# Tabletop Exercise: Cybersecurity Incident Response

## Exercise Overview

Scenario: A virus or ransomware attack has been detected on company computers.

Goal: Test and identify areas for improvement in the incident response plan.

## 1. Scenario Description

Introduction:

Provide a summary of the virus/ransomware attack scenario. Include background information relevant to the organization and current cybersecurity threats.

Detailed Scenario:

Describe the initial detection of the virus/ransomware. Outline the progression of the incident (e.g., files encrypted, systems locked, ransom demands made). Include specific timestamps and events to create a timeline.

## 2. Objectives and Goals

Primary Objectives:

* Test communication protocols.
Evaluate response procedures.
Improve interdepartmental coordination.
Identify gaps in the current plan.

Secondary Objectives:

* Assess the decision-making process.
Test the effectiveness of cybersecurity tools and resources.

## 3. Participants and Roles

Roles:

* Facilitator: Guides the exercise, provides injects, and ensures objectives are met.
Participants: Actively engage in the exercise, responding to the scenario and injects.
Scribe: Documents actions, decisions, and discussions.
Role Player: Simulates external entities (e.g., attackers, media).
Observers: Provide external perspectives and feedback.
Evaluator: Assesses performance and effectiveness.
Player: Actively involved in the response, taking on specific roles within the organization.

Departments Involved:

* IT Department
HR Department
Executive Management
Assistance from other relevant departments

## 4. Injects and Prompts

Injects:

* Initial detection of malware.
Notification of encrypted files.
Ransom demand received.
Media inquiry.
Customer data potentially compromised.
IT systems offline.

Prompts:

* How do you respond to the initial detection?
What steps are taken to secure the network?
How is the ransom demand handled?
What communication is made with stakeholders?

## 5. Documentation

Communication Log:

Record all internal and external communications made during the exercise.

Decision Log:

Document all decisions made, including the rationale and responsible parties.

## 6. Evaluation and Debrief

Evaluation Metrics:

* Response time to each inject.
Effectiveness of communication.
Decision-making process.
Coordination between departments.

Criteria:

* Clarity of roles and responsibilities.
Adherence to the incident response plan.
Identification and resolution of issues.

Debrief Questions:

* What went well?
What challenges were encountered?
What improvements can be made?

## 7. Action Plan

Improvements:

* Update communication protocols.
Refine incident response procedures.
Schedule additional training sessions.

Follow-Up:

* Plan regular tabletop exercises.
Review and update the incident response plan periodically.

## 8. Customization Options

Add/Remove Sections:

Ability to tailor the template based on specific needs and scenarios.

Predefined Fields:

Include fields for easy data entry and tracking.

Organizational Charts:

Visual representation of roles and responsibilities.

## 9. Pre-Exercise Logistics

Planning:

* Set objectives and goals.
Prepare the scenario and injects.
Brief participants on their roles and responsibilities.

Post-Exercise Logistics:

* Conduct the debrief session.
Compile the After Action Report (AAR).
Implement improvements based on feedback.