INFO~TECH
RESEARCH GROUP

Company Logo

Info-Tech Research Group
Security, Risk & Compliance

Security Incident Management Runbook: Ransomware

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 procedure to handle **ransomware** incidents.

Incident Assessment Methodology

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

Impact

Evaluate the effects of ransomware attacks 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.

Ransomware – Impact Criteria	
Rating	Definition
High	A ransomware campaign where any business-critical or sensitive data was affected and/or public notification is required. OR if critical systems are affected, OR if ransomware is publicly facing, OR a ransom payment was made.
Medium	A ransomware campaign where non-business-critical data are affected.
Low	A ransomware campaign targeting end users where no data was impacted, but the system is infected.

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.]

Ransomware – Scope Criteria	
Rating	Definition
High	Any critical systems AND/OR any servers are affected.
Medium	Multiple endpoints are infected.
Low	Single endpoint is 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 ransomware. A threat escalation protocol clearly defines escalation procedures for ransomware 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 ransomware incidents.

Threat Escalation Protocol	Criteria	Stakeholders
TEP 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
TEP 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
TEP Tier 3	• Low impact, medium scope • False positive	• End User • Help Desk • Cybersecurity

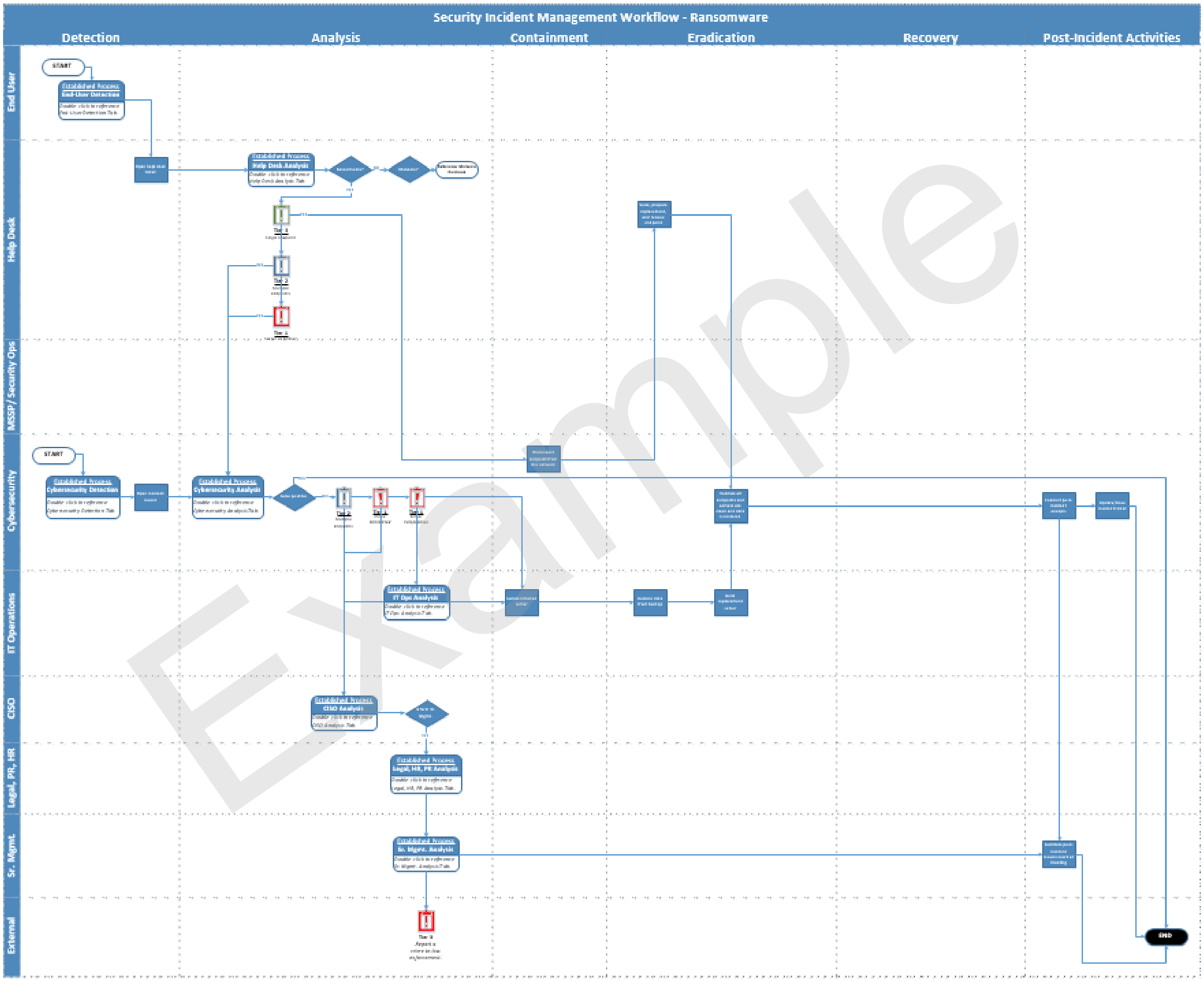
Incident Management Overview

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

What is ransomware?	Ransomware is a generic term used for a family of malware that will attempt to extort money from a user, locking either their system or some of their data and alerting them that if they pay a ransom, they will get access back.
What is the incident?	1. **Ransomware inbound communication detected:** Inbound ransomware campaign has been detected through end-user firewall, IPS/IDS, web proxy, etc. 2. **Ransomware outbound communication detected:** Outbound ransomware command and control traffic has been detected through firewall, IPS/IDS, web proxy, etc. 3. **Ransomware detected on an end-user device:** One or more managed end-user computing device(s) has been infected as a result of ransomware delivered through email, drive-by download, etc. 4. **Ransomware detected on a server:** One or more managed servers or network connected storage arrays (file server) has been infected with ransomware.
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 data. 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 ransomware incidents, stakeholders defined in the threat escalation protocol work collaboratively throughout the entire incident management process. Major activities that take place during ransomware 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:** Providing incident investigative support and sharing information.

Incident Management Workflow: Ransomware

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.



Response Procedures

The actions required to deal with ransomware 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 ransomware incident, for example, an endpoint or server was encrypted. Once an incident has been detected, a help desk ticket or an 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.	• What should I do with the suspicious email? • How do I resolve the issue with my endpoint? • When will my system or service be restored? • How do I remove the pop-up screen?	□ Report a suspicious email. □ Report an issue with an endpoint. □ Report a system or service disruption. □ Report a pop-up screen preventing access to an endpoint.
Detection: Help Desk	During the detection phase, help desk staff will monitor calls and submitted tickets.	• Are any end users experiencing ransomware 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 will monitor events and escalate incidents, as necessary.	• Are assets being targeted in a ransomware campaign? • Are assets actively communicating with a ransomware command-and-control server?	□ Review and monitor alerts and events, including the following: ○ Firewall event, IDS/IPS, anti-virus, anti-malware, email gateway events □ Open or auto-generate an incident record.
Detection: IT Operations	No incident management responsibilities.		
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 ransomware incident, and the notification of the threat will be escalated as appropriate.

Team	Description	Questions	Action
Analysis: End User	During the analysis phase, end users will provide information related to the incident as required.	• Are there emails with hostile content in my inbox? • Do I have access to my data?	□ Provide information related to the incident to the help desk.
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.	• 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 server? • Are there indications that a crime was committed (e.g. Bitcoin payment)?	□ Open a help desk ticket. □ Gather answers to incident-related questions. □ Identify incident-related keywords (*Bitcoin, ransom, encrypted, decrypted, lock, unlock, crypt*, etc.). □ Search ticketing platform to identify other impacted end users. If multiple end users are impacted, create a parent/child ticket. □ Document findings in a help desk ticket. □ Assign help desk ticket to cybersecurity team, as appropriate. □ Facilitate end-user notifications. □ Close help desk ticket, as appropriate.
Cybersecurity	During the analysis phase, cybersecurity staff will analyze appropriate logs, conduct open-source intelligence research, provide technical 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 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 server? • Are there indications that a crime was committed (e.g. Bitcoin payment)?	□ Determine any endpoint exposures and the potential risk implications. □ Assess your organizational exposure for all internet-facing endpoints. □ Maintain a dynamic and frequently updated listing of active endpoint ports. □ Close all unnecessary endpoint ports/services and restrict local admin rights. □ Gather answers to incident-related questions. □ Search web proxy logs to identify any outbound command and control traffic. □ Determine if the USB is infected. □ Conduct open-source threat intelligence analysis to identify comparative indicators of compromise (IOCs). □ Perform IOC search in firewall, IDS, IPS, email gateway, and system and server logs. □ Determine if any end-user devices were compromised.

			□ Assess if any servers were impacted and decide if any server infections are to be assigned to the infrastructure team. □ Decide if any local/server data was encrypted. □ If the incident was a false positive, update the ticket and close the incident record.
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 server? • Are there indications that a crime was committed (e.g. Bitcoin payment)? • Is the data backed up? Are those backups reliable?	□ Determine any server exposures and the potential risk implications. □ Assess your organizational exposure for any internet-facing servers. □ Maintain a dynamic and frequently updated listing of active server ports. □ Close all unnecessary server ports/services and adopt the principle of least privilege. □ Determine any impact to servers, applications, or storage. □ Determine exactly how much of your network has been infected and how many files have been compromised. □ Investigate the existence of reliable backups.
Analysis: CISO	During the analysis phase, the CISO will notify and coordinate with the relevant stakeholders and senior management.	• Has a crime been committed? • Has data been lost or stolen? • Are any business applications impacted? • Does a disaster recovery plan need to be enacted? • If reliable backups are not available, what is the next step?	□ Publish corporate-wide situational awareness alerts to inform end users of any system outages. □ Consult with senior management to identify next step if reliable backups are not available (e.g. pay ransom, build new). □ Coordinate and inform senior management of any incident updates. □ Approve the disaster recovery enactment plan. □ Report any external criminal activities to senior management. □ Engage Legal, HR, and PR to publicly address the scope of 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 any insider activity and brand or reputational damage.	• Was there any insider activity? • Was there any brand or reputational damage?	Legal: □ Determine if any regulatory, legal, or compliance mandates have been violated or impacted. □ 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 incident management analysis phase, senior management will notify and coordinate with the relevant stakeholders.	• Was there any insider activity? • Was there any brand or reputational damage? • Has a crime been committed? • Has data been lost, and does a disaster recovery plan need to be enacted? • If reliable backups are not available, what is the next step?	□ Determine plan for lost data (e.g. pay ransom, rebuild). □ Provide an incident summary/updates to the board of directors. □ Approve reporting crime to law enforcement. □ Approve communication of any incident information with external parties.

Containment Phase

During the containment phase, teams will isolate and contain the infected device(s), servers, and storage arrays, and ensure they are not allowed back on the network.

Team	Description	Questions	Action
Containment: End User	No eradication responsibilities beyond ongoing cooperation with incident responders.		
Containment: Help Desk	During the containment phase, the help desk will maintain communications with any impacted end users.	• Do any end users need to be notified?	□ Maintain communications with any impacted end users.
Containment: Cybersecurity	During the containment phase, cybersecurity staff will document all findings in the incident report.	• Which stakeholders need to be notified of the incident report findings?	□ Provide incident coordination support. □ Isolate or disconnect the infected endpoint from the network. □ Block all connections to TOR nodes.
Containment: IT Operations	During the containment phase, IT operations staff will remove any infected servers from the network.	• Was a server infected?	□ Create an OS-level image of any endpoint, servers, or storage arrays to prevent future data loss. □ Isolate or disconnect any servers.
Containment: CISO	During the containment phase, the CISO will update senior management.	• Are the current security controls sufficient?	□ Determine if the current security controls need to be improved. □ Provide senior management with incident updates.
Containment: Legal, HR, PR	During the containment phase, Legal, HR, and PR staff will evaluate if any public relations or legal actions need to be taken.	• Are there any legal requirements or notification requirements? • Does the public need to be informed? • Does any reputational damage need to be contained?	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.	- Has the incident impacted any core business functions? - Has any brand or reputational damage occurred?	□ Determine if any additional stakeholders need to be notified.

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 communications with impacted end users.	- Does the end user need to be notified?	□ Seize, prepare replacement, and reissue endpoint. □ Maintain communications with any impacted end users.
Eradication: Cybersecurity	During the eradication phase, cybersecurity staff will ensure all endpoints are clean.	- Are there any infected endpoints still on the network?	□ Perform vulnerability assessment and antivirus and anti-malware scans on any endpoints or servers to ensure the threat has been remediated.
Eradication: IT Operations	During the eradication phase, IT operations staff will restore data and identify defense gaps in the organization.	- What data needs to be restored? - What needs to be rebuilt? - Are there any controls gaps that allowed this incident to occur?	□ Restore data from backup. □ Build replacement server. □ If necessary, rebuild. □ Inform the CISO of any organizational anti-malware defenses control gaps.
Eradication: CISO	During the eradication phase, the CISO will develop any control weakness strategies, as appropriate.	- Do any new controls need to be implemented? - Do any controls need to be updated?	□ 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 public relations or legal actions need to be taken.	- Are there any legal requirements or notification requirements? - Does the public need to be informed? - Does any reputational damage need to be contained?	□ 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 process and procedures for the 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 recovery phase, the help desk will maintain communications 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 eradication phase, cybersecurity staff will determine if operations have been restored and document any findings in an incident report.	• 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 ransomware has been remediated. □ Determine if all endpoints are operating as expected. □ 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 eradication phase, IT operations staff will ensure that all servers and systems are back online and restored.	• 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.
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 and 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-	• What happened? • How did we respond? • What should we do next time?	□ Participate in lessons-learned meetings, as necessary. □ Update and close incident ticket. □ Update and distribute updated malware awareness and training material.

	incident activities, as appropriate.	• Are there any cybersecurity processes that need to be improved?	
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/lessons-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 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.

For acceptable use of this template, refer to Info-Tech's Terms of Use. These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.