BOARD INSIGHT MICRO LEARNING · I · JUNE 2026

Digital & Technology Resilience

Building confidence that your critical business services can withstand disruption

Digital Risk AWARE LIMITED

Modern organisations rely on technology to deliver almost every critical service.

Whether supporting customers, employees, supply chains or regulatory obligations, digital systems have become fundamental to business operations. As this dependence grows, so too does the impact of technology failures.

Cyber attacks, system outages, third-party failures, software defects and human error can all disrupt business operations.

The question is no longer whether disruption will occur, but whether the organisation is sufficiently prepared to continue delivering its most important services when it does.

Technology resilience is about far more than keeping systems available. It is the ability of an organisation to anticipate, withstand, respond to and recover from disruption while continuing to deliver the business services upon which customers, employees and stakeholders depend.

Importantly, technology resilience is not achieved through a single programme or capability. It is the outcome of multiple disciplines working together to reduce risk, improve preparedness and enable effective recovery. These include cyber resilience, change management, third-party management, business continuity, data protection and digital transformation. Weakness in any one of these areas can significantly reduce an organisation's overall resilience.

Resilience provides confidence that critical business services can continue to operate during periods of disruption, that significant incidents are managed effectively, and that the organisation can recover in a controlled and timely manner. Effective governance requires understanding how these interconnected disciplines contribute to the resilience of the organisation as a whole, rather than considering them in isolation.

Digital Risk AWARE LIMITED

Board Perspective - Why Technology Resilience Matters

The consequences of technology failures extend well beyond the IT department. A disruption affecting a single technology platform can quickly impact customers, operations, financial performance and organisational reputation.

Depending on the nature of the outage, organisations may experience:

- Are governance structures keeping pace with the complexity and scale of delivery?
- Inability to deliver products or services
- Customer dissatisfaction and reputational damage
- Regulatory scrutiny and enforcement action
- Financial losses arising from contractual obligations or compensation
- Operational disruption across multiple business functions
- Loss or corruption of critical business data

Digital Resilience Has Become a Strategic Business Imperative

Recent years have demonstrated that even mature organisations can suffer significant disruption. Global cyberattacks have halted manufacturing operations, cloud service failures have prevented organisations from accessing critical business applications, software defects have disrupted financial markets, and failures at third-party suppliers have affected thousands of organisations simultaneously.

These events have reinforced an important lesson: organisations are increasingly dependent upon complex digital ecosystems that extend far beyond their own infrastructure.

Recognising the growing importance of resilience, regulators around the world have introduced stronger expectations for Boards and senior management. The European Union's Digital Operational Resilience Act (DORA) establishes comprehensive requirements for the resilience of financial institutions and their critical technology providers, while the UK's operational resilience framework developed by the Financial Conduct Authority, Prudential Regulation Authority and Bank of England places greater emphasis on protecting important business services rather than individual systems.

Although these regulations focus on regulated sectors, the underlying principles represent recognised good practice for organisations across all industries. Customers, investors and stakeholders increasingly expect organisations to demonstrate that they can continue delivering critical services even when technology fails.

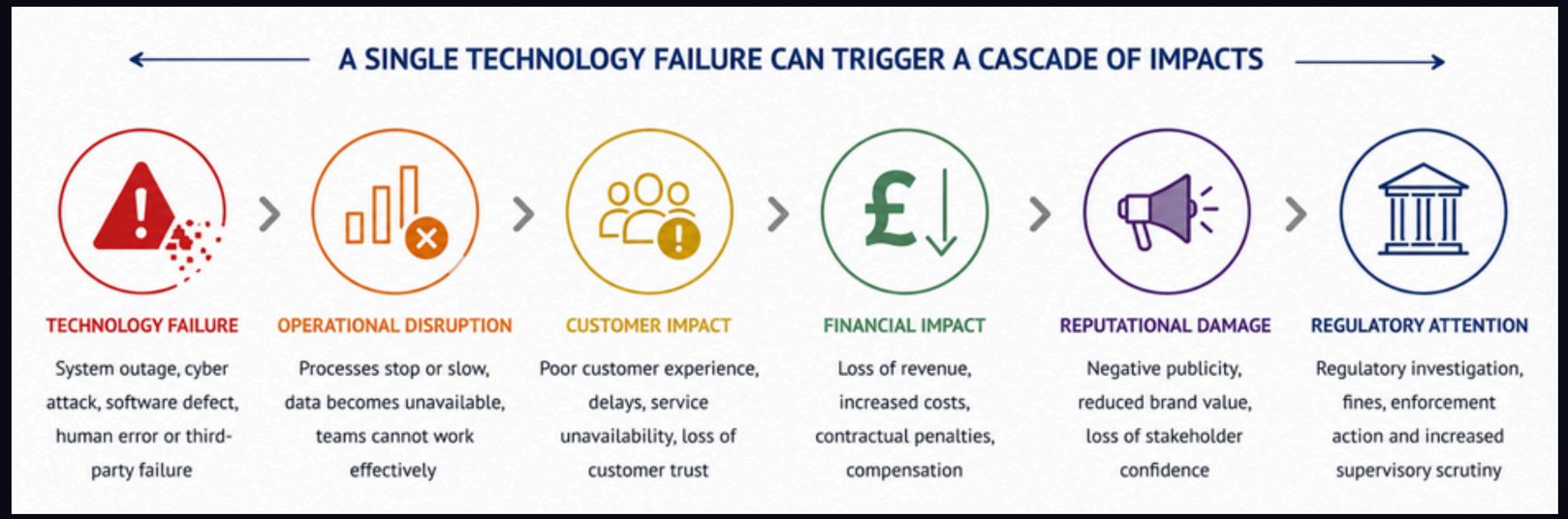
Digital Risk AWARE LIMITED

Questions Every Board Should Be Asking

Technology resilience is ultimately a governance issue. While management is responsible for designing and operating resilience capabilities, Boards are responsible for providing effective oversight, challenge and strategic direction.

Without becoming involved in technical detail, Boards should have confidence that they can answer questions such as:

- Which business services are most critical to the organisation?
- How dependent are those services on technology and third-party providers?
- What are our most significant resilience risks and vulnerabilities?
- Where are our potential single points of failure?
- What are the interdependencies associated with each single point of failure and does management have a plan in place for each dependency?
- How long could we tolerate disruption to our critical services?
- Have our resilience arrangements been tested under realistic scenarios?
- Would we recover in the timescales our customers, regulators and stakeholders expect?
- Do we receive meaningful information that enables effective oversight and challenge?
- Are we investing appropriately to strengthen resilience over time?



The answers to these questions provide far greater insight than simply understanding whether systems have backup arrangements or disaster recovery plans. They enable Boards to make informed decisions, prioritise investment and gain confidence that the organisation is prepared for disruption.

As organisations become increasingly dependent on digital technologies, effective Board oversight of technology resilience is no longer optional—it is a fundamental component of good governance.