

FACILITATOR GUIDE

Cyber Tabletop Exercise Kit

A tabletop exercise (TTX) is a discussion-based rehearsal of a cyber incident. Leaders walk through a realistic scenario, make decisions, and uncover gaps in plans, contacts, and authority before a real attacker does. This kit gives small and mid-sized businesses everything needed to run one in about two hours.

Why run a tabletop

- Cyber insurers, auditors, and customers increasingly ask for evidence of incident response testing.
- The NIST Cybersecurity Framework (CSF) 2.0 and NIST SP 800-61 Rev. 3 emphasize incident response preparation, testing, and improvement.
- Healthcare, defense, and financial regulations expect documented incident response and contingency planning.
- Most real incidents go wrong on decisions, contacts, and communication, not technology. Tabletops test exactly those.

Five steps to run your exercise

1. Plan (2 to 3 weeks before)	Choose a scenario from this kit that matches your top risks. Set two to four objectives, invite participants, book 90 to 120 minutes, and gather your incident response plan, contact list, insurance policy, and key contracts.
2. Brief (10 minutes)	Explain the ground rules: no-fault, no gotchas, decisions over perfect answers, and assume the scenario is real. Introduce roles and the scribe.
3. Play (60 to 90 minutes)	Read injects one at a time. Ask the discussion questions. Push for specifics: who, how, how fast, and with what information.
4. Hotwash (15 minutes)	Ask what went well, what was unclear, and what must change. Agree on three to five action items with owners and due dates. The scribe reads back the exercise log to confirm nothing was missed.
5. Document, report, and improve (within 2 weeks)	File the exercise log and After-Action Report with your incident response plan so the next exercise starts where this one ended. Update your plan and contact list, track action items to completion, and schedule the next exercise. Run at least one tabletop a year, and after major changes.

Ground rules to read aloud

- This is a no-fault environment. We are testing plans and processes, not people.
- Answer as you would in a real incident, using only the resources you actually have today.
- It is fine to say "I don't know." That is a gap we want to find.
- Decisions matter more than technical detail. Keep moving.
- What is said here stays here; action items go in the report.

Roles and responsibilities

In a small business one person may hold several roles. Assign each role before the exercise, and name a backup for every decision-maker.

Role	Responsibilities	Questions this role should be ready to answer
Facilitator	Runs the exercise. Keeps time, reads injects, asks follow-up questions, and keeps the discussion blame-free.	<ul style="list-style-type: none"> • What decision is needed right now, and who owns it? • What would you actually do in the first 15 minutes? • Where would you find that information at 2 a.m.?
Scribe / Observer	Records decisions, gaps, assumptions, and action items. Does not participate in the discussion.	<ul style="list-style-type: none"> • Which decisions took longest, and why? • Which contacts, documents, or tools were missing? • What did people assume that has never been tested?
Executive Sponsor (CEO / Owner)	Sets priorities, approves major decisions (shutting down systems, paying, notifying), and speaks for the company.	<ul style="list-style-type: none"> • What is our risk tolerance for downtime versus data loss? • Who is authorized to make decisions if I am unreachable? • When do we notify the board, customers, and lenders?
Incident Commander	Coordinates the response, assigns tasks, tracks status, and runs regular update calls. Often the virtual chief information security officer (vCISO) or IT/security lead.	<ul style="list-style-type: none"> • Have we declared an incident and opened an incident log? • What is our next status update time? • Which outside parties need to be engaged now?
IT Lead / Managed Service Provider (MSP)	Investigates, contains, and restores systems. Preserves evidence and logs.	<ul style="list-style-type: none"> • How do we isolate affected systems without destroying evidence? • Are backups offline, tested, and unaffected? • Which accounts and credentials must be reset first?
Security Lead / vCISO	Assesses scope and severity, guides containment and forensics, and maps actions to the incident response plan.	<ul style="list-style-type: none"> • What is the likely initial access point? • What data could have been accessed or taken? • Do we need outside digital forensics and incident response (DFIR) support?
Legal / Privacy Counsel	Advises on privilege, regulatory and contractual notification duties, law enforcement contact, and payment legality.	<ul style="list-style-type: none"> • Should outside counsel direct the investigation to preserve privilege? • Which laws and contracts set notification deadlines? • Are there sanctions concerns with any payment?
Communications / Public Relations	Prepares internal, customer, partner, media, and regulator messaging. Controls a single source of truth.	<ul style="list-style-type: none"> • What do we tell employees right now? • Who is authorized to speak externally? • What do we say if a reporter calls in the next hour?

Role	Responsibilities	Questions this role should be ready to answer
Finance / CFO	Manages payments, banking contacts, insurance claims, and emergency spending authority.	<ul style="list-style-type: none"> • Can we stop or recall any pending payments? • What emergency spending is pre-approved? • How do we document costs for the insurance claim?
Human Resources	Handles employee communications, insider issues, payroll continuity, and staff well-being during a long incident.	<ul style="list-style-type: none"> • Is any employee data affected? • How do we keep payroll running if systems are down? • Do we need to support staff working extended hours?
Operations / Business Continuity	Keeps the business serving customers using manual workarounds while systems are restored.	<ul style="list-style-type: none"> • Which processes must keep running today? • What manual workarounds exist and are they documented? • What is the maximum tolerable downtime for each?
Cyber Insurance / Broker Liaison	Notifies the carrier promptly and coordinates approved vendors (breach coach, forensics, negotiators).	<ul style="list-style-type: none"> • When must we notify our insurer, and how? • Which vendors must we use to stay covered? • Have we taken any action that could affect coverage?

Scenario menu

#	Scenario	Best for	Length
1	Ransomware with Data Extortion Attackers encrypt file servers and threaten to publish stolen data unless a ransom is paid.	All industries	90 to 120 minutes
2	Business Email Compromise and Wire Fraud A vendor's email account is compromised and used to redirect a large payment to a fraudulent bank account.	Finance, professional services, real estate, any business that sends payments	60 to 90 minutes
3	Deepfake Executive Voice and Video Fraud An employee joins a video call with what appears to be the CEO and CFO, who instruct a confidential urgent transfer.	All industries, especially those with public-facing executives	60 minutes
4	Cloud Account Takeover and Data Exposure (Microsoft 365 or Google Workspace) An administrator account is compromised through an MFA-fatigue attack, and sensitive files are shared externally.	Any business using cloud email and file sharing	75 minutes
5	Shadow AI Data Leak and AI Agent Misuse Confidential client data is pasted into an unapproved AI tool, and an AI agent with broad permissions sends sensitive files externally.	Any business adopting AI tools	60 to 75 minutes
6	Third-Party and MSP Compromise Your managed service provider's remote management tool is compromised and used to push malware to its clients.	Any business that relies on an MSP or key software vendor	75 minutes
7	Healthcare: EHR Outage and PHI Breach A ransomware attack takes the practice's electronic health record (EHR) offline, and patient records may have been taken.	Medical, dental, behavioral health, and other HIPAA-covered practices	90 minutes
8	Defense Supplier: CUI Exposure and DFARS Reporting A defense supplier discovers that an engineering file share containing CUI was accessed by an unknown actor.	Defense and aerospace suppliers handling controlled unclassified information (CUI)	75 minutes

Pre-exercise checklist

- Incident response plan (printed, in case systems are down)
- Emergency contact list: leadership, IT/MSP, legal, insurer, bank, forensics firm, FBI field office
- Cyber insurance policy and claim notification instructions
- Backup and recovery documentation

- Key customer and vendor contracts with notification clauses
- Name tents with role titles, a timer, and a whiteboard or shared screen

Scaling roles to your company size

You do not need twelve people. Combine roles to fit your organization, but always name a facilitator, a scribe, and one decision-maker.

Company size	Who should attend	How roles combine
Micro (1 to 10 people)	Owner, office manager, IT provider, and your insurance broker or attorney by phone	Owner is executive and incident commander; IT provider covers IT and security; a trusted outsider facilitates and the office manager keeps the log.
Small (10 to 50 people)	Owner or CEO, operations lead, finance, IT lead or MSP, HR or office manager	Operations lead runs the incident; finance also handles insurance; HR also handles communications; MSP covers IT and security.
Mid-sized (50 to 500 people)	Executive team, IT and security leads, legal or outside counsel, communications, HR, finance, operations	Assign each role in this kit to one person and name a backup; consider a separate technical tabletop for the IT team.

Exercise log (keep for next time)

The scribe records every inject, decision, and open question as the exercise happens. Keep this log with your incident response plan: it is your evidence for insurers and auditors, and your starting point for the next exercise.

Time	Inject / event	Decision or action	Owner	Gap or follow-up

--	--	--	--	--

After-Action Report template

Exercise date		Scenario	
Facilitator		Scribe	

Participants and roles

What went well (strengths)

Gaps and areas for improvement

Action items

#	Action	Owner	Due date	Status
1				
2				
3				
4				
5				
6				

Next exercise date and scenario: _____

Want an independent facilitator? Nexus Security Advisors designs and facilitates custom tabletop exercises for leadership teams, including ransomware, business email compromise, deepfake fraud, AI misuse, and regulatory-reporting scenarios, and delivers a written after-action report. Visit nexussecurityadvisors.com/get-started.