Creating an Incident Response Plan

Albert Moore

Presenter

NIST Special Publication 800-61 rev2

2.3.2 Plan Elements

Organizations should have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability. Each organization needs a plan that meets its unique requirements, which relates to the organization’s mission, size, structure, and functions. The plan should lay out the necessary resources and management support. The incident response plan should include the following elements:

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization.

The organization’s mission, strategies, and goals for incident response should help in determining the structure of its incident response capability. The incident response program structure should also be discussed within the plan. Section 2.4.1 discusses the types of structures.

NIST Element
Mission

DIT Mission

The mission of the North Carolina ESRMO Incident Response Team is to do the following:

- Implement, test, and maintain the North Carolina ESRMO Computer Security Incident Response Plan, a standard set of criteria for incident severity determination, responses to security problems, and protocols for inter-agency and departmental communication during an incident
- Assist in protecting the North Carolina state network infrastructure and agency computer systems and networks, and the data they contain, from the effects of computer security incidents
- Provide a central point of contact for the reporting and dissemination of information about computer security incidents
- Coordinate the activities of North Carolina ESRMO personnel and affected agency technical and management teams in the investigation of, response to, and recovery from computer security incidents
- Minimize any negative impact of a computer security incident on North Carolina DIT business operations, financial state, and public image
- Minimize disruption to both internal and external customers
- Collect necessary data and evidence for prosecution; and
- Ensure activities and actions are consistent with the priorities set forth earlier in the document

NIST Element
Strategies and goals

DIT Strategy

- Adopted the Incident Response principles established in NIST SP 800-53 Rev 4 “Incident Response” control guidelines as the official policy for this security domain.
- NIST Incident Response Lifecycle
  - Preparation
  - Detection and Analysis
  - Containment, Eradication, and Recovery
  - Post-incident Activity

NIST Element
Senior management approval

- IRP is based on the Statewide IR policy, CIO-SEC-308-00, which is approved by the Secretary of DIT
- Authority from N.C.G.S. §143B-1376 and § 143B-1379

NIST Element
Organizational approach to incident response

Know what you're protecting and why

Determine authority to call an incident

Build a Solid Team

Know what you're protecting and why[1]

- Complete inventory of your IT assets
- What systems and data are at greatest risk
- Prioritize their protection according to how critical they are to delivering business outcomes

[1] https://www.sungardas.com/en/about/resources/articles/creating-a-cyber-security-incident-response-plan
https://resources.infosecinstitute.com/category/certifications-training/csih-certification/incident-response-plan-steps/#gref

Determine authority to call an incident.[2]

- IRP should clearly state who has the authority to declare an incident.
- As soon as an incident is declared that should automatically invoke the IRP and convene the incident response team (IRT).

[2] Kroll - It’s Not If But When : How to Build Your Cyber Incident Response Plan

Build a Solid Team[3]

- Assemble a group of specialists within your organization.
- Clearly define each role when responding to an incident, and what steps need to be taken during different scenarios.
- Involve Relevant Departments - Not everybody in your incident response team needs to be an IT specialist

[3] https://resources.infosecinstitute.com/category/certifications-training/csih-certification/incident-response-plan-steps/#gref
Kroll - It’s Not If But When : How to Build Your Cyber Incident Response Plan

NIST Element
How the incident response team will communicate with the rest of the organization and with other organizations

Establish communications procedures and responsibilities.

Establish communications procedures and responsibilities.

- Determine how communication will flow. [4]
- How will the IRT communicate securely:
  - Where will you meet (war rooms)?
  - Is it safe to use corporate email?
- What should be communicated verbally, what should be written?
- Determine who will communicate with external parties, such as outside counsel, your insurance carrier, law enforcement, the media, and regulators.
- Determine who will report to executives

[4] Kroll - It’s Not If But When : How to Build Your Cyber Incident Response Plan

NIST Element

Metrics for measuring the incident response capability and its effectiveness

Develop KPIs & SLAs

Develop KPIs & SLAs[5]

- Number of Incidents Handled

- Time Per Incident [6]
  - Total amount of labor spent working on the incident
  - Elapsed time from the beginning of the incident to incident discovery, to the initial impact assessment, and to each stage of the incident handling process (e.g., containment, recovery)
  - How long it took the incident response team to respond to the initial report of the incident
  - How long it took to report the incident to management and, if necessary, appropriate external entities

[5] https://resources.infosecinstitute.com/category/certifications-training/csih-certification/incident-response-plan-steps/#gref

[6] NIST 800-61 r2

NIST Element

Roadmap for maturing the incident response capability

Review and test the plan

Review and test the plan

- Review the plan regularly. Pay special attention to any technology, policies, or roles that may have changed in the intervening time. Also ensure that contact information has been updated for your team members and outside resources. [7]
- Test plan- schedule annual tests[8]
- Identify any gaps and update plan[8]
- Establish an Incident Debriefing Process[9]

[7] Kroll - It’s Not If But When : How to Build Your Cyber Incident Response Plan

[8] https://www.sungardas.com/en/about/resources/articles/creating-a-cyber-security-incident-response-plan

[9] https://resources.infosecinstitute.com/category/certifications-training/csih-certification/incident-response-plan-steps/#gref

NIST Element

How the program fits into the overall organization

Team Models
Staffing Models

- **Team Models [10]**
  - Central Incident Response Team
    - Single incident response team handles incidents throughout the organization
    - Effective for small organizations and for organizations
    - Minimal geographic diversity in terms of computing resources
  - Distributed Incident Response Teams
    - Multiple incident response teams, each responsible for a particular logical or physical segment of the organization
    - 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).
    - 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.
    - Particularly important because multiple teams may see components of the same incident or may handle similar incidents.

[10] NIST 800-61 r2

- **Team Models**
  - Coordinating Team
    - An incident response team provides advice to other teams without having authority over those teams-for example, a departmentwide team may assist individual agencies' teams. This model can be thought of as a CSIRT for CSIRTs.
    - NIST Special Publication 800-61 rev2 does not further cover this type of team

[10]NIST 800-61 r2

- **Staffing Models**[11]
  - Employees
    - Organization performs all incident response work
  - Partially Outsourced
    - Common arrangement is for the organization to outsource 24-hours-a-day, 7-days-a-week (24/7) monitoring of intrusion detection sensors, firewalls, and other security devices to an offsite managed security services provider (MSSP). The MSSP identifies and analyzes suspicious activity and reports each detected incident to the organization’s incident response team.
    - Some organizations perform basic incident response work in-house and call on contractors to assist with handling incidents, particularly those that are more serious or widespread.
  - Fully Outsourced
    - Organization completely outsources incident response work
    - Most likely used when 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

[11] NIST 800-61 r2

NIST Special Publication 800-61 rev2
Incident Handling Scenarios

Scenario considerations

Preparation
Detection and Analysis
Containment, Eradication, and Recovery
Post-Incident Activity

NIST Special Publication 800-61 rev2
Incident Handling Scenarios

Compromised Database Server

On a Tuesday night, a database administrator performs some off-hours maintenance on several production database servers. The administrator notices some unfamiliar and unusual directory names on one of the servers. After reviewing the directory listings and viewing some of the files, the administrator concludes that the server has been attacked and calls the incident response team for assistance. The team's investigation determines that the attacker successfully gained root access to the server six weeks ago.

The following are additional questions for this scenario:

1. What sources might the team use to determine when the compromise had occurred?
2. How would the handling of this incident change if the team found that the database server had been running a packet sniffer and capturing passwords from the network?
3. How would the handling of this incident change if the team found that the server was running a process that would copy a database containing sensitive customer information (including personally identifiable information) each night and transfer it to an external address?
4. How would the handling of this incident change if the team discovered a rootkit on the server?

NIST Special Publication 800-61 rev2
Incident Handling Scenarios

Telecommuting Compromise

On a Saturday night, network intrusion detection software records an inbound connection originating from a watchlist IP address. The intrusion detection analyst determines that the connection is being made to the organization’s VPN server and contacts the incident response team. The team reviews the intrusion detection, firewall, and VPN server logs and identifies the user ID that was authenticated for the session and the name of the user associated with the user ID.

The following are additional questions for this scenario:

1. What should the team’s next step be (e.g., calling the user at home, disabling the user ID, disconnecting the VPN session)? Why should this step be performed first? What step should be performed second?
2. How would the handling of this incident differ if the external IP address belonged to an open proxy?
3. How would the handling of this incident differ if the ID had been used to initiate VPN connections from several external IP addresses without the knowledge of the user?

NIST Special Publication 800-61 rev2
Incident Handling Scenarios

Telecommuting Compromise -continued

4. Suppose that the identified user’s computer had become compromised by a game containing a Trojan horse that was downloaded by a family member. How would this affect the team’s analysis of the incident? How would this affect evidence gathering and handling? What should the team do in terms of eradicating the incident from the user’s computer?

5. Suppose that the user installed antivirus software and determined that the Trojan horse had included a keystroke logger. How would this affect the handling of the incident? How would this affect the handling of the incident if the user were a system administrator? How would this affect the handling of the incident if the user were a high-ranking executive in the organization?

NIST Special Publication 800-61 rev2
Incident Handling Scenarios

Disappearing Host

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.

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?

Questions?

Albert Moore
(919) 754-6245
Albert.Moore@nc.gov