

TEAM EXERCISE

Incident Response Tabletop Exercise Scenarios

Three realistic scenarios your leadership team can run to pressure-test your incident response plan. Allow 45-60 minutes per scenario.

How to run this exercise: Gather the people named in your incident response plan (incident commander, IT/security lead, legal, communications, an executive sponsor). Read the scenario aloud, then work through the discussion questions as a group. A facilitator should introduce new "injects" (twists) as the group discusses to keep the exercise realistic. Take notes on any gaps you uncover in your written IR plan.

Scenario 1: Ransomware

Ransomware Detection During Business Hours

It's 10:30 AM on a Tuesday. Your helpdesk starts receiving calls — several employees report they can't open files on the shared drive. Within 15 minutes, a ransom note appears on multiple workstations. Your backup server appears to be encrypted as well.

Discussion Questions:

- Who is notified first, and how? Is that person reachable right now?
- What is your first technical action — and who has the authority to take it?
- Your primary backup server is also encrypted. What's your fallback recovery path?
- At what point (if any) do you contact law enforcement or your cyber insurance carrier?
- New inject: A local news reporter calls asking if you've been hit by ransomware. Who responds, and how?

Scenario 2: Business Email Compromise

Fraudulent Wire Transfer Request

Your controller receives an email that appears to be from the CEO, marked urgent, requesting an immediate wire transfer of \$85,000 to a new vendor account for a "time-sensitive acquisition." The email address looks correct at a glance. The controller has already begun the transfer process.

Discussion Questions:

- What control should have stopped this before the transfer was initiated?
- Who has the authority to halt a wire transfer once it's in process?
- How quickly can you contact your bank to attempt a recall, and who owns that call?
- New inject: It turns out the transfer went through 20 minutes ago. What are your next 3 steps?
- What internal process change would prevent a repeat of this scenario?

Scenario 3: Insider Threat / Departing Employee

Data Access After Resignation

An employee in a sensitive role (finance or engineering) resigns with two weeks' notice. On their last day, IT discovers they downloaded a large volume of files to a personal cloud storage account three days before their departure was announced.

Discussion Questions:

- When should this employee's access have been reviewed or restricted — and by whom?
- What logging or DLP controls would have detected this download in real time?
- Who decides whether to involve legal counsel, and at what threshold?
- New inject: The files included a customer database with PII. Does this trigger breach notification obligations?
- What does your offboarding checklist need to add to prevent this next time?

After the exercise: Document every gap the group identified, assign an owner and deadline to close each one, and update your written incident response plan accordingly. Run a new set of scenarios at least annually.

Want a Facilitated Tabletop Exercise?

Cenova Cyber can facilitate a live tabletop exercise customized to your environment.

Contact us to schedule one.

www.cenovacyber.com