

# Ransomware Incident Response Playbook

Title	Ransomware Incident Response Playbook
Version	1.0
Date issued	DD-MM-YYYY
Status	In progress
Document owner	
Creator name	
Creator organization name	ECC
Subject category	Ransomware Incident Management
Access constraints	
Review cycle	Annually

## 1. Introduction

### 1.1 Incident Overview

Ransomware incidents compromise a system by locking its screen or encrypting critical files to prevent them from being accessed in the system. Attackers can also use the compromised network of an organization to distribute ransomware to other systems within that network. Once a system is infected by ransomware, attackers demand a ransom to decrypt these files or provide access to the system. Usually, attackers target and threaten organizations/users to sell/leak sensitive information if they are reluctant to pay the ransom demanded. Ransomware can infect a system in different ways such as by accessing unsafe websites, downloading and installing unknown applications, and clicking on malicious links.

Assume that CyberZee's systems were infected with ransomware after an employee accessed a compromised website. Subsequently, critical files on the systems were encrypted and users could not access these files until they paid the ransom displayed on the screen.

### 1.2 Purpose of Playbook

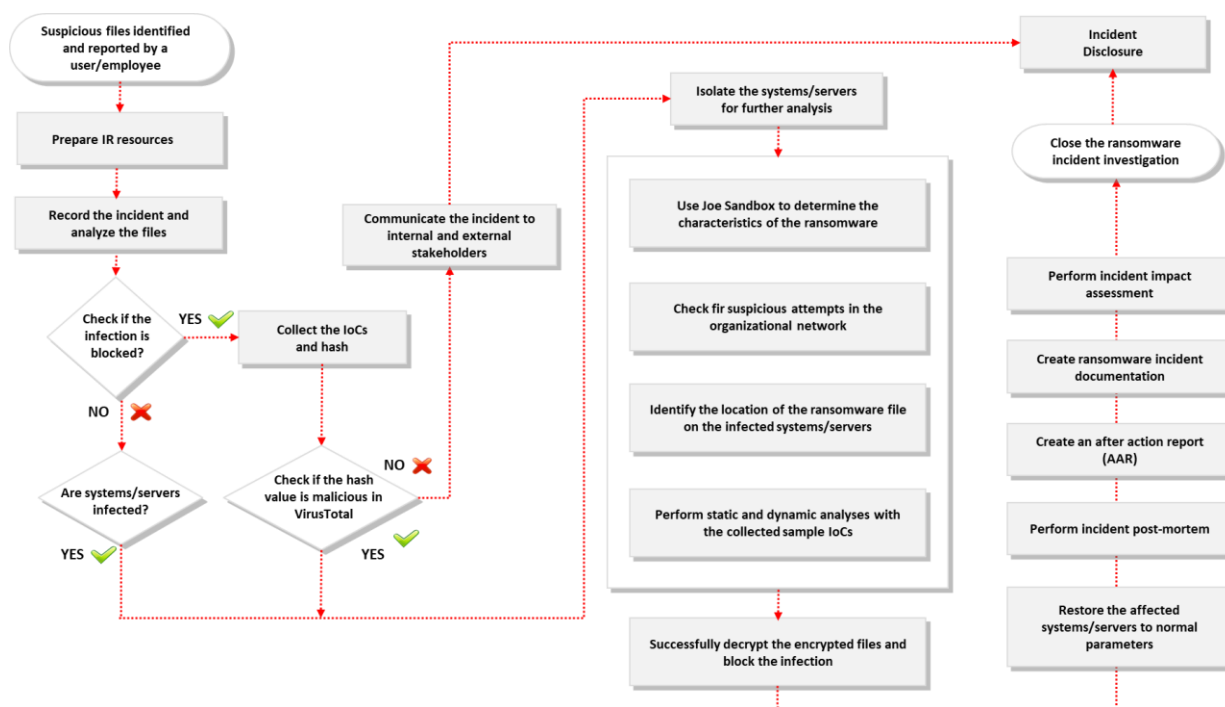
The main purpose of this ransomware playbook is to assist incident handlers in handling ransomware incidents in an organization. This playbook can be used as a guidance to handle ransomware incidents by establishing effective communication between the stakeholders during the entire incident response process.

### 1.3 Scope

This playbook is developed for the use of incident responders for handling ransomware incidents in an organization. Additionally, this document must be used alongside the incident response plan of the organization. The scope of this document is listed below (not limited to):

- Determine the business impact caused by a ransomware incident
- Detect and analyze the ransomware that infected the systems/servers
- Understand the reason behind the ransomware incident
- Implement the incident response plan under the supervision of higher authorities of the organization
- Efficiently contain, eradicate, and recover systems affected by the ransomware incident

### 1.4 Workflow Diagram



Workflow diagram for ransomware incident response

## 2. Preparation

### 2.1 Objectives

The main objective of the preparation phase involves:

- Preparing the organization to respond to ransomware incidents in a timely and effective manner

- Define various roles and their communication medium for the entire ransomware incident response process
- Prepare organizational systems, network, and data to handle any ransomware incident
- Prepare employees regarding their roles and reporting procedures during a ransomware incident

## 2.2 Activities Involved

*[Activities may differ based on organizational policies, but they are not limited to the following.]*

- Prepare for ransomware incident response:
  - Ensure that the IH&R team has extensive knowledge of each malware category, propagation method, and infection chain, along with the methods used to extract malware data from compromised devices
  - Ensure that the IH&R team understands how to use different malware detection tools, techniques, and configurations to extract malware from different systems
  - Collaborate with IT, administrative, and legal teams to get extended support during incident response
  - Ensure to have a secure workstation to handle files and systems affected by ransomware
  - Ensure to validate the existing resources and communication channels before beginning the incident response process
  - Inform the management about various solutions that must be included in the ransomware incident response toolkit
  - Get the required level of access to resources from the management to handle ransomware attacks
  - Discuss the various steps to be followed, from detection to post-incident activities, with subject matter experts (SMEs) and IH&R team members
  - Ensure to have liability insurance that covers malware attacks
  - Ensure that all systems and servers have active antimalware solutions such as Malwarebytes and Bitdefender Total Security
  - Ensure that the IH&R team members are aware of current malware trends and methods of malware detection
  - Ensure to have documents related to similar past incidents for the IH&R team
  - Ensure that the IH&R team has prior knowledge and awareness to safely handle malware and its importance

- Provide access to the required documentation such as incident response plan and network architecture for responding to a ransomware incident. Links of important documents are listed below:
  - Link 1:
  - Link 2:
  - Link 3:
- Prepare a questionnaire to be asked by tech support from the complainants to analyze the ransomware incident
- Ensure that all employees store their data on the shared drive with proper backup facility instead of local drives
- Remove local administrative rights if not required
- Establish secure communication channels such as telephone, message, and VoIP to report incidents and send data to the incident response team and other authorities
- Ensure to create rules and policies specific to the malware incident response process
- Run and test the incident response process multiple times before initiating the actual response process
- Inform the employees:
  - Conduct regular training and awareness programs regarding phishing incidents because most ransomware cases originate from phishing
  - Create a proper format for reporting and registering complaints
  - Ensure that training and awareness sessions are mandatory for employees handling critical data, systems, and servers of the organization
  - Provide proper contact information of personnel who can be contacted by users and employees in case of a ransomware incident

## 2.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Prepare for ransomware incident response <ul style="list-style-type: none"> <li>○ Create incident response processes and procedures</li> <li>○ Define roles and responsibilities</li> <li>○ Review recent incident reports</li> <li>○ Incorporate threat intelligence</li> <li>○ Maintain an incident response plan with the necessary documents</li> <li>○ Define threat indicators and incorporate alerting solutions</li> </ul>	CISO	Email, Phone, Text Message
	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Service Desk	Email, Phone, Text Message
	Service Delivery Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Technicians	Email, Phone, Text Message
	Administrators	Email, Phone, Text Message
	Legal Team	Email, Phone, Text Message
	Federal Agency	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
Inform the employees <ul style="list-style-type: none"> <li>○ Conduct training and awareness on ransomware incidents</li> </ul>	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	HR Manager/Director	Email, Phone, Text Message
	Administrators	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

## 2.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- Template for Preparing Malware Testbed.docx
- IH&R Plan Template.docx
- IH&R Plan Checklist.docx

### 3. Detection and Notification

#### 3.1 Objectives

The main objectives of the detection and notification phase are given below:

- Identify the type of ransomware infection
- Identify the type of files, folders, or keys encrypted by the malware
- Identify the source of an attack (i.e., phishing, malicious website access, unknown device plug-in, or unpatched software)
- Identify the type of communication channel established to operate the malware (such as Powershell, C&C, or GUI)
- Detect whether any post-exploitation frameworks are implemented
- Determine whether the attacker adopted any Ransomware as a Service (RaaS) business model
- Perform preliminary investigation and report the findings
- Assign the appropriate IH&R team members to handle the ransomware incident

#### 3.2 Activities Involved

*[Activities may differ based on organizational policies, but they are not limited to the following.]*

- Detect and report the ransomware incident:
  - Check SIEM solution alerts to identify ransomware incidents
  - Check for vulnerabilities in the recent patches released by the vendor
  - Check for the creation of duplicate files with an existing file name
  - Check for data encryption or breach
  - Check whether the antivirus solution installed in the victim system is in the disabled state
  - Check for files consuming more space than their usual size
  - Check for the installation of unauthorized software solutions
  - Check whether remote connections have been established with unknown IP addresses using tools such as Wireshark
  - Check for unusual processes or services running on the victim system using tools such as Nmap
  - Check whether any common files or folders have been locked without victim's knowledge
  - Check for special icons for the encrypted files and folders

- Check for files with unusual extensions
- Check whether any service has been exposed
- Check for malware in the encrypted network traffic using tools such as Flowmon and Cisco Encrypted Traffic Analytics
- Check for fileless malware threats in the network using tools such as AlienVault® USM Anywhere
- Check the systems using ransomware detection tools such as Malwarebytes, TotalAV, and Norton360
- Check for the potential indicators of compromise (IoCs) of the ransomware incident
- Escalate the incident to the stakeholders and other authorities through secure communication channels and procedures
- Gather the following information from initial investigation:
  - Type of ransomware such as malware family and variant
  - Identify the location of files infected by ransomware in the compromised system, extract a copy, and store it in a password protected zip file
  - Record incident details such as incident timeline and who detected the incident first; then, list the series of events in the order of occurrence
  - Identify the causes behind the incident
  - Check for suspicious attempts on the organizational network that can be considered IoCs
  - Identify whether the ransomware has modified or created any files that can be considered IoCs
  - Identify the type of endpoint security solution (such as antivirus and antimalware solutions) used to detect the ransomware incident

### 3.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Detect and report the ransomware incident <ul style="list-style-type: none"><li>○ Monitor security solutions</li></ul>	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

<ul style="list-style-type: none"> <li>○ Respond to manual and automated alerts</li> <li>○ Escalate the incident via the ticketing system (if not escalated)</li> </ul>	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Lead Area	Email, Phone, Text Message
Initial investigation <ul style="list-style-type: none"> <li>○ Collect initial evidence data</li> <li>○ Classify and prioritize the incident</li> </ul>	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Service Desk	Email, Phone, Text Message
Notification of the incident <ul style="list-style-type: none"> <li>○ Follow the defined IH&amp;R plan to notify the incident</li> </ul>	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Service Desk	Email, Phone, Text Message

### 3.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- d. Malware Analysis and Detection Template.docx
- e. Incident Identification and Validation Template.docx
- f. Incident Priority Template.docx
- g. Incident Communication Logs Template.docx
- h. Point-of-Contact Template.docx

## 4. Containment

### 4.1 Objectives

The main objective of the containment phase is to isolate systems and servers infected by ransomware from the organizational network and reduce the overall impact.

### 4.2 Containment Steps/Activities

*[Activities may differ based on organizational policies, but they are not limited to the following.]*

- Activities to contain the ransomware incident are listed below:
  - After confirming the ransomware infection, separate the compromised system from the operational network
  - Block C&C communication with remote machines



- Quarantine the email containing the ransomware
- Limit write permissions to host systems
- Ensure that endpoint protection services are updated; if not, update them
- Block malicious executables
- Remove unapproved applications on endpoint nodes
- Create temporary rules and procedures necessary to contain the ransomware
- If the ransomware has compromised multiple systems, isolate the network services of those systems and prioritize them according to the importance of affected hosts to maintain business continuity
- Implement access control networks or virtual private networks (VPNs) for providing connections to non-compromised devices
- Disable the targeted services, applications, and systems until the exploited vulnerabilities are patched
- Remove malicious registry entries added by the malware
- Review the network traffic and block access to the malware command and control server
- Block users from downloading applications from third-party websites
- Disable any core network connections (including switches) and internet communication
- Disable compromised services on servers or at the network level (if required)
- Configure firewalls to block IP addresses or ports associated with the service
- Isolate infected users and groups and prevent file sharing from infected accounts
- Reset all credentials, including passwords, especially for the administrator
- Use automated tools such as antimalware software, IDS, and IPS to contain the ransomware
- Temporarily disable unmoderated mailing lists or email servers to prevent the ransomware from spreading further
- Use tools such as Infoblox Solutions and Microsoft Defender for Endpoint to contain the ransomware incident
- Gather and analyze network system logs to find malware propagation events through shared files and connected systems
- Add IoCs such as hash value to endpoint protection and configure them to block and alert upon detection
- Rectify network or system misconfigurations to contain the ransomware

- Store the backups separate from the infected network and systems
- Configure firewalls and security solutions to block IP addresses or ports associated with the C&C
- Communicate the progress:
  - Regularly inform the stakeholders and authorities about the status of the incident handling process

#### 4.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Containment activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

#### 4.4 Additional information

**Note:** Refer to the following documents to fill the necessary details:

- i. Containment of Malware Incidents Checklist.docx
- j. Incident Containment Template.docx
- k. Incident Containment Checklist.docx

### 5. Analysis

#### 5.1 Objectives

The main objective of this phase is to analyze the ransomware incident and determine its scope. Another objective of this phase is to identify infected files/data and determine their impact for forensic investigation requirements to develop an effective mitigation strategy based on analysis results.

## 5.2 Activities

*[Activities may differ based on organizational policies, but they are not limited to the following.]*

- Perform live-system/dynamic analysis during the incident (wherever applicable):
  - Perform dynamic analysis using port monitoring tools (such as TCPView) and Windows command-line utility tools (such as netstat) to determine whether the malware is trying to access a particular port
  - Monitor processes using tools such as Process Monitor and OpManager to easily identify all processes started by the malware
  - Scan the registry values for suspicious entries that may indicate malware infection using tools such as RegScanner and Reg Organizer
  - Use Windows service monitoring tools such as Windows Service Manager (SrvMan) to trace malicious services initiated by suspicious files during dynamic analysis
  - Scan suspicious startup programs manually or by using startup program monitoring tools such as Autoruns for Windows and HiBit Startup Manager
  - Monitor event logs using tools such as Splunk Enterprise Security and New Relic for components that perform security operations
  - Monitor the installation of malicious executables in the background using tools such as Mirekrosoft Install Monitor and SysAnalyzer
  - Use tools such as PA File Sight and Tripwire File Integrity to scan for suspicious files and folders in systems
  - Scan for suspicious device drivers in systems using tools such as DriverView and Driver Detective to ensure that they are genuine and downloaded from the publisher's original site
  - Use network monitoring tools such as SolarWinds NetFlow Traffic Analyzer, Capsa Network Analyzer, and Wireshark to monitor and capture live network traffic to and from the victim's system for further analysis
  - Perform DNS monitoring using tools such as DNSQuerySniffer and DNSstuff to monitor DNS servers the malware tried to connect to and check their connection type
  - Monitor API calls made by applications using tools such as API Monitor and APImetrics
  - Monitor system calls using tools such as strace to view or trace system calls in a Linux system

- Monitor scheduled tasks using command-line tools such as schtasks and Windows Task Scheduler to retrieve the list of all system scheduled tasks and find the malware
- Monitor browser activities using network monitoring tools such as Wireshark and Colasoft Network Analyzer to monitor user browsing activities and identify malicious traffic
- Perform static analysis during the incident (where applicable):
  - Obtain the hash value of the ransomware file using tools such as HashMyFiles and mimikatz
  - Use online tools such as VirusTotal to check the hash values obtained and gather additional information related to the ransomware file for further investigation
  - Use tools such as BinText and FLOSS to extract embedded strings from executable files
  - Identify obfuscation methods or packing using tools such as PEid, MacroPack, and UPX, which can help in selecting tools to unpack the code of executable files
  - Find portable executable (PE) information using tools such as PE Explorer and PEView to obtain additional details of a file or program (such as its features)
  - Identify dependencies within malware executable files using tools such as Dependency Walker, dependency-check, and Snrk
  - Analyze the disassembled code for anti-reverse engineering malware using debugging tools such as IDA Pro, Ghidra, and OllyDbg
  - Analyze malicious MS Office documents using oleid, a Python-based tool, to review suspicious/malicious components
    - Now, parse malicious Office documents using the oledump tool to identify streams containing macros; then, extract the contents of these macro streams using the same tool
  - Perform memory dump analysis using tools such as Volatility Framework to extensively analyze and assess the malware impact, its location, and propagation methods
  - Use sandbox tools such as Joe Sandbox and CrowdStrike Falcon® Sandbox to determine the characteristics of the ransomware
  - Use tools such as yarGen to generate YARA rules and detect and classify malware and other malicious codes through a rule-based approach

- Perform intrusion analysis during the incident (wherever applicable):
  - Regularly monitor outbound malicious beaconing traffic using network monitoring tools such as CapLoader and Wireshark
  - Monitor unusual traffic to malicious or unknown external entities using network monitoring tools such as PRTG Network Monitor and GFI LanGuard
- After identifying the ransomware variant, examine the tactics, techniques, and procedures (TTPs) used, along with the attacker's toolkit, if possible, and proceed with the eradication procedure
- Take a snapshot of the compromised system
- Analyze logs from endpoints, hosts, and other networked systems
- Analyze the structure, phrases, and scripts used for ransomware creation
- Analyze the payment address or mode to track down the culprit
- Analyze the disabled software solution
- Analyze the popup contents while opening the infected file
- Analyze the discovered IoCs to scan internal ports and services

### 5.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Initiate evidence gathering and forensic analysis	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Analyze the scope of ransomware incident	CISO	Email, Phone, Text Message
	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Analyze the ransomware and report potentially compromised data and services	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

## 5.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- l. Malware Analysis and Detection Template.docx
- m. Malware Analysis Toolkit.docx
- n. Netstat Cheat Sheet.docx
- o. Safely Handling Malware Checklist.docx
- p. Volatility Framework Cheat Sheet.docx
- q. Evidence Gathering and Forensic Analysis Form.docx

## 6. Eradication

### 6.1 Objectives

The main objective of this phase is to eradicate/remove the ransomware and prevent the occurrence of such incidents in future by taking appropriate security measures.

### 6.2 Eradication Steps/Activities

*[Activities may differ based on organizational policies, but they are not limited to the following.]*

- Perform regular scans using antimalware solutions such as TotalAV and Bitdefender Antivirus Plus to detect and eliminate ransomware
- Use appropriate decryption tools to decrypt ransomware-infected systems and access the data
- Terminate all active sessions and external communication from the system
- Use content filtering tools such as BrowserContol, OpenDNS, and inCompass to block malware exhibiting static characteristics such as strings and loaders
- Blacklist services, programs, applications, and executables that install malware on the system
- Update the organizational malware database with signatures/definitions of the new malware
- Monitor TCP ports such as Remote Desktop Protocol (RDP) and Server Message Block (SMB) that are used by ransomware to infect systems
- Ensure that antimalware software and ransomware protection solutions are updated
- Ensure that the latest patches are installed on all target systems and applications
- Examine the real-time backup system and clear ransomware-related executables (if found)
- Sanitize the system before installing any software solution

- Update the system immediately after eliminating the malware to remove its persistent mechanisms
- Implement strong rules or signatures on defense systems to block similar incidents in future
- Patch all discovered vulnerabilities exploited by the ransomware and inform antimalware manufacturers or developers
- Limit user account privileges to prevent users from installing new applications
- Block websites containing malicious content and disable auto-downloads to prevent automatic malware downloads
- Block popups in browser settings
- Disable autorun for removable media such as USB drives
- Reset the password of all compromised accounts or create replacement accounts and permanently disable the compromised accounts
- Ensure regular data backup to prevent data loss owing to ransomware incidents
- Block the source email address (if the ransomware originated via phishing)
- Modify the firewall and segmentation rules based on the current outcome of the ransomware incident

### 6.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Develop an eradication plan ○ Perform technical and business analyses and create a prioritized eradication plan ○ Establish a communication strategy based on the eradication plan	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Internal/External Communications Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
Eradicate the ransomware incident	Information Security Manager	Email, Phone, Text Message
	Incident Response Team	Email, Phone, Text Message

## 6.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- r. Eradication of Malware Incidents Checklist.docx
- s. Incident Eradication Template.docx
- t. Incident Eradication Checklist.docx

## 7. Recovery

### 7.1 Objectives

The objective of this phase is to restore the affected systems, servers, and other resources from the incident impact and bring them back to the Business As Usual (BAU) state.

### 7.2 Recovery Steps/Activities

*[Activities may differ based on organizational policies, but they are not limited to the following.]*

- Activities to recover from ransomware incidents are listed below:
  - Perform full scans on the system and device backups to ensure that all malware traces have been removed before using backups to restore servers, systems, and databases
  - Initiate a disaster recovery plan and move the business services to a backup location or fail-over site, if required
  - Use sophisticated decryption utilities to recover encrypted files
  - Recover infected systems by reimaging and rebuilding them from scratch or by removing the temporary containment imposed on them
  - Regularly update the systems
  - Selectively back up the data, instead of backing up unnecessary data
  - Check the backup system for IoCs/signs of ransomware before using it to restore data
  - If the backup data cannot be restored, rebuild the system with a new image
  - After the necessary backup, reconnect the system to the network
  - Implement the 3-2-1 backup strategy for better recovery from backup storage
  - Recover the data lost owing to ransomware infection using data recovery tools such as EaseUS Data Recovery Wizard and Remo Recover
  - Reset the password of all employee accounts in the organization
  - Restore email services after blocking malicious email senders at the server-level
  - Disable automatic file sharing between systems



- Perform continuous system monitoring for an extended period even after restoring the data
- Involve legal authorities upon detecting any signs of data breach or exfiltration
- Connect systems to a clean network to download, install, and update the OS and other software
- Use the Windows System Restore utility tool to recover data in Windows systems using point-in-time backups
- Rebuild and clean critical software and components such as BIOS and drivers from a trusted software library and verify the software hashes

### 7.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Recovery activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

### 6.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- u. Recovery from Malware Incidents Checklist.docx
- v. Incident Recovery Procedure Template.docx
- w. Incident Recovery Checklist.docx

## 8. Post-incident Activities

### 8.1 Objectives

The main objective of this phase is to create the necessary reports for ransomware incidents, including incident post-mortem, after action report (AAR), lessons learned, incident documentation, and incident impact assessment. Another objective of this phase is to officially close the ransomware investigation and disclose its details to respective stakeholders through proper channels.

### 8.2 Activities Involved

- Create an incident post-mortem report, root cause analysis (RCA) report, or incident review to detect the root causes of the ransomware incident
- Create an AAR that includes information such as what worked effectively, areas of improvement, and strategies for enhancing response in case of similar ransomware incidents

- Conduct a lessons learned meeting to document the details of the ransomware incident; moreover, ensure that the following questions are answered in this meeting:
  - When and who detected the ransomware incident?
  - What happened exactly?
  - What caused the ransomware incident?
  - What were the challenges encountered?
  - What vulnerabilities or flaws were identified during the investigation?
  - To whom was the ransomware incident reported?
  - Was the organization adequately prepared for the ransomware incident?
  - How was the ransomware incident contained?
  - How were the impacted systems sanitized?
  - What procedures were followed during recovery?
  - Were the documented procedures followed by the response team?
  - How well did the incident response team and management perform in resolving the ransomware incident?
  - How should the incident response team and management respond to mitigate similar incidents in future?
  - Were there any gaps in communicating the ransomware incident?
  - Was the right amount of information shared with the right personnel?
  - What tools and resources are required to detect, analyze, and prevent similar ransomware incidents in future?
- Create concise and clear ransomware incident documentation in a standard format and get it reviewed by an editor
- Create an incident impact assessment report to determine the types of losses caused by the ransomware incident; this report must address the following if required:
  - Financial losses incurred owing to ransomware attack
  - Legal costs for investigating the case, lawyer's fees, etc.
  - Costs pertaining to analyzing the ransomware incident and recovering and installing software and hardware
  - Implementation costs
  - Costs related to the damage of goodwill as well as loss of customer trust and reputation

- Officially close the ransomware investigation by informing the management and securely retain investigation reports considering the retention policy of the organization
- Disclose incident details to the respective stakeholders by consulting with the legal department of the organization
- Conduct phishing awareness campaigns to educate employees or users on accessing specific links or websites
- Refine the existing security policies based on the recent incident handling process
- If certain plans did not work accordingly, review and update them wherever necessary

### 8.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Create an incident post-mortem report	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create an AAR	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Conduct a lessons learned meeting	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create incident documentation	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create an incident impact assessment report	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Officially close the investigation	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Management	Email, Phone, Text Message

Disclose incident details to the respective stakeholders	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	CISO	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Legal Team	Email, Phone, Text Message
	HR Manager	Email, Phone, Text Message
	Media	Email, Phone, Text Message
	Vendors	Email, Phone, Text Message
	Customers & General Public	Email, Phone, Text Message
	Business Partners	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

#### 8.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- x. Incident Postmortem Template.docx
- y. After Action Report Form Template.docx
- z. Incident Documentation Template.docx
- aa. Incident Impact Assessment Report Template.docx
- bb. Incident Closure Letter.docx
- cc. Incident Disclosure Form.docx
- dd. Incident Reporting Template.docx

### 9. Appendix