Company Logo

Info-Tech Research Group
Security, Risk & Compliance

Security Incident Management Runbook: Malware

Last revised: MM/DD/YY

Contents

Revision History

Version	Change	Author(s)	Date of Change
1.0	Initial Draft		

Introduction

Effective and efficient incident management involves a formal process to detect, analyze, contain, eradicate, recover, and conduct post-incident activities. This runbook provides detailed procedures that govern the incident management process to handle **malware** incidents.

Incident Assessment Methodology

The incident assessment methodology consists of the evaluation of impact, scope, and threat escalation.

Impact

Evaluate the effects of malware on business functions, data, and recovery efforts. Incident impact should be categorized based on the factors below:
[To be completed by and catered to the member organization. Below is an example.]

1. The current and future functional impact on any business function or operation.
2. The informational impact as it relates to the confidentiality, integrity, and availability of data.
3. The time and required resources needed to recover from the incident.

Malware Impact Criteria	
Rating	Definition
High	A malware campaign where servers were compromised and there are indications that: • Sensitive data or privileged account credentials were exfiltrated. • Command and control has been established. • Lateral movement has been identified. • Security defenses (IDS/IPS, AV, anti-malware, etc.) did not detect.
Medium	A malware campaign where endpoints were compromised and there are indications that: • Non-sensitive data or user credentials were exfiltrated. • Command and control was detected but blocked. • Security defenses (IDS/IPS, AV, anti-malware, etc.) did detect.
Low	A malware campaign where security defenses blocked and quarantined.

Scope

Evaluate the scope (i.e. breadth/magnitude) of the incident on systems, users, endpoints, etc. Incident scope is a critical component that aids in decision making throughout the incident management process.
[To be completed by and catered to the member organization. Below is an example.]

Malware Scope Criteria	
Rating	Definition
High	One or more servers are infected.
Medium	Multiple endpoints infected.
Low	Single endpoint infected.

Threat Escalation Protocol

A threat escalation protocol is used to define the type of stakeholders needed during the incident management process. Informing and consulting these stakeholders during the incident management process is crucial when defending the organization against malware. A threat escalation protocol clearly defines escalation procedures for malware incidents. [To be completed by and catered to the member organization. Below is an example.]

Table 1. Threat Escalation Protocol

Threat Escalation Protocol			
Impact	**Scope**		
	High	**Medium**	**Low**
High	Tier 1	Tier 1	Tier 2
Medium	Tier 1	Tier 2	Tier 2
Low	Tier 2	Tier 2	Tier 3

Threat Escalation Protocol

Below is the threat escalation protocol that will be used when dealing with malware incidents.

Threat Escalation Protocol	Criteria	Stakeholders
Tier 1	• High impact, high scope • High impact, medium scope • Medium impact, high scope	• End User • Help Desk • Cybersecurity • IT Operations • CISO • Legal, HR, PR • Senior Management • External Third Parties
Tier 2	• High impact, low scope • Medium impact, medium scope • Medium impact, low scope • Low impact, high scope • Low impact, medium scope	• End User • Help Desk • Cybersecurity • IT Operations • CISO
Tier 3	• Low impact, medium scope • False positive	• End User • Help Desk • Cybersecurity

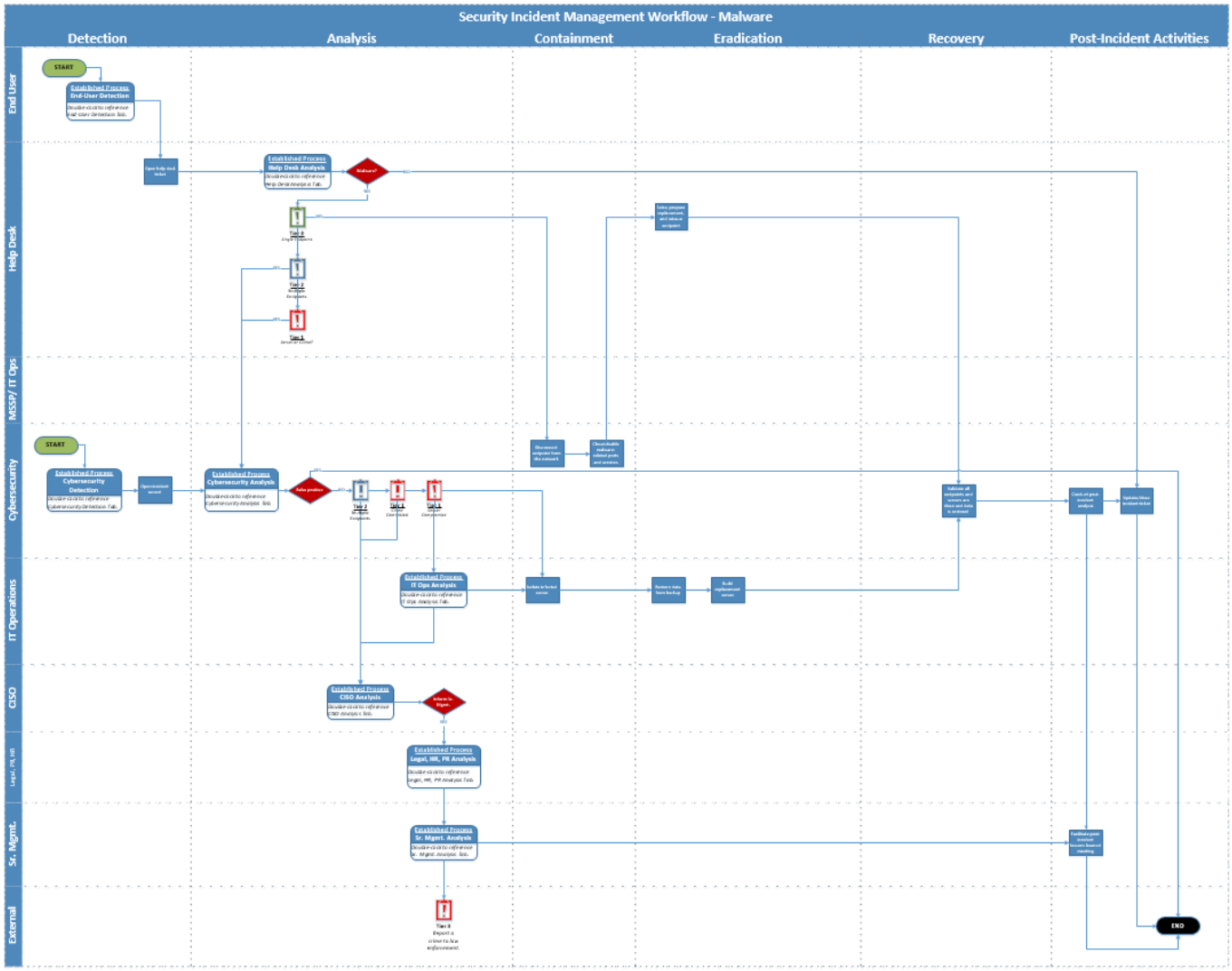
Incident Management Summary

The table below includes the definition of malware, the effects of malware on your organization, and a summary of the response required to deal with this incident.

Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system, or of otherwise annoying or disrupting the victim.
What Is the Incident?	**Malware inbound communication detected:** An inbound malware campaign has been detected (e.g. email, drive by download) through end user, firewall, IPS/IDS, or web proxy. **Malware outbound communication detected:** Outbound malware command and control traffic has been detected through firewall, IPS/IDS, or web proxy. **Malware detected on an end-user device:** One or more managed end-user computing devices has been infected and detected through endpoint protection (EPP) such as Bit9 or Symantec. **Malware detected on a server:** One or more managed servers or network assets has been infected with malware detected through EPP such as Bit9 or Symantec.
Why Should We Care?	Depending on the overall impact of the end-user device or server, this could potentially mean data corruption or loss. • In addition, the end user could be impacted waiting for recovered end-user device. • If a server is corrupted, there is a potential of other end-user devices also being compromised if connected to the impacted server or other data/systems becoming unavailable.
How do we respond?	During malware incidents, stakeholders defined in the threat escalation protocol work collaboratively throughout the entire incident management process. Major activities that take place during malware incidents include the following: 1. **End Users:** Report suspicious incidents and provide any support to help desk and cybersecurity staff. 2. **Help Desk:** Interact directly with the end user to gather incident-related information, create and update tickets, and coordinate with the end user throughout the incident management process. 3. **Cybersecurity:** Monitor security events, analyze logs, conduct open-source intelligence research, provide technical support, identify any control weaknesses, coordinate all incident activities, and document root cause and investigative activities in an incident record. 4. **IT Operations:** Monitor server events, analyze server logs, conduct open-source intelligence research, remove any infected servers from the network, and restore impacted data. 5. **CISO:** Notify and coordinate with the relevant stakeholders and senior management, evaluate control weaknesses, update policies, and facilitate any post-incident activities. 6. **Legal, HR, PR:** Evaluate any brand/reputational damage, determine regulatory compliance violations, conduct any employee disciplinary actions, and facilitate any external reporting. 7. **Senior Management:** Approve any proposed control strategy and allocate budget or resources. ***8.*** **External Third Parties:** Provide incident investigative support and share information.

Incident Response Workflow

The workflow diagram below outlines the incident management process from detection to post-incident activities, including the responsibilities of each stakeholder in each phase. The workflow outlines the decisions, actions, and pre-established processes that are required to deal with the incident at each stage, for all three threat magnitudes.



Response Procedures

The actions required to deal with malware are detailed below for each relevant stakeholder (team), in each of the six phases (detection, analysis, containment, eradication, recovery, and post-incident).

Detection Phase

During the detection phase, teams will evaluate a potential malware incident, for example, an endpoint or server is infected. Once an incident has been detected, a help desk ticket or incident record/ticket is opened to initiate the detection phase.

Team	Description	Questions	Action
Detection: End User	During the detection phase, the end user will report suspicious emails, endpoint issues, and system/service disruptions.	• Am I experiencing abnormal or suspicious behavior? • Did I receive a suspicious email with an attachment? • Am I experiencing an issue with my device, system, or service?	☐ Report a suspected incident or issue to the help desk. Common indicators of compromise include: ○ User receives a suspicious email. ○ User experiences system disruption (unavailable or limited functionality). ○ Other issue with endpoint.
Detection: Help Desk	During the detection phase, help desk staff will monitor calls and submitted tickets.	• Are any end users experiencing malware incidents?	☐ Open a help desk ticket. ☐ Determine if incident needs to be escalated to other stakeholders. Begin analysis phase. ☐ Maintain communications with any impacted end users.
Detection: Cybersecurity	During the detection phase, cybersecurity staff monitor the endpoint protection platform to identify events and incidents.	• Are assets being targeted in a malware campaign? • Were one or more endpoints infected? • Was a server infected? • Are there any EPP event triggers?	☐ Monitor endpoint protection platform (EPP) (e.g. Symantec Endpoint and Bit9 events). ☐ Conduct a preliminary assessment to determine the scope of the incident. Is it a server or endpoint infection? ☐ If multiple devices are infected, update the incident record/ticket with device information, and notify the CISO. ☐ If a server or network asset is infected, update the incident record/ticket with server information, and notify IT Operations and the CISO.
Detection: IT Operations	During the detection phase, IT operations staff will monitor servers and other **events,** and escalate **incidents** to Cybersecurity.	• Are servers being targeted in a malware campaign? • Were one or more servers infected? • Are there any EPP event triggers?	☐ Monitor endpoint protection platforms (EPP) (e.g. Symantec Endpoint and Bit9 events). ☐ Conduct a preliminary assessment to determine the scope of the incident. Is it a server infection? ☐ If a server or network asset is infected, update the incident record/ticket with server information, and notify the CISO.
Detection: CISO	No incident management responsibilities.		
Detection: Legal, HR, PR	No incident management responsibilities.		

Detection: Senior Management	No incident management responsibilities.		

Analysis Phase

During the analysis phase, teams will analyze the incident to determine the impact of the threat. Depending on the impact, a number of teams will be involved in the remediation of the malware incident, and the notification of the threat will be escalated as appropriate.

Team	Description	Questions	Action
Analysis: End User	No incident management responsibilities beyond ongoing cooperation with incident responders during information gathering.		
Analysis: Help Desk	During the analysis phase, help desk staff directly interact with the end user, ask incident-related questions, take actions, and document findings in the help desk ticket.	• What is the source of the suspected malware/incident? • Did the end user click a hyperlink? • Did the end user open a file attachment? • Did the end user visit a suspicious website? • Did the end user download software recently? • Did the end user plug in a flash drive? • Are any locally stored, suspicious file extensions identified? • Has the end user been denied access when accessing data or a server? • Are there indications that data was exfiltrated or an organizational asset was enrolled in a botnet?	☐ Open a ticket. ☐ Gather answers to incident-related questions. ☐ Search ticketing platform to identify other impacted end users. If multiple end users are impacted, create a parent/child ticket. ☐ Determine the impact and scope of the incident. ☐ If there are indications that data has been exfiltrated, an asset is enrolled in a bot, initiate corresponding runbook with cybersecurity team. ☐ Assign ticket to cybersecurity team, as appropriate. ☐ Facilitate end-user notifications. ☐ If the incident was a false positive, update the ticket and close the incident record.
Analysis: Cybersecurity	During the analysis phase, cybersecurity staff will analyze appropriate logs, conduct open-source intelligence research, provide technical	• What is the source of the suspected malware incident? • Did the end user click a hyperlink?	☐ Determine any endpoint exposures and the potential risk implications. ☐ Determine if EPP quarantined the malware. ☐ Determine if EPP triggered an anonymous event. ☐ Conduct open-source threat intelligence analysis to identify comparative IOCs.

	support, provide incident coordination support, directly interact with the end user, ask incident-related questions, take actions, and document findings in the incident record.	• Did the end user open a file attachment? • Did the end user visit a suspicious website? • Did the end user download software recently? • Did the end user plug in a flash drive? • Are any locally stored, suspicious file extensions identified? • Has the end user been denied access when accessing data or a server? • Are there indications that data was exfiltrated or an organizational asset was enrolled in a botnet?	☐ Perform limited scope IOC search in firewall, IDS, IPS, and email gateway logs. ☐ Assess the organizational exposure for all internet-facing endpoints. ☐ Investigate any malware ports and determine if they are active. ☐ Gather answers to incident-related questions. ☐ If a flash drive was used, determine if it is infected. ☐ Conduct open-source threat intelligence analysis to identify comparative indicators of compromise (IOCs). ☐ Perform IOC search in firewall, IDS, IPS, email gateway, system, and server logs. ☐ Determine if any end-user device was compromised. ☐ Assess if any servers were impacted and decide if any server infections are to be assigned to the IT operations team. ☐ Determine if data has been exfiltrated or if an organizational asset been enrolled in a botnet. If so, inform the CISO and initiate the data breach runbook.
Analysis: IT Operations	During the analysis phase, IT operations staff will analyze any appropriate server logs, conduct open-source intelligence research, provide technical support, ask incident-related questions, take actions, and document findings in the incident record.	• Are suspicious file extensions identified on the server? • Are any other IOCs identified on the server? • Has the end user been denied access when accessing data or a server? • Are there indications that data was exfiltrated or an organizational asset was enrolled in a botnet?	☐ Determine any server exposures and any potential risk implications. ☐ Assess your organizational exposure for any internet-facing servers. ☐ Investigate any malware server ports and determine if they are active. ☐ Close all unnecessary server ports/services and adopt the principle of least privilege. ☐ Determine any impact to servers, applications, or storage.
Analysis: CISO	During the incident management analysis phase, the CISO will notify and coordinate with the relevant stakeholders and senior management.	• Has data been exfiltrated or has an organizational asset been enrolled in a botnet? • Has data been lost or stolen? • Are any business applications impacted? • Does a disaster recovery plan need to be enacted?	☐ Publish corporate-wide situational awareness alerts to inform end users of any system outages. ☐ Coordinate and inform senior management of any incident updates. ☐ Approve enactment of the disaster recovery plan, if applicable. ☐ Report any external criminal activities to senior management. ☐ Engage Legal, HR, and PR to address the incident, as appropriate. ☐ Determine if any incident information should be shared with external parties.
Analysis: Legal, HR, PR	During the analysis phase, legal, HR, and PR staff will analyze	• Are there potential legal repercussions to the incident?	Legal: ☐ Determine if any regulatory, legal, or compliance mandates have been violated or impacted.

	any insider activity, brand, or reputational damage.	• Was there any insider activity or other misuse of resources that led to this incident? • Was there any brand or reputational damage?	☐ Determine if any breach notifications are required. HR: ☐ Determine if any employee acceptable-use or security policies have been violated. ☐ Determine if any employee disciplinary actions are required. PR: ☐ Determine if any public reputational or brand damage has occurred.
Analysis: Senior Management	During the analysis phase, senior management staff will notify and coordinate with the relevant stakeholders.	• Is there any brand/reputational damage? • Have we been informed of any crimes? • Is there any major business disruptions?	☐ Provide an incident summary and updates to the board of directors/stakeholders. ☐ Approve reporting crime to law enforcement, if necessary. ☐ Analyze and approve emergency budget, resource, or control requests, as appropriate. ☐ Approve communication of incident information with external parties.

Containment Phase

During the containment phase, teams will isolate and contain any infected endpoints, servers, or storage arrays, and ensure they are not allowed back on the network.

Team	Description	Questions	Action
Containment: End User	No containment responsibilities beyond ongoing cooperation with incident responders.		
Containment: Help Desk	During the containment phase, the help desk staff will maintain communications with any impacted end users.	• Do any end users need to be notified?	☐ Maintain communications with any impacted end users. ○ Inform users if any critical systems or data will be unavailable or affected during the response process.
Containment: Cybersecurity	During the containment phase, cybersecurity staff will document all activities in the incident report.	• What stakeholders need to be notified of the incident report findings? • Has the malware been successfully contained at the endpoint(s)? • Is a forensics endpoint image required?	☐ Provide incident coordination support to IT Operations. ☐ Isolate or disconnect the infected endpoint from the network. ☐ Block any malicious inbound or outbound connections to command and control servers. ☐ Close any malware-related ports and disable any malware-related services. ☐ Take a forensics image of the endpoint as required.
Containment: IT Operations	During the containment phase, IT operations staff will remove any infected	• Was a server infected? Which ones need to be isolated?	☐ Isolate or disconnect any servers. ☐ Take a forensics image of the server as required.

	servers from the network.	• Is a forensics server image required?	
Containment: CISO	During the containment phase, the CISO will evaluate any control weaknesses and make recommendations for remediation.	• Are the current security controls sufficient? • Has data been exfiltrated or has an organizational asset been enrolled in a botnet?	☐ Provide senior management with incident updates. ☐ Determine if the current security controls need to improved. ☐ Continue to coordinate with the cybersecurity group to determine if any data was exfiltrated or if an organizational asset was enrolled in a botnet.
Containment: Legal, HR, PR	During the containment phase, PR may address the public and other stakeholders to inform them of the status of the incident and contain possible rumors, speculation, and reputational damages. Legal and HR will continue ongoing efforts that began in the analysis phase.	• What types of communication are required? • Are there any legal and HR processes that need to be continued?	Legal: ☐ Continue legal actions as necessary, informing affected parties as required by regulations. PR: ☐ If necessary, address the affected stakeholders (including the public), informing them of the steps that have been taken to contain the incident and future steps to fully remediate the incident. HR: ☐ Continue HR actions, as necessary, particularly containing any further employee misuse or violations.
Containment: Senior Management	During the containment phase, senior management will determine if any core business function is impacted and will provide final approval for drastic measures.	• Do any business-critical services, systems, or data need to be taken offline for effective containment of the incident?	☐ Determine if any additional stakeholders need to be notified. Provide the notification. ☐ Provide final approval for taking business-critical systems offline or other major containment decisions.

Eradication Phase

During the eradication phase, teams will restore and reissue endpoints and servers. After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

Team	Description	Questions	Action
Eradication: End User	No eradication responsibilities beyond ongoing cooperation with incident responders.		
Eradication: Help Desk	During the eradication phase, the help desk will maintain	• Does the end user need to be notified of any updates?	☐ Seize, prepare replacement, and reissue endpoint, if necessary.

	communications with impacted end users and reissue devices, if necessary.	• Do any users need new/updated devices issued?	☐ Maintain communications with any impacted end users.
Eradication: Cybersecurity	During the eradication phase, cybersecurity staff will ensure the cause of the infection is eliminated.	• Are there any infected endpoints still on the network? • Is the root cause of the infection addressed?	☐ Clean endpoint(s) of malware. Delete unwanted files identified through malware scans. ☐ Inform the CISO of any organization anti-malware defense control gaps.
Eradication: IT Operations	During the eradication phase, IT Operations will install patches and eliminate other possible sources of the incident.	• Have systems/vulnerabilities adequately been patched?	☐ Install system/security patches to resolve malware/network/other vulnerabilities. ☐ Re-issue credentials, if necessary.
Eradication: CISO	During the eradication phase, the CISO will approve new or updated controls.	• Do any new controls need to be implemented? • Do any controls need to be updated? • Are there any control gaps that allowed this incident to occur?	☐ Approve new controls and the updating of existing ones.
Eradication: Legal, HR, PR	During the eradication phase, legal, HR, and PR staff will evaluate if any new findings have led to new actions, otherwise they will continue any ongoing processes.	• Are there any changes to legal, HR, or PR requirements?	☐ Reassess if any new findings have changed the required legal, HR, or PR actions. If so, address those requirements. ☐ Otherwise continue legal, HR, and PR efforts already begun.
Eradication: Senior Management	No specific eradication responsibilities beyond ongoing support and approval, as necessary.		

Recovery Phase

During the recovery phase, teams will enact processes and procedures for recovery and full restoration of any infected endpoints or servers during the incident. In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g. firewall rulesets, boundary router access control lists).

Team	Description	Questions	Action
Recovery: End User	No incident management responsibilities.		

Recovery: Help Desk	During the incident management recovery phase, the help desk staff will maintain communication with impacted end users.	• Does the end user need to be notified?	☐ Maintain communications with any impacted end users. Inform users: ○ When operations are back to normal. ○ Of any required changes (e.g. updates to systems, passwords). ○ Of updated training and awareness material regarding the incident. ☐ Re-issue end-user devices and credentials, if necessary. ☐ Ensure help desk ticket is updated with all relevant information.
Recovery: Cybersecurity	During the recovery phase, the cybersecurity team will verify that operations have been successfully restored and that the incident ticket is up-to-date.	• Has the endpoint been successfully redeployed in the network? • Is the incident report comprehensive?	☐ Perform vulnerability assessment and antivirus and anti-malware scans on any endpoints or servers to ensure the threat has been remediated. ☐ Determine if the redeployed endpoint is operating normally in the network. ☐ Ensure incident record/ticket is updated with relevant information. ☐ Advise the CISO of any controls, processes, or policies that need to be updated.
Recovery: IT Operations	During the recovery phase, IT Operations will recover and restore systems back to regular operations.	• Do any other servers or systems need to be restored?	☐ Restore systems/servers from backup or build replacement, as appropriate. ☐ Once restored, perform system/network/device validation and testing to verify that the system functions the way it was intended/had functioned in the past. Coordinate with the business units as needed.
Recovery: CISO	During the recovery phase, the CISO will evaluate any weaknesses in security controls or updates to policies as appropriate.	• Do any controls or policies need to be updated?	☐ Review any security policies or controls, as appropriate. ☐ Inform senior management that operations have been restored.
Recovery: Legal, HR, PR	During the recovery phase, legal, HR, and PR staff will complete their respective processes, ensuring all actions are documented.	• Do any employees need disciplinary action? • What message needs to be communicated to stakeholders/the public? • What legal or regulatory next steps are required?	☐ Legal: Follow up with any legal implications and requirements. ☐ HR: Ensure employee records are updated with any infractions (e.g. misuse of corporate resources causing an incident) and subsequent disciplinary actions. If disciplinary actions have not been issued yet, begin process in coordination with the employee's manager. ☐ PR: Communicate with stakeholders/public that the incident has been resolved, including next steps.
Recovery: Senior Management	No incident management responsibilities.		

Post-Incident Phase

During the post-incident phase, teams will perform root-cause analysis and lessons-learned activities with various teams and stakeholders within the organization. Any recommended outcomes should be implemented to ensure continuous improvement and all related active tickets should be updated and closed. This phase involves performing post-mortem, root-cause analysis, and lessons-learned activities with various teams and stakeholders within the organization.

Team	Description	Questions	Action
Post-Incident: End User	During the post-incident phase, affected users may provide additional details for post-incident meetings/reports and may participate in additional awareness and training.	• What happened? • What was learned? • What has changed?	☐ If necessary, a primary affected user may answer questions regarding the source of the incident. ☐ General end users may participate in updated awareness training as a result of the incident.
Post-Incident: Help Desk	During the post-incident phase, the help desk may participate in post-incident meetings, as necessary.	• What happened? • How did we respond? • What should we do next time?	☐ Participate in post-mortem/lessons-learned meetings, as necessary.
Post-Incident: Cybersecurity	During the post-incident phase, cybersecurity will support any post-incident activities, as appropriate.	• What happened? • How did we respond? • What should we do next time? • Are there any cybersecurity processes that need to be improved?	☐ Participate in lessons-learned meetings, as necessary. ☐ Update and close incident ticket. ☐ Update and distribute updated malware awareness and training material.
Post-Incident: IT Operations	During the post-incident phase, IT Operations will support any post-incident activities, as appropriate.	• What happened? • How did we respond? • What should we do next time? • Are there any IT operations processes that need to be improved?	☐ Participate in any post-incident meetings, as appropriate.
Post-Incident: CISO	During the post-incident phase, the CISO will facilitate any post-incident activities.	• How can the incident response process be improved?	☐ Determine if a full-fledged post-mortem/lesson-learned meeting is necessary. ☐ Determine who should participate (e.g. end users, Legal, HR, PR). ☐ Facilitate post-incident meetings (or assign the responsibility to another individual). Ensure a record is maintained.

Post-Incident: Legal, HR, PR	During the post-incident phase, legal, HR, and PR staff will support any post-incident activities, as appropriate.	• Are there any legal, HR, or PR processes that need to be improved?	☐ Participate in any post-incident meetings, as appropriate. ☐ If new findings become known as a result of post-incident activities, follow-up with any new or ongoing legal, HR, and PR duties that have not already been addressed. ○ Legal: Follow up with any legal actions, if required. ○ HR: Follow up with any employee disciplinary action, if required. ○ PR: Follow up on public and internal communications to address the resolution of the incident and steps being taken to prevent reoccurrences.
Post-Incident: Senior Management	During the incident management post-incident phase, senior management will support any post-incident activities, as appropriate.	• Are there any senior management processes that need to be improved?	☐ Participate in any post-incident meetings, as appropriate. ☐ Address stakeholders/board of directors, if necessary. ☐ Approve future investments to help prevent reoccurrences.