



WHITEPAPER

The *Incident* *Response* Playbook for SMEs

Surviving a Data Breach

01 • THE CASE FOR A PLAN

Most Businesses Meet a Breach Without a Plan

A breach is no longer unusual for a small or medium-sized business. What separates a bad week from a business-threatening one is whether your people already know **who decides, what to do first** and **who to tell**.

43% of UK businesses identified a cyber security breach or attack in the past 12 months

Source: DSIT, Cyber Security Breaches Survey 2025/26

31% of UK businesses give a board member responsibility for cyber security

Source: DSIT, Cyber Security Breaches Survey 2025/26

What Goes Wrong Without a Plan



Decisions Made in Panic

Nobody is sure who can authorise taking a system offline



Evidence Is Lost

Well-meant clean-up wipes the logs you need later



Deadlines Slip

The 72-hour ICO window starts when you become aware



Customers Hear It Elsewhere

Silence followed by rumour does more harm than a clear notice



Recovery Drags

Backups turn out to be untested, incomplete or encrypted too



Questions Go Unanswered

Insurers, regulators and clients all expect a clear record



Three in four UK businesses have no formal incident response plan.

Source: DSIT, Cyber Security Breaches Survey 2025/26

02 · THE RESPONSE LIFECYCLE

Six Phases From First Alert to Lessons Learned

The lifecycle draws on NIST SP 800-61 and the NCSC's incident management guidance, simplified for teams without a dedicated security function.

1		Prepare Name an incident lead, keep contacts and backups offline, agree who makes which decisions	OUTPUT Playbook and contact sheet
2		Detect Confirm an incident has happened, then record the time, source and systems involved	OUTPUT Incident log opened
3		Contain Isolate affected devices, disable compromised accounts, preserve evidence	OUTPUT Spread stopped, evidence kept
4		Eradicate Remove malware and attacker access, reset credentials, close the way in	OUTPUT Clean, verified environment
5		Recover Restore from known-good backups and bring services back in priority order	OUTPUT Services back, under watch
6		Review Hold a blameless review soon after recovery and update the playbook	OUTPUT Updated playbook, owned actions

Phases overlap in practice. Containment often starts while detection is still under way.

03 · THE FIRST 72 HOURS

What to Do, and When

The clock starts when you become aware of a breach, not when the investigation ends. The first day matters most.

72

 hours

The deadline to report a notifiable personal data breach to the ICO, counted from when you become aware of it.

Source: UK GDPR, Article 33

Hour by Hour

0–1 hour	1–24 hours	24–72 hours	72 hours on
			
Stop the Spread	Establish the Facts	Notify and Communicate	Recover and Learn
• Disconnect affected devices, leave them powered on • Disable compromised accounts • Open the incident log and note the time	• Work out what was accessed, and when • Preserve logs and copy key evidence • Call your insurer and IT partner	• Decide whether the ICO must be told • Tell affected people where risk is high • Report the crime to the police	• Restore from clean, tested backups • Reset credentials and close the entry point • Hold a blameless review

⊗ Five Mistakes to Avoid

- Wiping or reimaging machines before evidence is copied
- Deleting logs or emails to tidy up
- Announcing publicly before the facts are confirmed
- Paying a ransom before taking legal and insurer advice
- Discussing the incident on systems the attacker may be watching

04 · ROLES AND NOTIFICATION

Who Decides, Who Acts, Who Tells

In a small business one person may hold two roles. Every role needs a name against it, and a backup, before anything goes wrong.

			
Incident Lead	Technical Lead	Communications Lead	Legal and Compliance
Owns decisions and keeps the timeline	Contains, investigates and restores systems	Speaks to staff, clients and the press	Advises on the ICO, contracts and evidence
Primary	Primary	Primary	Primary
Backup	Backup	Backup	Backup

Do We Need to Notify?

A simplified view of UK GDPR Articles 33 and 34. Take advice on borderline cases.



If the risk is not high, record why you did not tell individuals.

05 · READINESS AND NEXT STEPS

Your Incident Readiness Checklist

Ten checks that turn this paper into a working plan. Tick what is true today, then give each gap an owner and a date.

- | | |
|---|--|
| ☐ Incident lead and a named backup agreed | ☐ Out-of-hours contact list stored offline |
| ☐ Backups tested by restoring, with one copy offline | ☐ Multi-factor authentication on email and admin accounts |
| ☐ A record of where personal data is held | ☐ Cyber insurance policy and claims line to hand |
| ☐ Breach log ready: what, when, who, data, decisions | ☐ Draft ICO and customer notices prepared |
| ☐ Playbook exercised in a tabletop session this year | ☐ Supplier and IT partner escalation contacts confirmed |

→ Three Steps This Week

1

Name your incident lead and a backup, and write both down

2

Prove a restore from backup, not just a completed backup job

3

Run a 60-minute tabletop exercise using pages 3 to 5

Book an Incident Readiness Review

We will walk through your playbook with you and close the gaps

0161 834 9345 | 0115 822 1860

contact@netmonkeys.co.uk