ECONOMIST IMPACT

Resilience by design

Building connected ecosystems for the age of disruption

Supported by Telstra

Contents

Foreword by Telstra International

Across industries and regions, business leaders are confronting the same reality: disruption has become continuous. The systems and networks that underpin modern enterprises are more powerful and interconnected than ever, but also more exposed. How organisations prepare for, respond to and recover from disruption now defines their ability to compete and grow.

Led by Economist Impact and supported by Telstra International, this research reflects this shift. Eighty-four percent of Asia-Pacific (APAC) leaders say that strengthening digital resilience delivers competitive advantage—which is why we are committed to supporting organisations as they strengthen resilience across their digital ecosystems.

We must also continue to improve how we manage digital disruption, because it's increasingly complex. We are operating in an era defined by the exponential growth of data, the rapid rise of AI, constant cyber challenges, and the increasing interdependence of digital infrastructure. Organisations now move vast volumes of information across clouds, borders and ecosystems every second. That creates incredible opportunity, but it also raises the stakes. When something fails, it rarely fails in isolation.

We need a more rigorous approach to understanding how digital resilience is built and sustained in today's environment. That's why we partnered with Economist Impact on this report. Together, we set out to understand three things: what is the reality of digital resilience in enterprises today, what breaks under pressure and what leaders can do to de-risk and build resilience across their enterprise and ecosystem.

The findings are clear. Digital resilience extends far beyond systems and tools—it is an enterprise-wide capability. One of the strongest signals from the research is that failed responses to disruption are most often driven by poor scenario planning. That insight highlights the need for ongoing planning, testing and adaptation across connected ecosystems. When scenario planning is shared across the organisation, it benefits from diverse expertise and informed human judgement, not just technical strength. While robust technology is critical, the report shows it delivers real value only when matched by cultural readiness—an area where many organisations still have work to do.

At Telstra International, resilience has long been part of our DNA. We build and operate networks engineered to keep critical traffic flowing, across diverse subsea and terrestrial routes in some of the world's most dynamic markets. But infrastructure alone is not enough. True digital resilience spans strategy, governance, culture and collaboration. It depends on people, expertise and partnerships working together, and on the willingness to learn, adapt and get stronger through each disruption.

We recognise that digital resilience is a journey, not a destination. I hope the report helps you build the confidence, capability and connected ecosystems needed to thrive in a world where disruption is the norm.

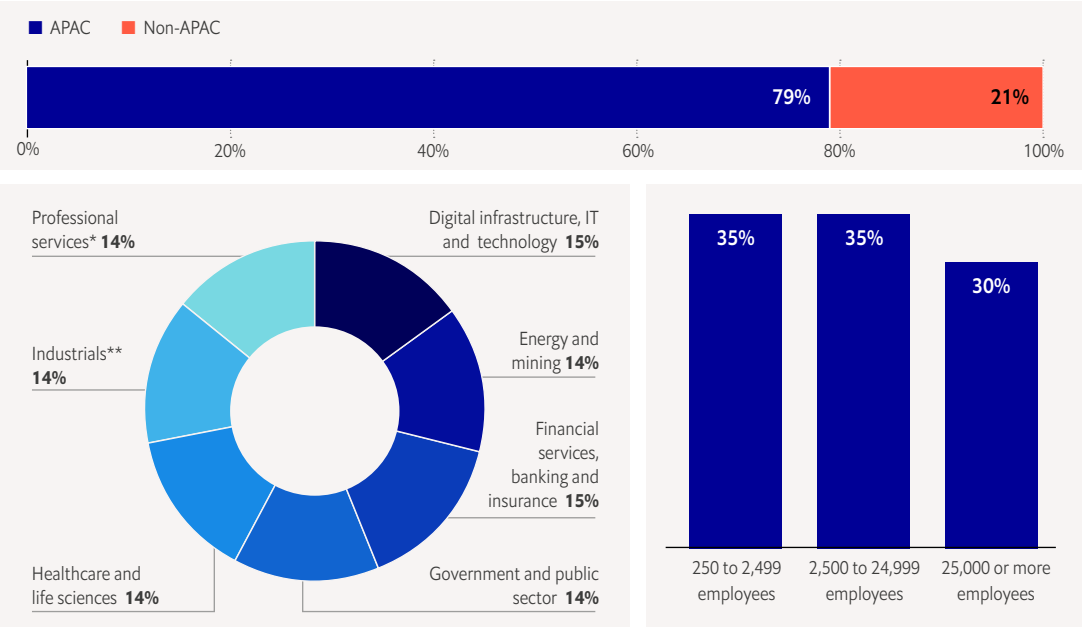
Roary Stasko
CEO, Telstra International

About this report

Resilience by design: building connected ecosystems for the age of disruption is an Economist Impact report, supported by Telstra International. It explores how organisations in APAC seek to build digital resilience amid an era of compounding risks and how connected ecosystems enable them to adapt and respond to disruption.

The report accompanies a barometer which assesses digital resilience capabilities across 11 APAC markets—Australia, mainland China, Hong Kong, India, Indonesia, Japan, the Philippines, Singapore, South Korea, Taiwan and Thailand—along with comparative benchmarks from the US, the UK and Germany. The analysis is based on a survey of 1,420 senior executives from large and mid-size organisations across seven sectors in these markets.

Figure 1: Demographics



*Includes: accounting services, legal firms, marketing and advertising, etc. **Includes: manufacturing, logistics and supply chain
Source: Economist Impact survey on Digital Resilience, 2025

Additional insights were obtained from in-depth interviews with the following executives and experts from across APAC, Europe and North America:

- **Eugene Huang**, chief information officer, DBS
- **Keith Ip**, chief technology officer, Li & Fung
- **Mihaela Isac**, chief information officer, APAC, DHL Supply Chain
- **Harry Jensen,** senior operations director of Australia and the Philippines, Equinix
- **Simon Lockington,** senior director of global solution architecture, APAC, Equinix
- **Brian O'Neill,** global head, group transformation, Standard Chartered
- **Clemens Philippi**, chief executive officer, MSIG Asia
- **Andreas Spanner,** chief architect, Red Hat
- **Nizar Trigui**, chief technology officer, GXO
- **Balaji Uppili**, senior director, Saas and digital innovation, GE HealthCare

Economist Impact bears sole responsibility for the content of this report. The findings and views expressed in it do not necessarily reflect the views of the interviewees or sponsors. The research was led by Charles Ross and Anushree Sharma. The report was written by Denis McCauley.

Although every effort has been taken to verify the accuracy of this information, Economist Impact cannot accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in it.

Executive summary

Business leaders have traditionally viewed digital resilience through the prism of cybersecurity. But this misses the bigger picture. Technology-related disruptions result not just from malicious attacks, but also from failures of enterprise technology and external communications networks, breakdowns among suppliers and other ecosystem partners, power outages, climate-related hazards and human error.

Digital resilience, once defined largely as the technical ability to respond to cyber attacks, has evolved to become an enterprise-wide discipline spanning infrastructure, systems, processes and people. It is an organisation's ability to anticipate, absorb, learn from and adapt to technology-related disruption.

Business leaders must treat digital resilience-building as an endeavour that transcends their IT and cybersecurity functions. Resilience hinges on the capabilities of an entire organisation, and the ecosystems of which it is part, to respond and adapt to digital disruption.

This report examines those capabilities at organisations in APAC and further afield. The analysis is based on a survey of 1,420 senior executives, combined with expert interviews in those markets. Singapore, Japan and Australia lead with stronger resilience in general, but even in these markets, resilience is uneven: cybersecurity and continuity planning are relatively mature, but leadership accountability, resilience-led investment decisions and ecosystem collaboration lag.

APAC organisations show a baseline level of digital resilience capability but in no markets do they demonstrate clear, end-to-end maturity. As digital risks grow, slow progress in building resilience capabilities, internally and across ecosystems, leaves organisations increasingly vulnerable.[1]

[1] Unless otherwise indicated, the figures we refer to in this report are these of the 11 APAC markets. In certain places, we compare those results to those from the US, UK and Germany, bringing the total to 14 markets.

The key findings

01 **Ecosystem resilience is the weakest link in digital resilience efforts.** APAC organisations are confident in their internal measures, such as training and testing, but confidence fades beyond their boundaries: only 12% have first-hand insight into suppliers' resilience. Limited information-sharing, infrequent joint simulations and weak partner governance make ecosystem interdependencies the main source of resilience failure. Without active governance of key partners, disruptions spread easily, no matter how strong internal controls are. Such governance should include setting shared standards, conducting joint tests and ensuring clear visibility into third-party risks.

02 **Workforce preparedness remains foundational rather than future-ready.** Resilience grows when planning and training focus on the ability to respond. Organisations must instil adaptive behaviours such as cross-functional co-ordination and under-pressure decision-making. The emphasis should be on how quickly teams can reorganise work when systems fail.

03 **Organisational gaps, not tools, derail incident response.** Organisations plan widely for responding to threats of digital disruption. But less than one-quarter (23%) of responses to real threats go according to plan. Plans fail not due to a lack of technology, but because decision-making, co-ordination and authority structures break down in practice. Organisations cannot rely on technology investment alone to strengthen resilience.

04 **Confidence is limited in external resilience enablers.** Executives express strong confidence in cybersecurity policy and planning (57%) but are far less assured in other external enablers of resilience, including the reliability of communications networks, regulatory clarity and the stability of power supply. This uncertainty requires organisations to factor in redundancy and enable degraded-mode operations, across regions and cloud providers.

05 **Risk management is largely reactive and monitoring is limited.** Most organisations have formal risk management frameworks, but these centre mainly on cyber and IT risks. Attention to regulatory, supplier, geopolitical and climate risks is limited, and monitoring is periodic. This leaves processes better suited to documenting known risks than to anticipating and managing fast-moving disruption. Continuous monitoring and forward-looking scenario-testing must become standard practice.

06 **Senior leaders recognise digital resilience, but shared ownership remains limited.** Senior-level responsibility for digital resilience tends to fall to one executive, such as the chief information officer (CIO). At most organisations, boards are not heavily involved in review or planning of resilience-building efforts, which constrains strategic oversight and weakens enterprise-wide co-ordination.

The digital resilience barometer 2026

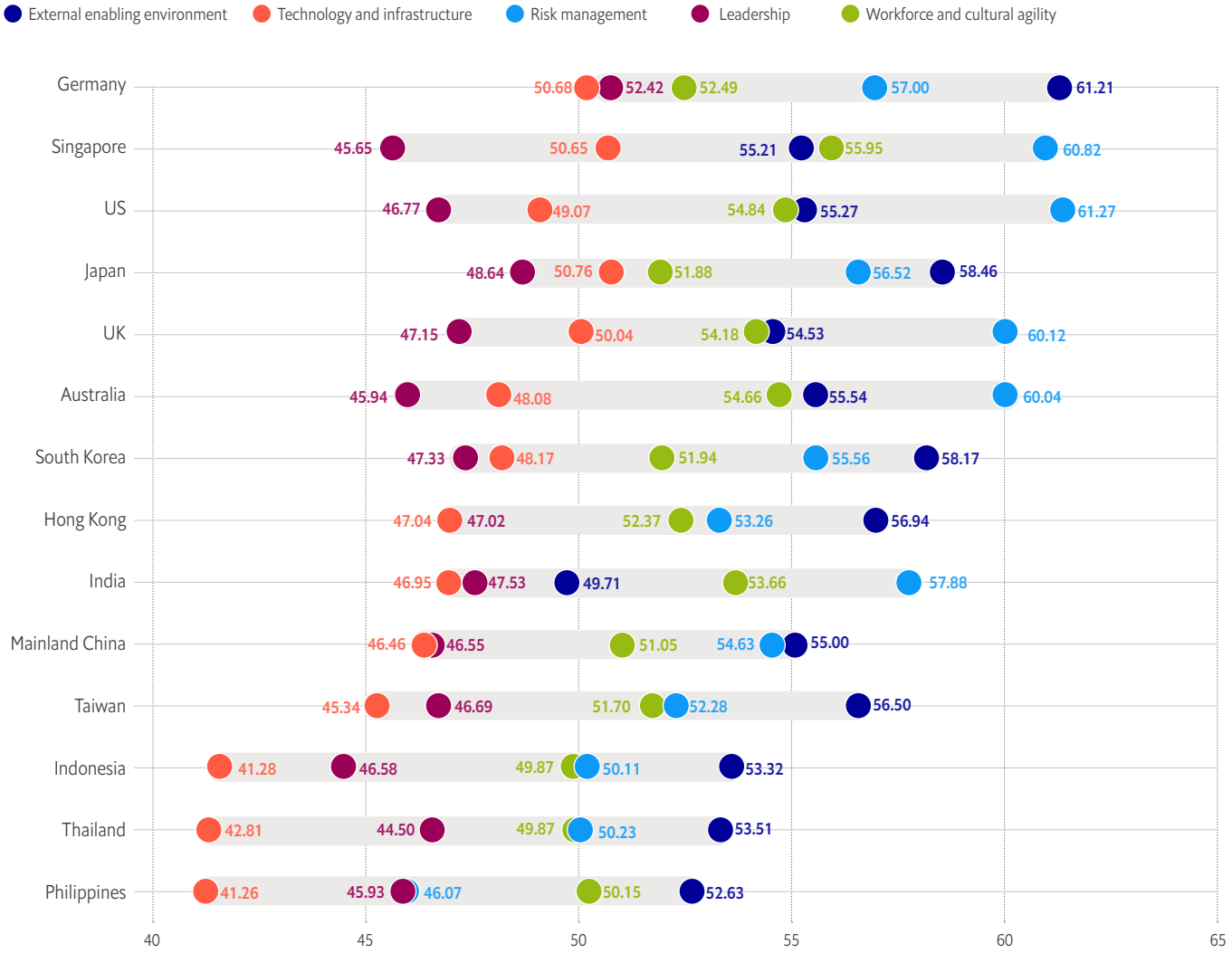
Economist Impact's digital resilience barometer is a composite measure of senior executives' confidence in their organisation's ability to anticipate, withstand and recover from disruption.

The scores are derived from the same late-2025 survey of executives across APAC, as well as the US, the UK and Germany, and reflect confidence across the following five core pillars of digital resilience:

Table 1: Five core pillars of digital resilience

Pillars	Market confidence
The external enabling environment	Executive confidence in the external conditions that support digital resilience. They include: reliability of surrounding infrastructure; stability of essential services; effective policy frameworks; and mechanisms of cross-sector collaboration.
Technology and infrastructure	The organisation's willingness to modernise and adopt new technologies with appropriate safeguards, including the extent to which core systems are being upgraded and resilience is embedded into new technologies in a proactive, future-oriented manner.
Risk management	The organisation's ability to anticipate, mitigate and respond to technology-related disruptions in a structured way, reflecting the maturity of its business continuity planning and preparedness for external risks.
Leadership	The extent to which digital resilience is recognised as a shared priority between the board and the C-suite. There should be a high degree of alignment and collaboration in treating digital resilience as a strategic, enterprise-wide priority.
Workforce and cultural agility	Executives' confidence in their organisation's ability to reskill and upskill at scale, and the presence of resilience-related behaviours such as collaboration, adaptability and crisis response capabilities.

Figure 2: Digital resilience capability scores across surveyed markets

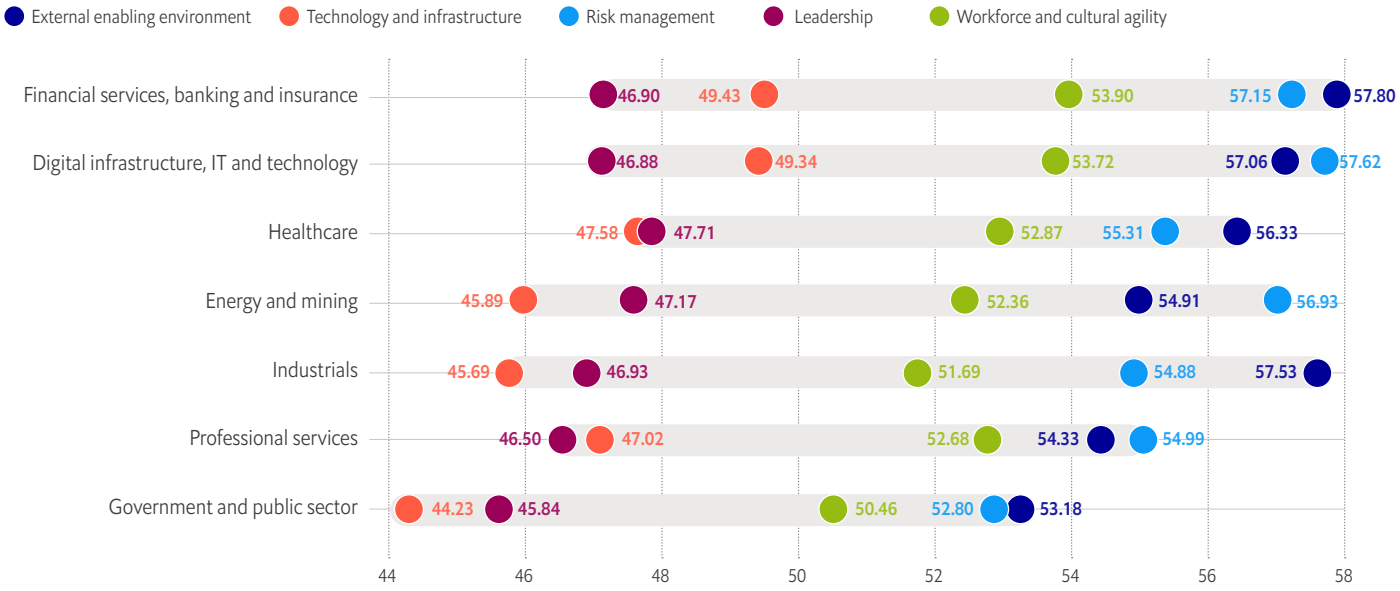


Source: Economist Impact survey on Digital Resilience, 2025

Market-level differences are driven by the distribution of resilience capabilities rather than overall maturity. Some markets exhibit more balanced performance across pillars, while others concentrate strength in risk controls with weaker leadership and ecosystem readiness.

- Japan, South Korea, Hong Kong and Taiwan lead on the external enabling environment, but Hong Kong and Taiwan's weaker risk management constrains resilience.
- Germany and Japan lead on regulatory clarity and infrastructure reliability; confidence is lowest across South-east Asia and India.
- Mainland China's core infrastructure resilience outpaces the UK and is at par with the US and Singapore, signalling high confidence in its digital backbone. However, this structural reliability is hindered by lower ecosystem trust than others in the region, including Japan, Hong Kong and Taiwan.
- Germany, Japan and Singapore lead in system modernisation. Meanwhile, Australia, the UK and the US stand out for factoring resilience into their investments, resulting in significant, documented improvements to their digital resilience.
- The US, the UK, Singapore and Australia lead on risk management, reflecting mature cyber and continuity practices.

Figure 3: Digital resilience capability scores across surveyed industries



Source: Economist Impact survey on Digital Resilience, 2025

- Germany leads with clearer board and C-suite alignment. Australia and Singapore show integration at par, but weaker accountability. India stands out for leadership capability despite gaps in skills and ecosystem readiness.
- Singapore, the US, the UK, Australia and India are investing in resilience-related behaviours, while other markets remain focused on awareness-led skills-building.
- Singapore leads on enterprise-wide capability in APAC; Indonesia, Thailand and the Philippines remain focused on building foundational risk and technology controls.

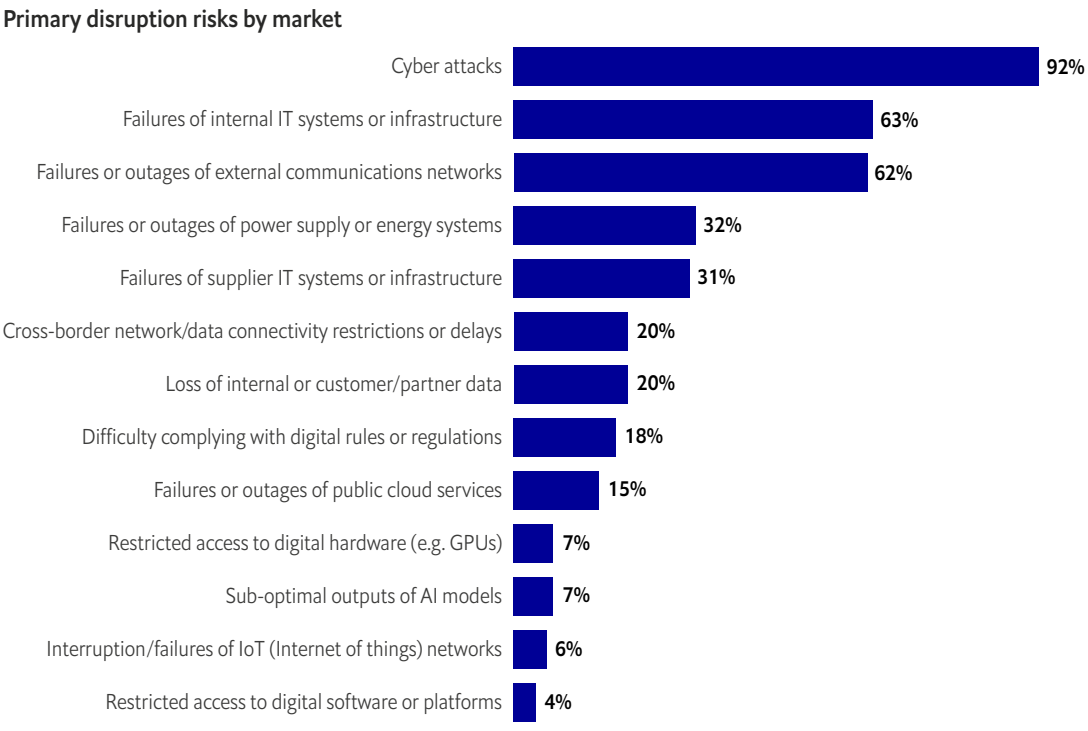
Industry-level differences are consistent across pillars. Financial services and digital infrastructure, IT and technology out-perform on execution-heavy capabilities such as risk management, technology modernisation and workforce skills, while under-performing on leadership accountability. Overall, technology and infrastructure emerges as a weak spot, owing to gaps in adoption safeguards and risk management.

Across markets and industries, enterprises are risk-ready within organisational boundaries, but not future-ready for cascading, ecosystem-level disruption.

A world of disruption

Threats of digital disruption are now a constant. Over the past year, cyber attacks have posed threats to 92% of the respondents' organisations. It's not only "bad actors" causing disruptions. Around two-thirds have also suffered potentially disruptive failures of internal IT systems (63%) and external communications networks (62%). Failures of suppliers' systems have disrupted operations for around one-third of respondents.

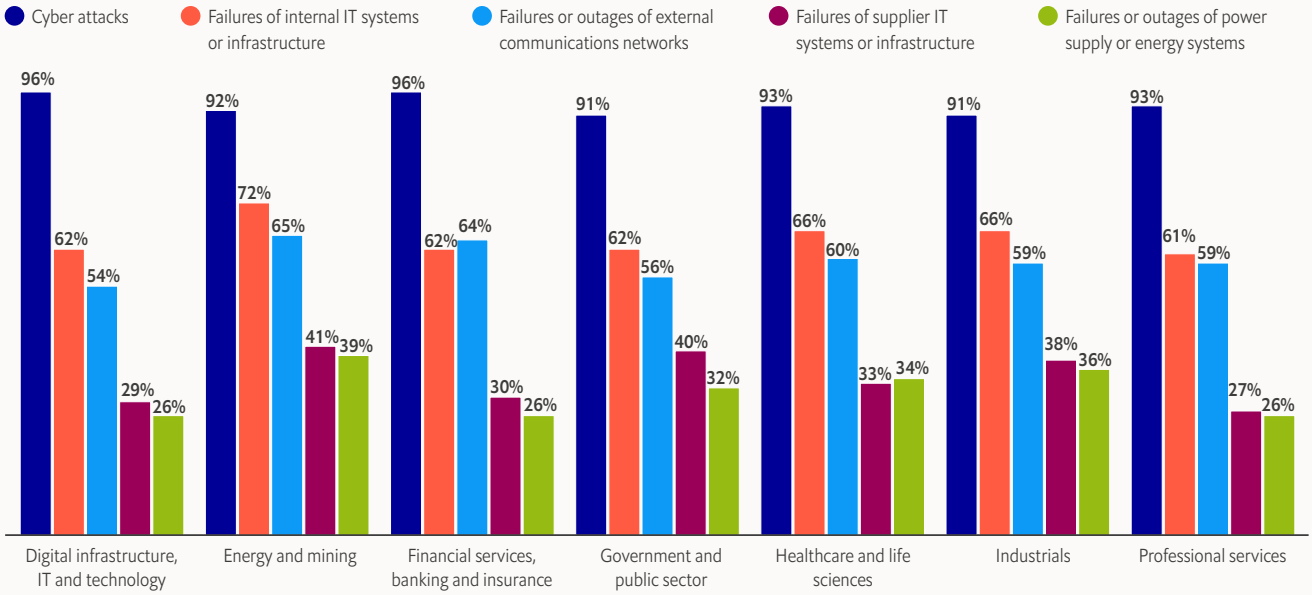
Figure 4: The threat landscape
Top factors threatening disruption to organisations' business or operations in the past 12 months



Source: Economist Impact survey on Digital Resilience, 2025

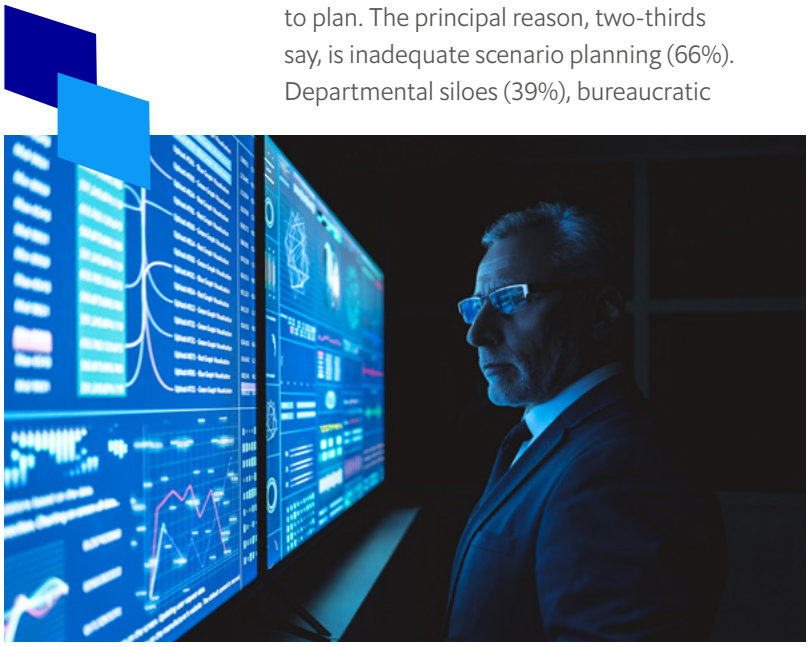
Figure 4: The threat landscape (cont.)

Primary disruption risks by industry
(across all markets surveyed)



Source: Economist Impact survey on Digital Resilience, 2025

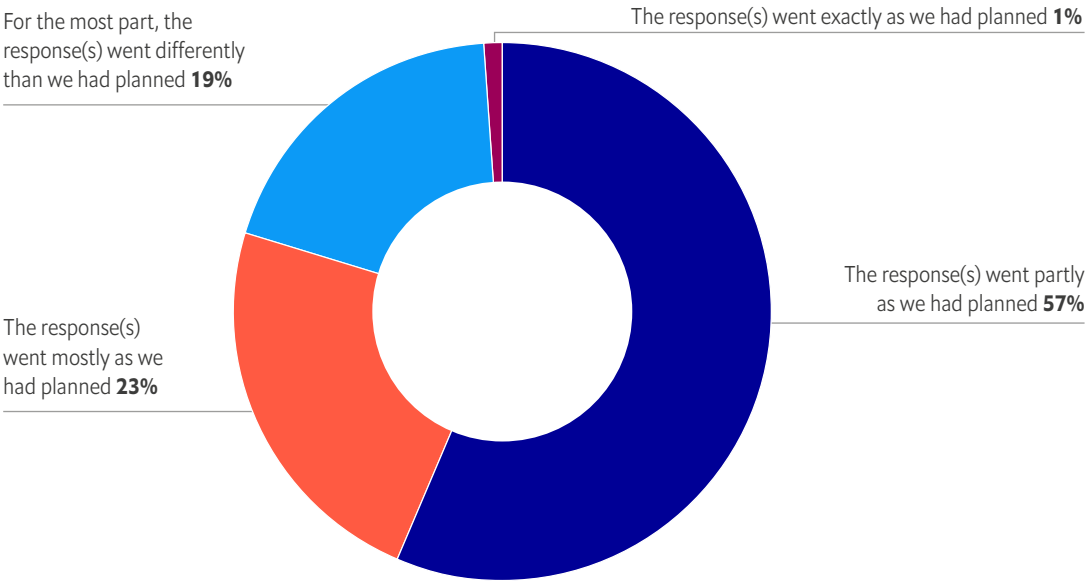
Responses to such threats highlight the need for ongoing resilience-enabling improvements. Less than one-quarter (23%) of respondents say their organisations' responses went largely to plan. The principal reason, two-thirds say, is inadequate scenario planning (66%). Departmental siloes (39%), bureaucratic decision-making processes (39%) and underestimation of threats (36%) are other major weaknesses.

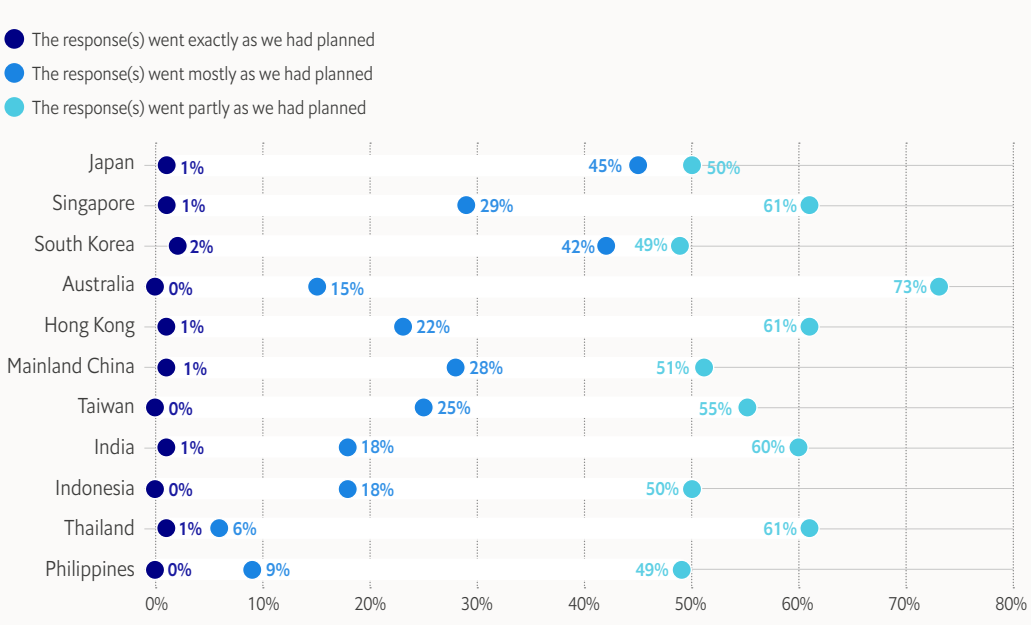


Mihaela Isac, chief information officer, APAC, DHL Supply Chain, points to a deeper structural gap. "Predefined plans are no longer sufficient as disruptions are too varied and fast-moving. We need to combine clear governance and well-tested playbooks with the flexibility for teams to make context-specific decisions in real time. This includes empowering technology teams to take fast, informed decisions with limited consultation, supported by the right steering bodies that can convene quickly in case of crisis. Scenario planning and simulations are essential, they help validate assumptions, strengthen muscle memory, and ensure teams can act decisively when escalation paths need to be activated. This blend of predictability and adaptability is now central to our risk-management approach."

Figure 5: Response effectiveness

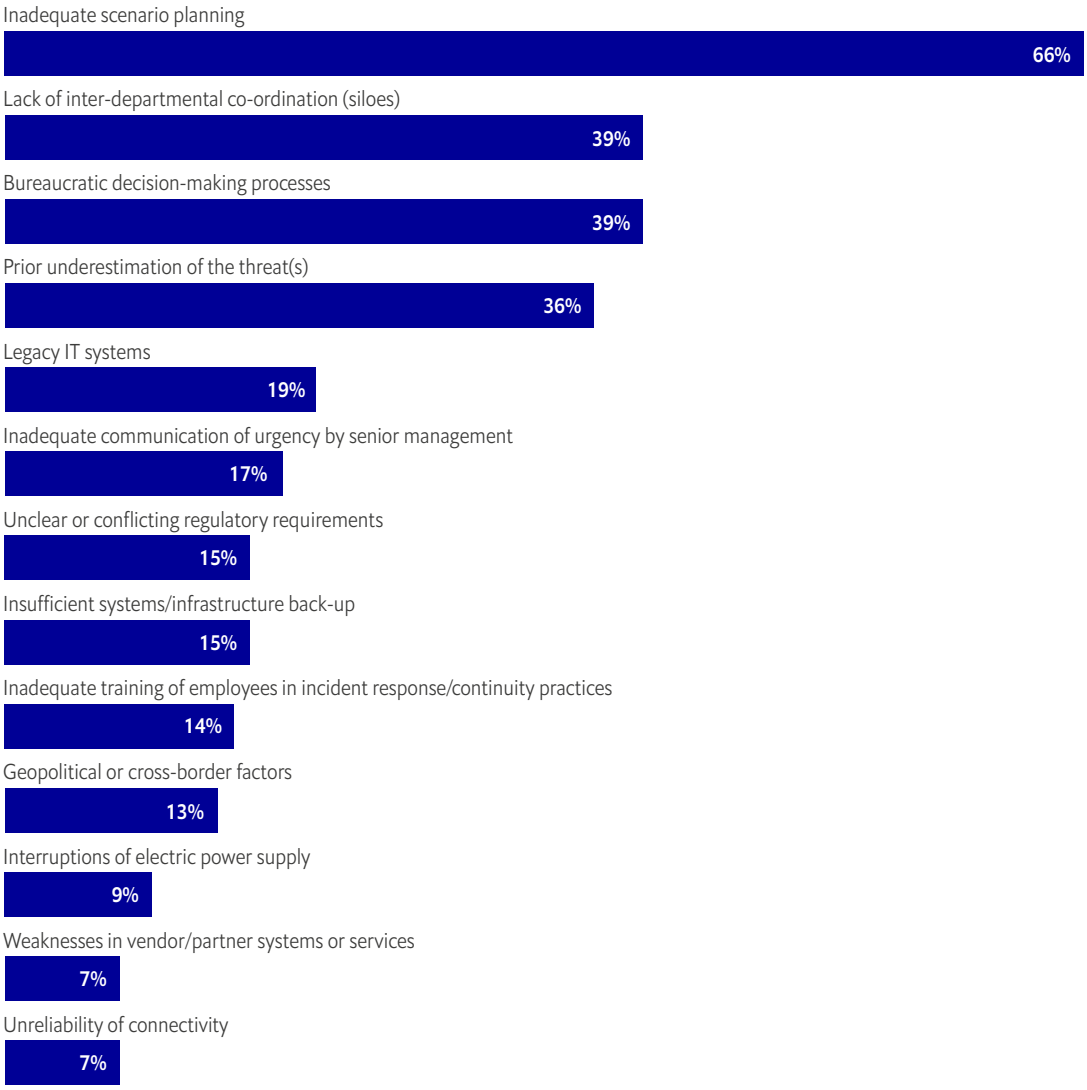
Which of the following most closely describes the organisation's response(s) to threats of disruption in the past 12 months?





Source: Economist Impact survey on Digital Resilience, 2025

Figure 6: Plans exist, but organisational gaps persist
The primary reasons why responses don't go as planned



Source: Economist Impact survey on Digital Resilience, 2025

Building digital resilience is clearly a work-in-progress for most APAC organisations. Examining how those surveyed address the core pillars of digital resilience helps illuminate the challenges they face.

The enabling environment for resilience

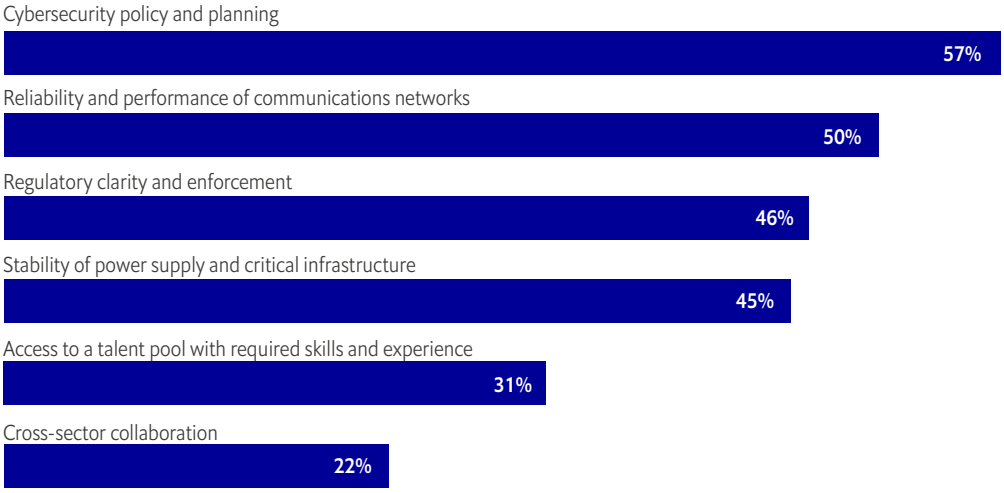
Digital resilience depends as much on the external environment as on internal capabilities. Even the strongest organisation remains vulnerable if its market's communications infrastructure and power supply are unstable and digital policy and regulatory frameworks are unclear. These elements are also integral to the smooth functioning of the organisation's ecosystem—its network of suppliers, partners and other third parties.

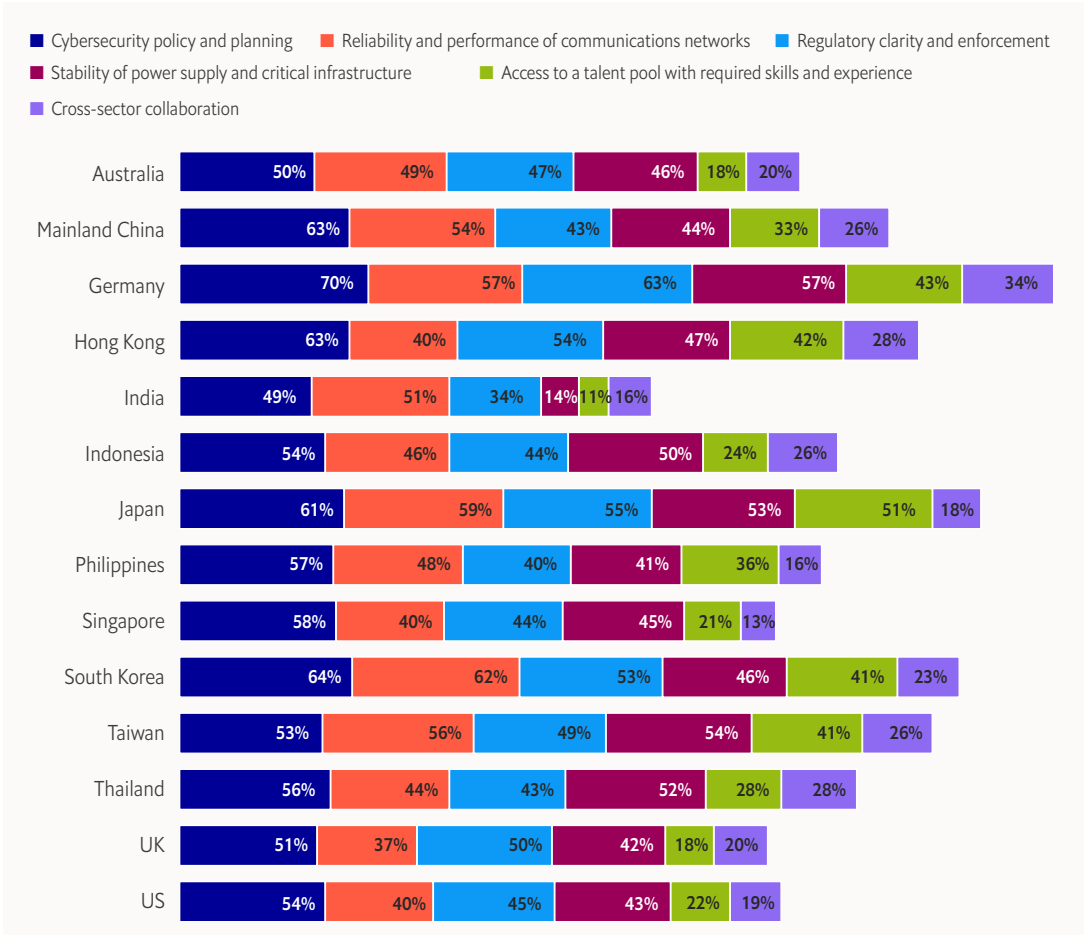
It is a concern, then, that the surveyed APAC executives have limited confidence in key enabling factors of resilience in their market environment. Only in cybersecurity policy and planning—the cyber regulations and incident response frameworks put in place and enforced by governments—do more than half (57%) express confidence.

With external enablers proving unreliable, experts suggest engineering resilience on the assumption that disruption will occur. "Resilience depends on redundancy in operations, compute, storage, networking and power," says Andreas Spanner, chief architect at Red Hat. "In the absence of either, operations quickly grind to a halt. This necessitates multi-cloud and multi-region strategies, systems designed to run in degraded modes, and out-of-band communication channels when core systems are unavailable."

Figure 7: Confidence in external operating environment

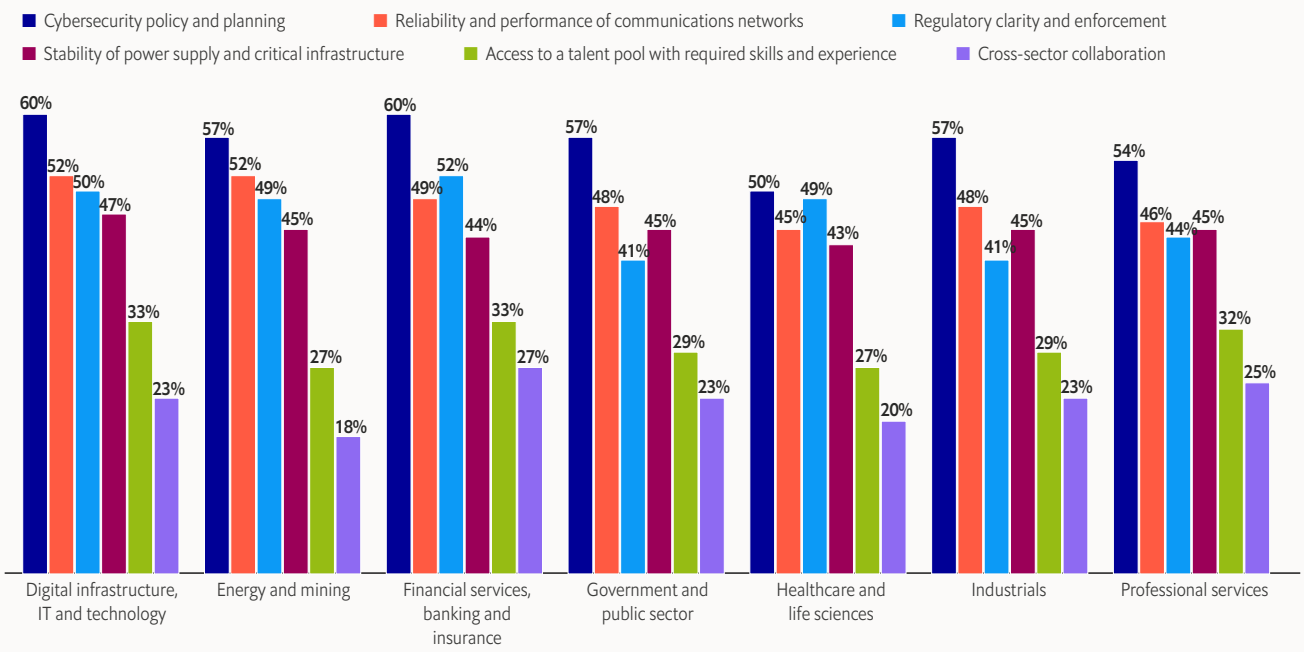
Executive confidence in elements of the external operating environment in APAC (share of respondents saying they are "somewhat" or "highly" confident)





Source: Economist Impact survey on Digital Resilience, 2025

Figure 7: Confidence in external operating environment (cont.)



Source: Economist Impact survey on Digital Resilience, 2025

Confidence levels decline sharply when it comes to more human-focused enablers of resilience in the external environment. For example, just 31% of respondents have confidence in the availability of necessary digital talent, with particularly low confidence reported in Australia (18%), India (11%), Singapore (21%), the UK (18%) and the US (22%). Fewer still (22%) believe that cross-sector collaboration—in information-sharing, for instance—is adequate.

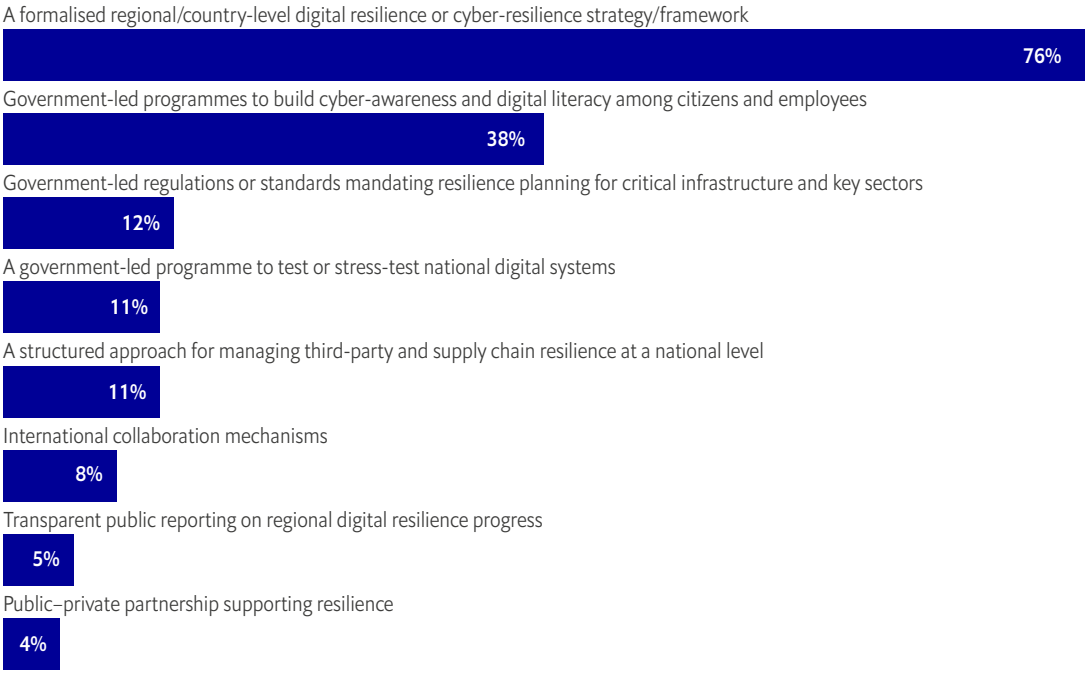
Regulatory ambiguity also hampers resilience-building. There may be confidence in digital and cybersecurity policymaking, but this does not extend to regulatory clarity and enforcement, in which 46% express confidence.

Government inputs to resilience

In addition to rule-making, governments can facilitate national or regional resilience-building efforts. These include initiatives to raise awareness, encourage information-sharing or promote standards for managing supply-chain resilience. Done effectively, these measures support the connected ecosystems that create additional business value.

Figure 8: Governance and institutional capacity

Share of respondents confirming that selected digital-resilience-related initiatives and mechanisms are currently in place in their market



Source: Economist Impact survey on Digital Resilience, 2025

Survey responses indicate that government efforts remain heavily focused on cybersecurity (76%), rather than system-wide resilience. Initiatives such as resilience standards for critical infrastructure (12%) and sustained public–private collaboration (4%) remain limited or uneven across markets.

Where governments do provide clearer direction and co-ordination, the benefits are tangible. "External partnerships play a critical role in enabling the right balance between strong infrastructure and organisational culture," says Singapore-based Eugene Huang, chief information officer at DBS. "We collaborate across the industry through platforms such as the Association of Banks in Singapore, and work closely with the Monetary Authority of Singapore on initiatives including phishing-resistant authentication, such as Fast IDentity Online."

In the absence of strong external enablers, organisations must work hard to ensure their own resilience foundations are solid. The discussion that follows focuses on those internal pillars of digital resilience.

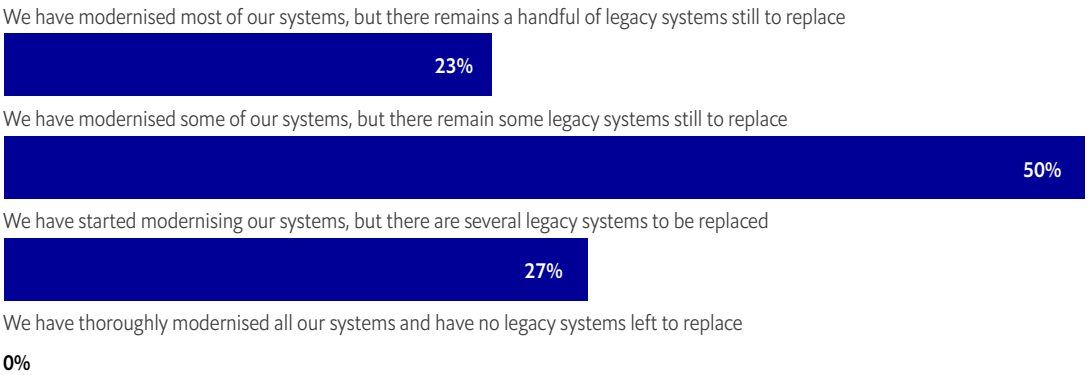
Technology foundations

This pillar considers three aspects of an organisation's technology preparedness: progress in modernising infrastructure and retiring legacy technology; the extent to which resilience shapes investment decisions in new technologies; and the safeguards applied when deploying advanced tools such as artificial intelligence (AI).

Legacy technology continues to hold back resilience across APAC. Just 23% of respondent organisations have modernised most or all of their technology systems. Viewed across the full maturity curve—including organisations that have modernised all, most or some systems—Japan (92%), Singapore (89%), Australia (88%) and South Korea (88%) emerge as regional leaders.

"Digital systems are now the backbone of how the business runs," says a senior director, from a leading medtech organisation. "Resilience is not just about cyber; it is about whether your systems can help you respond and re-orchestrate processes when disruptions happen. That is why continuous modernisation and simplification of legacy architecture are critical in addition to effective cyber threat management."

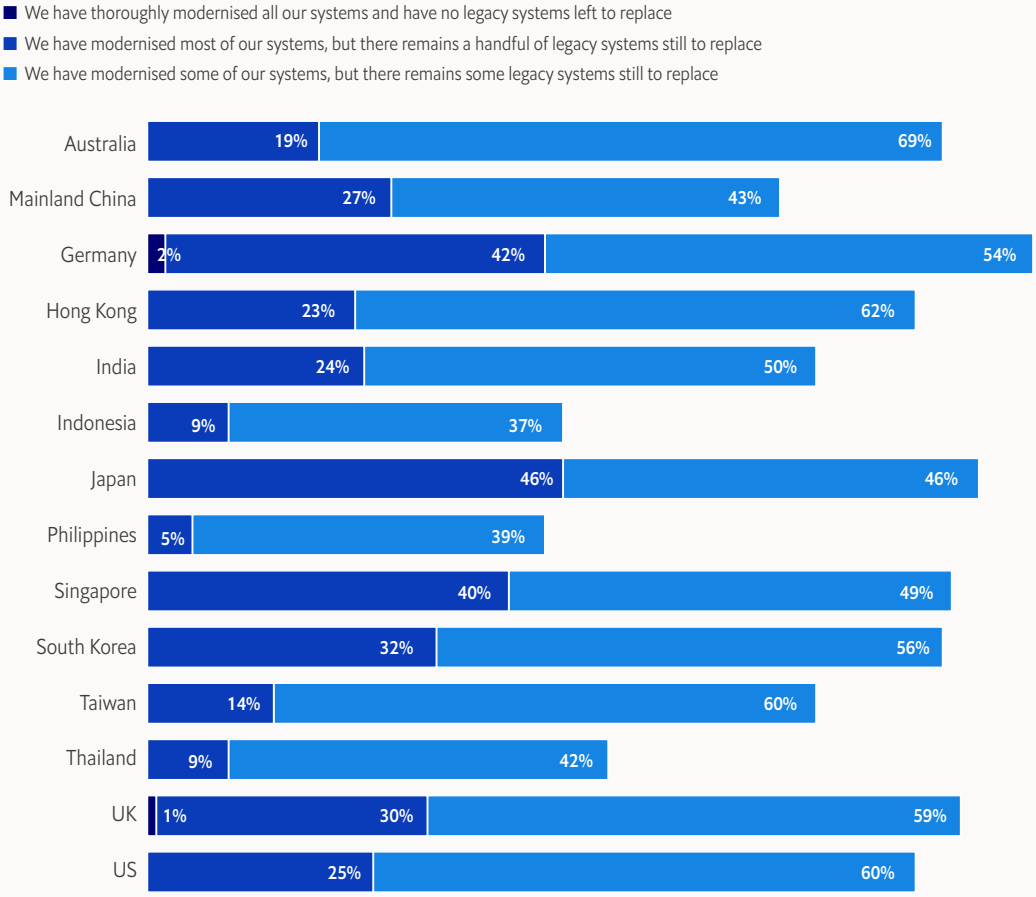
Figure 9: The legacy burden
The balance of legacy (older) and modernised systems in respondent organisations



Source: Economist Impact survey on Digital Resilience, 2025

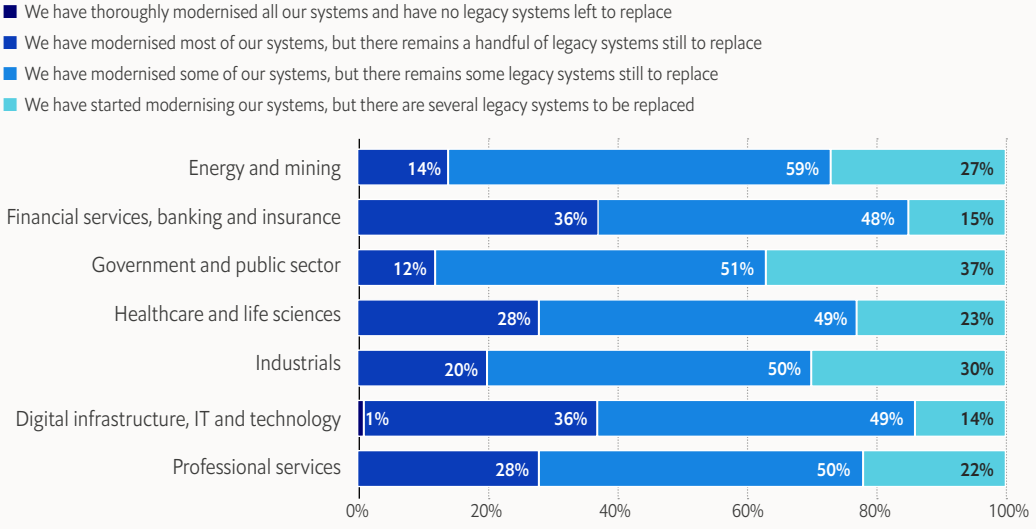
Figure 9: The legacy burden (cont.)

The balance of legacy (older) and modernised systems in respondent organisations



Industry-wide confidence

(across all markets surveyed)



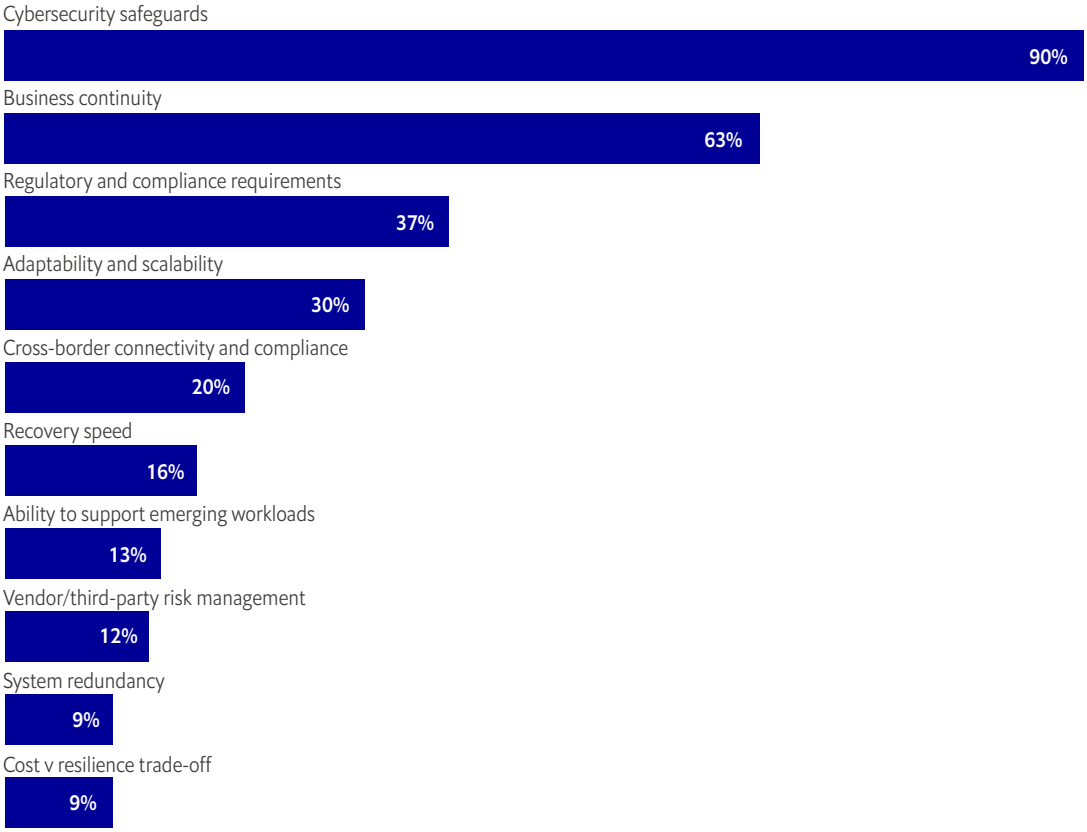
Source: Economist Impact survey on Digital Resilience, 2025

Modernisation, however, is not simply a matter of replacement. If new systems are neither modular nor reversible—and if suppliers are excluded from resilience testing—organisations risk reproducing old fragilities on newer platforms. As Brian O'Neill, global head of group transformation at Standard Chartered, notes: "New technologies can strengthen resilience, but they can also introduce vulnerabilities, from legacy compatibility issues to third-party dependence and governance gaps. These risks must be addressed during adoption, with strong controls built in from the start."

Resilience considerations loom large when organisations invest in new infrastructure and systems, including those with AI capabilities. However, those considerations skew heavily toward cybersecurity. While 90% of APAC respondents prioritise cybersecurity by design, far fewer emphasise adaptability (30%) or recovery speed (16%).

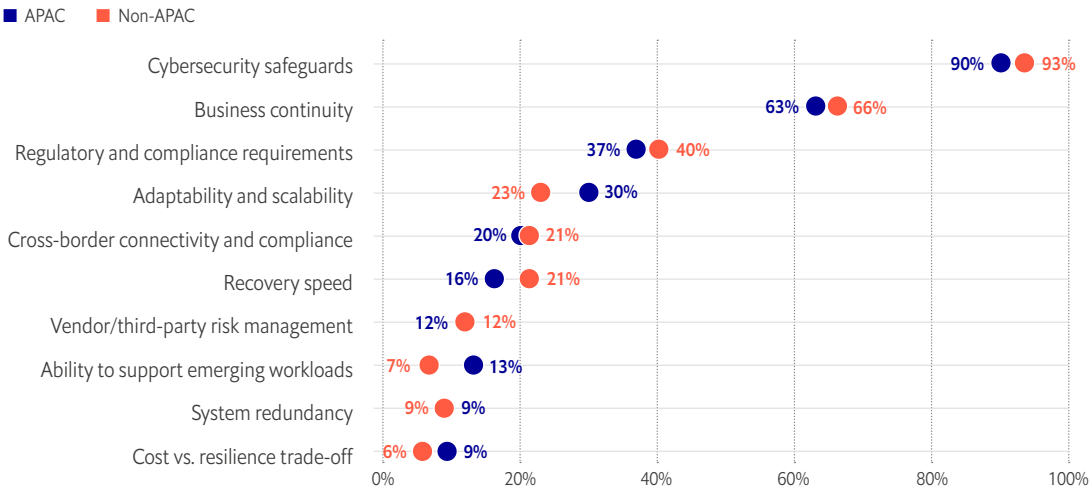
Figure 10: Investing for resilience

Digital resilience considerations that have received the most attention in respondents' technology investment decisions



Source: Economist Impact survey on Digital Resilience, 2025

Figure 10: Investing for resilience (cont.)
Digital resilience considerations that have received the most attention in respondents' technology investment decisions



Source: Economist Impact survey on Digital Resilience, 2025

"Organisations must treat resilience as something to be engineered rather than added later."

Eugene Huang, chief information officer, DBS

"Organisations must treat resilience as something to be engineered rather than added later," says Mr Huang. "This requires investment in layered, machine-led architectures that reduce reliance on manual intervention and enable faster recovery. AI and automation, for example, provide predictive insights that shorten recovery times, reduce complexity and enhance system stability."

Vendor resilience is rarely considered when making investment decisions: just 12% deem its evaluation important. This is curious in an age when a few big suppliers dominate the provision of vital technology services such as cloud access.[2] Careful assessments of vendor resilience, and how they manage aspects such as redundancy and uptime, are essential. "In a highly integrated environment, any weak link can stop the whole flow," warns Nizar Trigui, chief technology officer at GXO. "Every layer of the stack has to be equally resilient, and that requires transparency on uptime, redundancy and recovery capabilities."

[2] Srivathsan B, Sorel M, Sachdeva P, et al. AI Power: Expanding data centre capacity to meet growing demand. McKinsey & Company. October 2024. Available at: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/ai-power-expanding-data-center-capacity-to-meet-growing-demand

To assess and build vendor resilience, Mr Spanner cites the value of joint recovery scenarios and regular “game days”, which help shift supplier relationships from commercial transactions to engineering partnerships. From an infrastructure standpoint, Simon Lockington, senior director of global solution architecture, APAC at Equinix, adds that unannounced fail-over tests are often the only way to reveal whether systems and partners can perform under real-world pressure.

Guidance for the business

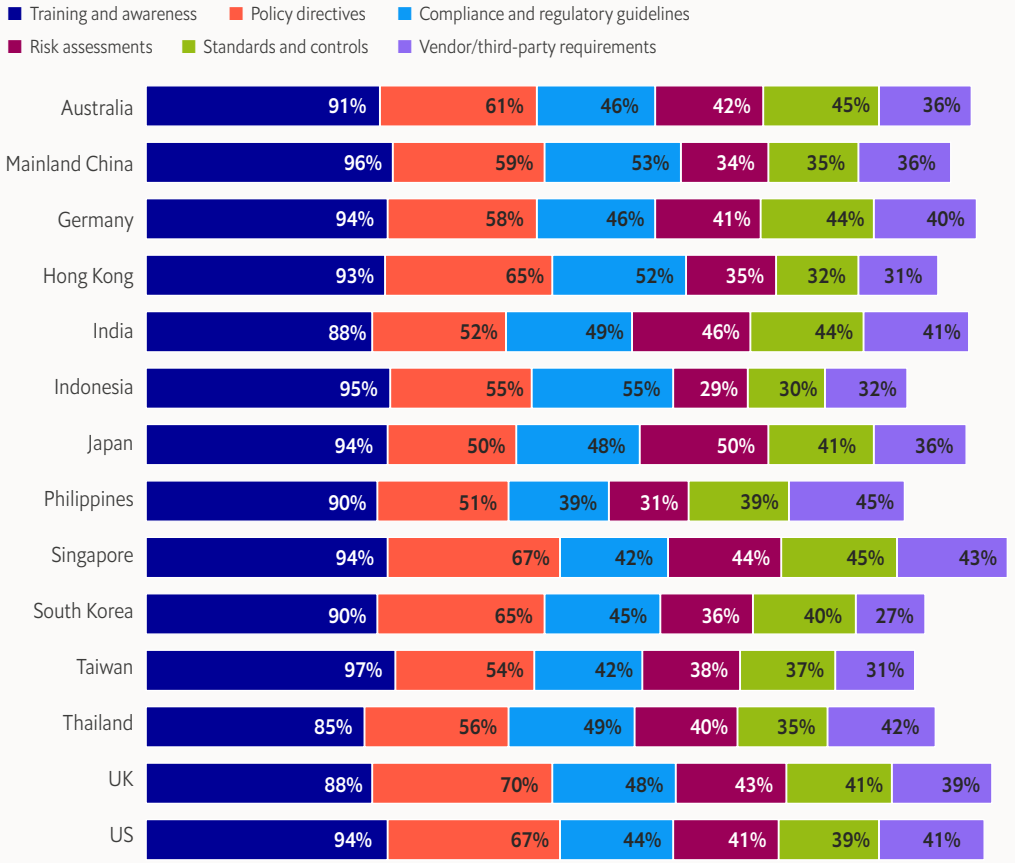
Almost all respondents (92%) say their organisations train employees in the safe use of new technologies. But considerably fewer complement training with other support measures. Just 36% provide guidance on how to evaluate the resilience of technology providers, for example.

The result is a widening gap between technological ambition and operational readiness. While most organisations equip employees to use new technologies, far fewer are embedding the cross-functional governance and resilience processes needed to manage them. As a result, organisations appear to be adopting advanced technologies faster than they are building the safeguards needed to govern them. This risks creating new vulnerabilities as enterprises modernise.

“Organisations need structured ways to evaluate technology providers and assess risk before deployment,” as one expert from a leading medtech organisation explains. “We prototype new technologies in isolated sandbox environments to understand the value first and only then consider integration. This allows the right guardrails, monitoring, and auditing to be designed upfront, preventing disruption rather than reacting after the fact.”

Figure 11: Safeguards for the use of new technologies

What organisations provide to business functions when adopting newer technologies or technology services (eg AI, edge computing, IoT, quantum-ready systems)



Source: Economist Impact survey on Digital Resilience, 2025

Resilience planning and processes

Modernised and secure technology is not enough to safeguard organisations against disruption. Practices must be embedded into the broader enterprise risk systems that support digital resilience. These should be reflected across the financial, operational and strategic risk management processes.

Our surveyed organisations display a handful of apparent strengths in this risk management pillar, but they are counterbalanced by several clear weaknesses.

Resilience frameworks

The focal points of risk management and resilience frameworks clearly skew toward relatively familiar technical threats to the exclusion of less familiar ones. Guarding against cybersecurity threats is a focus for those frameworks at nearly all the surveyed organisations. But just one-third incorporate regulatory and compliance risks associated with digital technologies. And little more than one-quarter address supplier and other third-party digital dependencies. This is despite our earlier finding (Figure 4) that third-party failures have threatened disruption at many organisations.

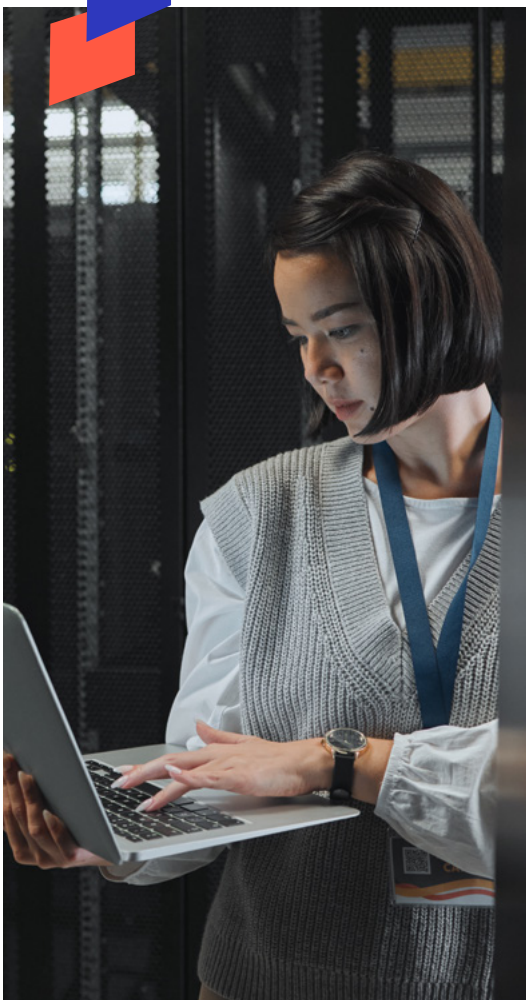
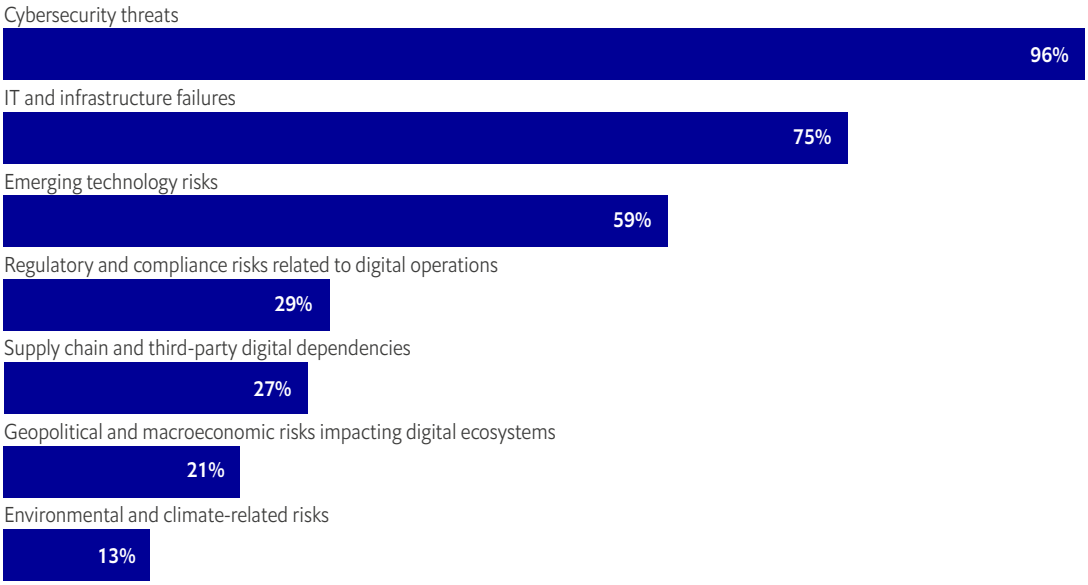
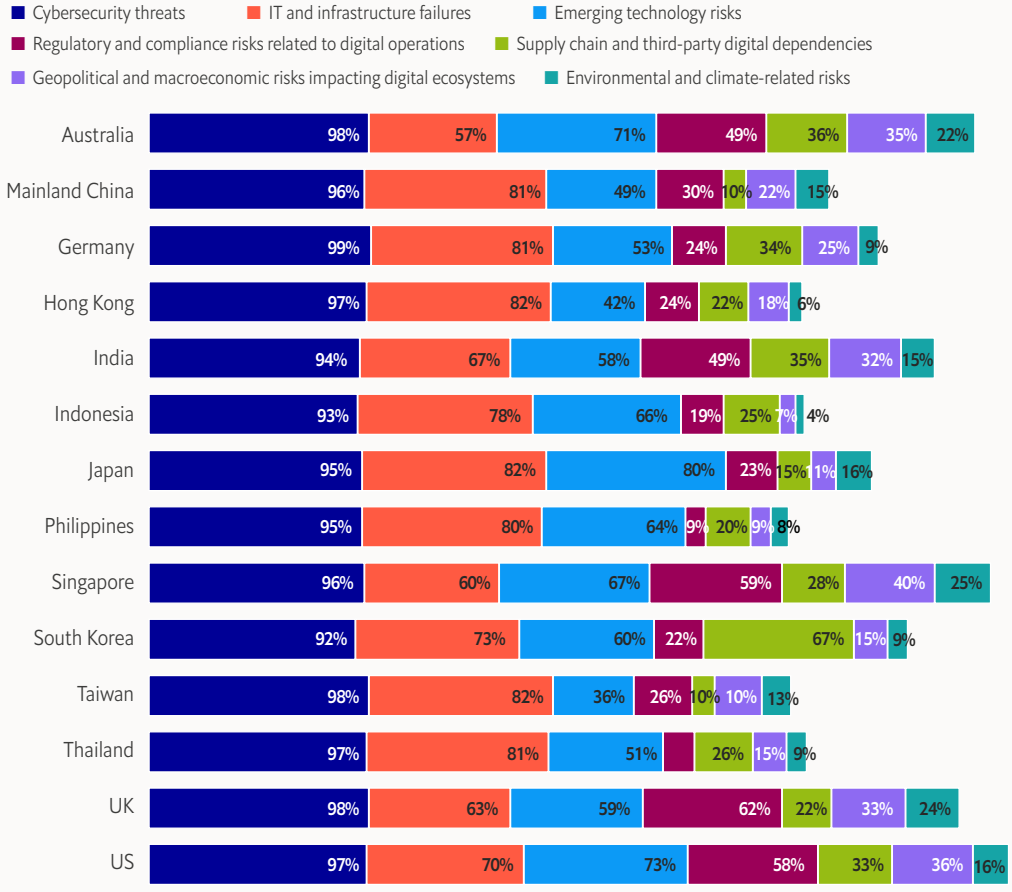


Figure 12: Risk management focal points

The risk categories formally included in organisation's digital resilience planning or enterprise risk management framework



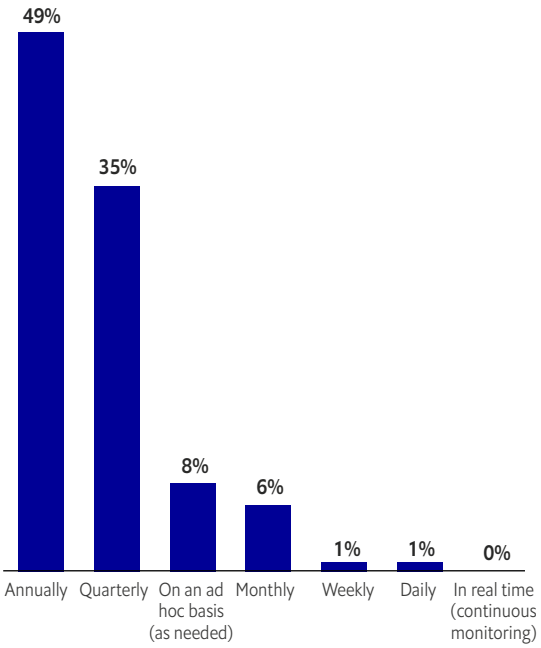


Source: Economist Impact survey on Digital Resilience, 2025

Environmental and climate-related risks appear sidelined in digital resilience planning. Only 13% of organisations formally account for them, despite their direct impact on power, data centres and recovery. Even in leading markets such as Australia and Singapore, fewer integrate climate risk.

Figure 13: Frequency of risk tracking

How frequently organisations track internal and external risks



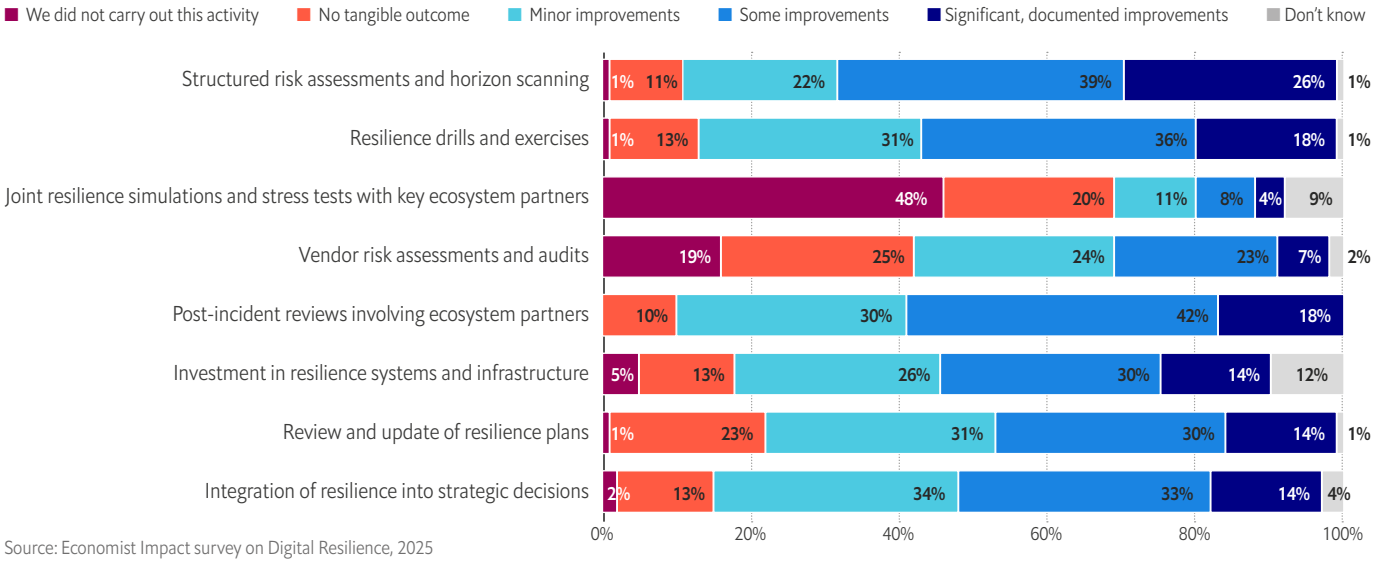
Source: Economist Impact survey on Digital Resilience, 2025

Most organisations appear to have adopted a largely reactive, rather than predictive, posture toward threats of digital disruption. More than half (57%) track digital and other risks no more than annually or on an ad hoc basis. Just 8% track more frequently than each quarter. Infrequent monitoring leaves organisations exposed to fast-moving developments that threaten disruption.

Most organisations conduct stress tests and reviews of their digital risk posture, with improvements typically made as a result. In the past year, for example, 68% of APAC organisations report making improvements to horizon scanning and other elements of the risk assessment process; 60% say they've improved post-incident reviews by including key ecosystem partners. Little has been done, however, to increase or improve the conduct of joint simulations or stress tests with those partners.

Figure 14: Seeking improvement

Outcome(s) of digital resilience activities at respondent organisations in the past 12 months



Source: Economist Impact survey on Digital Resilience, 2025

“Joint pilots, aligned KPIs and clear operating guardrails are what make ecosystems truly resilient and scalable.”

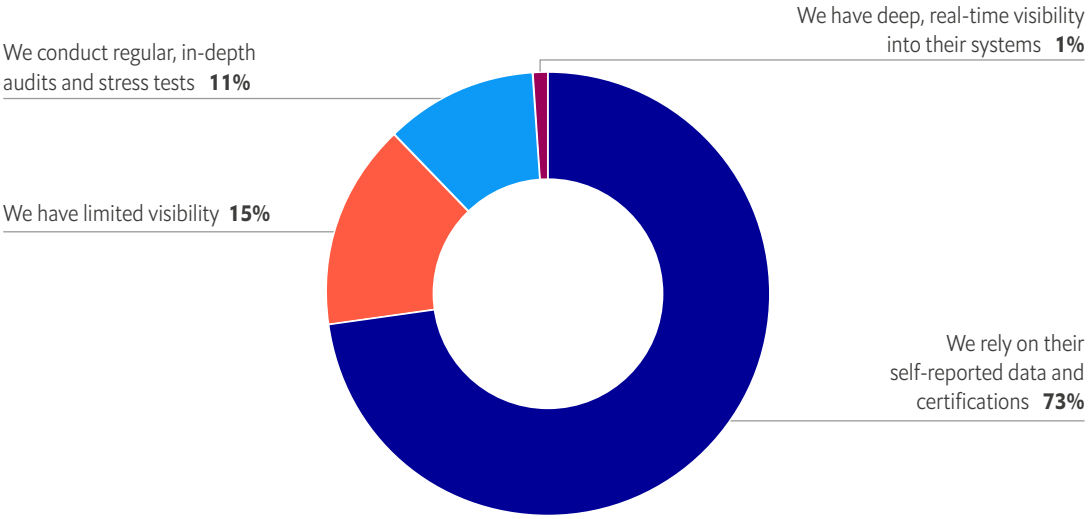
Mihaela Isac, chief information officer, APAC, DHL Supply Chain

In APAC, just 12% of organisations have direct visibility into the digital resilience of key suppliers through system access or regular audits. The US leads by comparison, with 27% conducting regular partner audits, more than twice the APAC level. The vast majority (73%) assess their partners based on the latter’s self-reported data and certifications.

As Clemens Philippi, chief executive officer, MSIG Asia notes, “Full real-time visibility into partner systems may sound ideal, but in most cases, it is just not feasible. There are legal, commercial and technical limits. What works better is a risk-based approach. This means going deeper with your most critical partners, and move away from one-off audits to something more continuous, with shared standards and regular information exchange.”

Ms Isac reinforces this approach. “Resilience depends on shared standards, strong governance and co-development with partners. Without reliable data and consistent oversight, even the best technology falls short. Joint pilots, aligned KPIs and clear operating guardrails are what make ecosystems truly resilient and scalable.”

Figure 15: Gaps in supplier oversight and visibility
Visibility into the resilience of critical third-party suppliers and partners



Source: Economist Impact survey on Digital Resilience, 2025

Turning incidents into resilience

Post-incident reviews are vital not only to identify the root causes of a failure, but also to determine what went well—the result being an updated response plan and stronger resilience posture. An effective review should be constructive, transparent and inclusive of all stakeholders.

Learn by doing

"A crisis is a perfect opportunity to upgrade your skills and capabilities," says Mr Spanner. "The purpose is to determine not who made a mistake, but what safeguards were missing. If the server ran out of space, for example, perhaps we lacked an auto-scaling policy for storage. The mindset evolves to human error is a symptom, not a cause, of a problem."

Reward transparency

The post-incident review is a cultural exercise in which transparency is paramount, insists Mr Lockington: "You have to demonstrate that you're doing the research for good. That means rewarding the people who give you the facts and don't try to hide anything."

Leadership sets the tone

The review must also involve supply-chain partners to ensure relevant insights into what went wrong, what went well and what improvements can be made.

Harry Jensen, senior operations director of Australia and the Philippines, at Equinix, adds: "Resilience does not happen by accident. Senior leadership has to ensure that testing takes place, issues are surfaced openly and people feel safe to say when something has not worked. That is how organisations learn quickly, before a real crisis forces the lesson."

Structure and dedication

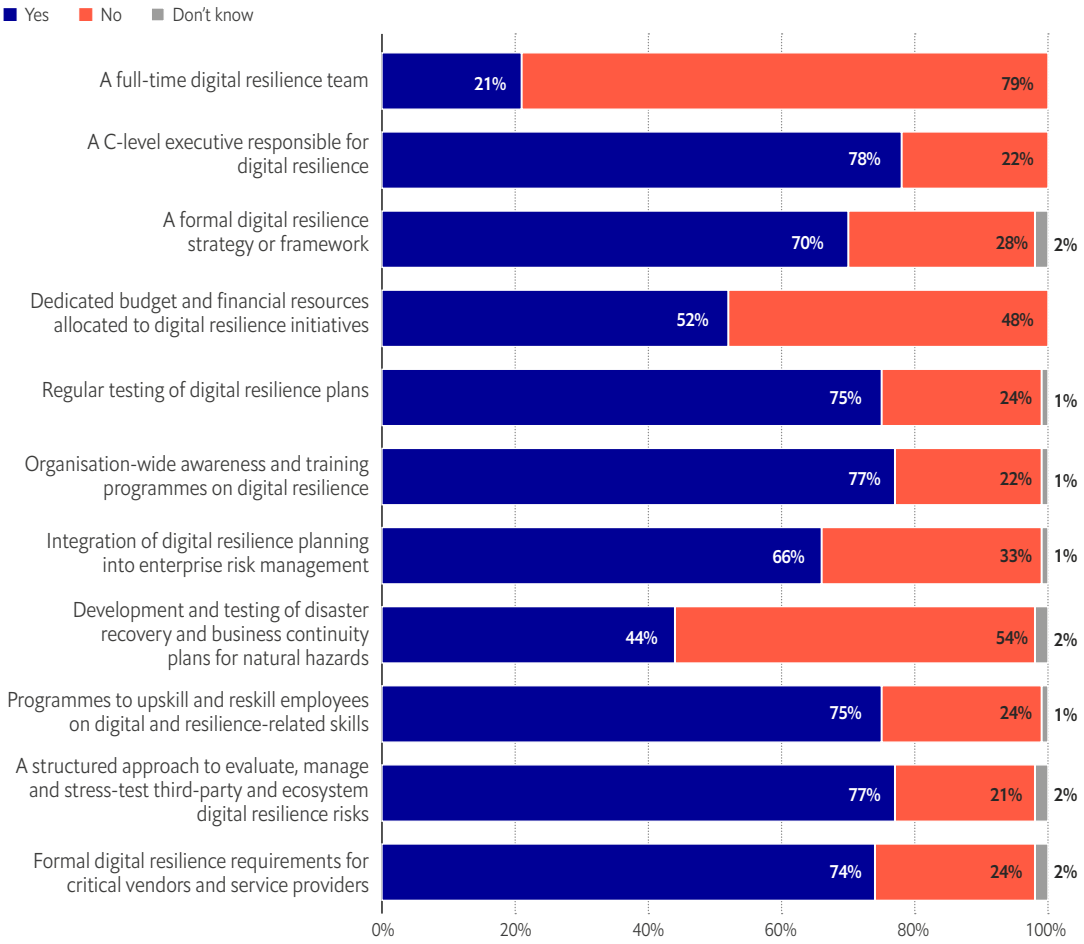
Most APAC organisations have already put in place several important building blocks of an effective digital resilience discipline. Upwards of 70% have a formal digital resilience strategy and widescale training programmes to support it. In addition, 77% report having a structured internal approach to stress testing, even where external frameworks are limited.

Resourcing, however, is far more limited. Just 21% of organisations have a full-time resilience management team, while no more than 52% have dedicated financial resources allocated to resilience initiatives.

Building strong digital resilience requires time and funding, says Mr Spanner. "There must be someone dedicated to managing and thinking about this, someone who's continuously improving the resilience posture and not just reacting to incidents. Digital resilience needs to be treated as a core business capability or even a product. Then it will have a life-cycle that lasts decades."

Figure 16: Resilience mechanisms

Digital resilience mechanisms currently in place at respondent organisations



Source: Economist Impact survey on Digital Resilience, 2025

The human element

The most significant gaps observed in technology and risk practices are not technical. They reflect how digital resilience is led, governed and reinforced across the organisation. While boards and senior leaders often endorse resilience in principle, few treat it as an enterprise-wide responsibility. But without a clear, unified mandate from on high, the need to build digital resilience will attract insufficient urgency.

While the urgency for resilience-building should originate from the board, leadership endorsement does not always translate into sustained oversight. For example, while most organisations have digital resilience strategies, just 28% say their boards regularly review them. When boards do conduct reviews, only 39% typically take follow-up action. "Resilience impacts every part of the business and the profit and loss,' says Mr Trigui. "You need proper councils, a clear path for escalation and the ability to raise issues to the board when investment or alignment is required."

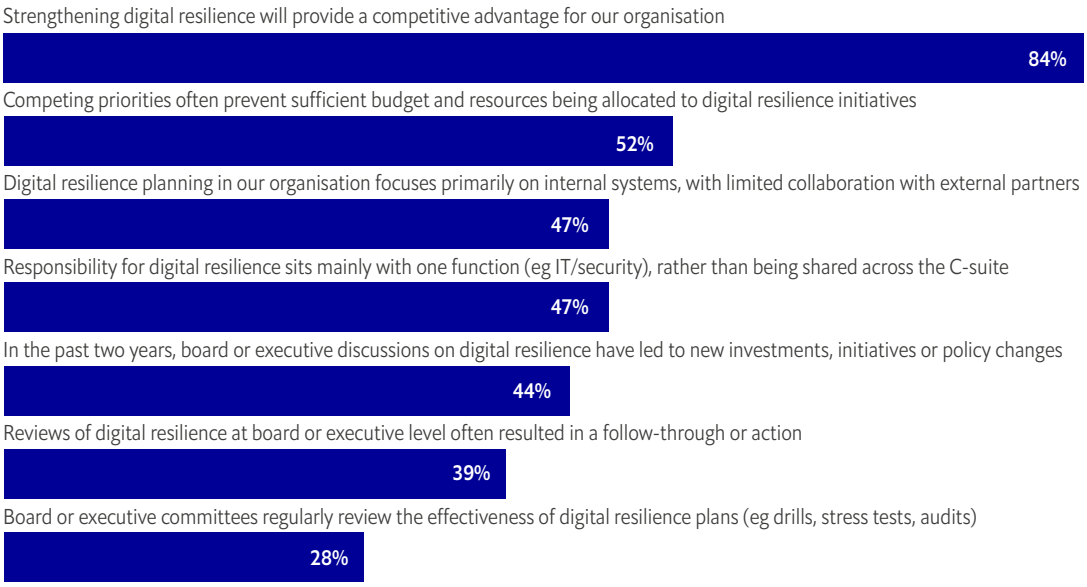
Below board level, responsibility for managing resilience-building is normally focused within a single function, such as IT (47%), rather than being shared across the C-suite—a pattern especially pronounced in Hong Kong, Thailand and Singapore.

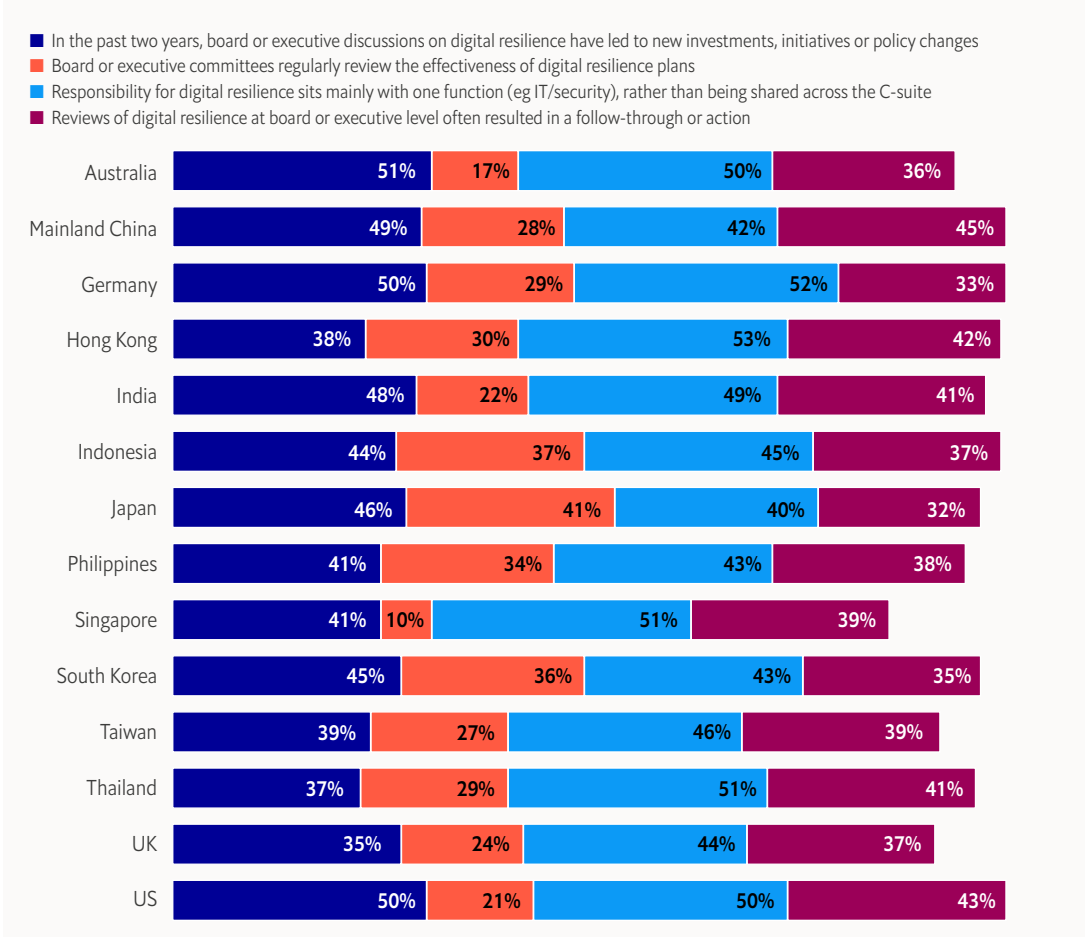
"Resilience impacts every part of the business and the profit and loss. You need proper councils, a clear path for escalation and the ability to raise issues to the board when investment or alignment is required."

Nizar Trigui, chief technology officer, GXO

Figure 17: Support from on high

Share of respondents agreeing with statements about their organisations' leadership of digital resilience efforts





Source: Economist Impact survey on Digital Resilience, 2025

Workforce skills and behaviours

This final pillar focuses on the extent to which the workforce is provided with the skills and guidance needed to develop resilience behaviours. The surveyed organisations' regular or frequent training in cyber hygiene (provided by 95%), data privacy (78%) and crisis communication (73%) offer a good foundation for this.

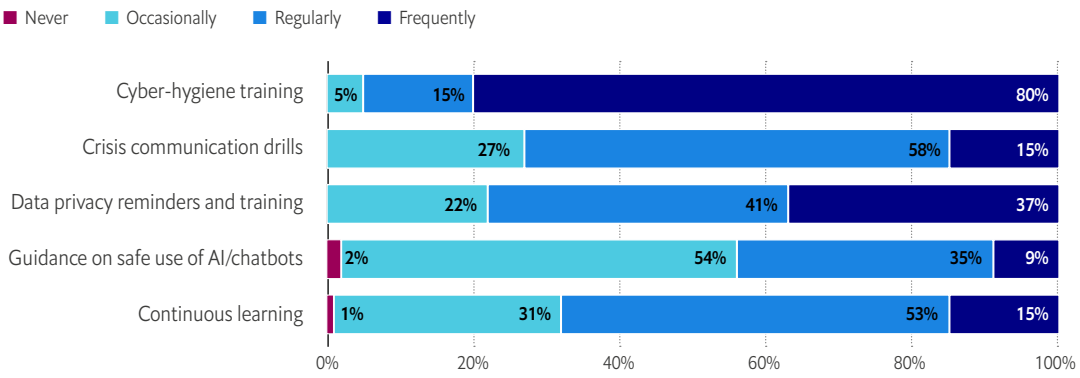
Resilience must extend beyond specialist teams, insists Mr O'Neill: "While we have dedicated teams focused on resilience, the real foundation is ensuring that every colleague understands how we prepare for potential disruptions. We align around our most critical services, run scenario exercises and provide training across the bank. Investing in resilience strengthens our systems, minimises disruption and reinforces long-term trust."

The development of future-ready behaviours is far less prevalent. Take, for example, the rapid growth of AI. Just 44% of respondent organisations provide regular or frequent workforce training or other guidance to employees on the safe use of AI. The majority (54%) do so occasionally at best. AI's capabilities are swiftly advancing. Organisations cannot afford to leave employees in the dark about its risks.

Skills alone are not enough. Organisations also need systems that reinforce accountability and behaviour. DBS's Technology Risk Culture Programme does this by promoting early risk identification, clear ownership and compliance. AI upskilling helps staff spot and adapt to emerging threats. Culture surveys, behavioural assessments and audit feedback monitor whether these efforts translate into practice.

With executives unsure they can hire enough people with the right technology skills (see Figure 7), organisations cannot rely on recruitment alone. Mr Philippi stresses the importance of partnerships, describing them as an important lever. "We collaborate with partners across different markets on advanced cyber risk solutions. This spans a wide area, ranging from threat detection to risk management, incident response and more. For instance, we work with insurtech firms to strengthen AI-powered anti-scam and cyber protection capabilities." He adds: "Regarding talent resilience, we have learned that it is not just about hiring more specialists. It is about equipping the whole organisation to operate confidently during disruption, and to that end, building strong partnerships across the ecosystem."

Figure 18: Inculcating resilience behaviours: 1
How often resilience behaviours are reinforced



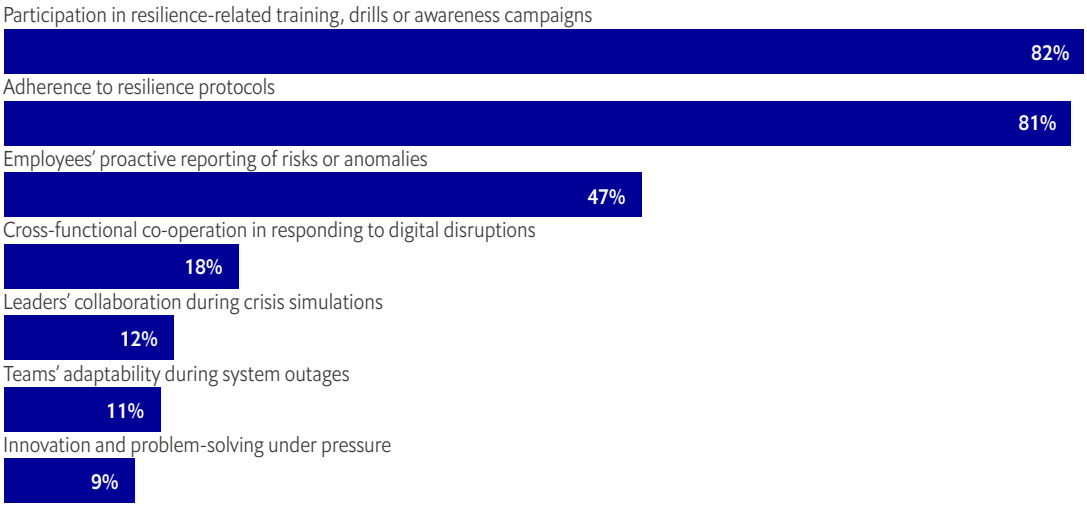
Source: Economist Impact survey on Digital Resilience, 2025

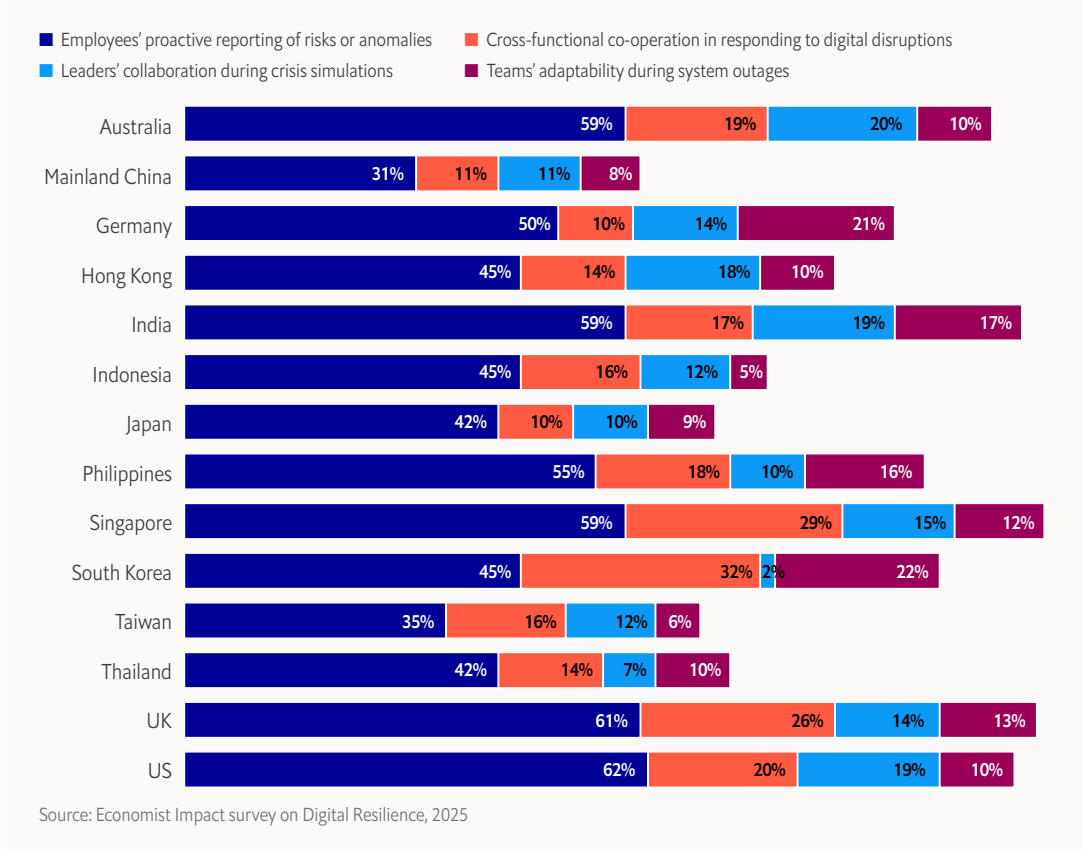
Enforcement of resilience protocols focuses on basic cybersecurity and business continuity. Around four-fifths of surveyed organisations mandate employee participation in relevant drills, tests and practices. Less than one-fifth, by contrast, mandate training in areas such as cross-functional crisis co-ordination, adaptive decision-making or problem-solving under pressure.

As the digital threat landscape grows more complex, management is likely to regard such capabilities as a must-have rather than a nice-to-have.

Figure 19: Inculcating resilience behaviours: 2

Resilience behaviours supported by mandatory training and policies





Source: Economist Impact survey on Digital Resilience, 2025

Conclusion

This research highlights three fundamental truths about digital resilience. The first is that it hinges on far more than robust cybersecurity; resilience means not just keeping attackers out but keeping systems running under stress. The second is that resilience does not exist in a vacuum; the safeguards built by ecosystem members are as important as internal ones. The third is that an organisation's ability to respond and adapt to digital disruption relies as much on its internal culture as on its technology.

Our analysis indicates that organisations in APAC understand those realities but are struggling to translate them into the governance, partnerships and cross-functional capabilities required to design resilient, connected ecosystems. Concerted action in five key areas will help address this:

- **Integrate ecosystem partners tightly into resilience-building.** The more proactive the monitoring and assessment of key vendors' resilience, the better. Relying on service level agreements may not be sufficient when real threats loom. Vendors should be involved, for example, in stress tests and incident reviews.
- **Treat resilience as a core business product, not a project.** Management should view digital resilience as an ongoing business requirement. It should be managed full-time by an individual and team with a dedicated budget, separate to IT and cybersecurity.
- **Shift from episodic risk management to continuous preparedness.** Stronger resilience requires continuous monitoring, frequent scenario-testing and systematic learning from near-misses. Stress testing should focus on cascading, cross-system failure, not isolated technical faults.
- **Nurture a positive culture of resilience.** The entire organisation needs to buy into the urgency of building digital resilience. That requires, among other things, nurturing an ethos of honesty, information-sharing and learning in the aftermath of tests and real incidents.
- **Don't let governance fall behind.** Enterprise adoption of advanced technologies such as AI shows no signs of slowing. Most organisations provide training and guidance in AI use, but they should also build across-business standards and controls.

Appendix: barometer results

Table 1: Digital resilience capability scores by market

Markets	External enabling environment	Technology and infrastructure	Risk management	Leadership	Workforce and cultural agility	Overall scores
Germany	61.21	50.68	57.00	52.42	52.49	54.76
Singapore	55.21	50.65	60.82	45.65	55.95	53.65
US	55.27	49.07	61.27	46.77	54.84	53.44
Japan	58.46	50.76	56.52	48.64	51.88	53.25
UK	54.53	50.04	60.12	47.15	54.18	53.20
Australia	55.54	48.08	60.04	45.94	54.66	52.85
South Korea	58.17	48.17	55.56	47.33	51.94	52.23
Hong Kong	56.94	47.04	53.26	47.02	52.37	51.33
India	49.71	46.95	57.88	47.53	53.66	51.15
Mainland China	55.00	46.46	54.63	46.55	51.05	50.74
Taiwan	56.50	45.34	52.28	46.69	51.70	50.50
Indonesia	53.32	41.28	50.11	46.58	49.87	48.23
Thailand	53.51	42.81	50.23	44.50	49.87	48.18
Philippines	52.63	41.26	46.07	45.93	50.15	47.21

Table 2: Digital resilience capability scores by industry

Industry	External enabling environment	Technology and infrastructure	Risk management	Leadership	Workforce and cultural agility	Overall scores
Financial services, banking and insurance	57.80	49.43	57.15	46.90	53.90	53.04
Digital infrastructure, IT and technology	57.06	49.34	57.62	46.88	53.72	52.92
Healthcare	56.33	47.58	55.31	47.71	52.87	51.96
Energy and mining	54.91	45.89	56.93	47.17	52.36	51.45
Industrials	57.53	45.69	54.88	46.93	51.69	51.34
Professional services	54.33	47.02	54.99	46.50	52.68	51.11
Government and public sector	53.18	44.23	52.80	45.84	50.46	49.30

ECONOMIST IMPACT

LONDON

The Adelphi
1-11 John Adam Street
London WC2N 6HT
United Kingdom
Tel: (44) 20 7830 7000
Email: london@eiu.com

GENEVA

Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@economist.com

SÃO PAULO

Rua Joaquim Floriano,
1052, Conjunto 81
Itaim Bibi, São Paulo,
SP, 04534-004
Brasil
Tel: +5511 3073-1186
Email: americas@economist.com

NEW YORK

750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@economist.com

DUBAI

Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@economist.com

HONG KONG

1301
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@economist.com

SINGAPORE

8 Cross Street
#23-01 Manulife Tower
Singapore
048424
Tel: (65) 6534 5177
Fax: (65) 6534 5077
Email: asia@economist.com