Executive Guide

Telstra

Resilience by design

Building connected ecosystems for the age of disruption

An Economist Impact report, supported by Telstra International

Digital resilience is now a leadership issue

Digital resilience is no longer about preventing disruption. It is about keeping the business running when disruption occurs.

Most executive teams recognise this shift. However, new research from Economist Impact, *Resilience by design: Building connected ecosystems for the age of disruption*, shows that many organisations struggle to turn awareness into real-world readiness.

The research draws on a survey of 1,420 senior executives across 11 Asia Pacific markets, with comparative benchmarks from the US, UK and Germany. It shows that while no market or industry is standing still, few organisations have reached digital resilience maturity.

Many organisations invest heavily in cybersecurity and modernisation. Yet they remain vulnerable to cascading failures caused by supplier incidents, infrastructure instability, accountability gaps and human error.

This Executive Guide summarises the research and highlights practical actions leaders can take.

How executives can improve digital resilience:

1. Embed ecosystem partners in digital resilience-building
2. Make resilience a core business capability
3. Move from periodic reviews to continuous preparedness
4. Build cultures that support digital resilience
5. Train leaders to make decisions in ambiguity
6. Strengthen governance as innovation scales

Ecosystem dependencies are the biggest blind spot

Only **12%** of organisations have first-hand insight into suppliers' resilience.

Executive confidence in digital resilience drops sharply beyond organisational boundaries.

Most organisations feel confident in their internal controls. However, only a small minority have first-hand visibility into the digital resilience of their suppliers. When communications infrastructure or power supply is unstable, regulatory frameworks are unclear, or organisations rely on vendors' self-reported controls, even mature organisations become vulnerable.

These gaps often stem from limited information sharing, infrequent or absent simulations with suppliers, and over-reliance on service level agreements to manage relationships.

Executive takeaway:

Embed ecosystem partners in digital resilience-building

- How does your organisation actively build digital resilience across its ecosystem?
- Do you run joint incident reviews with your partners?
- Do you have real-time information sharing in place with partners?

Leadership ownership remains fragmented

In **47%** of organisations, responsibility for digital resilience sits with a single function.

"Resilience has become an enterprise-wide capability – spanning technology, people, processes and partners – rather than a function owned by security teams alone."

Charles Ross, Head of Policy and Insights, Asia-Pacific, Economist Impact

Responsibility often rests with one role – typically IT or security – rather than being shared across the Board, C-suite and business. As a result, ownership remains fragmented.

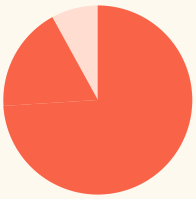
Boards provide inconsistent oversight, and organisations under-resource digital resilience initiatives. This increases risk and signals that digital resilience is not embedded in business strategy.

Executive takeaway:

Treat digital resilience as a standing capability, not a project

- Have you allocated sustained budget and resources to digital resilience?
- Is responsibility for digital resilience shared across the business?
- How does the Board engage on digital resilience as a strategic issue?

Digital resilience is broader than cybersecurity



92% of organisations faced cyber-related threats in the past year.

63% faced internal failures, and **62%** experienced external outages.

All organisations faced multiple threats of disruption in the past 12 months.

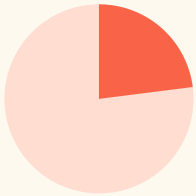
Cybersecurity remains critical, but it is only one part of digital resilience. Modern enterprises operate across complex partner ecosystems and distributed workforces. When one part of the network fails, disruption can quickly spread across regions, functions and customers.

Executive takeaway:

Move from periodic reviews to continuous preparedness

- How could your organisation move towards real-time monitoring?
- Does business continuity planning prepare for multiple, simultaneous disruptions?
- Does governance clearly define controls and accountability?

Incident response fails because of people and structures, not tools



Only **23%** of organisations say their disruption response went mostly to plan.

"Someone from senior leadership needs to be there making sure it's a safe environment and that everything is coming out in the wash."

Harry Jensen, Senior Director and Head of Operations, Australia and Philippines, Equinix

Most organisations have incident response plans and tools in place. Yet fewer than one in four real-world responses unfold as expected. When incidents escalate, failure is rarely caused by missing technology.

Instead, responses break down because of unclear decision-making, slow escalation, siloed teams and poor coordination. These structural and behavioural gaps matter more than the tools organisations deploy.

Executive takeaway:

Build cultures of digital resilience that encourage transparency and learning

- Do incident reviews include training and capability building?
- How do leaders create a safe environment that encourages openness during reviews?
- Do incident reviews focus on improving future outcomes, not just identifying what went wrong?

Decision-making in ambiguity is a critical leadership skill

Only **12%** of executives have confidence in their teams' ability to adapt during system outages.

When disruption escalates, leadership and organisational design matter as much as systems.

Gaps in digital resilience are rarely technical. They sit in leadership decision-making and governance, especially when teams must act under pressure with incomplete information.

Organisations can use culture surveys, behavioural assessments and audit feedback to test whether leadership structures and workplace culture support effective decision-making during disruption.

Executive takeaway:

Train leaders and teams to operate in ambiguity and disruption

- Does your organisation train leaders to make decisions under pressure?
- Does incident response planning support fast, effective decision-making?
- How does company culture enable teams to respond during disruption?

Technology upgrades are outpacing governance improvements

Only **39%** of organisations conduct cross-functional risk assessments before deploying new technologies.

Organisations must invest in governance, controls and resilience engineering alongside new and modernised platforms.

Many organisations are rapidly modernising systems and adopting technologies such as AI and automation. As a result, technology and infrastructure have become the most mature pillar of digital resilience in many regions. However, governance has not kept pace. Organisations often fail to build safeguards and oversight at the same speed, creating new risks and vulnerabilities.

Executive takeaway:

Strengthen governance alongside innovation

- Do modernisation programs integrate risk management and clear oversight?
- Are governance processes embedded into technology upgrades and reviews?
- Do leaders consistently record decisions taken and outcomes achieved?

Why this matters for leaders

Today's organisations operate in high-growth, high-complexity environments. Infrastructure maturity, regulatory clarity and access to talent vary widely across markets.

The research shows that leaders understand the challenge. The next step is disciplined execution, at scale.

A clear pattern stands out:

- Risk management and cybersecurity practices are relatively mature
- Leadership alignment, ecosystem readiness and workforce adaptability lag behind

What matters now is coordinated digital resilience across the organisation and its ecosystem.

The six shifts required to build digital resilience are leadership decisions, not technical ones.

> **"Digital systems are now the backbone of how the business runs."**
>
> Balaji Uppili, Senior Director, SaaS and Digital Innovation, GE Healthcare

Measure up: What the Digital Resilience barometer reveals

Economist Impact developed the *Digital Resilience barometer* to measure executive confidence across five core pillars of digital resilience:

1. External enabling environment
2. Technology and infrastructure
3. Risk management
4. Leadership
5. Workforce and cultural agility

Across APAC and benchmark markets, scores cluster tightly. No region has yet achieved end-to-end digital resilience maturity.

Go deeper: *Digital resilience by design: Building connected ecosystems for the age of disruption*

The full *Resilience by design* report provides:

- Detailed analysis across five core digital resilience pillars
- Deeper insight into the Digital Resilience Barometer findings
- Market- and industry-level benchmarks
- Practical perspectives from global business and technology leaders
- Clear analysis of how digital resilience shapes strategy, investment and growth

Download the report →

Contact your Telstra account representative for more details.

telstraenquiry@team.telstra.com telstrainternational.com

2026.03.31 110 PM