prevent future similar attacks; however, the secondary function is almost as important because it drives internal improvements that should help to improve detection, mitigation, and recovery.

Continuous process improvement uses the data gathered from multiple incidents over time to pinpoint areas for improvement in the incident response process. This data can reveal:

- Systemic security weaknesses and threats
- Changes in incident trends
- Information to impact risk assessments
- Effectiveness of the IRT
- Effectiveness of changes to IRT procedures (such as improvements for efficiency or cost reductions)

It's tempting to collect and look for trends in all data possible; however, the best data will point to specific actions. Examples of useful data to track are:

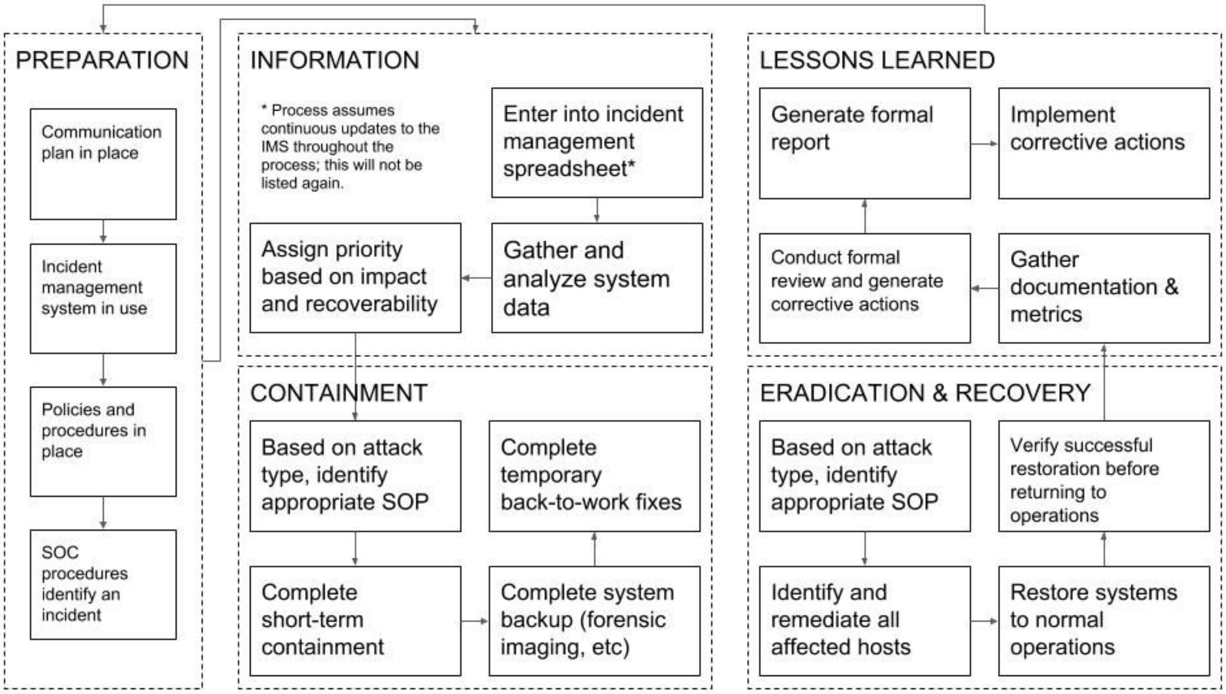
- Number of incidents per type handled over time
- Time per incident
  - Total labor
  - Time per phase, including time to discovery
  - Initial response time
  - Reporting time
- Assessment of performance
  - Adherence to procedures (Does one procedure consistently get ignored? Why?)
  - Identification of precursors and indicators (How effective was logging and assessment?)
  - Damage caused before detection
  - Damage caused between detection and containment

[5] NIST 800-61, Rev. 2, *Computer Security Incident Handling Guide*, Section 3.4.1, "Lessons Learned."
[6] Kral, Patrick. SANS Institute InfoSec Reading Room, *Incident Handler's Handbook*, Section 7, "Lessons Learned."

  - Whether the incident is recurrent
  - Difference between initial and final impact assessments
- Subjective team performance ratings of the overall process
- Subjective performance rating from the incident “victim”

These data are collected and evaluated over time to identify necessary changes to processes and policy, thereby driving change in the preparation phase of the incident response process.

Appendix I Process Map


PREPARATION
Communication plan in place
Incident management system in use
Policies and procedures in place
SOC procedures identify an incident
INFORMATION
* Process assumes continuous updates to the IMS throughout the process; this will not be listed again.
Enter into incident management spreadsheet*
Gather and analyze system data
Assign priority based on impact and recoverability
CONTAINMENT
Based on attack type, identify appropriate SOP
Complete short-term containment
Complete system backup (forensic imaging, etc)
Complete temporary back-to-work fixes
ERADICATION & RECOVERY
Based on attack type, identify appropriate SOP
Identify and remediate all affected hosts
Restore systems to normal operations
Verify successful restoration before returning to operations
LESSONS LEARNED
Gather documentation & metrics
Conduct formal review and generate corrective actions
Generate formal report
Implement corrective actions