Ekselens

EKSELENS360

EKSELENS INSIGHT · CYBER & RESILIENCE

The first 24 hours: making incident readiness real

Most incident plans fail in the first day, not the last. Decide in advance who decides, who is told and what the business does while systems are down.

THE EIGHT-PHASE METHOD



01 Discover · 02 Diagnose · 03 Design · 04 Plan · 05 Mobilise · 06 Deliver · 07 Embed · 08 Optimise

Ekselens Consulting

ekselens.com · info@ekselens.com

Changing how transformation is done

The EKSELENS360 family

CYBER & RESILIENCE · 12 NOVEMBER 2026 · 4 MIN READ

Most organisations have an incident response plan. Far fewer have one that works under pressure. The first 24 hours of a serious cyber or service incident decide much of what follows: how far the damage spreads, how long recovery takes, and whether customers, regulators and the board keep their confidence.

Those hours are rarely lost to a lack of technical skill. They are lost to unclear decisions.

Why plans fail in the first day

Incident plans tend to be written by technical teams for technical teams. When a real incident starts, the hardest questions are not technical:

- Who has the authority to take a core system offline?
- Who tells customers, staff and suppliers — and what do they say?
- When does the incident become reportable, and who makes that call?
- How does the business keep operating while systems are unavailable?

If those answers are worked out during the incident, hours disappear in meetings. Reporting deadlines are tight: personal data breaches must be reported to the ICO within 72 hours of becoming aware of them, and the UK's Cyber Security and Resilience Bill proposes an initial notification within 24 hours for significant incidents in scope.

Decide decision rights in advance

Write down, before anything goes wrong, who can make each critical call and who deputises when they are unavailable. As a minimum:

- **Incident lead:** runs the response and owns the timeline.
- **Business decision-maker:** authorises service shutdowns, customer-facing changes and spend.
- **Communications lead:** owns every external and internal message.
- **Regulatory lead:** decides reportability and makes notifications.
- **Supplier lead:** coordinates with any third party involved.

Keep the list short, current and available offline. An incident that takes out email and collaboration tools will also take out the plan if it lives only there.

Plan for the business, not just the systems

Technical recovery can take days. The business needs to keep serving customers in the meantime. For each important business service, agree:

- the manual or degraded way of working if systems are unavailable;
- how long that workaround can be sustained;
- which customers or activities take priority;
- what information staff need to operate it.

This is where incident readiness meets operational resilience. A service that cannot run in degraded mode has no real resilience, however good the technical recovery plan.

Make recovery dependable

Recovery depends on assets that attackers increasingly target first. Check that:

- backups are isolated from the main environment and cannot be altered or deleted from it;
- restores are tested regularly, at realistic scale, with timings recorded;
- critical system documentation and credentials are available if the main environment is lost;
- the order in which services are restored has been agreed in advance.

An untested backup is an assumption, not a control.

Rehearse with the people who will decide

Tabletop exercises are most valuable when executives take part, not just technical teams. Run a realistic scenario — ideally one that starts with a supplier — and walk through the first 24 hours hour by hour. Record every point where a decision was unclear or slow, then fix it.

Good exercises are uncomfortable. They show where authority is missing, where messages have not been prepared, and where a dependency was not understood. That is the point.

Evidence the readiness

Boards, auditors and regulators increasingly want evidence that readiness is real, not asserted. Keep a simple record of:

- the current decision-rights list and when it was last reviewed;
- exercises run, issues found and actions closed;
- backup restore tests and their results;
- incidents and near misses, with the lessons applied.

This is the difference between a plan on a shelf and a capability the organisation can prove.

A practical starting point

In the next 30 days, confirm the decision-rights list, check that the plan is available offline, and schedule an executive tabletop exercise. None of this requires new technology. It requires leadership to decide, in calm conditions, what they would otherwise have to decide in a crisis.

Want to talk this through?

Book a 45-minute discovery conversation. Bring one challenge, leave with three prioritised next steps — written up within 24 hours.

ekselens.com/contact
info@ekselens.com
+44 (0) 20 7874 7217

© Ekselens Consulting. All rights reserved.