

Cyber Incident Playbook Pack

Condensed, defensive playbooks for the incidents UK SMEs face most. Do the first-15-minutes basics first (see the checklist), then follow the relevant playbook.

1. Phishing / Business Email Compromise

A member of staff entered their password into a fake login page and an attacker is in the mailbox.

INVESTIGATE

- Recent sign-ins and locations; MFA events and new sign-in methods
- New mailbox rules, forwarding, delegated permissions, app (OAuth) consents
- Sent / deleted items; emails about payments or bank details
- Internal phishing sent from the account; other accounts hit the same way

RECOVER

- Block the account; reset password; re-secure MFA
- Revoke active sessions and tokens (not just future logins)
- Remove malicious rules, forwarding, delegations and app consents
- Investigate any payment fraud; monitor closely

2. Microsoft 365 Account Compromise

A confirmed Microsoft 365 / Entra ID account takeover, with or without email fraud.

CONTAIN AND INVESTIGATE

- Disable sign-in; revoke sessions and refresh tokens; reset credentials
- Review conditional access, registered devices and authentication methods
- Audit unified sign-in and admin logs; check for new global admin or app registrations
- Review SharePoint / OneDrive access and downloads

A password reset alone can leave a live session open. Always revoke sessions and tokens.

3. Ransomware

Files are encrypted and a ransom note has appeared.

ACT

- Isolate affected systems; do not shut everything down indiscriminately
- Segment the network to stop spread; protect still-clean systems
- Protect backup infrastructure (attackers target it deliberately)
- Check identity compromise, hypervisor/server impact, internet/VPN exposure
- Look for data theft; preserve the ransom note and any attacker messages

THEN

- Bring in external incident-response support; involve insurer and, where relevant, NCSC and Report Fraud
- Restore only from known-good data; validate before reconnecting

A backup is not automatically clean just because it predates the visible encryption. Attackers often dwell for weeks. Rebuild rather than restore where unsure.

4. Data Breach / Exfiltration

You suspect data has been copied out of the business.

ESTABLISH

- Exactly what data, whose, how sensitive, how many records/people, whether protected
- Was it merely accessible, or demonstrably accessed/taken? What is the evidence?

ACT

- Contain the exposure; run the personal data breach assessment
- Check contractual notification duties; consider informing affected individuals

5. Lost or Stolen Device

A laptop or phone has gone missing.

- Who reported it and when; which device; what data it held
- Was it encrypted? Enrolled in MDM (remote lock / wipe)?
- Active sessions, saved tokens and credentials; local admin rights
- Report as appropriate; run a short risk assessment

"Laptop stolen" and "unencrypted laptop with the customer database, stolen while signed in" are not the same incident.

6. Supplier / Third-Party Compromise

A supplier or software provider tells you they have been breached.

- Map exposure: integrations, credentials/API keys, remote access, VPN, shared accounts, delegated Microsoft 365 access, shared data
- Revoke or rotate any access they hold; look for misuse on your side
- Understand onward supply-chain impact; check contractual obligations; monitor

7. Website / Public Service Compromise

Your website is defaced, redirecting, or serving malicious code.

- Find the mechanism: injected code, redirect, credential theft, compromised CMS admin, hosting or registrar compromise, DNS changes
- Consider customer-data implications
- Clean to a known-good state; patch the root cause; rotate every relevant secret (CMS, hosting, database, API)

Defensive guidance only. Full detail and context: systemforce.co.uk/blog/2026/08/26/cyber-incident-response-plan-uk/ · Practical guidance, not legal advice.