Lab: Tabletop Ransomware Simulation (2 hours)

Overview

In this lab, you will participate in a tabletop simulation of a ransomware attack affecting CloudNova. The goal is to practice **how a Crisis Management Team (CMT) responds during the first hours of a major cyber disruption**, including escalation, communication, coordination, and decision-making.

This is not a technical exercise. The focus is on **leadership, timing, judgment, and alignment**

Your Mission

CloudNova has been hit by a suspected ransomware attack affecting its analytics platform. Systems are locking up, customers are reporting outages, and early signs point to possible data encryption. You are acting as the Crisis Management Team.

Your job is to:

1. Assess the situation,
2. Decide if and when to declare a crisis,
3. Activate the right roles,
4. Coordinate communications and escalation,
5. Decide on next steps and priorities for stabilization.

Your Objectives

By the end of this lab, you will:

- Apply crisis declaration criteria to a real scenario.
- Decide when and how to escalate to the CMT.

- Practice role clarity and coordination under uncertainty.
- Build a structured crisis response timeline.
- Understand the difference between *incident response* and *crisis leadership*.

How to Work Together

Form groups of 5–7 and assign roles:

- **Crisis Manager (Lead)**
- **Communications/PR Lead**
- **Legal/Compliance Lead**
- **Business Owner / Executive Sponsor**
- **Technical Liaison (not engineering lead)**
- **Risk & Stakeholder Manager**
- **Recorder / Scribe**

Each role speaks only from their position's perspective — this reinforces realism and decision hierarchy.

Steps to Complete the Simulation

Step 1: Initial Situation Brief

You will receive an incident summary with:

- Early symptoms
- Unknown risks
- Conflicting signals
  Your first task is to decide: **Is this a disruption, an incident, or a crisis?**
  You must justify your reasoning.

Step 2: Declaration Decision

Using activation criteria from the lesson, decide whether to:

- Monitor
- Escalate
- Declare a crisis
  You must state:
- Who declares it
- When it is declared
- What changes once it is declared

Step 3: Role Activation

Each role outlines:

- What they do in the first hour
- Who they must notify
- What information they need to proceed

Step 4: Live Injects Begin

You will receive timed “injects” such as:

- Customer complaints growing rapidly
- A major client threatening contract breach
- A journalist requesting comment
- A regulator inquiring about impact
- Rumors spreading on social media
- Engineering uncertain about root cause

Your team must:

- Respond in real time
- Decide what to communicate
- Document decisions and tradeoffs

Step 5: External Coordination

You decide if and when to contact:

- Law enforcement
- Regulators
- Key clients
- Cyber insurance

You must justify timing — **too early** vs **too late** both have consequences.

Step 6: Stabilization Strategy

You choose one of several possible crisis directions:

- Containment-first approach
- Communications-first approach
- Client protection-first approach
- Evidence preservation-first approach

There is no “perfect” answer — only tradeoffs you must be able to defend.

Step 7: Mini Press Briefing (Internal Only)

Your Communications/PR Lead prepares a short holding statement. The team must approve it:

- What do you say publicly?

- What do you NOT say yet?
- What wording protects the company?

Step 8: After-Action Debrief

At the end of the tabletop, you reflect on:

- What triggered the crisis declaration
- Whether escalation timing was correct
- Role clarity vs role overlap
- Where decision “friction” occurred
- What information was missing

What You Will Deliver

Each group will produce a short summary of:

1. Crisis declaration decision (and why)
2. Activation timeline (first 60–90 minutes)
3. Stakeholder actions taken
4. A draft holding statement
5. Top 3 lessons learned

Tips for Success

- Focus on **leadership clarity**, not technical steps.
- Prioritize **stakeholder trust** as much as system recovery.
- Avoid “wait and see” — indecision is also a decision.

- In a crisis, perception moves faster than facts.
- Speak as your role, not as yourself.