

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	<ul style="list-style-type: none"> • Who has authority to shut down the network? • Under what conditions, if any, would we consider paying?

Role	Questions
IT Lead / MSP	<ul style="list-style-type: none"> • How do we isolate systems while preserving evidence? • How long would a full restore take, and in what order?
Legal / Privacy Counsel	<ul style="list-style-type: none"> • Which notification laws and contracts are triggered by possible data theft? • What sanctions screening is needed before any payment?
Communications	<ul style="list-style-type: none"> • What do we tell employees, customers, and the reporter today?
Finance / CFO	<ul style="list-style-type: none"> • When do we notify the insurer, and what costs are covered?
Everyone	<ul style="list-style-type: none"> • 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.