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.	• 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.	• 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.	• 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.	• 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.	• 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.	• 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.	• 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.	• 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.	• 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.	• 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.	• 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).	• 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.

SCENARIO 1 | ALL INDUSTRIES

Ransomware with Data Extortion

Attackers encrypt file servers and threaten to publish stolen data unless a ransom is paid.

Suggested length	90 to 120 minutes	**NIST CSF 2.0 functions**	Govern, Detect, Respond, Recover

Exercise objectives

- Validate how the organization declares an incident and assembles the response team
- Test backup recovery assumptions and restoration priorities
- Practice the ransom payment decision process, including legal, insurance, and sanctions considerations
- Exercise customer, employee, and regulator communications

Recommended participants

Facilitator and scribe, Executive Sponsor, Incident Commander, IT Lead / MSP, Security Lead / vCISO, Legal / Privacy Counsel, Communications, Finance / CFO. Add the roles named in the discussion questions below. Smaller teams can combine roles; see "Scaling roles to your company size" in the Facilitator Guide.

Injects

Read each inject aloud, then pause for discussion before moving to the next. Facilitators may add or skip injects to fit the time available.

#	When	What happens
1	**Monday, 6:40 a.m.**	Staff report that shared drives show files ending in an unknown extension. A text file named README_RESTORE.txt appears in every folder. The email server is still working.
2	**7:30 a.m.**	The MSP confirms that two file servers and the accounting system are encrypted. Some workstations are affected. Backup status is unclear; the last successful backup report is from four days ago.
3	**10:00 a.m.**	The attackers post a sample of your client files on a leak site and demand payment within 72 hours. A customer emails asking whether their data is safe.
4	**Day 2, 9:00 a.m.**	Your cyber insurer's breach coach asks what you have already done and whether you have contacted the attackers. A local reporter calls asking for comment.

Discussion questions by role

Role	Questions
Executive Sponsor	• Who has authority to shut down the network? • Under what conditions, if any, would we consider paying?

Role	Questions
IT Lead / MSP	• How do we isolate systems while preserving evidence? • How long would a full restore take, and in what order?
Legal / Privacy Counsel	• Which notification laws and contracts are triggered by possible data theft? • What sanctions screening is needed before any payment?
Communications	• What do we tell employees, customers, and the reporter today?
Finance / CFO	• When do we notify the insurer, and what costs are covered?
Everyone	• What information do we need that we do not have? • Who outside the company must we contact, and do we have their numbers offline? • What would we do differently tomorrow?

Key decisions and good practices to look for

- Declare an incident and open an incident log
- Isolate affected systems; preserve logs and evidence
- Notify the cyber insurer and engage approved vendors
- Determine whether data was exfiltrated and what notification duties apply
- Report to the Federal Bureau of Investigation (FBI) through its Internet Crime Complaint Center (IC3) or a local field office
- Restore from known-good backups in business-priority order

Hotwash (last 15 minutes): What went well? What surprised us? Which three action items will we complete in the next 30 days, and who owns each? Record them in the After-Action Report template.
Document it: the scribe keeps the Exercise Log (see the Facilitator Guide) so the next exercise builds on this one.

This scenario is fictional and for training purposes. Legal and regulatory references are general information, not legal advice; confirm requirements with counsel.

SCENARIO 2 | FINANCE, PROFESSIONAL SERVICES, REAL ESTATE, ANY BUSINESS THAT SENDS PAYMENTS

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.

Suggested length	60 to 90 minutes	**NIST CSF 2.0 functions**	Protect, Detect, Respond

Exercise objectives

- Test payment verification and bank-change procedures
- Practice rapid bank recall and law enforcement reporting
- Identify mailbox compromise indicators and containment steps

Recommended participants

Facilitator and scribe, Executive Sponsor, Incident Commander, IT Lead / MSP, Security Lead / vCISO, Legal / Privacy Counsel, Communications, Finance / CFO. Add the roles named in the discussion questions below. Smaller teams can combine roles; see "Scaling roles to your company size" in the Facilitator Guide.

Injects

Read each inject aloud, then pause for discussion before moving to the next. Facilitators may add or skip injects to fit the time available.

#	When	What happens
1	**Tuesday, 2:15 p.m.**	Accounts payable receives an email from a long-time supplier with new bank details and an urgent request to pay a $186,000 invoice before Friday.
2	**Thursday, 10:00 a.m.**	The payment was sent on Wednesday. The real supplier calls asking why their invoice is unpaid.
3	**Thursday, 11:30 a.m.**	IT finds an inbox rule in your controller's mailbox that moves all messages from the supplier to an obscure folder, created from an unfamiliar overseas IP address.

Discussion questions by role

Role	Questions
Finance / CFO	• How fast can our bank initiate a recall? • Who verified the bank change, and how?
IT Lead / MSP	• How did the attacker get into the controller's mailbox, and what else could they read?
Legal / Privacy Counsel	• Does the mailbox contain personal data that triggers notification?

Role	Questions
Executive Sponsor	• Who bears the loss, and do we need to involve the supplier's insurer?
Everyone	• What information do we need that we do not have? • Who outside the company must we contact, and do we have their numbers offline? • What would we do differently tomorrow?

Key decisions and good practices to look for

- Call the bank's fraud line immediately to request a recall
- File a complaint with the FBI at ic3.gov as soon as possible
- Reset credentials, revoke sessions, remove malicious inbox rules, and enforce multi-factor authentication (MFA)
- Review mailbox access logs to determine data exposure
- Adopt call-back verification on a known number for all bank changes

Hotwash (last 15 minutes): What went well? What surprised us? Which three action items will we complete in the next 30 days, and who owns each? Record them in the After-Action Report template.
Document it: the scribe keeps the Exercise Log (see the Facilitator Guide) so the next exercise builds on this one.

This scenario is fictional and for training purposes. Legal and regulatory references are general information, not legal advice; confirm requirements with counsel.

SCENARIO 3 | ALL INDUSTRIES, ESPECIALLY THOSE WITH PUBLIC-FACING EXECUTIVES

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.

Suggested length	60 minutes	**NIST CSF 2.0 functions**	Govern, Protect, Respond

Exercise objectives

- Test whether payment controls hold up against convincing AI impersonation
- Establish verification steps for voice and video requests
- Prepare communications if a deepfake of an executive circulates publicly

Recommended participants

Facilitator and scribe, Executive Sponsor, Incident Commander, IT Lead / MSP, Security Lead / vCISO, Legal / Privacy Counsel, Communications, Finance / CFO. Add the roles named in the discussion questions below. Smaller teams can combine roles; see "Scaling roles to your company size" in the Facilitator Guide.

Injects

Read each inject aloud, then pause for discussion before moving to the next. Facilitators may add or skip injects to fit the time available.

#	When	What happens
1	**Friday, 4:40 p.m.**	A finance specialist receives a message from the CEO's personal phone number asking them to join a quick, confidential video call.
2	**4:50 p.m.**	On the call, the 'CEO' and 'CFO' explain a confidential acquisition and ask for two transfers totaling $240,000 before the weekend. The video is slightly laggy but convincing.
3	**Monday, 9:00 a.m.**	The real CEO has no knowledge of the call. A second deepfake video of the CEO making false statements about a product recall begins circulating on social media.

Discussion questions by role

Role	Questions
Finance / CFO	• What controls should have stopped this, and did they?
Executive Sponsor	• Do executives have a verbal code word or verification process?
Communications	• How do we prove the video is fake and correct the record quickly?
Legal / Privacy Counsel	• Which platforms and authorities do we contact for takedown and reporting?

Role	Questions
Everyone	• What information do we need that we do not have? • Who outside the company must we contact, and do we have their numbers offline? • What would we do differently tomorrow?

Key decisions and good practices to look for

- Require dual approval and out-of-band call-back for all urgent or confidential payments
- Create executive code words or verification questions
- Report to the bank and to IC3
- Request platform takedowns and publish an official statement
- Train staff on deepfake red flags (urgency, secrecy, new channels)

Hotwash (last 15 minutes): What went well? What surprised us? Which three action items will we complete in the next 30 days, and who owns each? Record them in the After-Action Report template.
Document it: the scribe keeps the Exercise Log (see the Facilitator Guide) so the next exercise builds on this one.

This scenario is fictional and for training purposes. Legal and regulatory references are general information, not legal advice; confirm requirements with counsel.

SCENARIO 4 | ANY BUSINESS USING CLOUD EMAIL AND FILE SHARING

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.

Suggested length	75 minutes	**NIST CSF 2.0 functions**	Protect, Detect, Respond

Exercise objectives

- Test cloud logging, alerting, and administrator account protections
- Practice cloud containment: session revocation, app consent review, and sharing cleanup
- Determine data exposure and notification duties

Recommended participants

Facilitator and scribe, Executive Sponsor, Incident Commander, IT Lead / MSP, Security Lead / vCISO, Legal / Privacy Counsel, Communications, Finance / CFO. Add the roles named in the discussion questions below. Smaller teams can combine roles; see "Scaling roles to your company size" in the Facilitator Guide.

Injects

Read each inject aloud, then pause for discussion before moving to the next. Facilitators may add or skip injects to fit the time available.

#	When	What happens
1	**Wednesday, 11:58 p.m.**	Your IT administrator approves an MFA prompt on their phone after receiving more than 20 prompts in a few minutes.
2	**Thursday, 8:15 a.m.**	Alerts show a new mail-forwarding rule, a new third-party app granted full mailbox access, and 1,400 files shared with an external address.
3	**Thursday, 10:00 a.m.**	Your MSP discovers audit logging was only retained for seven days, and the shared files include HR records and client contracts.

Discussion questions by role

Role	Questions
IT Lead / MSP	• How quickly can we revoke sessions, remove the app, and undo the sharing? • Are admin accounts separate from daily-use accounts?
Security Lead / vCISO	• Why was MFA fatigue possible, and how do we move to phishing-resistant MFA?

Role	Questions
Legal / Privacy Counsel	• Which individuals and clients must be notified?
Human Resources	• How do we communicate with employees whose HR records were exposed?
Everyone	• What information do we need that we do not have? • Who outside the company must we contact, and do we have their numbers offline? • What would we do differently tomorrow?

Key decisions and good practices to look for

- Disable the account, revoke sessions and tokens, and remove malicious app consents and forwarding rules
- Extend audit log retention and enable alerting
- Adopt phishing-resistant MFA and number matching for admins
- Separate administrator accounts and apply conditional access
- Assess against CISA Secure Cloud Business Applications (SCuBA) baselines

Hotwash (last 15 minutes): What went well? What surprised us? Which three action items will we complete in the next 30 days, and who owns each? Record them in the After-Action Report template.
Document it: the scribe keeps the Exercise Log (see the Facilitator Guide) so the next exercise builds on this one.

This scenario is fictional and for training purposes. Legal and regulatory references are general information, not legal advice; confirm requirements with counsel.

SCENARIO 5 | ANY BUSINESS ADOPTING AI TOOLS

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.

Suggested length	60 to 75 minutes	**NIST CSF 2.0 functions**	Govern, Identify, Protect, Respond

Exercise objectives

- Test whether an AI acceptable-use policy and approved-tools list exist and are followed
- Practice investigating AI-related data exposure
- Review least-privilege controls for AI agents and copilots

Recommended participants

Facilitator and scribe, Executive Sponsor, Incident Commander, IT Lead / MSP, Security Lead / vCISO, Legal / Privacy Counsel, Communications, Finance / CFO. Add the roles named in the discussion questions below. Smaller teams can combine roles; see "Scaling roles to your company size" in the Facilitator Guide.

Injects

Read each inject aloud, then pause for discussion before moving to the next. Facilitators may add or skip injects to fit the time available.

#	When	What happens
1	**Monday, 1:00 p.m.**	A client reports that a proposal you sent contains a paragraph from another client's confidential strategy. An employee admits using a free AI chatbot to 'clean up' both documents.
2	**Tuesday, 9:30 a.m.**	Your new AI email assistant, connected to the shared drive, replies to an external email by attaching an internal pricing spreadsheet. The external message contained hidden instructions telling the assistant to do so.
3	**Tuesday, 3:00 p.m.**	An industry publication asks whether your firm has an AI policy.

Discussion questions by role

Role	Questions
Executive Sponsor	• Do we have an AI policy, and do employees know about it?
Security Lead / vCISO	• What permissions did the AI assistant have, and who approved them? • How do we defend against prompt injection?

Role	Questions
Legal / Privacy Counsel	• Was confidential or personal data disclosed, and what do our client contracts require?
Communications	• How do we respond to the publication and to the affected clients?
Everyone	• What information do we need that we do not have? • Who outside the company must we contact, and do we have their numbers offline? • What would we do differently tomorrow?

Key decisions and good practices to look for

- Disable the AI assistant's external sending and reduce its data access
- Inventory AI tools in use (shadow AI discovery)
- Publish an AI acceptable-use policy and approved-tools list
- Require human approval for AI agents that send, share, or delete
- Map controls to the NIST AI Risk Management Framework and OWASP Top 10 for Large Language Model (LLM) Applications

Hotwash (last 15 minutes): What went well? What surprised us? Which three action items will we complete in the next 30 days, and who owns each? Record them in the After-Action Report template.
Document it: the scribe keeps the Exercise Log (see the Facilitator Guide) so the next exercise builds on this one.

This scenario is fictional and for training purposes. Legal and regulatory references are general information, not legal advice; confirm requirements with counsel.

SCENARIO 6 | ANY BUSINESS THAT RELIES ON AN MSP OR KEY SOFTWARE VENDOR

Third-Party and MSP Compromise

Your managed service provider's remote management tool is compromised and used to push malware to its clients.

Suggested length	75 minutes	**NIST CSF 2.0 functions**	Govern (supply chain), Respond, Recover

Exercise objectives

- Understand dependency on third parties and shared tools
- Test contract terms, contacts, and notification expectations with vendors
- Practice operating when your IT provider is also a victim

Recommended participants

Facilitator and scribe, Executive Sponsor, Incident Commander, IT Lead / MSP, Security Lead / vCISO, Legal / Privacy Counsel, Communications, Finance / CFO. Add the roles named in the discussion questions below. Smaller teams can combine roles; see "Scaling roles to your company size" in the Facilitator Guide.

Injects

Read each inject aloud, then pause for discussion before moving to the next. Facilitators may add or skip injects to fit the time available.

#	When	What happens
1	**Saturday, 7:00 a.m.**	News reports that a popular remote monitoring and management (RMM) tool has been abused to deploy ransomware. Your MSP uses it.
2	**Saturday, 11:00 a.m.**	Your MSP is overwhelmed and has not returned calls. Several of your laptops show the RMM agent running an unknown script.
3	**Monday, 8:00 a.m.**	Your MSP confirms your environment was affected and asks for patience; they are prioritizing larger clients.

Discussion questions by role

Role	Questions
Operations / Business Continuity	• Can we operate Monday without IT support?
IT Lead / MSP	• Who else has admin access to our environment, and can we disable the RMM agent ourselves?
Legal / Privacy Counsel	• What does our MSP contract say about incident notification and liability?

Role	Questions
Cyber Insurance Liaison	• Does our policy cover third-party-caused incidents?
Everyone	• What information do we need that we do not have? • Who outside the company must we contact, and do we have their numbers offline? • What would we do differently tomorrow?

Key decisions and good practices to look for

- Identify an independent incident response firm in advance
- Maintain break-glass admin access you control
- Review vendor contracts for security and notification terms
- Keep an inventory of third-party tools with access to your systems
- Reassess vendor risk after the incident

Hotwash (last 15 minutes): What went well? What surprised us? Which three action items will we complete in the next 30 days, and who owns each? Record them in the After-Action Report template.
Document it: the scribe keeps the Exercise Log (see the Facilitator Guide) so the next exercise builds on this one.

This scenario is fictional and for training purposes. Legal and regulatory references are general information, not legal advice; confirm requirements with counsel.

SCENARIO 7 | MEDICAL, DENTAL, BEHAVIORAL HEALTH, AND OTHER HIPAA-COVERED PRACTICES

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.

Suggested length	90 minutes	**NIST CSF 2.0 functions**	Respond, Recover

Exercise objectives

- Test downtime procedures for patient care
- Practice the HIPAA breach risk assessment and notification timeline
- Coordinate with the EHR vendor and business associates

Recommended participants

Facilitator and scribe, Executive Sponsor, Incident Commander, IT Lead / MSP, Security Lead / vCISO, Legal / Privacy Counsel, Communications, Finance / CFO. Add the roles named in the discussion questions below. Smaller teams can combine roles; see "Scaling roles to your company size" in the Facilitator Guide.

Injects

Read each inject aloud, then pause for discussion before moving to the next. Facilitators may add or skip injects to fit the time available.

#	When	What happens
1	**Thursday, 7:45 a.m.**	Front-desk staff cannot log in to the EHR or scheduling system. Patients are arriving for appointments.
2	**9:30 a.m.**	The EHR vendor says your cloud tenant is unaffected, but your on-site server that syncs with it is encrypted, and the attackers claim to have patient records.
3	**Day 3**	Forensics confirms that files containing protected health information (PHI) for about 3,200 patients were copied.

Discussion questions by role

Role	Questions
Operations / Business Continuity	• How do we see patients today using paper downtime procedures?
Legal / Privacy Counsel	• How do we complete the four-factor breach risk assessment, and what are the HIPAA notification deadlines?
Communications	• What do we tell patients at the front desk today?

Role	Questions
IT Lead / MSP	• Which business associates and vendors need to be notified?
Everyone	• What information do we need that we do not have? • Who outside the company must we contact, and do we have their numbers offline? • What would we do differently tomorrow?

Key decisions and good practices to look for

- Activate downtime procedures to protect patient safety
- Notify affected individuals without unreasonable delay and no later than 60 days after discovery
- Notify the U.S. Department of Health and Human Services (HHS); breaches affecting 500 or more people also require media notice in the affected state or jurisdiction
- Review business associate agreements
- Adopt HHS 405(d) Health Industry Cybersecurity Practices

Hotwash (last 15 minutes): What went well? What surprised us? Which three action items will we complete in the next 30 days, and who owns each? Record them in the After-Action Report template.
Document it: the scribe keeps the Exercise Log (see the Facilitator Guide) so the next exercise builds on this one.

This scenario is fictional and for training purposes. Legal and regulatory references are general information, not legal advice; confirm requirements with counsel.

SCENARIO 8 | DEFENSE AND AEROSPACE SUPPLIERS HANDLING CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Defense Supplier: CUI Exposure and DFARS Reporting

A defense supplier discovers that an engineering file share containing CUI was accessed by an unknown actor.

Suggested length	75 minutes	**NIST CSF 2.0 functions**	Govern, Respond

Exercise objectives

- Practice the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 72-hour reporting process
- Test evidence preservation and media retention requirements
- Review readiness for Cybersecurity Maturity Model Certification (CMMC) incident response requirements

Recommended participants

Facilitator and scribe, Executive Sponsor, Incident Commander, IT Lead / MSP, Security Lead / vCISO, Legal / Privacy Counsel, Communications, Finance / CFO. Add the roles named in the discussion questions below. Smaller teams can combine roles; see "Scaling roles to your company size" in the Facilitator Guide.

Injects

Read each inject aloud, then pause for discussion before moving to the next. Facilitators may add or skip injects to fit the time available.

#	When	What happens
1	**Tuesday, 3:00 p.m.**	Your firewall vendor alerts on large outbound transfers from the engineering file server to an unfamiliar cloud storage service over the past week.
2	**Wednesday, 10:00 a.m.**	IT confirms the files include drawings marked CUI for a prime contractor's program. Nobody has a Department of Defense (DoD)-approved medium assurance certificate to log in to the DIBNet reporting portal.
3	**Thursday, 9:00 a.m.**	The prime contractor's security office calls asking whether you have had any incidents.

Discussion questions by role

Role	Questions
Security Lead / vCISO	• When does the 72-hour clock start, and who will submit the report?
IT Lead / MSP	• How do we preserve images of affected systems for at least 90 days?

Role	Questions
Executive Sponsor	• How do we communicate with the prime contractor?
Legal / Privacy Counsel	• What are our contractual obligations beyond DFARS?
Everyone	• What information do we need that we do not have? • Who outside the company must we contact, and do we have their numbers offline? • What would we do differently tomorrow?

Key decisions and good practices to look for

- Report to the DoD through DIBNet within 72 hours of discovery
- Obtain a medium assurance certificate before you need it
- Preserve images of affected systems and relevant monitoring data for at least 90 days
- Coordinate with the prime contractor as the contract requires
- Update the System Security Plan and Plan of Action and Milestones

Hotwash (last 15 minutes): What went well? What surprised us? Which three action items will we complete in the next 30 days, and who owns each? Record them in the After-Action Report template.
Document it: the scribe keeps the Exercise Log (see the Facilitator Guide) so the next exercise builds on this one.

This scenario is fictional and for training purposes. Legal and regulatory references are general information, not legal advice; confirm requirements with counsel.