BLACK SWAN TECHNOLOGIES

Incident Response Scenarios Playbook

It's no longer a case of **IF** but **WHEN** you will have a security incident. Incident Response Programs are critical and this Incident Response Scenario Playbook will strengthen the skills you and your organization need to be prepared.

BLACK SWAN TECHNOLOGIES
Phone: 877-300-3798
Email: info@blackswantechnologies.com
Web: blackswantechnologies.com

Incident Response Scenario Playbook

DISCLAIMER: *The following document has been customized and is based on the NIST Special Publication 800-61 rev. 2, Computer Security Incident Handling Guide. It is intended to be a primer for the development of an incident response program. This document is free to use.*

Sample responses have been entered to function as a starting reference point and to provide further guidance. Each scenario has a response section for each department within the organization. NOTE: Not all organizations or incidents will require a response from every department.

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.

Scenario Questions

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.

Preparation:

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

Detection and Analysis:

3. What precursors of the incident, if any, might the organization detect? Would any precursors cause the organization to take action before the incident occurred?
4. What additional tools might be needed to detect this particular incident?
5. How would the incident response team analyze and validate this incident? What personnel would be involved in the analysis and validation process?
6. To which people and groups within the organization would the team report the incident?
7. How would the team prioritize the handling of this incident?

Containment, Eradication, and Recovery:

8. What strategy should the organization take to contain the incident? Why is this strategy preferable to others?
9. What could happen if the incident were not contained?
10. What additional tools might be needed to respond to this particular incident?
11. Which personnel would be involved in the containment, eradication, and/or recovery processes?

12. 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?

Post-Incident Activity:

13. Who would attend the lessons learned meeting regarding this incident?
14. What could be done to prevent similar incidents from occurring in the future?
15. What could be done to improve detection of similar incidents?

General Questions:

16. How many incident response team members would participate in handling this incident?
17. Besides the incident response team, what groups within the organization would be involved in handling this incident?
18. 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?
19. What other communications with external parties may occur?
20. What tools and resources would the team use in handling this incident?
21. 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)?
22. What aspects of the handling would have been different if the incident had occurred at a different physical location (onsite versus offsite)?

Cybersecurity Event Recovery Scenarios

Scenario 1: Domain Name System (DNS) Server Denial of Service (DoS)

On a Saturday afternoon, external users start having problems accessing the organization's public websites. Over the next hour, the problem worsens to the point where nearly every access attempt fails. Meanwhile, a member of the organization's networking staff responds to alerts from an Internet border router and determines that the organization's Internet bandwidth is being consumed by an unusually large volume of User Datagram Protocol (UDP) packets to and from both the organization's public DNS servers. Analysis of the traffic shows that the DNS servers are receiving high volumes of requests from a single external IP address. Also, all the DNS requests from that address come from the same source port.

The following are additional questions for this scenario:

1.1. *Whom should the organization contact regarding the external IP address in question?*

Response: *(e.g. Managed Security Service Provider, Website Hosting Company)*

1.2. *Suppose that after the initial containment measures were put in place, the network administrators detected that nine internal hosts were also attempting the same unusual requests to the DNS server. How would that affect the handling of this incident?*

Response: *(e.g. All internal hosts should be checked for compromise)*

1.3. *What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact?*

Response: *(e.g. Monitoring by MSSP and end-point protection solutions, firewall logs)*

1.4. What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact?

Response: *External: Network Solutions and DNS providers have multiple redundant servers/systems to reduce the impact a DDOS attack. Additionally, the eBanking provider and website hosting provider both have mitigating controls to minimize the impact of a DDOS.*

Detection and Analysis:

1.5. What precursors of the incident, if any, might the organization detect?

Response: (e.g. *Increased calls to the call center and IT helpdesk, notification from MSP)*

1.6. Would any precursors cause the organization to take action before the incident occurred?

Response: (e.g. *Not likely, the near real-time impact of DDOS attacks would mean that any notification from customers/members or system generated alerts would indicate that the attack was already underway.)*

1.7. What additional tools might be needed to detect this particular incident?

Response: (e.g. *3rd party monitoring/alerting. For internal; network monitoring tools.)*

1.8. How would the incident response team analyze and validate this incident? What personnel would be involved in the analysis and validation process?

Response: *(*e.g. *Third-parties including Network Solutions, Network Carrier (ATT), MSSP, Security Network Engineer.)*

1.9. To which people and groups within the organization would the team report the incident?

Response: (e.g. CIRT, Sr. Management, Internal Audit, Information sharing groups: FS-ISAC)

1.10. How would the team prioritize the handling of this incident?

Response: (e.g. Communication to customers/members, Production critical systems would be addressed first)

Containment, Eradication, and Recovery:

1.11. What strategy should the organization take to contain the incident? Why is this strategy preferable to others?

Response: (e.g. Communication to customer/members and 3rd-party vendors will be a priority to minimize reputational damage)

1.12. What could happen if the incident were not contained?

Response: (e.g. Reputational Damage, Financial impact)

1.13. What additional tools might be needed to respond to this particular incident?

Response (e.g. Incident response services from a third-party vendor to assist with forensic evidence collection process, FBI)

1.14. Which personnel would be involved in the containment, eradication, and/or recovery processes?

Response: (e.g. members of the CMT (crisis management team). This will include marketing/communications, operations and IT)

1.15. *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?*

Response: (e.g. forensic evidence will be collected following best practice and will include 3rd-party vendor expertise. Sources could include desktop/server/application logs)

Department Responses:

Each department should consider the potential impact of the incident scenario and document the necessary action steps that will be taken during the incident. Not all scenarios will require a response from every department. The exercise is intended to foster discussion among departments and the incident response team to maximize the effectiveness of the response.

Third-Party vendors are critical to an organization and should be included in the organizations Incident Response Program. Scenarios can and should be shared with critical vendors to ensure program gaps are identified and addressed.

The list of departments (below) is an example and is not an exhaustive list and may not represent your organizations structure.

Departments

Operations
Marketing/Communications
Finance
HR
Facilities
Information Technology
Information Security/Risk Management

Response:

Third-Party Vendors

Response:

2. Scenario 2: Worm and Distributed Denial of Service (DDoS) Agent Infestation

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.

The following are additional questions for this scenario:

2.1. *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?*

Response: (e.g. 30 days of log data from servers/desktops/apps will be gather and stored off-line. Evidence collection will be performed by contracted 3rd party forensic evidence vendor to ensure best practice)

2.2. *How would the incident response team identify all infected hosts?*

Response: (e.g. Asset management & patch management systems are in place and will be used to ensure that all hosts on the network are scanned)

2.3. *How would the organization attempt to prevent the worm from entering the organization before antivirus signatures were released?*

Response: (e.g.)

2.4. *How would the organization attempt to prevent the worm from being spread by infected hosts before antivirus signatures were released?*

Response: (e.g. Network segmentation, Windows share ports will be blocked to temporality prevent propagation of infection)

2.5. *Would the organization attempt to patch all vulnerable machines? If so, how would this be done?*
Response: (e.g. Yes, vulnerable machines would be patched via the patch management system and would follow patch management procedures currently in place.)

2.6. *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?*

Response: (e.g. Prioritization would change to include notify of the other organization and implementation of firewall rules to prevent network communication)

2.7. *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?*

Response: (e.g., Notification to employees of the possible exposure of PII would be handled by the HR dept.)

2.8. *How would the incident response team keep the organization's users informed about the status of the incident?*

Response: (e.g., The organization will follow the BCP communication procedure to continue to inform impacted employees)

2.9. *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)?*
Response: (i.e. IT/HR communications as well as blocking connection from remote teleworkers until patches have been verified)

Department Responses:

Each department should consider the potential impact of the incident scenario and document the necessary action steps that will be taken during the incident. Not all scenarios will require a response from every department. The exercise is intended to foster discussion among departments and the incident response team to maximize the effectiveness of the response.

Third-Party vendors are critical to an organization and should be included in the organizations Incident Response Program. Scenarios can and should be shared with critical vendors to ensure program gaps are identified and addressed.

The list of departments (below) is an example and is not an exhaustive list and may not represent your organizations structure.

Departments
Operations
Marketing/Communications
Finance
HR
Facilities
Information Technology
Information Security/Risk Management
Response:

Third-Party Vendors
Response:

3. Scenario 3: Stolen Documents

On a Monday morning, the organization receives a call from the Federal Bureau of Investigation (FBI) regarding some suspicious activity involving the organization's systems. Later that day, an FBI agent meets with members of management and the legal department to discuss the activity. The FBI has been investigating activity involving public posting of sensitive documents, and some of the documents reportedly belong to the organization. The agent asks for the organization's assistance, and management asks for the incident response team's assistance in acquiring the necessary evidence to determine if these documents are legitimate or not and how they might have been leaked.
The following are additional questions for this scenario:

3.1. From what sources might the incident response team gather evidence?

Response: (e.g., change management logs, surveillance records, access controls logs, DLP logs)

3.2. What would the team do to keep the investigation confidential?

Response: (e.g., Limit the number of involved IRT members)

3.3. How would the handling of this incident change if the team identified an internal host responsible for the leaks?

Response: (i.e. Internal host would be removed/quarantined for evidence and shared with FBI)

3.4. How would the handling of this incident change if the team found a rootkit installed on the internal host responsible for the leaks?

Response: (e.g., All systems would be checked for the identified rootkit)

Department Responses:

Each department should consider the potential impact of the incident scenario and document the necessary action steps that will be taken during the incident. Not all scenarios will require a response from every department. The exercise is intended to foster discussion among departments and the incident response team to maximize the effectiveness of the response.

Third-Party vendors are critical to an organization and should be included in the organizations Incident Response Program. Scenarios can and should be shared with critical vendors to ensure program gaps are identified and addressed.

The list of departments (below) is an example and is not an exhaustive list and may not represent your organizations structure.

Departments
Operations
Marketing/Communications
Finance
HR
Facilities
Information Technology
Information Security/Risk Management
Response:

Third-Party Vendors
Response:

4. Scenario 4: 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:

4.1. What sources might the team use to determine when the compromise had occurred?

Response: (e.g., SIEM logs, MSSP logs, Change Management tickets)

4.2. 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?

Response: (e.g., Administrative/Privileged and non-administrative account passwords would be changed for all employees.)

4.3. 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?

Response: (e.g., Notify appropriate authorities, i.e. FBI, local PD of potential PII exposure, notify impacted employees of potential exposure)

4.4. How would the handling of this incident change if the team discovered a rootkit on the server?

Response: (e.g., Server would be removed from production environment for forensic evidence collection. All servers would be scanned for identified rootkit. BCP process would be executed for impacted server.)

Department Responses:

Each department should consider the potential impact of the incident scenario and document the necessary action steps that will be taken during the incident. Not all scenarios will require a response from every department. The exercise is intended to foster discussion among departments and the incident response team to maximize the effectiveness of the response.

Third-Party vendors are critical to an organization and should be included in the organizations Incident Response Program. Scenarios can and should be shared with critical vendors to ensure program gaps are identified and addressed.

The list of departments (below) is an example and is not an exhaustive list and may not represent your organizations structure.

Departments
Operations
Marketing/Communications
Finance
HR
Facilities
Information Technology
Information Security/Risk Management
Response:

Third-Party Vendors
Response:

5. Scenario 5: Unknown Wireless Access Point

On a Monday morning, the organization's help desk receives calls from three users on the same floor of a building who state that they are having problems with their wireless access. A network administrator who is asked to assist in resolving the problem brings a laptop with wireless access to the users' floor. As he views his wireless networking configuration, he notices that there is a new access point listed as being available. He checks with his teammates and determines that this access point was not deployed by his team, so that it is most likely a rogue access point that was established without permission.

The following are additional questions for this scenario:

5.1. *What should be the first major step in handling this incident (e.g., physically finding the rogue access point, logically attaching to the access point)?*

Response: (e.g., Physically locating the device, Network Access Control (NAC) logs will be reviewed. Change logs for enable/disable ports will be reviewed to identify rogue location)

5.2. *What is the fastest way to locate the access point? What is the most covert way to locate the access point?*

Response: (Scan network for rogue devices)

5.3. *How would the handling of this incident differ if the access point had been deployed by an external party (e.g., contractor) temporarily working at the organization's office?*

Response: (e.g., Contact contract owner and vendor(s). Review approval documents for installation of wireless device, Review SOW from contractor., Identify gaps in vendor management process)

5.4. How would the handling of this incident differ if an intrusion detection analyst reported signs of suspicious activity involving some of the workstations on the same floor of the building?

Response: (e.g., Scope of incident response will be expanded to include scanning of workstations on the same floor as well as servers/application accessible from the workstations)

5.5. How would the handling of this incident differ if the access point had been removed while the team was still attempting to physically locate it?

Response: (e.g., Forensic evidence (logs will be reviewed/preserved to identify point of entry)

Department Responses:

Each department should consider the potential impact of the incident scenario and document the necessary action steps that will be taken during the incident. Not all scenarios will require a response from every department. The exercise is intended to foster discussion among departments and the incident response team to maximize the effectiveness of the response.

Third-Party vendors are critical to an organization and should be included in the organizations Incident Response Program. Scenarios can and should be shared with critical vendors to ensure program gaps are identified and addressed.

The list of departments (below) is an example and is not an exhaustive list and may not represent your organizations structure.

Departments

Operations
Marketing/Communications
Finance
HR
Facilities
Information Technology
Information Security/Risk Management

Response:

Third-Party Vendors

Response:

BLACK SWAN TECHNOLOGIES

BLACK SWAN TECHNOLOGIES
Phone: 877-300-3798
Email: info@blackswantechnologies.com
Web: blackswantechnologies.com