Ransomware Playbook Template

Table of Contents

OBJECTIVE

Overview

The purpose of the Playbook is to rapidly recognize and recover quickly from a ransomware attack. This response plan includes key people, decisions, and processes necessary to respond to a ransomware attack.

The goal of the Ransomware Playbook is to identify structure and outline specific response procedures and around responding to a ransomware event. This includes:

- Define roles and responsibilities during an attack
- Identify response priorities
- Outline strategies for containment
- Payment considerations
- Legal considerations
- General Communications strategy

MAIN DEFINITIONS

Ransomware: a type of malicious software designed to block access to a computer system until a sum of money is paid. Ransomware encrypts data but may also exfiltrate information including intellectual property, passwords, confidential information, and information protected by regulatory requirements.

ROLES & RESPONSIBILITIES

ROLE	TASKS
Communications	Develops messaging for communications; may act as liaison with internal and external stakeholders as needed.
Executive Team	Risk management and reputational risk assessment; crisis management strategic planning
Finance	Evaluation of financial impact, liaison with insurance, legal and other support teams, authorize funding.
HR	Provides input and analysis on impacts to employees, supports internal messaging
Incident Commander	Coordinates all aspects of incident response, communicates, and updates all other roles
IT Security	Threat intelligence, containment, eradication, and recovery.
IT/CIO	Containment, Eradication and Recovery
Legal	Notification and evaluation. Approve all messaging prior to release.
Operations	Business Impact Analysis

Use this section to further describe roles and assign to specific personnel.

PROCEDURE

Initial Assessment

Determine Impact and Severity and attempt to answer the following questions:

- How many devices are impacted?
- What division(s) of company affected?
- What data is lost/compromised/inaccessible?

Describe what threshold will activate the Incident Response Plan and Ransomware Playbook.

Incident Response Team Formation

IT will escalate notifications to other members of the IR team and appoint an Incident Response Coordinator; the IR Coordinator will them establish the following:

- Communications plan: identify what services and communications channels are safe and available to use and notify team members of the primary communication method for exchanging information.
- Establish meeting spaces: virtual or physical.
- Establish update schedule: As the incident is in progress, the IRC establish a schedule updating supporting teams as the incident progresses and more data becomes available. Updates may be presented in a formal meeting or communicated through one of channels established.

Containment and Assessment

This phase in the initial crisis response focuses on limiting damage and assessing the impact to infrastructure.

To estimate recovery operations, the initial IT assessment should include a report on:

- Impacted platforms, systems, and OS
- Locations – localized or wide-spread? Single or multiple locations?
- Devices and Functions or Roles – servers, workstations, databases, virtual machine, infrastructure, gaming support, etc.
- Exploit pattern – random or relational
- Storage – local, cloud storage and services
- Impacted backups – verify backup integrity and availability
- Email and messaging – check for rogue email rules as well as impacts to communications channels
- Data or credential exfiltration – is there a claim of exfiltration? Has a data sample been provided?
- Malicious files and types (scripts, programs, archives)
- Messages, warnings, and information from the attacker

The table below identifies best practices for containment and damage assessment.

Containment	Damage Assessment

• Scan Systems
• Block inbound and outbound Ips
• Terminate Processes
• Quarantine/Take systems offline
• Account Lock
• Isolate malware/ransomware for investigation
• Check for rogue email rules
	• Research/Investigate ransomware characteristics
	  ○ Scareware or Fake Ransomware
	  ○ Immediate Action or Delayed
	  ○ Automatic or Human-Directed
	  ○ One Device or Multiple Devices
	  ○ Trojan or Worm
	  ○ File encryption or boot infection
	  ○ Encryption level
	  ○ Single Encryption or Multiple Payload (encryption, exfiltration, credential compromise, spear phishing, DDoS attack
	  ○ How much is the ransom request? What is the demand? How long do we have to pay it?
	  ○ Information on the attackers; location; specific known group.

Track/note damage to inform Technical Impact Analysis:
• OS affected
• Location (local or widespread)
• Device types
• Roles (general users, privileged, system accounts)
• Exploit pattern (random or relational)
• Local storage or cloud
• Portable media
• Backups
• Email
• Data or Credential Exfiltration
• Malicious files
• Ransom notes
	Technical Impact Analysis attempts to answer:
	• What services are not available?
	• What dependencies are there between services?
	• What resources are needed to recover?
	• Can we fully recover, or do we need to consider ransom payment?
	• Recovery time objective – how long until systems are restored?
	• What is the impact of downtime and what can we quantify?
	  ○ Lost revenue from downtime
	  ○ Reputational damage
	  ○ Intellectual property loss
	  ○ Recovery costs

Check backups • Does a usable, unaffected backup exist for all compromised devices?	

• Where do those backups exist? • How much data may be lost if rebuilding systems from backup?	

Communications team members focus on developing a communications plan: communicate early and often (as information becomes known) or wait until specific information is known and verified. These communications apply to internal and external stakeholders but are always coordinated with Legal. The communication strategy will vary based on the incident.

To begin developing a communications strategy, initial communications will:

- Develop internal notifications
- Develop draft communication to external stakeholders
- Identify potential regulatory notifications
- Identify reputational risks
- Coordinate with legal for messaging approval

Legal determines whether individual notifications, law enforcement, or other notifications are required. Legal actions that may be necessary during the assessment and containment phase:

- Identify and contact authorities, regulatory bodies, and criminal investigative services
- Ensure evidence collection is done and completed lawfully according to legislation to be usable in court
- Investigating legality of paying ransom

Legal will determine regulatory notification requirements, specifically the scope and type of data affected, location of data impacted, and the number of devices.

Remediation and Recovery

IT and the IR Team will collectively make the decision to recover compromised devices or rebuild the environment.

Prior to system changes, evidence preservation and forensic capture will be completed to support legal issues and root cause investigations. IT should maintain a Priority Restoration List that dictates the order to restore systems and services.

Depending on the analysis completed in previous phases, the feasibility of recovering using backups, and whether a ransom was paid the steps to recover may differ slightly.

Without Decryption Key	Paid Ransom or Key Obtained
Identify systems to recover and systems to rebuild	Create VM and test prior to use on production systems
Remove malware from recovery systems and ensure attacker access points have been closed.	Identify systems to recover and systems to rebuild

Refer to Priority Restoration List and dependencies	Refer to Priority Restoration List and dependencies
Preserve evidence through forensic copy	Ensure malware is removed, attacker access points have been closed and decrypt production systems
Recover systems	Preserve evidence through forensic copy
	Recover systems

Refer to IT specific procedures for rebuild protocols for specific systems. Once complete, confirm the environment is fully recovered and conduct an after-action review.

During the remediation phase, the communications team will continue to manage messaging and coordinate across teams as needed.

Legal continues to manage and approve communications with internal and external parties. Depending on the notifications required, Legal may continue to:

- Approve and make Regulatory Communications
- Approve Internal Comms
- Approve PR statements to External Comms
- Contact and coordinate with law enforcement
- Continue to approve comms messaging

Summary Checklist

- ✓ Activate IRP
- ✓ Establish alternate communications plans if needed
- ✓ Contain spread
- ✓ Determine scope of infection and damages
    - Is external assistance needed?
- ✓ Draft or revise communications based on known information
    - Internal
    - External
- ✓ Evaluate risk at various stakeholder levels: clients, employees, shareholders, reputational
- ✓ Assess ransomware strain and gather intelligence on strain, attacker, motivation
    - Is decryption possible?
    - How much is the ransom?
    - What is the demand? Decryption, extortion/data release, other?
- ✓ Based on scope of infection, evaluate the ability to recover from backups including time and recovery point
    - If recovery is possible, look for and eliminate backdoors and secondary malware
    - Preserve evidence
    - Proceed with backup recovery
    - Rebuild systems
    - Restore to clean and trusted state
- ✓ If recovery is not possible determine if ransom should be paid
    - Begin negotiations
    - Identify funding source
    - Obtain key and test in isolated environment
- ✓ Evaluate notification requirements
- ✓ Assess and predict business impact
    - Cost
    - Downtime
    - Reputational risk
- ✓ Recover or rebuild systems
- ✓ Conduct After Action Review
- ✓ Apply additional risk management strategies to prevent re-infection