Incident Response Plan for Ransomware Attacks

[1. Scope and Purpose 2](#_Toc989329400)

[2. Roles and Responsibilities 2](#_Toc1740178842)

[3. What is Ransomware 2](#_Toc154468728)

[4. How do ransomware attacks happen? 2](#_Toc352016007)

[5. Common delivery methods 3](#_Toc1798637326)

[6. Incident Response Plan for a Ransomware Attack 3](#_Toc1359867707)

[a. Preparation 3](#_Toc907597641)

[b. Detection and Initial Response (Identification): 3](#_Toc1945077833)

[c. Containment and Investigation (Containment): 4](#_Toc1947783282)

[d. Eradication 4](#_Toc2000919063)

[e. Mitigation and Recovery (Recovery): 4](#_Toc1932171381)

[f. Communication and Reporting: 5](#_Toc910841088)

[g. Lessons Learned: 6](#_Toc604503453)

[7. Plan Testing or Exercise Requirements 7](#_Toc845904243)

[8. Plan Review and Update Schedule 7](#_Toc1749906235)

[9. Process/Procedure for Recovery 7](#_Toc2002527426)

[10. Playbook for a ransomware incident of 3rd parties/MSPs (Test Scenario) 8](#_Toc1213844526)

# Scope and Purpose

* 1. Purpose: The purpose of this incident response plan is to provide a comprehensive framework for responding to and recovering from ransomware attacks.
  2. Scope: This plan applies to all employees, contractors, and stakeholders who handle or have access to sensitive information and systems within the organization.

# Roles and Responsibilities

* 1. Incident Response Team: Responsible for coordinating and executing the response plan during a ransomware incident. This team typically includes representatives from IT, cybersecurity, legal, communications, and executive management.
  2. IT Operations: Responsible for implementing technical measures, such as isolating affected systems, restoring backups, and ensuring the recovery of critical systems.
  3. Cybersecurity Team: Responsible for analyzing the ransomware, identifying its characteristics, and implementing appropriate security measures to prevent further infections.
  4. Legal Team: Responsible for advising on legal and regulatory requirements, engaging with law enforcement agencies, and handling any potential negotiations with attackers.
  5. Communications Team: Responsible for managing internal and external communications, including notifying affected parties, customers, employees, and media, as well as managing public relations.
  6. Executive Management: Responsible for providing strategic direction, making key decisions, and allocating necessary resources during a ransomware incident.

# What is Ransomware

Ransomware is a type of malicious software that encrypts files or restricts access to a victim's computer system, typically accompanied by a demand for payment (usually in cryptocurrency) to restore access or decrypt the files. It is a form of cyber extortion where attackers seek financial gain by exploiting vulnerabilities in systems or tricking users into executing malicious code.

# How do ransomware attacks happen?

* 1. Phishing Emails: Attackers send deceptive emails containing infected attachments or malicious links. When users click on these links or open attachments, the ransomware is downloaded and executed.
  2. Malvertising: Attackers inject malicious code into legitimate online advertisements, redirecting users to websites hosting ransomware.
  3. Exploit Kits: Attackers use software vulnerabilities in outdated or unpatched systems to deliver ransomware payloads.
  4. Remote Desktop Protocol (RDP) Exploitation: Attackers exploit weak or compromised RDP credentials to gain unauthorized access to a system and deploy ransomware.
  5. Drive-by Downloads: Attackers compromise legitimate websites with malicious code, exploiting vulnerabilities in users' browsers to automatically download and execute ransomware.
  6. USB or Removable Media: Attackers may infect USB drives or other removable media devices, hoping that users will unknowingly execute the malware when inserting the infected media into their systems.

# Common delivery methods

* 1. Email Attachments: Ransomware payloads are disguised as email attachments, commonly in the form of executable files, macros within office documents, or compressed archives.
  2. Malicious Links: Emails, instant messages, or websites may contain links that, when clicked, lead to the download and execution of ransomware.
  3. Watering Hole Attacks: Attackers compromise legitimate websites frequented by their targets and inject malicious code to deliver ransomware.
  4. Malicious Advertisements: Online ads may contain malicious code that redirects users to websites hosting ransomware.
  5. Social Engineering: Attackers may use social engineering techniques to manipulate users into downloading and executing ransomware, such as posing as a trusted entity or using urgent and enticing messages.

# Incident Response Plan for a Ransomware Attack

## Preparation

* + 1. Establish an incident response team with defined roles, responsibilities, and communication channels.
    2. Identify and document critical assets, systems, and data that are most vulnerable to ransomware attacks.
    3. Implement appropriate security controls and measures to mitigate the risk of ransomware incidents.

## Detection and Initial Response (Identification):

* + 1. Implement Intrusion Detection and Prevention Systems (IDPS) to monitor network traffic and identify potential indicators of a ransomware attack, such as unusual network connections or communication patterns.
    2. Deploy endpoint protection solutions that include behavior-based detection mechanisms, which can identify suspicious activities or processes associated with ransomware.
    3. Use centralized logging and log analysis tools to monitor system and application logs for any anomalous activities or patterns indicative of a ransomware attack.
    4. Train employees on recognizing phishing emails, suspicious attachments, and links that could potentially introduce ransomware into the organization's systems.
    5. Set up real-time alerts and notifications that can trigger when certain ransomware-related events occur, such as multiple failed logins attempts or file encryption attempts.
    6. Employ network segmentation to contain the impact of a potential ransomware attack and limit lateral movement within the network.
    7. Consider utilizing threat intelligence feeds and security information and event management (SIEM) solutions to correlate and analyze security events for early detection of ransomware activity.

## Containment and Investigation (Containment):

* + 1. Isolate affected systems to prevent further spread of ransomware.
    2. Engage the incident response team and provide them with relevant information.
    3. Preserve evidence by creating forensic images or snapshots of affected systems.
    4. Analyze the ransomware variant and determine the initial attack vector.
    5. Assess the scope and impact of the ransomware infection.
    6. Identify and remediate vulnerabilities that allowed the attack.
    7. Collect additional data such as network logs and system configurations.
    8. Coordinate with external entities if necessary, such as incident response experts or law enforcement agencies.
    9. Document the investigation process, including steps taken, evidence collected, and key findings.

## Eradication

* + 1. Analyze ransomware samples:
       1. Collect ransomware samples from infected systems for analysis.
       2. Work with incident response or cybersecurity experts to analyze the ransomware and understand its behavior and characteristics.
    2. Identify the entry point and attack vector:
       1. Determine how the ransomware gained access to the systems (e.g., phishing emails, exploit kits, vulnerable software).
       2. Analyze network logs, endpoint logs, and any available forensic evidence to identify the initial attack vector.
    3. Remove ransomware and malicious artifacts:
       1. Use reliable and up-to-date antivirus and anti-malware tools to scan and remove the ransomware from infected systems.
       2. Manually search for and remove any remaining malicious artifacts, such as malicious files or registry entries.

## Mitigation and Recovery (Recovery):

* + 1. Restore systems from backups:
       1. Identify and verify the integrity of the organization's data backups.
       2. Restore affected systems and data from clean and secure backups to a trusted state.
       3. Validate the restoration process and ensure the recovered data is free from malware.
    2. Patch and update systems:
       1. Apply necessary security patches, updates, and firmware upgrades to address vulnerabilities exploited by the ransomware.
       2. Validate the integrity and functionality of the restored environment before resuming normal operations.
       3. Implement a robust patch management process to ensure timely updates and minimize future risks.
    3. Strengthen security controls:
       1. Review and enhance security controls, such as firewalls, intrusion detection systems, and endpoint protection solutions.
       2. Implement or strengthen security measures, such as multi-factor authentication, network segmentation, and encryption.
       3. Regularly monitor and update security configurations to mitigate potential vulnerabilities.
    4. Monitor for re-infection:
       1. Implement robust monitoring and threat intelligence capabilities to detect any signs of re-infection or new ransomware attacks.
       2. Continuously monitor systems, networks, and endpoints for indicators of compromise or malicious activity.
       3. Stay up to date with the latest threat landscape and ransomware trends to proactively adopt security measures.
    5. Engage third-party support if necessary:
       1. Seek assistance from external experts, such as incident response consultants or cybersecurity service providers, to ensure a thorough recovery process.
       2. - Engage with relevant vendors or third-party organizations for additional support or expertise in mitigating the impact of the ransomware incident.
    6. Update stakeholders:
       1. Communicate the progress of the recovery efforts to internal and external stakeholders, providing reassurance and transparency.
       2. Share any additional preventive measures implemented to prevent future incidents.
       3. Address concerns or questions raised by stakeholders and provide ongoing support and guidance.

## Communication and Reporting:

* + 1. Internal communication:
       1. Notify key stakeholders within the organization about the ransomware incident.
       2. Provide regular updates on the status of the incident, containment efforts, and investigation progress.
       3. Establish clear communication channels and designated points of contact for reporting concerns or incidents.
    2. External communication:
       1. Determine the external parties that need to be informed, such as clients, partners, and regulatory bodies, based on the incident's nature and impact.
       2. Comply with legal and regulatory requirements for reporting data breaches or security incidents to the appropriate authorities.
       3. Manage external communications in coordination with legal counsel and public relations teams.
    3. Incident documentation:
       1. Maintain a comprehensive incident log documenting communication and actions taken.
       2. Document key incident details, including timelines, actions, decisions made, and communication with internal and external parties.
       3. Capture lessons learned and recommendations for future incident response improvements.
    4. Incident reporting:
       1. Prepare incident reports summarizing the ransomware incident, impact, and response actions taken.
       2. Include details of detection, containment, investigation findings, and remediation steps.
       3. Share incident reports with senior management, relevant departments, and stakeholders.
    5. Regulatory and legal obligations:
       1. Ensure compliance with applicable laws, regulations, and contractual obligations for incident reporting and disclosure.
       2. Consult legal counsel to understand legal requirements and implications associated with the incident.
       3. Provide necessary notifications and reports to regulatory bodies or data protection authorities as required.
    6. Public relations management:
       1. Work with the public relations team to develop a communication strategy that balances transparency, accuracy, and stakeholder trust.
       2. Craft clear and consistent messages addressing the incident's impact and the organization's response.
       3. Monitor and respond to media or public inquiries, aligning with the organization's overall messaging.

## Lessons Learned:

* + 1. Conduct post-incident testing:
       1. Perform comprehensive security testing, including vulnerability assessments and penetration testing, to identify any remaining vulnerabilities.
       2. Validate the effectiveness of security controls and incident response procedures through tabletop exercises or simulated scenarios.
    2. Improve incident response capabilities:
       1. Incorporate lessons learned from the ransomware incident into the incident response plan.
       2. Enhance incident response procedures, documentation, and communication channels based on identified gaps or areas for improvement.
       3. Provide additional training and awareness programs for employees to strengthen their ability to detect and respond to future incidents.

# Plan Testing or Exercise Requirements

* 1. Define testing objectives and desired outcomes.
  2. Select appropriate testing methods (e.g., tabletop exercises, functional exercises).
  3. Develop realistic testing scenarios that simulate different ransomware incidents.
  4. Establish roles and responsibilities for participants.
  5. Conduct testing or exercise, following the defined scenarios and objectives.
     1. Execute the planned testing or exercise, following the defined scenarios and objectives.
     2. Simulate the incident response process, including detection, containment, communication, and recovery activities.
     3. Encourage active participation and collaboration among participants to simulate real-time decision-making and coordination.
  6. Evaluate and analyze the results, documenting observations and lessons learned.
     1. Assess the performance and effectiveness of the incident response plan during the testing or exercise.
     2. Document observations, lessons learned, and identified areas for improvement.
     3. Collect feedback from participants to gather their insights and perspectives on the strengths and weaknesses of the plan.
  7. Update the incident response plan based on the findings and recommendations.
  8. Schedule regular plan testing to maintain preparedness and adapt to evolving threats.

# Plan Review and Update Schedule

* 1. Establish a schedule for reviewing and updating the ransomware response plan at regular intervals (e.g., annually or as per organizational policy).
  2. Assign responsibility to a designated team or individual for plan review and update.
  3. Document any changes made to the plan, including the date of the update and the person responsible.

# Process/Procedure for Recovery

* 1. Activate the IT Disaster Recovery Plan:
     1. Define the process for activating the IT disaster recovery plan in response to a ransomware incident.
     2. Specify the triggers for activating the plan, such as the severity or extent of the attack.
  2. Prioritize Recovery Efforts:
     1. Establish criteria for prioritizing the recovery of systems and data based on their criticality and business impact.
     2. Ensure that the most critical systems are restored first to minimize downtime and operational disruption.
  3. Restore Systems and Data:
     1. Document step-by-step procedures for restoring systems and data from backups or clean sources.
     2. Include verification steps to ensure the integrity and security of restored systems and data.
  4. Post-Recovery Assessment:
     1. Define the process for conducting a post-recovery assessment to validate the effectiveness of the recovery efforts.
     2. Review and document any vulnerabilities or weaknesses identified during the recovery process and incorporate them into future prevention and response strategies.

# Playbook for a ransomware incident of 3rd parties/MSPs (Test Scenario)

* 1. Preparation Phase:
     1. Establish a dedicated incident response team for handling ransomware incidents involving third parties or managed service providers (MSPs).
     2. Identify and document the critical systems, applications, and data hosted by the third parties or MSPs that could be impacted by a ransomware attack.
     3. Develop communication protocols and establish points of contact with the affected third parties or MSPs to ensure effective coordination during an incident.
     4. Review and validate the security controls and measures implemented by third parties or MSPs to mitigate the risk of ransomware attacks.
  2. Identification Phase:
     1. Train employees and stakeholders to recognize signs of a ransomware incident and report any suspicious activities or indicators promptly.
     2. Monitor network and system logs to identify potential indicators of compromise (IOCs) related to ransomware attacks.
     3. Collaborate with the affected third parties or MSPs to gather information about the incident, including the type of ransomware, affected systems, and the extent of the compromise.
  3. Containment Phase:
     1. Isolate the affected systems or networks hosted by the third parties or MSPs to prevent the spread of ransomware.
     2. Implement network segmentation to limit the lateral movement of the ransomware within the infrastructure.
     3. Temporarily suspend or restrict access to the compromised systems or networks to prevent further damage and unauthorized access.
  4. Eradication Phase:
     1. Collaborate with the affected third parties or MSPs to identify the root cause of the ransomware incident and determine the necessary steps for remediation.
     2. Remove or remediate the ransomware from the affected systems or networks, following established incident response procedures.
     3. Patch and update all software and systems to prevent future exploitation of known vulnerabilities.
  5. Recovery Phase:
     1. Restore the affected systems or networks from clean and verified backups to ensure business continuity for the third parties or MSPs.
     2. Conduct thorough testing and validation of the restored environment to ensure the integrity and functionality of the recovered systems and data.
     3. Implement additional security measures and controls in collaboration with third parties or MSPs to enhance resilience against future ransomware attacks.
     4. Lessons Learned Phase:
        1. Conduct a post-incident review to analyze the response efforts and identify areas for improvement in the incident handling process.
        2. Document lessons learned from the ransomware incident and update the incident response playbook, processes, and procedures accordingly.
        3. Share the key findings and recommendations with the affected third parties or MSPs to facilitate their security enhancements and prevent future incidents.