Security Incidents Handling

Adir Abraham

adir@computer.org

DC9723

23/04/2013

Incident - Definition

(included, but not limited to:)

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

Discussing security incidents – why?

- Cyber-security attacks have become more damaging and disruptive
- Performing incident response effectively is a complex undertaking
- An incident response capability is necessary for detecting incidents, minimizing loss & destruction, fixing weaknesses that were exploited and restoring service.

Handling security incidents – why?

- Understanding threats and identifying modern attacks in their early stages is key to preventing subsequent compromises
- Proactively sharing information among organizations regarding the signs of these attacks is an increasingly effective way to identify them.

Need for incident response

- Responding quickly and effectively when security breaches occur
- Responding support should be done systematically
- Help to minimize loss and as previously described
- Gaining information effectively while handling the security incident to prepare better for future security incidents

How to build an incident response team

- Create an incident response policy and plan
- Develop procedures for performing incident handling and reporting
- Set guidelines for communicating with outside parties regarding incidents
- Select a team structure and staffing model
- Establish relationships and lines of communications between the incident response team and other related group (e.g. legal department and law enforcement agencies)
- Determine what services the incident response team should provide
- Staffing and training the incident response team

Create an incident response policy and plan

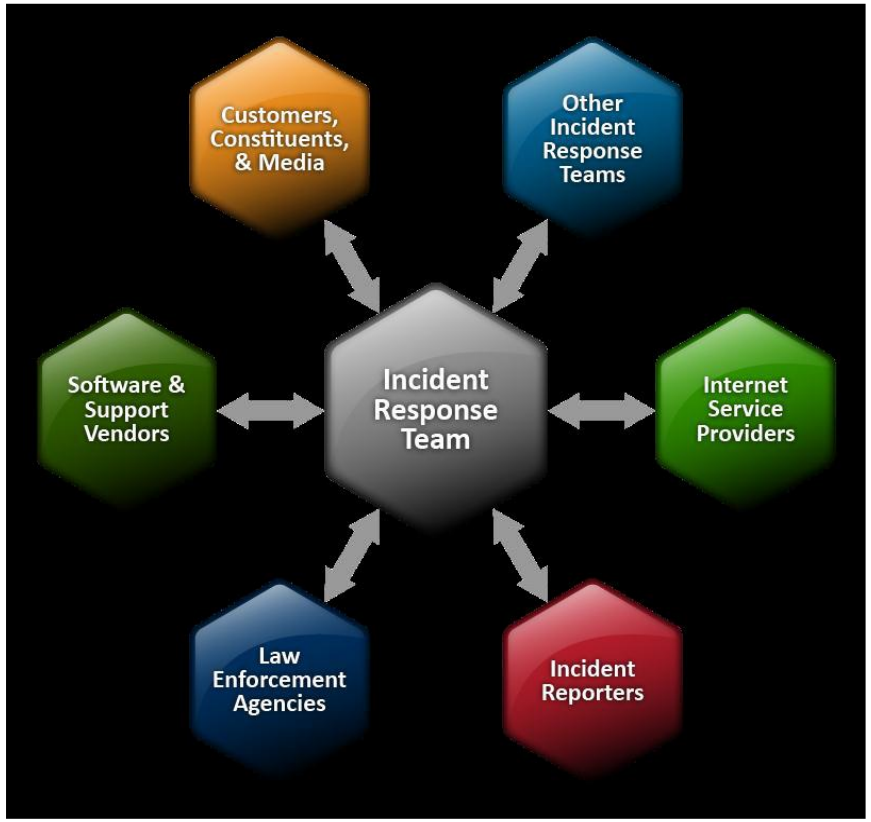
- The authority of the security response team to confiscate or disconnect equipment and to monitor suspicious activity
- What type of incidents should be reported
- How to report an incident (whom, when and over what channels)
- Prioritize ratings of incidents
- Plan: mission, strategies, goals etc.

Develop procedures for performing incident handling and reporting

- Procedures should be based on the incident response policy and plan
- Standard operating procedures are technical processes, techniques, checklists, and forms used by the incident response team

Set guidelines for communicating with outside parties regarding incidents

- Organizations need to communicate with outside parties regarding an incident (due to law enforcement, contacting their customers or the media)
- Organizations need to discuss the incident with other involved parties, such as ISPs, the vendor of vulnerable software or other incident response teams.
- Incident report teams should establish policies and procedures regarding information sharing, so no sensitive information will be leaked.


Customers, Constituents, & Media
Other Incident Response Teams
Software & Support Vendors
Incident Response Team
Internet Service Providers
Law Enforcement Agencies
Incident Reporters

Select a team structure and staffing model

- 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.

- Coordinating teams

An incident response team provides advice to other teams without having authority over those teams

Relationships with other related groups

- Management establishes incident response policy, budget, and staffing.
- Information security staff members may be needed during certain stages of incident handling (prevention, containment, eradication, and recovery)—for example, to alter network security controls (e.g., firewall rulesets).
- IT technical experts (e.g., system and network administrators) not only have the needed skills to assist but also usually have the best understanding of the technology they manage on a daily basis. This understanding can ensure that the appropriate actions are taken for the affected system, such as whether to disconnect an attacked system.

Relationships with other related groups

- Legal experts should review incident response plans, policies, and procedures to ensure their compliance with law and Federal guidance, including the right to privacy.
- Public Affairs and Media Relations. Depending on the nature and impact of an incident, a need may exist to inform the media and, by extension, the public.
- Human Resources. If an employee is suspected of causing an incident, the human resources department may be involved—for example, in assisting with disciplinary proceedings.

Relationships with other related groups

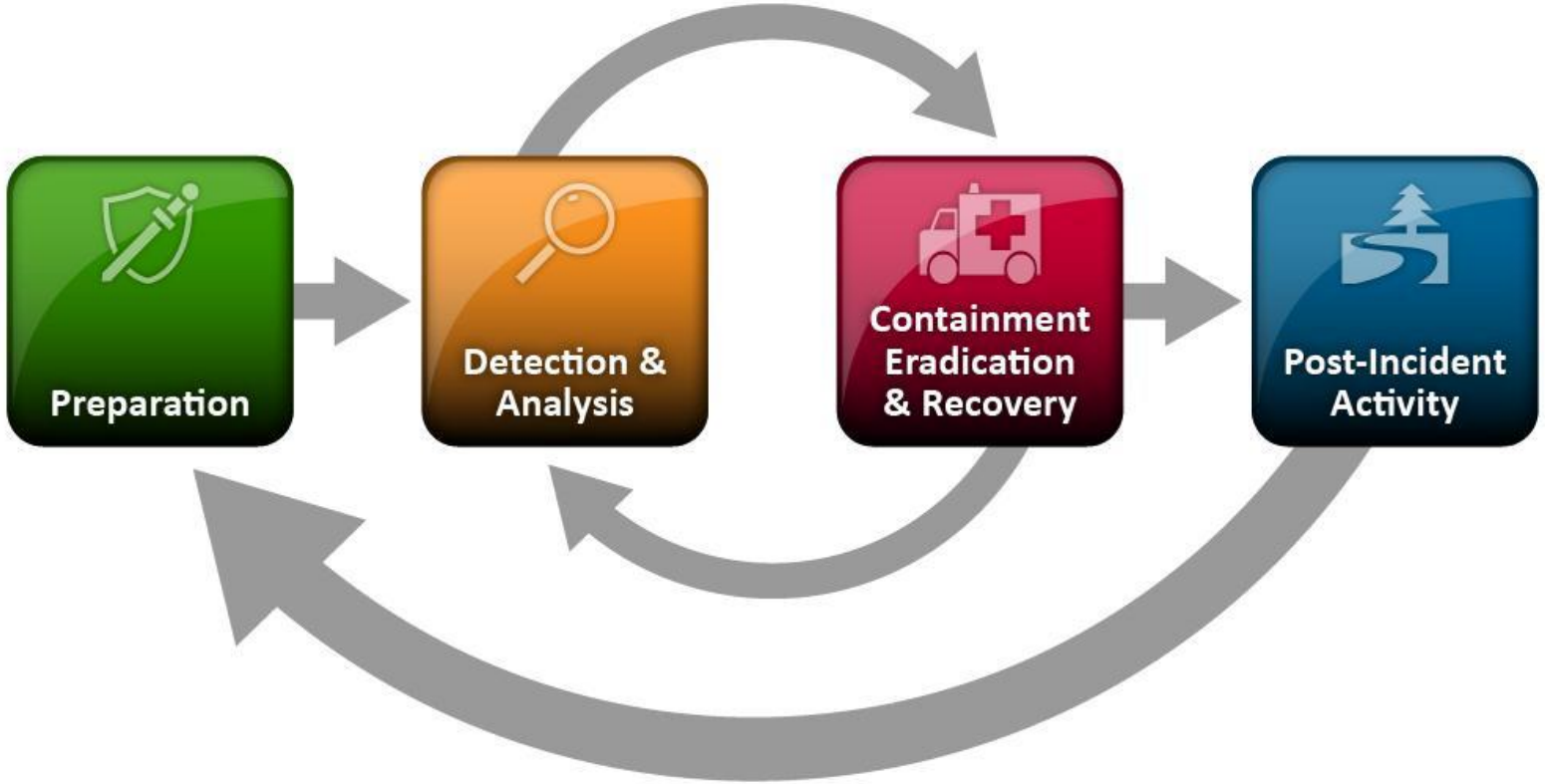
- Business continuity planning professionals should be made aware of incidents and their impacts so they can fine-tune business impact assessments, risk assessments, and continuity of operations plans.

- Physical Security and Facilities Management. Some computer security incidents occur through breaches of physical security or involve coordinated logical and physical attacks. The incident response team also may need access to facilities during incident handling—for example, to acquire a compromised workstation from a locked office.

Incident response team services

- The first tier of an incident response team often assumes responsibility for intrusion detection. It should be poised to analyze incidents more quickly and accurately, based on the knowledge it gains of intrusion detection technologies.
- A team may issue advisories within the organization regarding new vulnerabilities and threats. 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 abuse in their social engineering.
- 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.

Handling an incident



Handling an incident - Preparation

- Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs.

Handling an incident - Preparation

- Incident handler communication and facilities, such as contact information, issue tracking system, smartphones, communication encryption software, war room and secure storage facility.
- Incident analysis software and hardware, such as laptops, workstations, blank removable media, disk images analyzers and evidence gathering accessories such as digital cameras and audio recorders.
- Incident analysis resources such as port lists, documentation and network diagrams

Handling an incident - Prevention

- Although incident response teams are generally not responsible for securing resources, they can be advocates of sound security practices.
- Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities. Each risk should be prioritized, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached.

Handling an incident - Prevention

- 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.
- Hosts should have auditing enabled and should log significant security-related events. The security of hosts and their configurations should be continuously monitored.
- 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.

Handling an incident - Prevention

- Software to detect and stop malware should be deployed throughout the organization. Malware protection should be deployed at the host level (OS), the application server level, and the application client level.
- Users should be made aware of policies and procedures regarding appropriate use of networks, systems, and applications.

Handling an incident – Detection & 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.

Handling an incident – Detection & Analysis

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. For example: integrity checking of files.
- 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. One way to gain this knowledge is through reviewing log entries and security alerts.

Handling an incident – Detection & Analysis

- 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.
- Perform Event Correlation. Evidence of an incident may be captured in several logs that each contain different types of data. For example, a firewall log may have the source IP address that was used, whereas an application log may contain a username. Correlating events among multiple indicator sources can be invaluable in validating whether a particular incident occurred.

Handling an incident – Detection & Analysis

- 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.

Handling an incident – containment eradication & recovery

- 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 strategies vary based on the type of incident. For example, the strategy for containing an email-borne malware infection is quite different from that of a network-based DDoS attack.

Handling an incident – containment eradication & recovery

- 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.
- 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.

Handling an incident – post-incident activity

- 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.

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)	

Incident Handling Scenarios

- On a Tuesday morning, a new worm is released; it spreads itself through removable media, and it can copy itself to open Windows shares. When the worm infects a host, it installs a DDoS agent. The organization has already incurred widespread infections before antivirus signatures become available several hours after the worm started to spread.

Incident Handling Scenarios

- The following are questions for this scenario:
- 1. How would the incident response team identify all infected hosts?
- 2. How would the organization attempt to prevent the worm from entering the organization before antivirus signatures were released?
- 3. How would the organization attempt to prevent the worm from being spread by infected hosts before antivirus signatures were released?
- 4. Would the organization attempt to patch all vulnerable machines? If so, how would this be done?
- 5. How would the handling of this incident change if infected hosts that had received the DDoS agent had been configured to attack another organization's website the next morning?
- 6. How would the handling of this incident change if one or more of the infected hosts contained sensitive personally identifiable information regarding the organization's employees?
- 7. How would the incident response team keep the organization's users informed about the status of the incident?
- 8. What additional measures would the team perform for hosts that are not currently connected to the network (e.g., staff members on vacation, offsite employees who connect occasionally)?

Incident Handling Scenarios

- On a Thursday afternoon, a network intrusion detection sensor records vulnerability scanning activity directed at internal hosts that is being generated by an internal IP address. Because the intrusion detection analyst is unaware of any authorized, scheduled vulnerability scanning activity, she reports the activity to the incident response team. When the team begins the analysis, it discovers that the activity has stopped and that there is no longer a host using the IP address.

Incident Handling Scenarios

- The following are additional questions for this scenario:
- 1. What data sources might contain information regarding the identity of the vulnerability scanning host?
- 2. How would the team identify who had been performing the vulnerability scans?
- 3. How would the handling of this incident differ if the vulnerability scanning were directed at the organization's most critical hosts?
- 4. How would the handling of this incident differ if the vulnerability scanning were directed at external hosts?
- 5. How would the handling of this incident differ if the internal IP address was associated with the organization's wireless guest network?
- 6. How would the handling of this incident differ if the physical security staff discovered that someone had broken into the facility half an hour before the vulnerability scanning occurred?

Final words

- These notes are heavily related to NIST SP800-61v2 Documentation:

http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

- This documentation is highly recommended to read and be used as a guide to handle security incidents in your organization or even at your home office.

Questions?