First 72 Hours Checklist

Print this and keep it with your offline incident plan. Work top to bottom. Tick as you go.

> The quality of the first few decisions usually matters more than the speed of random action. Isolate and preserve first; investigate second; recover last.

First 15 minutes — get control

- [ ] Stop and assess. Do not react on instinct.
- [ ] Declare an incident if it looks real; say a provisional severity out loud.
- [ ] Start the incident log with the current time.
- [ ] Notify the incident lead (or become it).
- [ ] Isolate suspect devices from the network — leave them powered on.
- [ ] Switch to safe communications if email may be compromised.
- [ ] Pause payments if money or bank details are involved.
- [ ] Preserve evidence. Do not delete, wipe or tidy up.

Do

- [ ] Write down what you see, with times
- [ ] Ask for help early

Do not

- [ ] Wipe a device that looks infected
- [ ] Reset every password at once

First hour — establish command

- [ ] Confirm the incident lead; get key people on a call.
- [ ] Nominate the recorder (owns the timeline).
- [ ] Set the severity and write it down.
- [ ] Identify affected services and what still works.
- [ ] Decide containment priorities to limit spread.
- [ ] Check whether privileged / identity accounts are involved (treat as Critical if so).
- [ ] Contact your IT provider / incident-response specialist if warranted.
- [ ] Contact your cyber insurer early if the policy requires it.
- [ ] Begin the data protection / legal assessment in parallel.
- [ ] Export logs before they roll off; screenshot what you see.
- [ ] Set up safe out-of-band communications and an update cadence.
- [ ] Write the first situation report (SITREP).

First 4 hours — scope and contain

- [ ] Review recent sign-ins, MFA events and new authentication methods.
- [ ] Check mailbox rules, forwarding, delegated permissions and app consents.
- [ ] Look for lateral movement and data exfiltration indicators.
- [ ] Identify exposed credentials; rotate where needed.

- [ ] Check backup integrity and recovery dependencies.
- [ ] Confirm the attacker no longer has access — do not just assume it.

First 24 hours — decisions and communications

- [ ] Continue investigation and evidence preservation.
- [ ] Complete the legal / regulatory analysis; meet insurer requirements.
- [ ] Assess customer and service impact; agree minimum viable operation.
- [ ] Communicate with staff and, where appropriate, customers (facts only).
- [ ] Rotate credentials and secrets; verify payment / bank-detail changes independently.
- [ ] Log every significant decision and why.

> Management should be able to answer: what do we know / not know? Is the attacker still active? What is unavailable? Is personal data involved? Has anything left the organisation? Who must we tell, and by when?

24 to 72 hours — obligations and safe recovery

- [ ] Assess whether a notifiable personal data breach occurred (see the breach assessment form).
- [ ] If notifiable, report to the ICO within 72 hours of becoming aware; report early, update later.
- [ ] Report to the NCSC (ncsc.gov.uk/report) and Report Fraud where relevant.
- [ ] Recover from known-good sources through the recovery gate only.
- [ ] Reconnect systems in controlled stages under heightened monitoring.
- [ ] Keep the complete decision record, including decisions not to act.

> Practical guidance, not legal advice. Check current ICO and NCSC guidance. Full detail: systemforce.co.uk/blog/2026/08/26/cyber-incident-response-plan-uk/