Tabletop Exercise Pack

Four ready-to-run scenarios for rehearsing your incident response. Each takes about an hour. Also used in System Force webinars.

How to facilitate. Gather your responders and a decision maker. Read the scenario, then release each timed inject in turn, pausing for discussion. Nominate a note-taker. There are no trick questions; the aim is to surface gaps in your plan, roles, logs and communications. Capture lessons and actions at the end. Keep it no-blame.

Exercise 1 — Microsoft 365 account compromise and invoice fraud

SCENARIO

It is Tuesday morning. A supplier calls: they have paid an invoice to a new bank account, quoting an email from your finance manager. Finance did not send it. The finance manager's mailbox has a rule that deletes replies containing the word "bank".

INJECTS

09:10 — IT confirms a sign-in to the finance mailbox from an unfamiliar location last night, with MFA satisfied.

09:25 — Two more customers say they have received "updated bank details" from your finance manager.

09:40 — You find a forwarding rule sending all invoices to an external address.

DISCUSSION QUESTIONS

- Who leads, and what is the first containment step?
- How did MFA get satisfied, and what does that tell you?
- What do you tell customers, and when?
- Is this a personal data breach? Who assesses that?
- What evidence must you preserve before changing anything?

EXPECTED THEMES

- Revoke sessions/tokens, not just reset the password; remove rules and forwarding
- Independent verification of bank-detail changes; involve the bank
- Assess for ICO reporting; consider affected individuals

Exercise 2 — Ransomware at 08:15 on a Monday

SCENARIO

Staff arriving cannot open files on the shared drive. A "readme" note demands payment. Microsoft 365 email still works. The managing director asks whether to switch everything off.

INJECTS

> **08:30** — The infection appears to be spreading; a second server is now affected.

> **08:50** — Your backup console shows last night's backup job failed.

> **09:20** — A staff member finds a text file claiming 40GB of data has been stolen.

DISCUSSION QUESTIONS

- Isolate or shut down? Who decides, and on what basis?
- How do you protect the backups and still-clean systems?
- What is your minimum viable operation this morning?
- Who do you report to, and in what order?
- How do you decide when it is safe to restore?

EXPECTED THEMES

- Isolate rather than blanket shutdown; protect backups; check identity
- Assume data theft; preserve the note; bring in specialists and insurer
- Recovery gate before reconnecting; a backup may not be clean

Exercise 3 — Stolen executive laptop

SCENARIO

A director's laptop is stolen from a car. It was used ten minutes earlier. It holds exported customer records and was signed into Microsoft 365.

INJECTS

> **+30 min** — You cannot immediately confirm whether the device was encrypted.

> **+1 hr** — MDM shows the device online and reachable.

> **+2 hr** — The director mentions passwords were saved in the browser.

DISCUSSION QUESTIONS

- What do you do in the first 30 minutes?
- Encryption unknown — how does that change your risk assessment?
- Remote lock, wipe, or investigate first? What are the trade-offs?
- What about the active session and saved credentials?
- Is this reportable, and what evidence supports your decision?

EXPECTED THEMES

- Encryption + MDM state drive the whole assessment
- Revoke sessions; rotate saved credentials; consider remote wipe
- Personal data breach assessment; document the decision

Exercise 4 — Critical supplier announces a breach

SCENARIO

A software supplier that integrates with your systems emails to say they have suffered a security incident and are investigating. They hold delegated access to your Microsoft 365 and an API key to your line-of-business app.

INJECTS

> **Day 1** — The supplier cannot yet say whether your data or access was affected.

> **Day 1 PM** — You notice unusual API activity on your app overnight.

> **Day 2** — A customer asks whether their data held in that app is safe.

DISCUSSION QUESTIONS

- What access does this supplier have, and can you list it quickly?
- Do you revoke or rotate access now, before you know more?
- What evidence do you gather on your own side?
- What is your contractual position, and who owns the customer response?

EXPECTED THEMES

- Map and revoke/rotate supplier access; hunt for misuse
- Their access can become your breach; check contracts and onward impact
- Prepare a factual customer holding response

Capture lessons and actions at the end of each exercise (owner, priority, due date). See also the NCSC's free Exercise in a Box. Practical guidance, not legal advice.