Computer security incident management

In the fields of computer security and information technology, **computer security incident management** involves the monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events. Computer security incident management is a specialized form of incident management, the primary purpose of which is the development of a well understood and predictable response to damaging events and computer intrusions.[1]

Incident management requires a process and a response team which follows this process. This definition of computer security incident management follows the standards and definitions described in the National Incident Management System (NIMS). The *incident coordinator* manages the response to an emergency security incident. In a Natural Disaster or other event requiring response from Emergency services, the *incident coordinator* would act as a liaison to the emergency services incident manager.[2]

Overview

Computer security incident management is an administrative function of managing and protecting computer assets, networks and information systems. These systems continue to become more critical to the personal and economic welfare of our society. Organizations (public and private sector groups, associations and enterprises) must understand their responsibilities to the public good and to the welfare of their memberships and stakeholders. This responsibility extends to having a management program for “what to do, when things go wrong.” Incident management is a program which defines and implements a process that an organization may adopt to promote its own welfare and the security of the public.

Components of an incident

Events

An event is an observable change to the normal behavior of a system, environment, process, workflow or person (components). There are three basic types of events:

1. Normal—a normal event does not affect critical components or require change controls prior to the implementation of a resolution. Normal events do not require the participation of senior personnel or management notification of the event.
2. Escalation – an escalated event affects critical production systems or requires that implementation of a resolution that must follow a change control process. Escalated events require the participation of senior personnel and stakeholder notification of the event.
3. Emergency – an emergency is an event which may
    1. impact the health or safety of human beings
    2. breach primary controls of critical systems
    3. materially affect component performance or because of impact to component systems prevent activities which protect or may affect the health or safety of individuals
    4. be deemed an emergency as a matter of policy or by declaration by the available incident coordinator

Computer security and information technology personnel must handle emergency events according to well-defined computer security incident response plan.

Incident

An incident is an event attributable to a human root cause. This distinction is particularly important when the event is the product of malicious intent to do harm. An important note: all incidents are events but many events are not incidents. A system or application failure due to age or defect may be an emergency event but a random flaw or failure is not an incident.

Incident response team

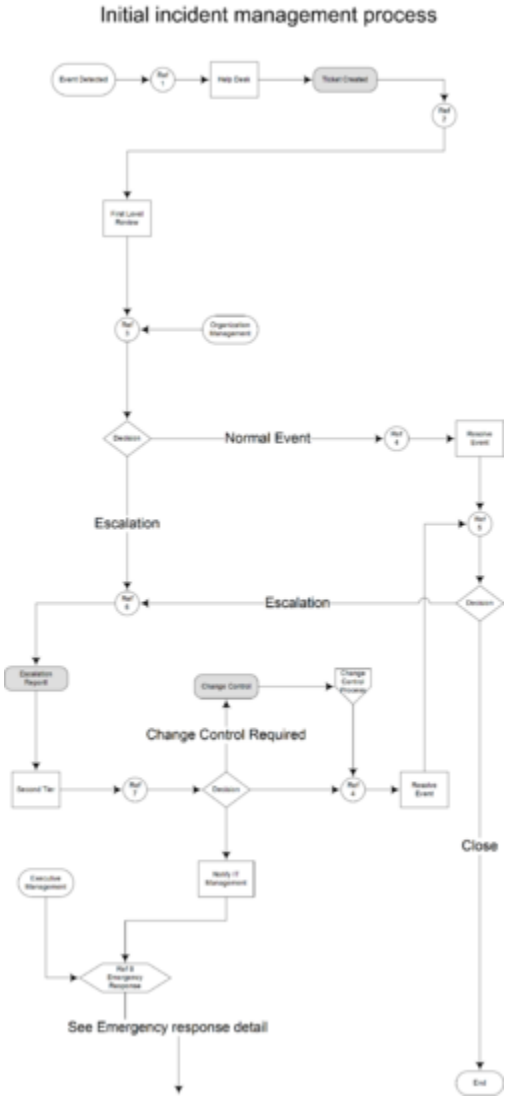
The security *incident coordinator* manages the response process and is responsible for assembling the team. The coordinator will ensure the team includes all the individuals necessary to properly assess the incident and make decisions regarding the proper course of action. The incident team meets regularly to review status reports and to authorize specific remedies. The team should utilize a pre-allocated physical and virtual meeting place.[3]

Incident investigation

The investigation seeks to determine the circumstances of the incident. Every incident will warrant or require an investigation. However, investigation resources like forensic tools, dirty networks, quarantine networks and consultation with law enforcement may be useful for the effective and rapid resolution of an emergency incident.

Process

Initial incident management process

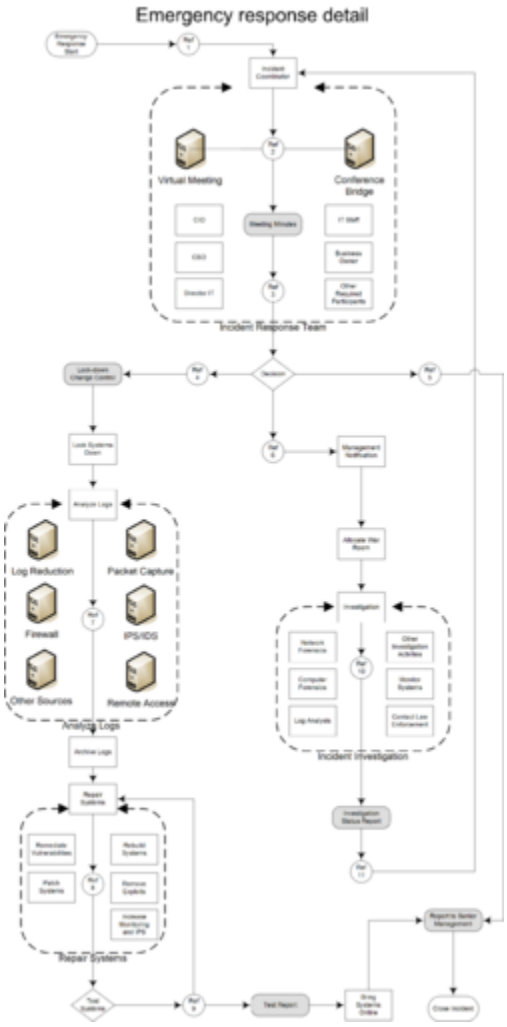


Author: Michael Berman (tanjstaffl)

1. Employee, vendor, customer, partner, device or sensor reports event to *Help Desk*.
2. Prior to creating the ticket, the help desk may filter the event as a false positive. Otherwise, the help desk system creates a ticket that captures the event, event source, initial event severity and event priority.
    1. The ticket system creates a unique ID for the event. IT Personnel must use the ticket to capture email, IM and other informal communication.
    2. Subsequent activities like change control, incident management reports and compliance reports must reference the ticket number.
    3. In instances where event information is “Restricted Access,” the ticket must reference the relevant documents in the secure document management system.

3. The *First Level Responder* captures additional event data and performs preliminary analysis. In many organizations the volume of events is significant relative to the staff. As a result, automation may be applied, typically in the form of a SOAR (security orchestration, automation and response) tool,[4] integrated with an intelligence API. The SOAR tool automates the investigation via a workflow automation workbook.[4] The cyber intelligence API enables the playbook to automate research related to the ticket (lookup potential phishing URL, suspicious hash, etc.). The First Responder determines criticality of the event. At this level, it is either a Normal or an Escalation event.
    1. Normal events do not affect critical production systems or require change controls prior to the implementation of a resolution.
    2. Events that affect critical production systems or require change controls must be escalated.
    3. Organization management may request an immediate escalation without first level review – 2nd tier will create ticket.
4. The event is ready to resolve. The resource enters the resolution and the problem category into the ticket and submits the ticket for closure.
5. The ticket owner (employee, vendor, customer or partner) receives the resolution. They determine that the problem is resolved to their satisfaction or escalate the ticket.
6. The escalation report is updated to show this event and the ticket is assigned a second tier resource to investigate and respond to the event.
7. The Second Tier resource performs additional analysis and re-evaluates the criticality of the ticket. When necessary, the Second Tier resource is responsible for implementing a change control and notifying IT Management of the event.
8. Emergency Response:
    1. Events may follow the escalation chain until it is determined that an emergency response is necessary.
    2. Top-level organization management may determine that an emergency response is necessary and invoke this process directly.

Emergency response detail



Author: Michael Berman (tanjstaffl)

1. Emergency response is initiated by escalation of a security event or be direct declaration by the CIO or other executive organization staff. The CIO may assign the incident coordinator, but by default, the coordinator will be the most senior security staff member available at the time of the incident.
2. The incident coordinator assembles the incident response team. The team meets using a pre-defined conference meeting space. One of the (CIO, CSO or Director IT) must attend each incident team meeting.
3. The meeting minutes capture the status, actions and resolution(s) for the incident. The incident coordinator reports on the cost, exposure and continuing business risk of the incident. The incident response team determines the next course of action.

4. Lock-down and Repair – Perform the actions necessary to prevent further damage to the organization, repair impacted systems and perform changes to prevent a re-occurrence.
5. False Positive – The incident team determines this issue did not warrant an emergency response. The team provides a written report to senior management and the issue is handled as either a normal incident or it is closed.
6. Monitor and Capture – Perform a thorough investigation with continued monitoring to detect and capture the perpetrator. This process must include notification to the following senior and professional staff:
    1. CEO and CFO
    2. Corporate Attorney and Public Relations
7. Review and analyze log data to determine nature and scope of incident. This step should include utilizing virus, spyware, rootkit and other detection tools to determine necessary mitigation and repair.
8. Repair systems, eliminate vector(s) of attack, and mitigate exploitable vulnerabilities.
9. The *Test Report* documents the validation of the repair process.
    1. Test systems to ensure compliance with policy and risk mitigation.
    2. Perform additional repairs to resolve all current vulnerabilities.
10. Investigate incident to determine source of attack and capture perpetrator. This will require the use of forensics tools, log analysis, clean lab and dirty lab environments and possible communication with Law Enforcement or other outside entities.
11. The “Investigation Status Report” as captures all current information regarding the incident. The Incident response team uses this information to determine the next course of action. (See Ref 2 and Ref 3)

Definitions

First Responder/First level review
first person to be on scene or receive notification of an event, organizations should provide training to the first responder to recognize and properly react to emergency circumstances.
Help Desk Ticket (Control)
an electronic document captured in a database and issue tracking/resolution system
Ticket Owner

person reporting the event, the principal owner of the assets associated with the event or the common law or jurisdictional owner.

Escalation Report (Control)

First Responder's documentation for ticket escalation, the Responder writes this information into the ticket or the WIKI log for the event. The ticket references the WIKI log for the event.

Second Tier

Senior technical resources assigned to resolve an escalated event.

Incident Coordinator

individual assigned by organization senior management to assemble the incident response team, manage and document response to the incident.

Investigation Status Report (Control)

documentation of the current investigation results, the coordinator may document this material in the ticket, WIKI or an engineer's journal.

Meeting Minutes (Control)

documentation of the incident team meeting, the minutes document the attendees, current nature of the incident and the recommended actions. The coordinator may document this material in the ticket, WIKI or an engineer's journal.

Lock-down Change Control

a process ordered as a resolution to the incident. This process follows the same authorization and response requirements as an Emergency Change Control.

Test Report (Control)

this report validates that IT personal have performed all necessary and available repairs to systems prior to bringing them back online.

War Room

a secure environment for review of confidential material and the investigation of a security incident.

Report to Senior Management (Control)

the *incident coordinator* is responsible for drafting a senior management report. The coordinator may document this material in the ticket, WIKI or an engineer's journal

Incident Response Steps

- **Detection** – An incident can be detected by a sensor, a network analyst or a user reporting something unusual with his/her PC.
- **Containment** – In the event of malicious network traffic or a computer virus, the Incident Response Manager should stop the traffic by taking the computer off the network.

- **Clean** – Run a virus scan to remove the virus or wipe the computer clean and reimage the machine.
- **Reverse Engineering** – Use computer forensics tools to understand why the malicious traffic occurred in the first place. Once the incident is completely understood make plans to decrease your future risk.

See also

- Computer emergency response team
- Proactive cyber defence
- United States' National Incident Management System

References

1. *"ISO 17799|ISO/IEC 17799:2005(E)" (http://www.iso.org) . Information technology - Security techniques - Code of practice for information security management. ISO copyright office. 2005-06-15. pp. 90–94.*
2. *"NIMS - The Incident Command System" (https://web.archive.org/web/20070318154341/http://www.nimsonline.com/nims_3_04/incident_command_system.htm) . National Incident Management System. Department of Homeland Security. 2004-03-01. Archived from the original (http://www.nimsonline.com/nims_3_04/incident_command_system.htm) on 2007-03-18. Retrieved 2007-04-08.*
3. *"Creating a Computer Security Incident Response Team" (http://www.cert.org/archive/pdf/csirt-handbook.pdf) (PDF). Computer Emergency Response Team. US-CERT. 2003-04-01. Retrieved 2007-04-08.*
4. *"What is SOAR (Security Orchestration, Automation and Response) ?" (https://searchsecurity.techtarget.com/definition/SOAR) . SearchSecurity. 2019-12-06. Retrieved 2019-12-06.*

Further reading

- Handbook for Computer Security Incident Response Teams (CSIRTs) http://www.sei.cmu.edu/library/abstracts/reports/03hb002.cfm

Last edited 14 days ago **by** MrOllie