

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	<ul style="list-style-type: none"> • Do we have an AI policy, and do employees know about it?
Security Lead / vCISO	<ul style="list-style-type: none"> • What permissions did the AI assistant have, and who approved them? • How do we defend against prompt injection?

Role	Questions
Legal / Privacy Counsel	<ul style="list-style-type: none"> • Was confidential or personal data disclosed, and what do our client contracts require?
Communications	<ul style="list-style-type: none"> • How do we respond to the publication and to the affected clients?
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

- 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.