Ransomware Response Plan

Document Information

Document Owner: [Insert Name/Role]

Last Updated: [Insert Date]

Version: [Insert Version Number]

Review Frequency: [Insert Review Period]

Table of Contents

Introduction

This ransomware response plan outlines the procedures and guidelines for responding to a ransomware incident within [Organization Name]. This document aims to provide a structured approach to detecting, containing, eradicating, and recovering from ransomware attacks while minimizing disruption to business operations and data loss.

Purpose

The purpose of this plan is to:

- Establish a systematic approach to responding to ransomware incidents
- Define roles and responsibilities during an incident
- Outline communication protocols for internal and external stakeholders
- Provide guidance for technical response procedures
- Facilitate a quick and effective recovery
- Ensure compliance with legal and regulatory requirements

What is Ransomware?

Ransomware is a type of malicious software that encrypts files or locks systems, rendering them inaccessible until a ransom is paid. Modern ransomware attacks may also involve data theft, where attackers exfiltrate sensitive data before encryption and threaten to publish it unless payment is made.

Scope

This plan applies to all ransomware incidents affecting [Organization Name]'s IT systems, including:

- Corporate network infrastructure
- Cloud environments
- Servers and endpoints
- Data storage systems
- Operational technology environments
- [Add other relevant systems]

Ransomware Response Team

The following table outlines the key members of the Ransomware Response Team and their responsibilities:

Role	Name	Contact Information	Responsibilities
Incident Response Manager	[Name]	[Phone/Email]	Overall coordination of response efforts
IT Security Lead	[Name]	[Phone/Email]	Technical investigation and containment
System Administrators	[Name(s)]	[Phone/Email]	System recovery and restoration
Legal Counsel	[Name]	[Phone/Email]	Legal guidance and compliance oversight
Communications Lead	[Name]	[Phone/Email]	Internal and external communications
Executive Sponsor	[Name]	[Phone/Email]	Decision-making authority for critical issues
[Other roles as needed]	[Name]	[Phone/Email]	[Responsibilities]

Preparation

Preparation is critical for effective ransomware response. The following measures should be implemented and regularly reviewed:

Technical Controls

- [ ] Implement and maintain up-to-date endpoint protection solutions
- [ ] Deploy network segmentation to limit lateral movement
- [ ] Maintain regular, tested, and air-gapped backups
- [ ] Implement email filtering and web filtering solutions
- [ ] Deploy multi-factor authentication across all systems
- [ ] Maintain detailed network diagrams and asset inventories
- [ ] Implement privileged access management
- [ ] Deploy monitoring and logging solutions with alerting capabilities
- [ ] Implement application whitelisting where appropriate
- [ ] [Add organization-specific controls]

Organizational Preparation

- [ ] Conduct regular cybersecurity awareness training for all employees
- [ ] Develop and maintain contact lists for all stakeholders
- [ ] Establish relationships with external security partners and law enforcement
- [ ] Maintain current cyber insurance coverage
- [ ] Conduct tabletop exercises to test the ransomware response plan
- [ ] Document critical systems and their recovery priorities
- [ ] Establish out-of-band communication methods
- [ ] [Add organization-specific preparations]

Detection and Analysis

Early detection and analysis are crucial for limiting the impact of ransomware.

Detection Methods

- System and network monitoring alerts
- Endpoint detection and response (EDR) alerts
- User reports of suspicious activity
- Unusual network traffic patterns
- Multiple file access attempts or unauthorized changes

- Explicit ransom notes or locked screens
- [Add organization-specific detection methods]

Initial Assessment

When potential ransomware activity is detected, the Incident Response Manager should be notified immediately. The initial assessment should include:

1. **Confirm the Incident**
   - Verify if the activity is indeed ransomware
   - Document affected systems
   - Identify the type of ransomware if possible
   - Determine initial infection vector if apparent
2. **Assess the Scope**
   - Identify affected systems and networks
   - Estimate the potential business impact
   - Determine if sensitive data is at risk
3. **Declare the Incident**
   - If confirmed, formally declare a ransomware incident
   - Activate the Ransomware Response Team
   - Notify executive leadership
   - Initiate the communication plan

Containment

Containment strategies aim to prevent the spread of ransomware to additional systems.

Immediate Containment Actions

1. **Network Isolation**
   - Disconnect affected systems from the network
   - Isolate critical network segments
   - Disable affected user accounts
   - Block suspicious IP addresses and domains
2. **Preserve Evidence**
   - Create forensic images of affected systems when possible
   - Preserve logs from affected systems

- Document all observed indicators of compromise
- Capture screenshots of ransom notes or other artifacts

Strategic Containment

1. **Account Security**
   - Force password resets for all accounts
   - Review and restrict administrative privileges
   - Enhance monitoring of authentication activities
2. **System Protection**
   - Deploy additional monitoring on unaffected systems
   - Implement temporary access restrictions
   - Update antivirus signatures and security tools
   - [Add organization-specific containment strategies]

Eradication

Eradication involves removing the ransomware from all affected systems.

Investigation

- Identify the ransomware variant
- Determine the infection vector
- Identify all compromised systems
- Assess if data exfiltration occurred

Ransomware Removal

- **Decision Point:** Determine whether to:
  - Rebuild systems from clean baselines
  - Remove the ransomware using specialized tools
  - [Organization's preferred approach]

Payment Considerations

[Organization Name]'s policy on ransom payment is: [Insert policy]

If payment is considered, the following steps must be taken:

- Consult with legal counsel and cyber insurance provider

- Engage with law enforcement
- Conduct risk assessment of payment vs. non-payment
- Ensure compliance with applicable regulations
- Document the decision-making process
- [Add organization-specific payment considerations]

Recovery

Recovery focuses on restoring systems and data to normal operations.

Prioritized Recovery

1. **Recovery Prioritization**
   - Identify critical business functions for priority restoration
   - Establish recovery time objectives for each system
   - Sequence recovery operations based on dependencies
2. **System Restoration**
   - Restore systems from clean backups
   - Rebuild systems from trusted images
   - Implement enhanced security controls
   - Verify system integrity before reconnection
3. **Data Restoration**
   - Restore data from secure backups
   - Validate data integrity
   - Document any unrecoverable data
   - [Add organization-specific recovery procedures]

Verification

- Test restored systems for functionality
- Verify no signs of continued infection
- Validate security controls are operating correctly
- Monitor for suspicious activity

Post-Incident Activities

After the incident has been contained and systems restored, conduct post-incident activities.

Documentation

- Document all actions taken during the incident
- Record timeline of events
- Document affected systems and recovery actions
- Calculate estimated costs and impacts

Lessons Learned

- Conduct a formal post-incident review meeting
- Identify what went well and what could be improved
- Update the ransomware response plan based on findings
- Document recommendations for preventing similar incidents

Follow-up Actions

- Implement additional security controls
- Update training and awareness programs
- Enhance detection capabilities
- Review and update the incident response plan
- [Add organization-specific follow-up actions]

Communication Plan

Effective communication is essential during a ransomware incident.

Internal Communications

Stakeholder Group	Communication Method	Frequency	Responsible Party
Executive Leadership	[Method]	[Frequency]	[Role]
Employees	[Method]	[Frequency]	[Role]
IT Department	[Method]	[Frequency]	[Role]
[Other groups]	[Method]	[Frequency]	[Role]

External Communications

Stakeholder Group	Communication Method	Timing	Responsible Party
Customers	[Method]	[Timing]	[Role]
Partners/Vendors	[Method]	[Timing]	[Role]
Regulatory Bodies	[Method]	[Timing]	[Role]
Law Enforcement	[Method]	[Timing]	[Role]
Media	[Method]	[Timing]	[Role]
[Other groups]	[Method]	[Timing]	[Role]

Communication Templates

[Include pre-approved communication templates for various stakeholders in an appendix]

Legal and Regulatory Considerations

Ransomware incidents may trigger legal and regulatory obligations.

Data Breach Notification

- Determine if the incident constitutes a reportable data breach
- Identify applicable regulations (e.g., GDPR, HIPAA, state laws)
- Document notification timelines and requirements
- Prepare necessary notifications with legal counsel
- [Add organization-specific regulatory requirements]

Law Enforcement Engagement

- Determine when to engage law enforcement
- Document contact information for relevant agencies:
  - FBI: [Contact Information]
  - Local Law Enforcement: [Contact Information]
  - [Other relevant agencies]
- Prepare necessary information for law enforcement reports

Documentation for Legal Purposes

- Maintain chain of custody for all evidence
- Document all incident response actions
- Preserve communications related to the incident

- [Add organization-specific legal documentation requirements]

Appendices

Appendix A: Contact Information

[Comprehensive contact list for all internal and external stakeholders]

Appendix B: Ransomware Identification Resources

[Resources for identifying ransomware variants and available decryptors]

Appendix C: System Recovery Procedures

[Detailed technical procedures for system recovery]

Appendix D: Communication Templates

[Pre-approved templates for various stakeholders]

Appendix E: Decision Trees

[Decision frameworks for key response actions]

Appendix F: External Resources

*[List of external resources, including:

- Cyber insurance contact information
- External incident response providers
- Forensic investigation services
- Legal services
- Public relations services]*

Appendix G: Glossary

[Definitions of technical terms used in this document]

This template is provided for educational purposes. Organizations should customize this template to meet their specific needs and seek appropriate legal, technical, and cybersecurity advice when developing their ransomware response plan.