

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	<ul style="list-style-type: none"> • How quickly can we revoke sessions, remove the app, and undo the sharing? • Are admin accounts separate from daily-use accounts?
Security Lead / vCISO	<ul style="list-style-type: none"> • Why was MFA fatigue possible, and how do we move to phishing-resistant MFA?

Role	Questions
Legal / Privacy Counsel	<ul style="list-style-type: none"> • Which individuals and clients must be notified?
Human Resources	<ul style="list-style-type: none"> • How do we communicate with employees whose HR records were exposed?
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 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.