JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Policy & Procedures

CYBER INCIDENT RESPONSE

Incident Response Policy

- Foundation of the organization’s Incident Response program
- Guides efforts at a high-level
- Provides authority for response efforts
- Approved by CEO or CIO
- Should be fairly timeless

Contents of the Policy

- Statement of management commitment
- Purpose
- Objectives
- Scope of policy
- Definitional terms
- Roles, responsibilities, and authority
- Incident prioritization scheme
- Measures of performance for CSIRT
- Reporting requirements
- Contact information

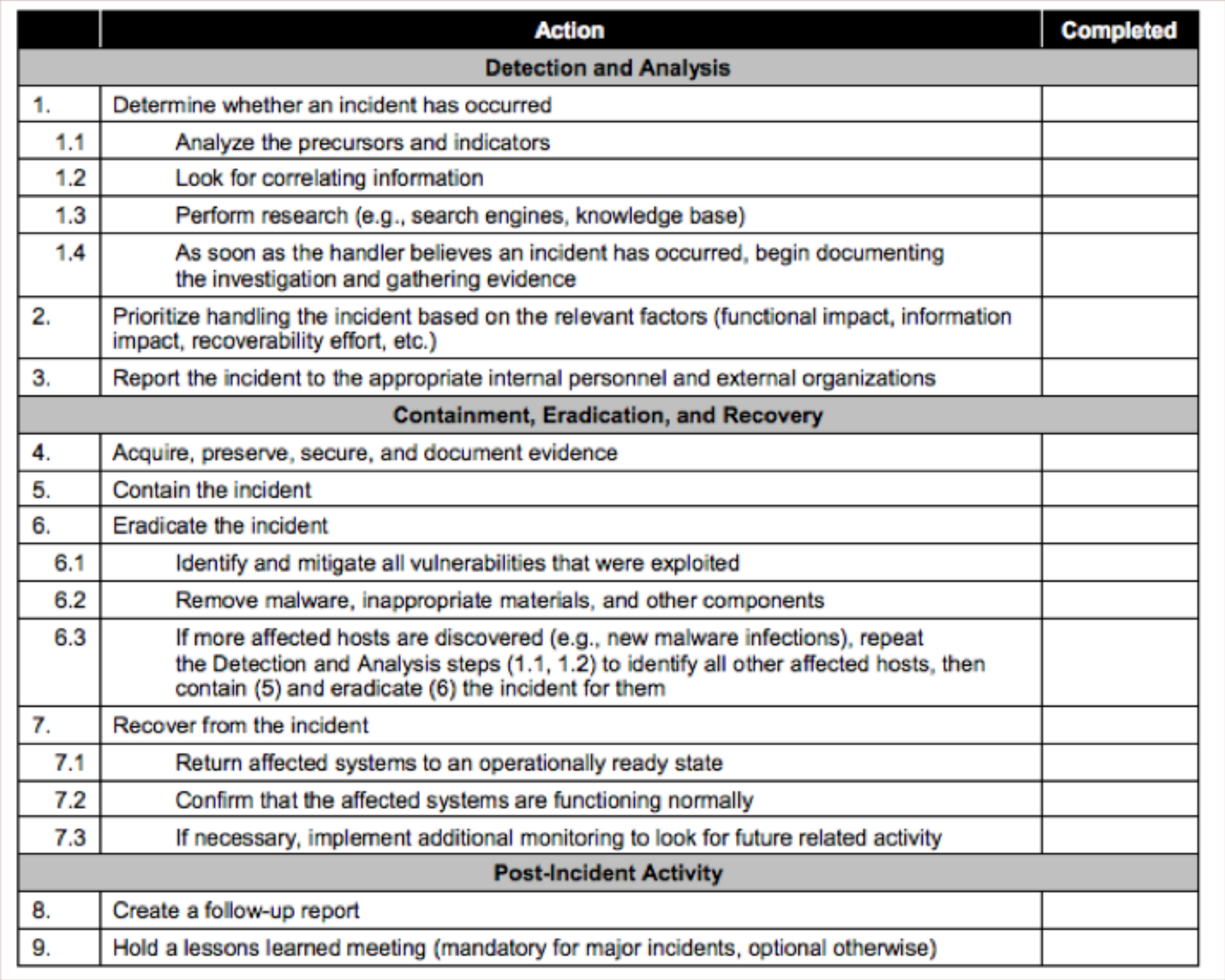
Incident Response Procedures

- Detailed information
- Step-by-step guidelines
- Not a replacement for CSIRT’s professional judgement and expertise
- Often developed as a specific *playbook*

What is a Playbook?

- Describes a response to a high severity type of incident, such as:
  - Data breach of financial information
  - Data breach of personally identifiable information
  - Phishing attack against customers
  - Web server defacements
  - Loss of corporate laptop
  - Intrusion into the corporate network
  - Windows Golden Ticket reset

Incident Response 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)	

NIST SP 800-61

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE