Incident Management and Response

Table of Contents

If you're currently dealing with a security incident, remember these four basic tips: 1) Don't panic. 2) Do a quick assessment. 3) Report the problem. 4) Determine a course of action.

Getting Started

No matter the extent of our defenses, it inevitable that Information Security Incidents will occur. For this reason establishing, periodically assessing, and continually improving incident management processes and capabilities is very important. If you are just getting started in this area of your security program, then the following areas are very useful stepping stones that are covered in this chapter:

1. **Define** what constitutes an information security incident and review how varied incidents can be classified.
2. **Consider** what constitutes an information security incident that requires special handling (vs. common security events). Review incident classification schemes that allow for aligning handling procedures to potential impacts and risks.
3. **Identify** and establish essential roles and procedures needed for effective incident management.
4. **Evaluate** the technical and operational capabilities of your organization to detect and respond to security incidents. Consider how senior management support can be gained to formalize effective incident management processes. Formulate procedures and workflow for effectively addressing incidents throughout their lifecycle (see HEISC Incident Checklist).
5. **Create** effective communication, coordination, and reporting plans for broad spectrum of incidents including data breach events.
6. **Identify** key partners and stakeholders and levels of communication and engagement. Review the legal and contractual communication requirements associated with data types that may be involved in Information Security Incidents. (see HEISC Data Incident Notification Toolkit).
7. **Adapt and learn** from security incidents and strive for continual improvement by identifying and planning for training needs and enhancement of response capabilities.

Top of page

Overview

Software complexity, near universal worldwide connectivity, and the criminals determined to profit from these factors, make information security incidents inevitable. The goal of an effective information security incident management strategy is a balance of driving the impact of the incidents down, while processing incidents as efficiently as possible. Good incident management will also help with the prevention of future incidents.

How this plays out is to develop a program that prepares for incidents. From a management perspective, it involves identification of resources needed for incident handling, as well as developing and communicating the formal detection and reporting processes. An effective security program includes important aspects of detecting, reporting, and responding to adverse security events as well as weaknesses which may lead to events, if they are not appropriately addressed. The primary elements of incident management are:

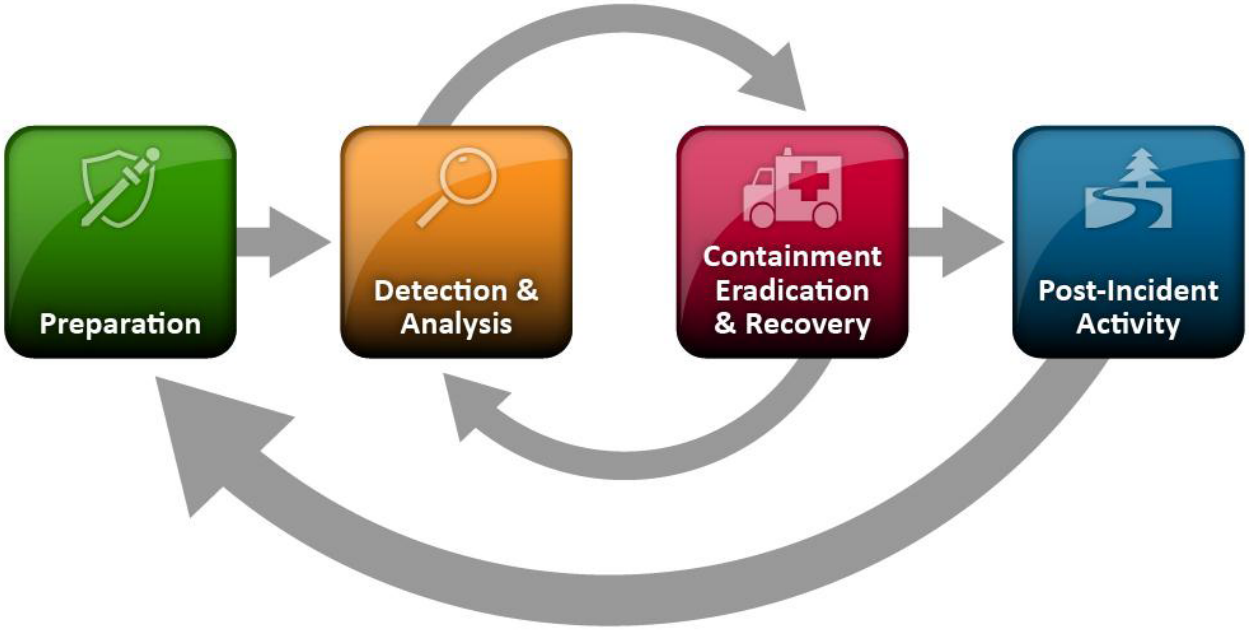
- **Preparation, Detection, and Reporting**
- **Security Incident Response and Process Improvement**

Effective incident response in many organizations other than IT, involve having trained personnel equipped and ready for response. So it is with information security incident management. Having trained individuals ready to respond with advance **preparation** is the first task. Designing an effective means of the detection of incidents is also essential (and this often consists of trained users and administrators, together with technical controls.) Effective, appropriate communication at all levels of an organization is essential for limiting the impact of security events, using formal **detection and reporting** processes. All members of the community should be trained and comfortable regarding procedures for reporting failures, weaknesses, and suspected incidents; methods to recognize and detect problems with security protections; as well as how to escalate reporting appropriately.

In addition, technical controls must be implemented for the automated detection of security events, coupled with as near real-time reporting as possible, to investigate and initiate immediate responses to problems. For new IT systems, often the best time to develop automated detection of security events is when the preventive security controls are being architected.

Confirmation of an adverse security event is an inevitable outcome in any organization. A formal management procedure and policy for **incident response**, including roles and responsibilities for each aspect of the response is essential. Aspects include funding and cost models, analysis, containment and recovery responsibilities, decision making authority for notifications; legal and/or law enforcement involvement; forensic investigations; responsibility for after-incident debriefing; and policy, procedure, and **process improvements**.

NIST, in their 800-61 Computer Security Incident Handling Guide, describes the "Incident Lifecycle" as:



Top of page

Management of Information Security Incidents and Improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

The reality of security incidents, breaches and loss of data has become all too familiar to a growing number of institutions and organizations. Efforts to be prepared need to be engaged prior to these episodes occurring through a comprehensive approach involving on premise, qualified team construction, vendor participation, appropriate insurance or retainers, and institutional counsel.

The best reaction to an information security incident is being proactive and the worst is proceeding without caution, expertise and proper guidance. If qualified personnel do not exist on staff, external assistance needs to be contracted and ready to employ. Without previous agreements even qualified vendors may have difficulties meeting your required timeline. Proceeding without consistent, fully-developed response plan can lead to lost evidence, data, and inability to verify loss and recovery leading to a false sense of containment and resolution of the event.

The incident management plan should be clear, concise describing the steps to be taken, resources utilized and their respective roles and the timelines under which the tasks are to be performed. The getting started section included articles, papers, presentation, sample policies flowcharts and checklists to help an organization get the process started. The remainder of this document provides resources and processes to help ensure that a proper and complete assessment, analysis, containment and response are in order.

Recommended resource: Cyber Liability Insurance FAQ (2015)

Top of page

Responsibilities and Procedures

Objective: Ensure personnel are trained and equipped to detect, report, and respond to adverse events, providing the foundation for effective Information Security Incident Management.

Preparation involves identification of resources needed for incident handling and having trained individuals ready to respond, and by developing and communicating a formal detection and reporting process. Effective, appropriate communication at all levels of an organization is essential for limiting the impact of security events. NIST suggests the following policy components:

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (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, to monitor suspicious activity, and the requirements for reporting certain types of incidents)
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact resources

An ECAR Research Bulletin titled "Information Technology Security Policy: Keys to Success" gives valuable insight on important elements of policy.

The SANS Reading Room also has a wealth of published white papers on the subject of Incident Handling.

Prioritization of incidents is an important element, as are escalation procedures. Interestingly, incident priorities differ between institutions depending on their culture and other policies, and there are certain types of incidents that one institution may tolerate while another may not. In addition, policies are required to outline permitted monitoring of system and network activities, and under what specific circumstances. It is also advisable to have policies that specify who can access data relating to an incident under what circumstances and what auditing is required to document the access. Separate policies should be considered describing the data retention of non-incident related log data and data preserved during investigation of an incident.

The State of Iowa Regents Universities collaboratively developed a guideline for retention of network and security log information, which can be considered when developing institutional guidelines. See Log Retention Guideline.

The term ***forensic*** is used to describe a characteristic of ***evidence that satisfies its suitability for admission as fact*** and its ability to persuade based on proof (or high statistical confidence). This applies to disciplinary hearings in an institutions as well as legal proceedings in court. Even when an incident will be handled internally by an institution and will not result in legal action, the associated digital evidence should be handled using the same principles as digital evidence that is destined for court. This evidence ***provides the foundation for conclusions and decisions*** relating to an incident. Weak evidence can lead to inaccurate conclusions and poor decisions that can cause more damage and liability than the incident itself. For instance, when an employee is fired as a result of an incident but claims that his/her dismissal was unfair or unfounded, improperly processed evidence can make it more difficult to justify the decision and defend against the unfair dismissal claims. This puts the institutions in a potentially costly situation if the employee sues.

Other guidelines instruct incident responders to preserve related digital evidence relating to computer crimes but discourage computer security professionals from examining that evidence themselves. This is an institutional decision, or it may be a legal issue. For example, it may be necessary for computer security professionals to perform some forensic examination and analysis to determine whether an incident is serious enough to report to law enforcement under the auspices of data breach notification laws. Ultimately, as long as digital evidence relating to an incident is properly preserved and you perform any examination or analysis work on a duplicate of the evidence to avoid altering the original, your efforts will not hinder law enforcement when they are needed.

Another important foundation for effective incident handling is to ***configure systems with evidence preservation in mind***. Forensic readiness can include creating a file system baseline to help detect changes, utilizing a central syslog server, maintaining network level logging at key control points on the network, and time synchronization using central NTP servers for systems that generate logs to sync to, all of which are useful for responding to incidents. A central syslog server and network activity logs (for example, network flow records, firewall logs) are generally more reliable than logs stored on a compromised system, particularly if the intruder had the ability to alter or potentially destroy the local logs. Central authentication servers (for example, RADIUS, Kerberos, Microsoft Active Directory) can also be useful when responding to certain incidents, and some institutions regularly dump ARP tables from switches and routers to help detect and respond to device problems on their network. Whatever types of data an institution decides to maintain, keeping system clocks synchronized to a central time source makes it easier to correlate data from multiple systems.

Once you have decided what types of data you are going to maintain, it is prudent to take steps to preserve their integrity and document their location, format, and any other associated details. A simple hash algorithm such as MD5 can be used to document the integrity of log files. By routinely rotating log files and calculating their MD5 values, you can recalculate their hash values later to demonstrate that they were not altered since they were created. Documenting the location of important data sources, and outlining how these data can be accessed and interpreted, will help use the data efficiently when necessary. Marking the location of important data sources on a network topology map is a useful way to summarize this information graphically, facilitating evidence gathering during high pressure incidents. This type of graphical view of data sources on a network can also be useful for finding gaps in coverage and developing better approaches to monitoring system activities and preserving existing data.

In addition to preparing data sources for incidents, it is also important to be operationally prepared for incidents. This involves purchasing the necessary equipment, and training at least one individual to handle to incidents and use tools for recovering and examining data.

- Are you Ready? A Planning Tool for Managing Sensitive Data Incidents - EDUCAUSE Security Professionals Conference 2012
- Data Breach Notification: Discussing Reactive Processes and Proactive Strategies - EDUCAUSE Security Professionals Conference 2011
- Cyber Liability Insurance FAQ (2015)

Training: The SANS (SysAdmin, Audit, Network, Security) Institute is a premier cooperative research and education organization, providing information security training programs in a number of formats. Two relevant courses for Information Security Incident Management are:

- Hacker Techniques, Exploits, and Incident Handling (Security 504)
- Incident Response Management (Management 535)

Reporting Information Security Events

Detection and Reporting

Designing an effective means of the detection of incidents is also essential, using both trained users and trained system administrators, and various technical controls. All members of the community should be trained and comfortable regarding

- procedures for reporting failures, weaknesses, and suspected incidents
- methods to recognize and detect problems with security protections
- how to escalate reporting appropriately

In addition, technical controls must be implemented for the automated detection of security events, coupled with as near real-time reporting as possible, to investigate and initiate immediate responses to problems. For new IT systems, often the best time to develop automated detection of security events is when the preventive security controls are being developed and implemented.

The most fundamental approaches to detecting intrusions are to monitor server logs for signs of unauthorized access, to monitor firewall or router logs for abnormal events, and to monitor network performance for spikes in traffic. Since intruders can alter or destroy local logs, a best practice is to take the precaution of sending logs to a remote log server. This includes a combination of host-level and network-level detections, which when used together provide the most powerful system for detecting problems.

A frequently used tool for system level, or HIDS (Host Intrusion Detection System) log analysis, monitoring, and alerting is OSSEC, an open source solution that has a lot of flexibility. A recent presentation at EDUCAUSE Annual Security conference features one strategy and implementation:

- Using OSSEC for Intrusion Detection - EDUCAUSE Security Professionals Conference 2010

Identity Finder - University of Pennsylvania

Another example of a strategy to accomplish a combination of network and system level intrusion detection is the subject of another EDUCAUSE Security presentation:

- PaIRS IDS: Finding bad actors without looking at content - EDUCAUSE Security Professionals Conference 2011
- Malware Detection and Mitigation with Passive DNS and Blackhole DNS - EDUCAUSE Security Professionals Conference 2011

Reporting Information Security Weaknesses

Even if a college or university installs a network intrusion detection system or other monitoring systems, the resulting alerts can quickly overload personnel. An effective approach is to use analysis tools to help manage intrusion detection systems and summarize the data. Even when log summarization is used, maintaining and monitoring intrusion detection systems can require resources and technical skill that are beyond some institutions' means. A less expensive alternative to developing your own IDS capabilities is to collaborate with other higher education institutions, helping each other deploy intrusion detection systems and even having a single person monitoring all systems, or to contract for the service with your ISP.

Two major weaknesses of network IDS are that they cannot detect attacks in encrypted traffic and they cannot determine what is occurring within a targeted compromised host. Host-based intrusion detection systems (HIDS) can address both of these issues and can be used to monitor systems processes, file system changes, and log files for suspicious activities. Many commercial endpoint security offerings now include HIDS functionality, and servers can utilize open source monitoring tools. Communicating security alerts through an interface that system administrators use to monitor the status and performance of their systems increases the likelihood that they will notice problems quickly.

Top of page

Assessment of and Decision on Information Security Events

Objective: Build an effective, timely, repeatable methodology for managing information security incidents that meets legal requirements and is continually improved.

A formal management procedure and policy for incident response, including roles and responsibilities for each aspect of the response is essential. Aspects to document include funding and cost models; analysis, containment and recovery responsibilities; decision making authority for notifications; legal and/or law enforcement involvement; forensic investigations; responsibility for after-incident debriefing; and policy, procedure, and process improvements.

The primary goals of security incident response are to determine the cause and effect of incidents, including any sanctions which may be appropriate and any new preventive measures that may need to implemented, as well as to restore the affected infrastructure to an operational state in a timely manner.

The general activities, or stages to an effective response and improvement are described in the table below. Some may of necessity be serially processed and some may run as concurrent activities. For example, once an event has been identified, the prioritization and assessment may occur at the same time as containment for an active intrusion situation.

Stages:	**Activities:**
Identification and prioritization of incident, and performing a timely assessment of the situation	Determine the scope/impact. The number of users affected, or number of devices, or segments of the network should be considered. Is a single user or account involved?
	Assess the severity. What is the sensitivity of data involved? What is the criticality of the service, or system, or application? What is the potential for damage or liability? Is there potential for harm?
	Assess the urgency of the event. Is it an active problem, threat, or event-in-progress? Was the problem discovered after the fact? Is the intrusion "dormant", or completed? Does this involve use of an account rather than a system? Is this involve the safety or privacy of individuals?
Containment of the event	Does the system need to be removed from the network? Does active memory need to be imaged or captured?
	Are there user accounts or system-level accounts that need to be disabled or changed? Are there sessions that need to be dropped?
Investigation of what occurred and how (includes "root cause" analysis)	An incident tracking record needs to be created. If deemed necessary, due to the scope, seriousness, or complexity of the incident, an incident notes log should also be created.
	Gathering and preserving relevant information should be conducted by trained security personnel.
	Evaluation of evidence commences. It may be a "forensic" caliber assessment, or a less comprehensive analysis, depending on the type of incident and your institution's policies. Decisions with respect to the appropriate resolution and response should be discussed with decision makers and key stakeholders.
Response (effect)	Eradication of the problem, and associated changes to the system need to be applied. This includes technical actions such as operating system and application software installs, new or changed firewall rules, custom configurations applied, databases created, backup data restored, accounts created and access controls applied

	Recovery to a fully operational state always follows appropriate testing or assurance of the system integrity and stability. Effective customer service includes regular communications with stakeholders who may be anxious for recovery.
	Outcomes, including possible sanctions should be determined. Sanctions, if they are deemed appropriate to the response, may be internal, such as disciplinary action, or they may be external, such as referral to law enforcement.
Follow up (Improvements)	After incident debriefing. Its important to review the process and how it could have been better, after an incident is closed. This is especially valid for new types of incidents, and particularly severe or costly incidents.
	Consider policy and process changes. Were any procedures missing, communications unclear, or stakeholders that were not appropriately considered? Did the technical staff have appropriate resources (information as well as equipment) to perform the analysis and/or the recovery?
	Consider controls improvements, leading to prevention. What can we do to ensure this does not happen again? What improvements can we implement to make our response and recovery more timely?

Response to information security incidents

Incident Analysis and Forensics

In many cases, a more in-depth evaluation of the incident and circumstances is warranted. It may be to determine if confidential information was involved in, or stored on, the system in question. It may also to be an effort to determine the vulnerability or action that enabled the incident to occur. This is typically where a forensic evaluation comes into play.

Training: The SANS Institute is a premier cooperative research and education organization, providing information security training programs in a number of formats. This organization provides an entire track of training courses in the area of computer forensics, such as:

- Advanced Computer Forensic Analysis and Incident Response (Forensics 508)

Unfortunately, in some cases an incident will involve or expose confidential information, such as PII (personally identifiable information) that is protected by law, other policy, or local practices. When this occurs there is often some sort of requirement in response stage for notification to affected persons. The following toolkit has a number of resources to assist with notifications.

- When to Declare an Information Security Incident and How to Respond Once you do - EDUCAUSE Security Professionals conference 2013
- Data Incident Notification Toolkit
- Breaches and a Lawsuit: An Institutions Road to Recovery - EDUCAUSE Security Professionals Conference 2013
- Cyber Liability Insurance FAQ (2015)

Learning from Information Security Incidents

Metrics to Support Improvement

The purpose of metrics here are to identify the major causes and sources of incidents, to measure damage caused by incidents, and to observe trends in both. If metrics show that a particular vulnerability is causing the most losses, you may decide reconfigure the network to protect vulnerable systems and make an exerted effort to fix them. If an increasing number of attacks are coming through the VPN, you may decide to install a dedicated firewall and/or intrusion detection system to block these attacks. If metrics show that the total annual cost of incidents is increasing steadily, your institution may decide to devote more resources to preventative security measures.

Metrics may include the total incidents handled, time spent on incidents, the number of different types of incidents, and the number of Windows versus UNIX systems impacted. *It is not sufficient to just count the number of incidents because as your program improves, these increase.* Some useful incident measures to consider are:

- the number of detected but unsuccessful intrusion attempts to compare with the number of successful ones
- the damage/losses caused by disruptive incidents, to help develop plans for reducing outages and the staff hours spent responding to incidents
- reductions in downtime of the network or critical systems
- metrics for any special security initiatives such as alarms or monitoring of systems, to help in assessing their effectiveness

For more information, see the CIS Consensus Information Security Metrics initiative.

The EDUCAUSE Technologies, Operations, and Practices Working Group sponsored a Security Metrics initiative that resulted in the development of a toolkit with Security Metrics resources, featuring a recommended set of "starting metrics" in the areas of compliance, incidents, operations, and executives.

- A Guide to Effective Security Metrics

Top of page

Collection of Evidence

Recommended Tools and Resources for Incident Handlers

The following lists are from Table 3.1 of the NIST Computer Security Incident Handling Guide.

Incident Handler Communications and Facilities:

- Contact information including after hours (on-call) information
- Incident reporting mechanisms
- Pagers and/or cell phones

- Encryption software
- Secure storage location/area
- Work area

Incident Analysis Hardware and Software:

- Computer forensic workstations and/or backup devices, laptops
- Spare (workstations servers and networking) devices
- Blank media, cables, housings, converters, and write blockers
- Portable printer
- Packet sniffers and protocol analyzers
- Computer forensic software
- Removable media
- Evidence gathering accessories (such as notebooks, cameras, recorders, chain of custody forms, evidence collection bags)

Incident Analysis Resources:

- Port lists
- OS documentation
- Network diagrams
- Lists of critical assets
- Baselines
- Cryptographic hashes of critical files

Incident Mitigation Resources:

- Media (OS and application software)
- Security patches
- Backup images

Resources

Campus Case Studies On This Page
Identity Finder - University of Pennsylvania

EDUCAUSE Resources

- Cyber Liability Insurance FAQ (2015)
- Incident Handling and Response
- Intrusion Detection and Prevention
- Network Security
- Vulnerability Management
- Using OSSEC for Intrusion Detection
- PaIRS IDS: Finding bad actors without looking at content
- Malware Detection and Mitigation with Passive DNS and Blackhole DNS
- Are you Ready? A Planning Tool for Managing Sensitive Data Incidents
- Data Breach Notification: Discussing Reactive Processes and Proactive Strategies

Initiatives, Collaborations, & Other Resources

- NIST Computer Security Incident Handling Guide (SP800-61)
- CIS Consensus Information Security Metrics initiative
- Log Retention Guideline
- FIRST (Forum for Incident Response and Security Teams)
- SANS Training Courses
- How To Take Control of Incident Management Costs

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security

27002:2013 Information Security Management **Chapter 16**: Information Security Incident Management	**800-53**: Recommended Security Controls for Federal Information Systems and Organizations **800-61**: Computer Security Incident Handling Guide **800-83**: Guide to Malware Incident Prevention and Handling **800-86**: Guide to Integrating Forensic Techniques into Incident Response **800-94**: Guide to Intrusion Detection and Prevention Systems Rev 1	**APO11.06** **APO12.06** **APO11.06** **BAI01.10** **BAI01.13** **DSS02.07** **DSS04.03** **DSS04.05**	**Req 11** **Req 12**	**PR.IP-8** **PR.IP-9** **DE.AE-2** **DE.DP-4** **DE.DP-5**	**45 CFR 164.308(a)(6)**

Top of page