

Incident Response Tabletop Exercise Template

A fillable planning template and sample ransomware scenario — companion to CyberClan's "The Incident Response Tabletop Exercise: A Step-by-Step Guide for Mid-Market Companies." Use this to structure your first exercise, or to run a sharper version of one you've already tried.

Before You Start

A tabletop exercise tests a plan — it doesn't create one. Confirm these first

- ☐ A written incident response plan exists (even a rough first version covering preparation, detection, containment/recovery, and post-incident steps).
- ☐ The plan has been reviewed or updated in the last 12 months — if not, treat this exercise as the forcing function to update it.
- ☐ You've identified who has real authority to make containment decisions (e.g., taking production systems offline).

Participants and Roles

Fill in names/contacts before the session — not just IT should be in the room

Role	Name	Contact (Phone/Email)
Executive sponsor (decision authority)		
IT / security lead		
Legal / outside counsel		
Communications / marketing		
HR (if employee data involved)		
Finance		
Facilitator (runs scenario — not a response role)		
Scribe (captures decisions and gaps)		
Insurance broker / IR retainer contact		

Exercise Setup

Date of exercise: Duration planned:

Objective — what specific question(s) should this exercise answer?

Scenario summary — one paragraph describing the starting incident:

Sample Scenario: Ransomware

Ransomware is the standard starting scenario — it's the most statistically likely serious incident most mid-market companies face, and it forces decisions across every part of the business, not just IT. This is an illustrative starting point: customize the injects to your own environment, systems, and risk profile before running it.

T+0

A user reports their machine is running slowly and some files won't open. IT also notices an unusual login alert from an unfamiliar location overnight.

Discuss: *What would we do right now? Who decides? Who do we notify? What don't we know yet?*

T+15–20m

IT confirms the slow machine has encrypted file extensions. A second, unrelated department reports similar issues on a shared drive.

Discuss: *What would we do right now? Who decides? Who do we notify? What don't we know yet?*

T+30–40m

A ransom note is discovered on multiple systems, naming a ransomware group and a deadline. IT confirms three more servers are now encrypted, including a system tied to production.

Discuss: *What would we do right now? Who decides? Who do we notify? What don't we know yet?*

T+50–60m

Your cyber insurance broker's breach coach calls, asking for a decision within a set window and outlining policy requirements you may not currently meet.

Discuss: *What would we do right now? Who decides? Who do we notify? What don't we know yet?*

T+70–80m

A local reporter emails asking to confirm “reports of a cyberattack” at your company, with a same-day response deadline.

Discuss: *What would we do right now? Who decides? Who do we notify? What don't we know yet?*

T+90–100m

IT reports backups exist but the most recent tested restore was over a year ago — and initial checks suggest backups may also be affected.

Discuss: *What would we do right now? Who decides? Who do we notify? What don't we know yet?*

Timing shown is illustrative (roughly 15–20 minutes between injects, per the companion guide). Adjust the pace, injects, and specifics to match your systems, your industry, and what you actually want to test.

Debrief — Complete Immediately After the Exercise

20–30 minutes, while it's fresh — this is usually the most valuable part

What worked well?

What didn't work, or broke down?

What was unclear — e.g., a moment nobody knew who was in charge?

Action Items

Every gap gets an owner and a deadline — an exercise that changes nothing wasn't worth running

Gap Identified	Owner	Deadline

How Often to Run One

Once a year is the reasonable minimum for most mid-market companies — every six months if you've had leadership turnover, a significant infrastructure change, or your last exercise surfaced major gaps. Alternate scenarios (ransomware one year, business email compromise or a vendor breach the next) so the team is tested, not just rehearsed.

Want This Facilitated Instead of Self-Run?

CyberClan's incident response team designs and facilitates tabletop exercises for mid-market companies — the same team that would run point during a real incident can help test whether your organization is actually ready for them to.

[Schedule a complimentary Cyber Resilience Consultation](#)

24/7 EMERGENCY INCIDENT RESPONSE HOTLINE:

US/CA: 1 800 762 3290

UK: 0800 368 8731

AU: 61 1800 413 128

Adapted from CyberClan's "The Incident Response Tabletop Exercise: A Step-by-Step Guide for Mid-Market Companies." The sample scenario above is illustrative — build injects around your own environment. For structuring your own scenarios from scratch, CISA's public Tabletop Exercise Packages ([cisa.gov](https://www.cisa.gov)) are a free, solid starting point. This template is an educational resource, not a substitute for legal, insurance, or compliance advice specific to your organization.



Incident Hotline

US/CA 1 800 762 3290
UK 0800 368 8731
AU 61 1800 413 128
response@cyberclan.com

General Inquiries

US/CA 1 855 685 5785
UK 0800 048 7360
info@cyberclan.com