RESILIENTLY

Cybersecurity made clear.

Ransomware Tabletop Exercise Kit

A complete kit for running ransomware incident response tabletop exercises with your team.

Free Template from Resiliently

resiliently.co/tools/templates

Version 1.0 | May 2026

Exercise Overview

This tabletop exercise simulates a ransomware attack on your organization. The goal is to test your incident response procedures, identify gaps, and improve team coordination.

Duration: 2-3 hours

Participants: IT/Security team, Executive leadership, Legal, Communications, HR, Business unit leaders

Exercise Date

Facilitator Name

Participating Teams/Departments

Pre-Exercise Preparation

- [ ] Distribute this kit to all participants 1 week before the exercise
- [ ] Ensure all participants have access to current incident response plan
- [ ] Reserve conference room with video capability for remote participants
- [ ] Prepare whiteboard/flipchart for capturing notes and action items
- [ ] Assign roles for the exercise (see Role Cards section)
- [ ] Prepare props: sample ransom note, mock news article, timeline board
- [ ] Notify stakeholders this is an EXERCISE, not a real incident

Scenario Background

It is Tuesday morning at 8:47 AM. Your organization's IT helpdesk begins receiving calls from employees reporting they cannot access files on the network. Within 30 minutes, the helpdesk has received 47 calls.

At 9:15 AM, the IT Security team discovers that multiple file servers have been encrypted. A ransom note has been placed on each affected system demanding 50 Bitcoin (approximately $2.1 million) within 72 hours.

Initial investigation reveals:

- Encryption began at approximately 3:00 AM

- Multiple business-critical systems are affected including ERP, file shares, and email

- The Active Directory appears compromised

- Backup systems are currently being assessed

- The attackers claim to have exfiltrated sensitive data and will publish it if ransom is not paid

Scenario Injects

Inject 1: Initial Discovery (Time: 0:00)

The helpdesk manager escalates to IT leadership. Multiple employees are locked out of systems. Some employees report seeing a ransom note on their screens.

Discussion Questions:

1. What are the immediate first steps your team should take?

2. Who needs to be notified immediately?

3. How do you determine the scope of the incident?

Inject 2: Scope Expands (Time: +30 min)

Investigation reveals that 80% of file servers are encrypted. The ERP system is down. Initial assessment suggests backups may also be affected. The attacker's ransom note includes samples of stolen employee and customer data.

Discussion Questions:

1. How do you communicate with employees about the outage?

2. What is your backup recovery strategy?

3. How do you handle the data exfiltration threat?

Inject 3: External Pressure (Time: +2 hours)

A journalist contacts your communications team asking about rumors of a ransomware attack. A key customer calls asking why their orders aren't processing. The attackers send a follow-up message reducing the deadline to 48 hours.

Discussion Questions:

1. What is your external communication strategy?

2. How do you handle customer communications?

3. What are the legal/regulatory notification requirements?

Inject 4: Critical Decision Point (Time: +6 hours)

IT confirms that recent backups are intact but recovery will take 5-7 days. The CFO calculates business losses at $500,000 per day. Legal advises on potential regulatory fines if customer data is published. The board is asking for a decision on paying the ransom.

Discussion Questions:

1. What factors influence the pay/don't pay decision?

2. Who has authority to make this decision?

3. What are the implications of each choice?

Inject 5: Recovery Phase (Time: +24 hours)

The decision has been made not to pay. Recovery efforts are underway. Law enforcement has been engaged. The attackers publish some stolen data online. Media coverage is increasing.

Discussion Questions:

1. How do you manage the data publication?

2. What is your communication to affected individuals?

3. How do you prioritize system recovery?

Role Cards

Assign participants to the following roles for the exercise. Each person should respond from the perspective of their assigned role.

Incident Commander

Leads the overall response effort, makes key decisions, coordinates between teams.

Technical Lead

Manages technical investigation, containment, and recovery efforts.

Communications Lead

Handles all internal and external communications, media inquiries, customer notifications.

Legal Counsel

Advises on legal obligations, regulatory requirements, ransom payment considerations.

Executive Sponsor

Represents executive leadership, makes budget/authority decisions, interfaces with board.

Business Unit Representative

Represents operational business needs, prioritizes system recovery, assesses business impact.

Exercise Ground Rules

- [ ] This is a learning exercise, not a test - there are no wrong answers
- [ ] Speak from your assigned role's perspective
- [ ] Assume you only know what has been shared in the scenario
- [ ] Document all decisions and reasoning
- [ ] Note any gaps in current plans or procedures
- [ ] Keep phones on silent unless needed for the exercise
- [ ] What happens in tabletop stays in tabletop (no blame)

Post-Exercise Evaluation

Complete this section after the exercise to document findings and improvements.

What worked well in our response?

What gaps or challenges were identified?

Were roles and responsibilities clear?

Was the incident response plan effective?

Communication effectiveness (internal/external)

Decision-making process observations

Action Items

Document specific improvements to be made based on exercise findings.

Action Item	Owner	Priority	Due Date

Appendix: Sample Ransom Note

---BEGIN RANSOM NOTE---

YOUR NETWORK HAS BEEN ENCRYPTED

All your files have been encrypted with military-grade encryption. Do not attempt to recover the files yourself - this will permanently destroy them.

We have also downloaded 150GB of your sensitive data including: employee records, customer database, financial documents, and intellectual property.

To recover your files and prevent data publication:

1. Send 50 Bitcoin to: [WALLET ADDRESS]

2. Email proof of payment to: [EMAIL]

3. You will receive decryption keys within 24 hours

DEADLINE: 72 hours from encryption start time

After the deadline: Price doubles. After 7 days: Data published.

Do not contact law enforcement. Do not hire recovery firms. We are watching.

---END RANSOM NOTE---