Tabletop Exercise Starter Kit

A tabletop exercise is a guided discussion where your team walks through a realistic incident, step by step, without touching any live systems. It is the cheapest way to find gaps in your plans before an attacker does. This kit gives you everything you need to run your first one in about 90 minutes.

Before the session

Who to invite

- **Facilitator:** runs the scenario and reads the injects. Ideally someone who won't be a decision-maker on the day.
- **Scribe:** records decisions, questions and gaps.
- **Participants:** IT and security, a senior decision-maker, legal or data protection, communications, and the owner of the affected business area.

Ground rules

- It's a no-blame exercise: the aim is to find gaps, not to grade people.
- Answer as you would on a real day, using the plans and tools you actually have.
- “I don't know” is a valuable answer. Write it down.
- Phones away, except to look up real contact details.

Suggested 90-minute agenda

Time	Activity
0 – 10 min	Welcome, objectives and ground rules.
10 – 70 min	Run the scenario: read each inject, then discuss the questions before moving on.
70 – 85 min	Hot debrief: what went well, what was unclear, what was missing.
85 – 90 min	Agree owners and dates for the top three improvements.

© 2026 Scarlet Dragonfly · scarlet-dragonfly.com · Free to use and share with attribution

Scenario 1: Ransomware on a Friday evening

Objective: test escalation, decision-making and recovery when key systems are encrypted outside business hours.

> **Inject 1 · Friday 18:40.** The service desk receives calls from staff who cannot open shared files. Several file names now end in an unfamiliar extension.
> Who is told first, and how? Who has the authority to declare an incident out of hours? What do you do with the affected machines?

> **Inject 2 · Friday 20:15.** A ransom note appears on servers demanding payment within 72 hours. It claims data has also been copied and will be published.
> Do you have offline or immutable backups, and when were they last tested? Who decides whether to engage with the attackers? Who do you notify: insurer, regulator, law enforcement?

> **Inject 3 · Saturday 09:00.** A journalist emails asking for comment on a post on a leak site naming your organisation.
> Who speaks for you? What do you tell staff and customers, and when? What is your recovery priority list for Monday morning?

Scenario 2: Invoice fraud through a compromised mailbox

Objective: test detection of business email compromise, payment controls and supplier communication.

> **Inject 1 · Day 1.** Finance pays a regular supplier invoice of £84,000 to new bank details, following an email from the supplier's usual contact.
> What checks should happen before bank details change? Were they followed?

> **Inject 2 · Day 6.** The real supplier chases the unpaid invoice. They never changed their bank details.
> Who contacts the bank, and how quickly? Was it the supplier's mailbox or yours that was compromised? How would you find out?

> **Inject 3 · Day 7.** IT finds a hidden inbox rule in a finance user's mailbox that forwards all emails containing “invoice” to an external address.
> What other data might have been exposed? Is this a reportable personal data breach? What controls would have stopped it?

Scenario 3: Customer data exposed by a supplier

Objective: test third-party risk management, regulatory notification and customer communication.

> **Inject 1 · Day 1.** A security researcher emails to say a cloud storage bucket containing your customers' names and addresses is publicly accessible. It belongs to a marketing agency you use.
> How do you verify the claim? Who contacts the supplier, and what does your contract require of them?

© 2026 Scarlet Dragonfly · scarlet-dragonfly.com · Free to use and share with attribution

> **Inject 2 · Day 2.** The supplier confirms the bucket was public for five months and holds 120,000 customer records.
> Is this notifiable to the regulator within 72 hours? Who is the data controller? Do you need to tell affected customers?

> **Inject 3 · Day 3.** Customers start posting about suspicious emails that use their personal details.
> What goes on your website and social media? How do you support affected customers? What changes to supplier due diligence will you make?

© 2026 Scarlet Dragonfly · scarlet-dragonfly.com · Free to use and share with attribution

After-action report template

Complete this within a week, while the discussion is fresh, and share it with everyone who took part.

Item	Notes
Exercise date and scenario	
Participants	
Objectives	
What worked well	
Gaps and issues found	
Questions we couldn't answer	

Improvement actions

Action	Owner	Due date	Status

Tip: run a tabletop exercise at least once a year, and after any major change to your systems, team or suppliers. Rotate scenarios so you test different parts of your response.

Scenarios are fictional and for training use only. For facilitated exercises tailored to your organisation and sector, contact Scarlet Dragonfly at scarlet-dragonfly.com.

© 2026 Scarlet Dragonfly · scarlet-dragonfly.com · Free to use and share with attribution