Resilience Health Check 2026

Dennis Martin

Director Business Resilience, Axians UK

Belvedere House, Basing View, Basingstoke, Hampshire, RG21 4HG| Office: +44 (0)1256 312 350

Axians Networks Limited with registered No. 04407184

www.axians.co.uk

Questions every Board should be able to answer

Most organisations believe they are resilient. Far fewer have tested whether that belief holds when decisions must be made quickly, with incomplete information, and real consequences.

Recent crises, including high-profile ransomware attacks, have shown that disruption rarely remains a technical issue. What begins as an operational problem can rapidly become a strategic, legal, financial and reputational event. The organisations that navigate these situations well are rarely the ones with the thickest documentation. They are the ones that have tested their assumptions, clarified decision rights, and rehearsed how leadership behaves under pressure.

This Resilience Health Check is not a maturity model and not a compliance checklist. It is a structured set of questions designed to help Boards and executive teams assess whether resilience is assumed or proven.

It can be used as:

- A focused 60-minute Board discussion
- A structured executive self-assessment
- A precursor to a resilience or crisis simulation exercise

If these questions cannot be answered clearly and consistently, that is not a failure. It is valuable insight.

1. Do we have credible plans for when critical things fail?

Resilience requires more than intent. It requires practical, workable arrangements that allow the organisation to continue operating or recover when key systems, people or suppliers are unavailable.

- Have we clearly identified our most critical processes and services?
- Do we understand the systems, data, facilities, suppliers and individuals they depend on?
- Do we have documented recovery or continuity arrangements for those critical elements?
- Have we identified single points of failure across technology, suppliers and decision makers?
- Can we operate key processes at reduced or degraded performance if necessary?

Plans developed in isolation often conflict. A recovery plan that assumes systems will be restored in hours is ineffective if technical recovery realistically takes days.

2. Have we tested our plans, or are we trusting assumptions?

Strategies, controls and plans are essential. Without realistic testing, they remain assumptions.

- When were our most critical resilience and crisis arrangements last tested?
- Were those tests designed to challenge our assumptions, or to confirm them?
- Did they include executive decision-making, communications and escalation, not just operational recovery?

- Have we tested cross-functional coordination, including legal, communications and business leadership?
- What tangible changes were made as a result?

Testing is not about passing. It is about discovering friction, ambiguity and unrealistic expectations before they matter.

Test, do not trust.

3. Can we make fast, defensible decisions with incomplete information?

In serious incidents, the quality and timeliness of decisions matter more than the quality of documentation. Delayed or unclear decisions frequently cause more damage than the initial disruption.

- Who is empowered to make time-critical decisions in a crisis?
- Is it clear which decisions sit at operational, executive and Board level?
- Do decision-makers understand the organisation's risk appetite under pressure?
- Are decisions documented clearly enough to be explained and defended later?
- Where have decisions stalled in previous incidents, and why?

Resilience is demonstrated by timely decisions that can be justified afterwards, even if the outcome was imperfect.

4. Would we recognise a crisis early enough?

Most major crises do not begin as obvious Board-level events. They escalate when weak signals are missed, misinterpreted or downplayed.

- What indicators suggest an operational issue is becoming a strategic one?
- Who has authority to escalate an incident to executive or Board level?
- Have we rehearsed scenarios where escalation is ambiguous rather than clear-cut?
- Do we actively reward early escalation, even when it later proves unnecessary?

Early recognition preserves options. Late recognition reduces them.

5. Are cyber incidents treated as business crises?

Cyber incidents now routinely trigger regulatory, legal, operational and reputational consequences. Treating them as technical problems for too long is a recurring failure pattern.

- Have we exercised a cyber scenario that required business, legal and reputational trade-offs?
- Is it clear who decides whether to shut systems down, communicate externally or notify authorities?
- Would the Board understand its expected role during a major cyber event?
- Have these expectations been tested under realistic pressure?

In ransomware incidents, for example, organisations are often forced into high-stakes decisions about system shutdowns, public communication, regulatory notification and, in some jurisdictions, ransom payment. These decisions cannot be improvised effectively. They require prior clarity on authority, principles and risk tolerance.

Cyber resilience is not only about technical controls. It is about executive readiness.

6. Do we genuinely understand our critical dependencies?

Third-party resilience is frequently assumed rather than examined. Questionnaires and contractual clauses provide assurance, but not necessarily capability.

- Which suppliers or partners could materially disrupt our operations if they failed?
- How quickly would we feel the impact?
- What assumptions are we making about their recovery capabilities?
- Which of those assumptions have we actively challenged?
- Do we understand concentration risk across technology providers or shared services?

Exposure becomes manageable only when it is visible.

7. What does our culture do when things go wrong?

Culture determines behaviour when plans, hierarchies and processes are under strain. It is often the hidden factor in resilience outcomes.

- Do people feel safe escalating bad news quickly?
- Is constructive challenge welcomed during incidents?
- Are leaders rewarded for transparency under pressure?
- Have we unintentionally trained the organisation to minimise issues to avoid scrutiny?

No framework can compensate for a culture that suppresses reality. Conversely, a culture that encourages early disclosure and disciplined challenge can compensate for imperfect plans.

A final question for the Board

If a major disruption began in the next six months, would these questions already have clear answers?

Or would the Board be discovering them in real time, under pressure, with limited information and external scrutiny?

Resilience is not demonstrated by documentation.

It is demonstrated by behaviour, clarity and decisions when it matters most.

Belvedere House, Basing View, Basingstoke, Hampshire, RG21 4HG| Office: +44 (0)1256 312 350
Axians Networks Limited with registered No. 04407184
www.axians.co.uk