

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	<ul style="list-style-type: none"> • Can we operate Monday without IT support?
IT Lead / MSP	<ul style="list-style-type: none"> • Who else has admin access to our environment, and can we disable the RMM agent ourselves?
Legal / Privacy Counsel	<ul style="list-style-type: none"> • What does our MSP contract say about incident notification and liability?

Role	Questions
Cyber Insurance Liaison	<ul style="list-style-type: none"> • Does our policy cover third-party-caused incidents?
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

- 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.