Table 3-5. 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)	

Appendix A—Incident Handling Scenarios

Incident handling scenarios provide an inexpensive and effective way to build incident response skills and identify potential issues with incident response processes. The incident response team or team members are presented with a scenario and a list of related questions. The team then discusses each question and determines the most likely answer. The goal is to determine what the team would really do and to compare that with policies, procedures, and generally recommended practices to identify discrepancies or deficiencies. For example, the answer to one question may indicate that the response would be delayed because the team lacks a piece of software or because another team does not provide off-hours support.

The questions listed below are applicable to almost any scenario. Each question is followed by a reference to the related section(s) of the document. After the questions are scenarios, each of which is followed by additional incident-specific questions. Organizations are strongly encouraged to adapt these questions and scenarios for use in their own incident response exercises.[48]

A.1 Scenario

Questions

Preparation:

1. Would the organization consider this activity to be an incident? If so, which of the organization’s policies does this activity violate? *(Section 2.1)*
2. What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact? *(Section 3.1.2)*

Detection and Analysis:

1. What precursors of the incident, if any, might the organization detect? Would any precursors cause the organization to take action before the incident occurred? *(Sections 3.2.2, 3.2.3)*
2. What indicators of the incident might the organization detect? Which indicators would cause someone to think that an incident might have occurred? *(Sections 3.2.2, 3.2.3)*
3. What additional tools might be needed to detect this particular incident? *(Section 3.2.3)*
4. How would the incident response team analyze and validate this incident? What personnel would be involved in the analysis and validation process? *(Section 3.2.4)*
5. To which people and groups within the organization would the team report the incident? *(Section 3.2.7)*
6. How would the team prioritize the handling of this incident? *(Section 3.2.6)*

Containment, Eradication, and Recovery:

1. What strategy should the organization take to contain the incident? Why is this strategy preferable to others? *(Section 3.3.1)*
2. What could happen if the incident were not contained? *(Section 3.3.1)*
3. What additional tools might be needed to respond to this particular incident? *(Sections 3.3.1, 3.3.4)*
4. Which personnel would be involved in the containment, eradication, and/or recovery processes?
   (Sections 3.3.1, 3.3.4)
5. What sources of evidence, if any, should the organization acquire? How would the evidence be acquired? Where would it be stored? How long should it be retained? *(Sections 3.2.5, 3.3.2, 3.4.3)*

Post-Incident Activity:

1. Who would attend the lessons learned meeting regarding this incident? *(Section 3.4.1)*
2. What could be done to prevent similar incidents from occurring in the future? *(Section 3.1.2)*
3. What could be done to improve detection of similar incidents? *(Section 3.1.2)*

General Questions:

1. How many incident response team members would participate in handling this incident? *(Section 2.4.3)*

2. Besides the incident response team, what groups within the organization would be involved in handling this incident? *(Section 2.4.4)*

3. To which external parties would the team report the incident? When would each report occur? How would each report be made? What information would you report or not report, and why? *(Section 2.3.2)*

4. What other communications with external parties may occur? *(Section 2.3.2)*

5. What tools and resources would the team use in handling this incident? *(Section 3.1.1)*

6. What aspects of the handling would have been different if the incident had occurred at a different day and time (on-hours versus off-hours)? *(Section 2.4.2)*

7. What aspects of the handling would have been different if the incident had occurred at a different physical location (onsite versus offsite)? *(Section 2.4.2)*