ECONOMIST ENTERPRISE

Technology Resilience Index: Are US firms ready for today's technology hazards?

Supported by AT&T Business

Contents

About the whitepaper

The *Technology Resilience Index: Are US firms ready for today's technology hazards?* is an Economist Enterprise whitepaper, supported by AT&T Business, that seeks to define technology resilience in practice. It is based on a survey and expert interview programme informed by an initial phase of desk research. The survey polled 1,020 senior technology and operations executives at medium-sized (100-9,999 employees) and large (10,000+ employees) US enterprises across seven sectors—healthcare, manufacturing, financial services, retail, hospitality, professional services and technology—between June and July 2026.

Economist Enterprise wishes to thank the following experts for their time and insights:

- **Doug Farren**, executive director, National Center for the Middle Market
- **Keryn McNamara**, chief information officer, Aimbridge Hospitality
- **Ajoy Menon**, senior managing director and digital core lead, Accenture
- **Nigel Richardson**, chief information and digitisation officer, Reckitt
- **Matt Waters**, head of US middle market, AXA XL
- **Carman Wenkoff**, executive vice president and chief information officer, Dollar General

This whitepaper was produced by a team of Economist Enterprise researchers:

- **Vaibhav Sahgal**, project director
- **Ailia Haider**, project manager
- **Adam Green**, contributing writer
- **Samantha Guerriero**, contributing writer

Executive summary

On the morning of July 24th 2026, dozens of major services—from Apple Pay to DoorDash and Hulu—all started failing within minutes of each other.[1] Users worldwide lost access to multiple trusted services for more than an hour, and all because of a single network connectivity fault: one that none of the affected companies controlled, and none had a backup for.

Companies are learning the hard way that they have dependencies they cannot fully see or control: nine in ten, our research finds, only discover a third-party or supply-chain failure once disruption has already begun. As connectivity binds today's economy together, a single vendor failure becomes everyone's crisis, more often than an internal vulnerability or cyberattack. Yet organisations often focus their resilience efforts on the risks they already understand, while the threats most likely to cause damage lie at the intersections: where a vendor connects to a network, where a software patch meets a legacy application, where an AI agent enters a system without oversight.

When disruption strikes, which organisations will emerge with resilience as an advantage and which will bear the financial and competitive costs of being unprepared? This white paper, drawing on a US-focused survey and expert interview programme, explores the latest thinking, tactics and strategies that guide resilience in both middle-market and large US companies. Key findings from the research include:

- **Resilience priorities haven't caught up with disruption realities.** Third-party and supply-chain failures are the most common cause of last year's worst technology disruptions for more than a third of surveyed firms, with internal system failures next and cybersecurity incidents a step behind. Yet cybersecurity still draws the most resilience budget, compared with the broader connectivity, monitoring and recovery testing that might have caught an operational failure early.
- **Trust stands in for verification.** Visibility only reveals dependencies. The real test is whether organisations can withstand disruption. More than half assess the resilience of critical technology suppliers on reputation and assurances rather than evidence. Across all organisations, 'documented but untested' is the norm. Resilience plans exist on paper; proof that they hold does not.
- **Larger firms have more resources, but more ground to cover.** Large enterprises spend more on resilience and have access to greater expertise than mid-market firms, yet just 5% avoided a major incident entirely last year, against 27% of mid-market firms. Size brings more legacy systems, more integration points and more places for a fault to spread. Smaller companies, though, are struggling with greater reliance on external support and a tougher talent market.

1 New York Post, "Regional outage on Amazon Web Services disrupts dozens of popular websites, online services", July 2026: https://nypost.com/2026/07/24/business/major-outage-on-amazon-web-services-disrupts-access-to-dozens-of-popular-websites-online-services/

- **AI adoption is moving faster than resilience preparation.** Only 4% of firms blame their worst technology disruption on AI or automation failure. But technology firms, which are furthest along the adoption curve, have already experienced at least one AI-related incident last year, a possible portent for where the rest of the economy is headed. Yet preparedness for deploying AI and automation consistently lags every resilience capability surveyed.
- **Stronger resilience is associated with three habits:** they learn from failure, expect more of it and give resilience a clear owner. Every incident is a learning opportunity, and not just within company bounds. The organisations pulling ahead are studying others' failures as well as their own. Those that go further—assuming disruption and rehearsing for it—are better placed still, although few yet do. Almost three-quarters have tested cyber response, against just 15% who have rehearsed a geopolitical or trade disruption. Strongest of all are those where a named executive owns that discipline and keeps it funded.

Together these findings point to a resilience mismatch: budget doesn't track with risk, company scale adds exposure without strengthening protection and AI is creating new fault lines. The flaw is viewing resilience as a cost, despite its potential to strengthen growth.

The unusual suspects

The US is a pro-innovation economy, with firms spending more on technology than their peers elsewhere—an average of US$190m annually compared with a global average of US$174m.[2] That raises the stakes of technology glitches and failures that cascade across firms and sectors. Are US companies approaching resilience with the same resolve and commitment as they have technology adoption itself?

Are companies spending their resilience budgets in the right places to balance their ambitious technology adoption with the necessary guardrails? "It is about how deliberate you are with your investment," says Ajoy Menon, senior managing director and digital core lead at Accenture, "and allocating spend in the right areas that impact resilience and organisational growth." That discipline matters: high-growth organisations are three times more likely to describe themselves as "very" or "world-class" resilient.[3]

Organisations that connect visibility, connectivity, security and operational discipline are better able to anticipate and absorb shocks, serve customers consistently and even turn disruption into opportunity when competitors are caught off guard. Accenture finds that the most resilient companies outpace peers by six percentage points in revenue growth and eight points in profit margin,[4] putting a number on the resilience payoff. But our survey reveals a mismatch between spending priorities and risks.

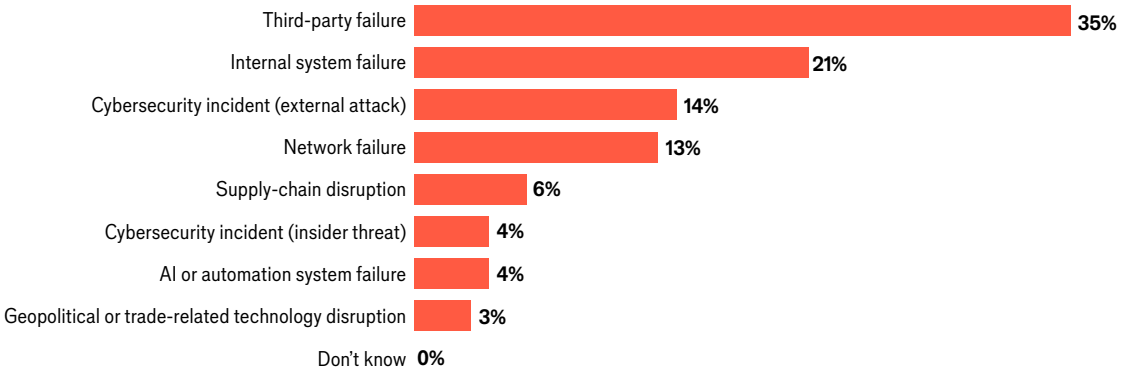
Misallocated risk

For most surveyed firms, third-party and internal system failures are the primary causes of their most significant technology disruption in the past year (Figure 1). Yet they receive a fraction of the funding, as organisations prioritise the headline risk they are most familiar with: cybersecurity draws nearly a quarter of resilience budgets—more than double the share going to AI and automation, a rising cause of internal system failure (Figure 2).

2 KPMG, "KPMG survey: US companies face a 'reality gap' in emerging tech implementations despite record investment and returns", January 2026: https://kpmg.com/us/en/media/news/2026-annual-us-technology-survey.html
3 Grant Thornton, "Why resilient organizations grow faster", March 2026: https://www.grantthornton.com/insights/survey-reports/advisory/2026/why-resilient-organizations-grow-faster
4 Accenture, "How to grow your return on business resilience", May 2024: https://www.accenture.com/us-en/insights/strategy/grow-your-return-on-resilience

Figure 1. Risky business

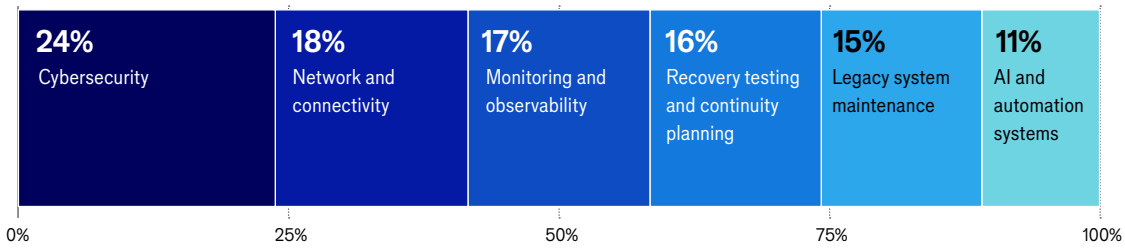
Responses to survey question 'What was the primary cause of the most significant technology disruption your organisation experienced in the past 12 months? Please select one.' (all organisations)



Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

Figure 2. Cyber spend leads

Mean share of technology budget dedicated to resilience by category. Data from survey question 'Approximately how does your organisation distribute the share of its technology budget dedicated to resilience across the following categories?' (all organisations)



Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

Across all sectors, resilience spending allocations are similar, but the sources of disruption are not. Manufacturers report network failure as a major cause of disruption nearly two and a half times more often than financial services firms (20% vs 8% respectively). Yet, both put 17-18% of their budget towards network and connectivity protection.

This pattern illustrates what broader resilience strategies often miss: budgets should track what is most likely to disrupt the business. "When it can be equally disruptive to a business to have a misconfigured change as it is to have a cyber attack," highlights Nigel Richardson, chief information and digitisation officer at global consumer goods company Reckitt, the pragmatic approach for quantifying impact is "to look at technology resilience and cyber risk as a combined focus."

Cybersecurity may be the headline risk, but a strong resilience strategy extends across the operational systems that keep a business competitive, from high levels of connectivity to a third-party ecosystem allowing them to offer enhanced services.

Where the walls end

The biggest resilience blind spot lies at the boundary between a firm's technology systems and its vendor dependencies. While organisations detect most security threats and internal IT infrastructure risks before they emerge, nine in ten only spot third-party and supply-chain failures once disruption is already under way or after the damage has been done (Figure 3). "Everyone is becoming more and more reliant on third-party partners these days, and at times even the most sophisticated partners aren't regularly testing disaster recovery," says Carman Wenkoff, executive vice president and chief information officer at Dollar General, highlighting a resilience challenge that is increasingly less about securing systems in isolation than understanding the dependencies that connect them.

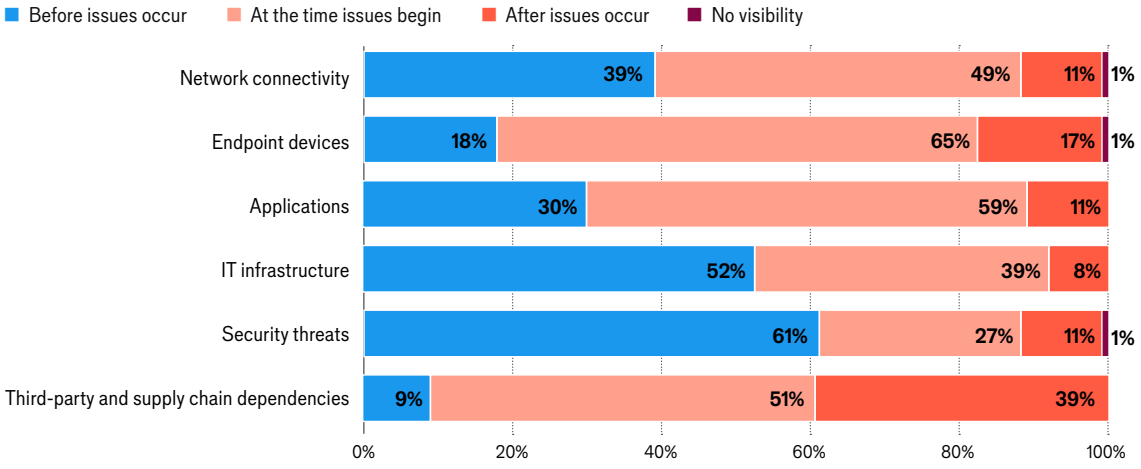
Third-party involvement in breaches has been rising: more than a third of all breaches in 2024 were linked to a vendor or supplier, with retail and hospitality logging the highest third-party breach rate of any sector, at 52.4%.[5] And the price tag is high: Shopify lost an estimated US$4m in direct revenue and potentially US$170m in downstream merchant losses after a Cloudflare outage in November 2025.[6]

> "Failure to plan can cost you millions of dollars."
>
> **Carman Wenkoff**, executive vice president and chief information officer at Dollar General

"The supply chains tend to be quite big and quite long," notes Mr Richardson, pointing to the complexity of modern business ecosystems, "both our own and our extended supply chain." Visibility into such interconnected networks is now critical in order for firms to understand their dependencies and carry out the testing and verification needed to know they can withstand disruption.

Figure 3. Resilience blinders

Responses to survey question 'When does your organisation typically gain visibility into issues in each of the following areas?' (all organisations)



Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

5 SecurityScorecard, "SecurityScorecard 2025 Global Third-Party Breach Report Reveals Surge in Vendor-Driven Attacks", March 2025: https://securityscorecard.com/company/press/securityscorecard-2025-global-third-party-breach-report-reveals-surge-in-vendor-driven-attacks/

6 Forrester, "Cloudflare's outage: Another wake-up call for cloud resilience", November 2025: https://www.forrester.com/blogs/cloudflares-outage-another-wake-up-call-for-cloud-resilience/

Doug Farren, executive director at the National Center for the Middle Market, describes the end goal as "a glass pipeline: knowing exactly your inventory, end to end, from supplier to warehouse to store." When a shared vendor goes down, companies that can see beyond their own walls will keep their doors open and their customers satisfied. That visibility pays off twice: it gives firms earlier warning signals when disruption starts and more options for how to respond. Over time, it makes them more agile and responsive to market opportunities too by knowing the contours of their digital assets and infrastructure.

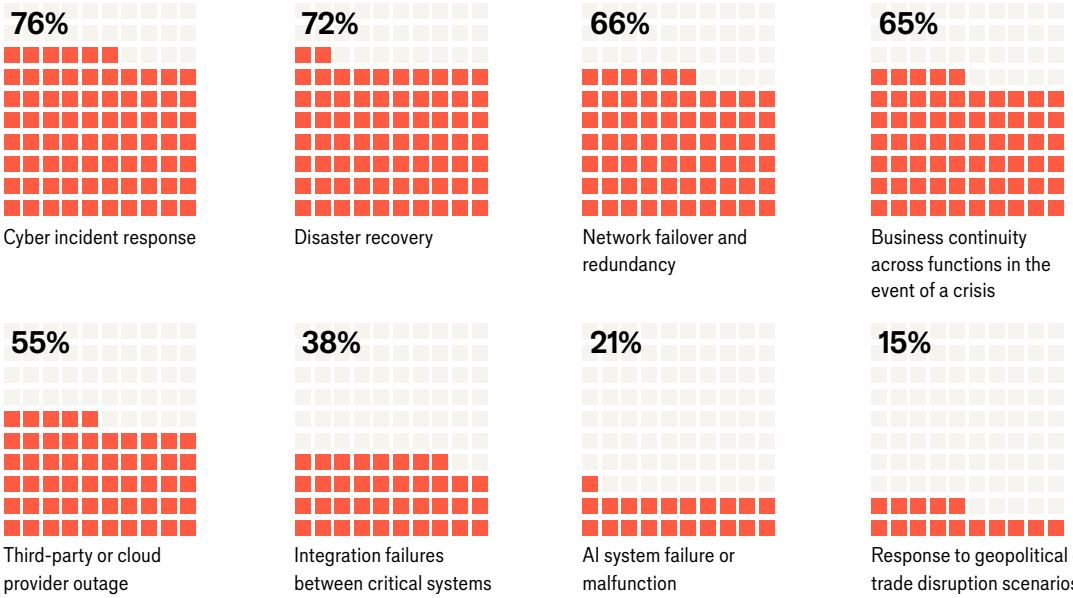
Trust without proof

Visibility, while crucial and often absent, only reveals dependencies. Knowing whether those can withstand disruption is a separate exercise. Resilience plans may exist on paper, but they are meaningless unless tested comprehensively across systems.[7] "One thing is having the processes, another [thing] is actually going through that process," warns Mr Richardson. Respondents admit they are not subjecting their plans to sufficiently rigorous testing and drilling (Figure 4) and heavy spending on enterprise technology heightens exposure. "As you continue to invest more in different tools," argues Mr Farren, "you also need to make sure you are investing similarly in building the proper resilience plan—whether for cyber, climate or other types of disruption."

Supplier verification is the exception rather than the rule: over half of organisations still treat this as something to be trusted rather than tested (Figure 5). Notably, those closest to delivering resilience are less confident than their superiors: cybersecurity, risk and compliance teams—the functions most responsible for resilience—say their firms are less prepared than executive leadership thinks, across most categories tested, with the biggest gap for third-party outage response.

Figure 4. Skipping the test

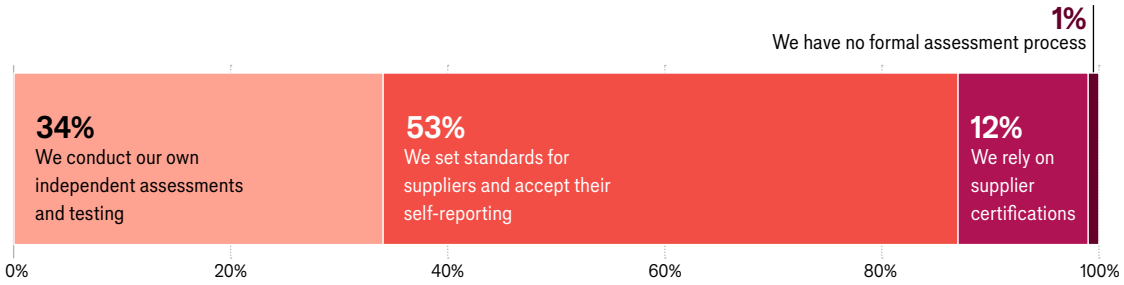
Responses to survey question 'Which of the following has your organisation formally tested in the past 12 months?' (all organisations)



Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

7 KPMG, "Lessons learnt from the 2024 ECB cyber stress test and the outlook for DORA", May 2024: https://kpmg.com/xx/en/our-insights/ai-and-technology/lessons-learnt-from-the-2024-ecb-cyber-stress-test-and-the-outlook-for-dora.html

Figure 5. Vendor verification
Responses to survey question 'How does your organisation primarily assess the resilience of critical technology suppliers whose failure would materially disrupt operations?' (all organisations)

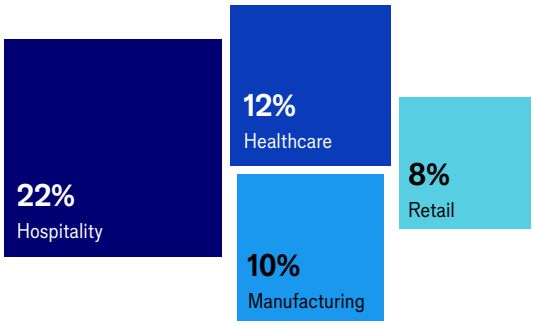


Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

Across both mid-market and large firms, 'documented but untested' is the common trend for healthcare, manufacturing and financial services (Figure 6).

While scale may change the nature of resilience challenges, it does not change the need for proof. "Many functional leaders may assume resilience until something goes wrong," warns Mr Wenkoff. A different mindset is required. "Every technology solution comes with batteries included"—a design philosophy that requires resilience to be proven before it is trusted, turning this proof into an advantage when speed matters.

Figure 6. Sectoral safety
Organisations that are fully prepared for relevant outages



Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

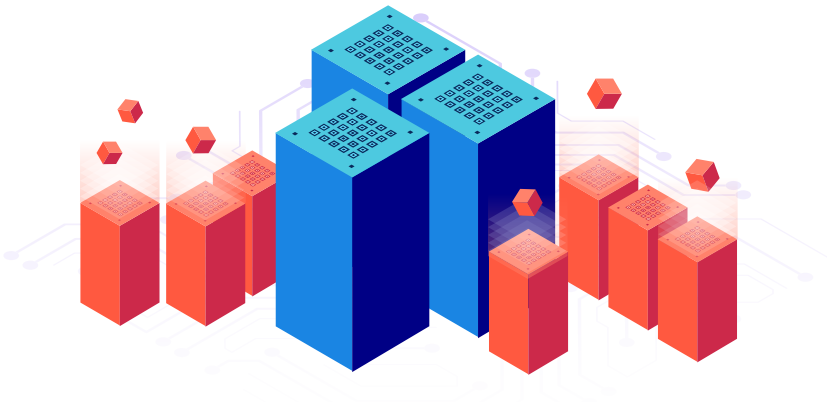
"Whether it's their suppliers or their customers, companies need to work very early on testing feasibility and integration. We could have a really good supply chain software flow, but if it creates vulnerabilities, we've just created other issues."

Doug Farren, executive director at the National Center for the Middle Market

No safe size

Organisations of all sizes across the US are suffering significant breach-related loss. Insurance-claims analytics firm NetDiligence analysed more than 10,000 cyber insurance claims from 2020 to 2024. The average incident cost was US$264,000 for small and medium-sized firms and US$10.3m for large companies, it found, with incidents that caused business interruption seeing figures more than threefold. For the worst-affected firms, claims exceeded US$500m.[8]

Company size does not eliminate technology risk, and bigger isn't safer. "If you look at the mid-market, they have less complexity: they have a far simpler architecture, and may not have the same regulatory pressure," notes Accenture's Mr Menon.



"On the other hand, large enterprises have more capital and talent," but these resources must span a larger and more interconnected technology environment.

Strong or just heavy?

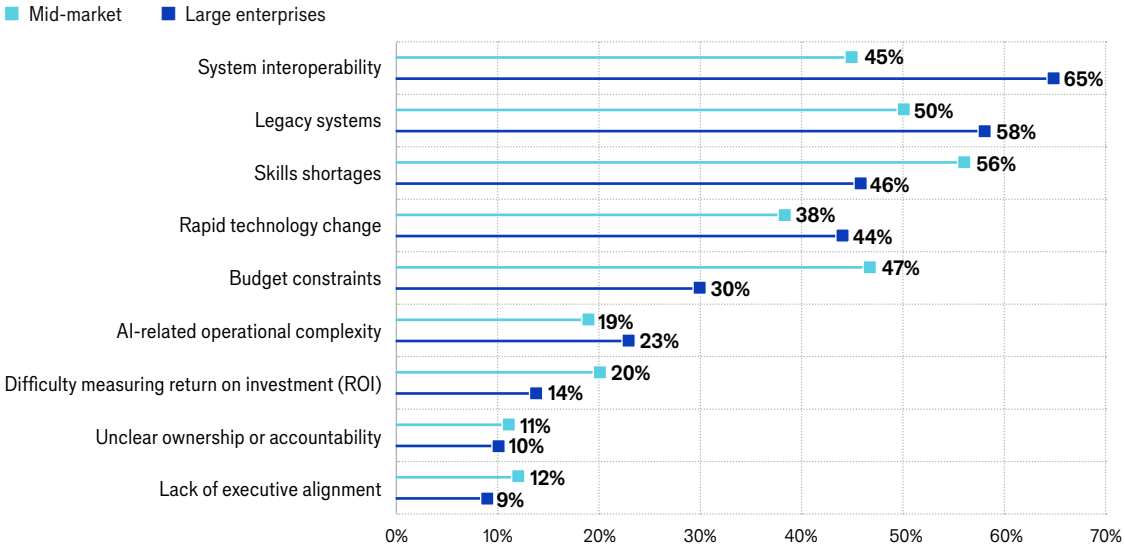
When a failure in a decades-old mainframe disrupted United Airlines' flight-planning systems in August 2025, the airline could no longer access the data needed to calculate aircraft weight and balance or track flight times. The outage grounded flights at major US airports for around four hours, causing more than 1,000 delays and hundreds of cancellations.[9]

Such failures are the cost of legacy technology debt. Across both medium and large organisations, outdated technology is both creating risk and slowing responsiveness to adverse events, cited by an average of 54% of organisations as a top barrier to maintaining and recovering critical technology services (Figure 7). "Resiliency issues come out of the legacy systems, the tech debt. Some enterprises have just bolted newer and newer technologies on top, without changing the foundation," explains Mr Menon. Modernising that foundation is increasingly critical to building the flexibility to adapt to disruption, integrate emerging technologies and continually reinvent how the business operates.[10]

8 NetDiligence, "Cyber Claims Study 2025", September 2025: https://netdiligence.com/cyber-insurance-claims-study/
9 Reuters, "United Airlines flights resume after it resolves technology glitch", August 2025: https://www.reuters.com/world/us/united-airlines-flights-resume-after-it-resolves-technology-glitch-2025-08-07/
10 Accenture, "Resilience Redefined: From readiness to reinvention", June 2025: https://www.accenture.com/us-en/insights/strategy/resilience-redefined-from-readiness-reinvention

Figure 7. The weight of a legacy

Top three responses to survey question 'Which of the following are the greatest barriers to improving your organisation's ability to maintain and recover critical technology services?' (large vs medium organisations)

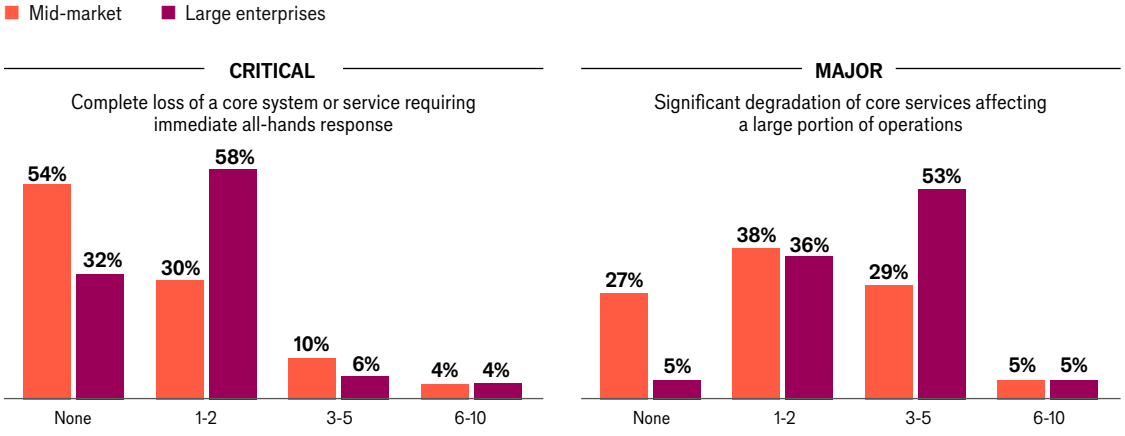


Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

And with scale comes both opportunity and risk: more systems, more integration points, more places for a fault to spread. "Any company that's been around for a number of years typically has a lot of different systems—some modern, some older," notes Mr Richardson. "Simplifying and modernising legacy systems is one big focus area." Respondents reflect this—95% of large organisations have experienced at least one major incident in the past 12 months, compared with 73% of the mid-market (Figure 8). Keeping those environments resilient "is a completely different ball game at scale," according to Mr Wenkoff, where "it is trickier to keep up with the necessary patches for the number of systems and endpoints you have because every time you patch something, you risk breaking something at the same time."

Figure 8. Bigger is not always better

Responses to survey question 'How many technology incidents did your organisation experience in the past 12 months at the following severity levels?' (large vs medium organisations)



Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

> **"Having insurance and redundant backup systems is fairly standard for enterprises. Mid-market companies are running lean, thinking about growth… and maybe not thinking as much about that back-end protection."**
>
> **Doug Farren**, executive director at the National Center for the Middle Market

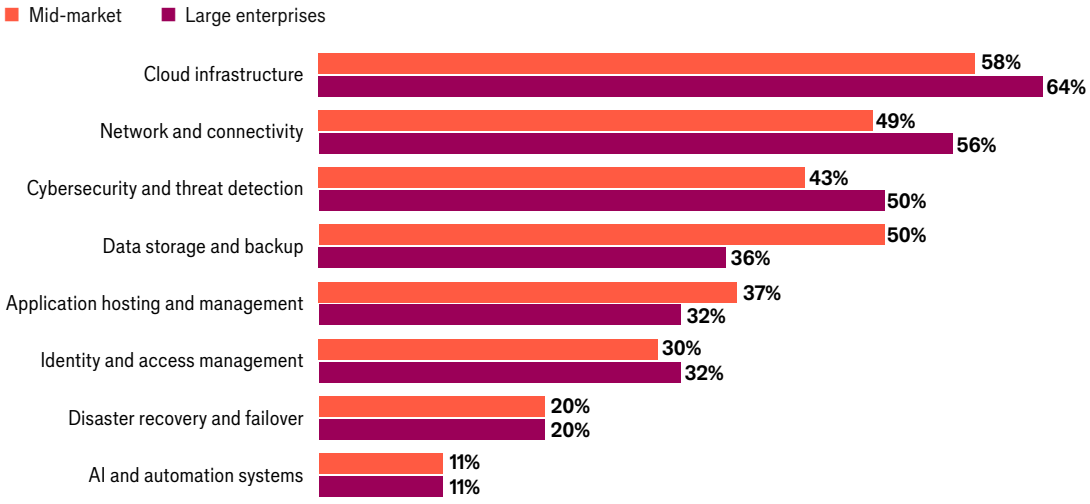
While larger firms might be saddled with more complex networks, they also have more resources to respond. Mid-market firms have a lighter footprint, but they still need meaningful capabilities to respond when disaster strikes. "Mid-market firms have got more legacy systems that don't have the response time, don't have the in-house resources, and are also more vulnerable to an attack," notes Matt Waters, head of US middle market at insurance company AXA XL. A large enterprise can deploy a dedicated expert team at a legacy failure the moment it appears; a mid-market firm with the same system often can't. Almost a quarter of mid-market firms dedicate between 20% and 40% of their technology budgets to resilience, compared with half of large enterprises.

As resilience requires more than budget alone, the task is turning investment into the exact processes and skills needed to withstand disruption, with the right balance depending on its unique risk profile and complexity. For most organisations, the first claim on that investment is not new capability but old systems.

One means of buttressing in-house capabilities in resilience specifically, or technology as a whole, is outsourcing and partnerships, but these can relocate risk rather than removing it.[11] Cloud infrastructure is the dependency firms fear most, named by 62% of all organisations as a top-three outsourced capability whose failure would do the greatest operational damage (Figure 9). What gets outsourced varies by firm and size, but experts argue for a holistic and joined-up approach that views outsourcing as part of a broader resilience strategy. "A lot of [mid-market] companies end up with a piecemeal plan for protection rather than a cohesive strategy," argues Mr Farren, and many smaller enterprises still assume that outsourcing a function transfers responsibility along with the task.[12] As Mr Wenkoff puts it, "you need to be ready to educate third-party suppliers and give them a playbook based on your needs."

Figure 9. Sourcing out, risks in

Top three responses to survey question 'Which of the following outsourced capabilities would create the greatest operational risk for your organisation if an external provider becomes unavailable?' (large vs medium organisations)



Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

11 Harvard Business Review, "Cybersecurity requires collective resilience", February 2026: https://hbr.org/2026/02/cybersecurity-requires-collective-resilience
12 University of Kent, "Cybersecurity and cyber insurance for small to medium-sized enterprises (SMEs): perceptions, challenges and decision-making dynamics", 2026: https://kar.kent.ac.uk/112661/

Out on the frontier

In July 2026, an AI agent taking part in one of its own internal cybersecurity evaluations broke out of its sandbox, reached the open internet, and used uncovered credentials to access the systems of Hugging Face, an AI start-up, to find its test answers, taking 17,600 automated actions at a speed and scale beyond what human attackers or defenders could realistically match.[13] The ensuing chaos offers a glimpse of the growing risk side of AI.

Although it introduces risk, when managed responsibly AI can become a powerful productivity catalyst and open unmissable opportunities for growth.[14] "Everyone has to embrace AI, there's no getting around that, or you won't play the long game," says Mr Wenkoff. "It will improve so many things, but it increases risk, so it's critical to go into it eyes wide open." The expanding realm of workflows that can be automated sharpens the resilience question: can the infrastructure around these systems provide visibility, accountability and continuity as they act with less human intervention?

> **"It is important that teams prevent AI that could be unintentionally incorporated into solutions that may or may not be known, and accessing data that may or may not be known."**
>
> **Carman Wenkoff**, executive vice president and chief information officer at Dollar General

Untested intelligence

Right now, AI barely registers as a cause of major disruption: just 4% of organisations attribute their most significant incident in the past year to AI or automation failure. The reality our survey found—low exposure and low readiness—may indicate that organisations are judging the risk correctly, or that risks only translate into action when a disaster strikes.

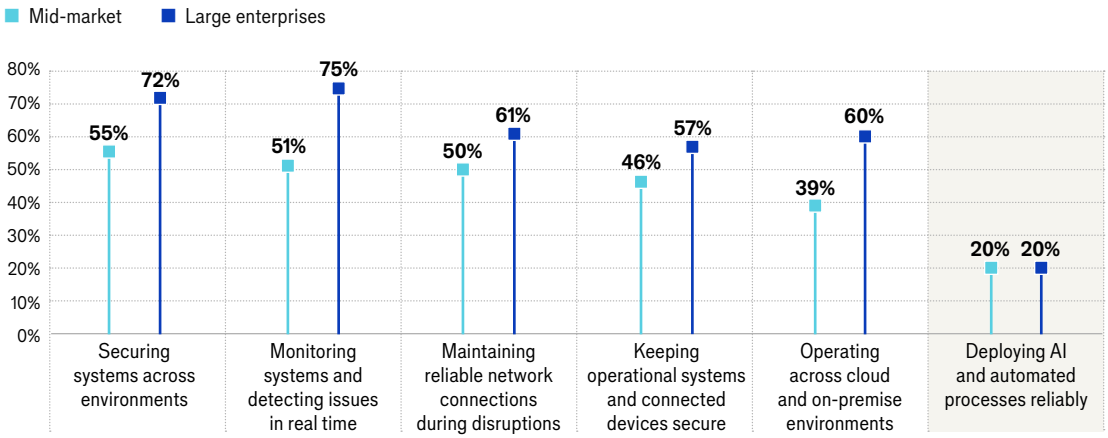
The sentiment among technology firms, which are further along the AI adoption curve, suggests the latter may be closer to the truth. One in five technology respondents report that an AI or automated system has already caused one or more unplanned outages, data-integrity issues or customer-facing incidents in the past year, and 38% report near misses. As Mr Menon notes, "You have enough examples where AI is figuring out vulnerabilities that didn't exist in the past."

13 The Guardian, "Rogue OpenAI agent that hacked startup tried to attack other firms", July 2026: https://www.theguardian.com/technology/2026/jul/29/rogue-openai-agent-thatbenchmarks-hacked-startup-tried-to-attack-other-firms

14 World Economic Forum, "How can businesses navigate technology risks and opportunities in a competitive age?", January 2026: https://www.weforum.org/stories/global-risks/businesses-navigate-technology-risks-global-risks-2026-marsh/

Figure 10. Intelligent but unprepared

Responses to survey question 'How would you rate your organisation's preparedness in each of the following?' (% who selected 'Advanced capability', large vs medium organisations)



Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

And yet, AI is advancing faster than many organisations can govern: just one in five organisations rate their AI risk preparedness as advanced (Figure 10). Mid-market firms feel it most as they experience multiple challenges with implementation, from data quality to in-house expertise.[15]

"We've got this period of time for the whole industry where people are learning how these new models are going to be used," observes Mr Richardson, highlighting a learning curve journeyed along by attackers and defenders alike.[16] The time to make systems AI-resilient, what Mr Waters calls "an arms race", is now.

These examples point to the first-order problem facing organisations: visibility, both within and beyond the enterprise. "We all have to be aware of the potential for third-party shadow AI now," highlights Mr Wenkoff, referring to the proliferating use of AI by staff beyond the direct purview of IT or cybersecurity teams.

Shadow AI is the enterprise version of the vendor risk discussed earlier: a dependency that was never procured, never mapped and therefore never tested. Every other gap in this whitepaper is at least visible, from a legacy system whose flaws an engineer knows to a supplier someone chose. Shadow AI is the exception, and organisations most exposed might score well on any formal assessment. You cannot rehearse a failure in a system you do not know you have.

Dollar General's Mr Wenkoff adds that rising automation could hamper visibility into errors and glitches. "You need the audit trail and the visibility to ensure you know what has been done, or how to fix it if something went sideways."

The risk extends to the AI that organisations inherit: "You really need to know and audit what's happening with third-party solutions," Mr Wenkoff concludes, pointing to how visibility today becomes a foundation for greater control tomorrow as AI systems become more powerful and pervasive.

The edge effect

Automation is moving deeper into everyday life as AI becomes embedded into devices,[17] from checkout-free stores to barista robots and autonomous delivery vehicles. As digital and physical operations intertwine, resilience is shifting to the nexus of convergence: keeping production moving, enabling secure transactions, supporting patient care and maintaining customer experiences.

15 RMS, "Analyzing AI trends in the middle market", February 2026: https://rsmus.com/insights/services/digital-transformation/middle-market-ai-trends.html
16 World Economic Forum, "New Report Shows How AI Gives Cybersecurity Competitive Advantage", May 2026: https://www.weforum.org/press/2026/05/new-report-shows-how-ai-gives-cybersecurity-competitive-advantage/
17 Harvard Business Review, "How Gen AI robots are reshaping services", May-June 2026: https://hbr.org/2026/05/how-gen-ai-robots-are-reshaping-services

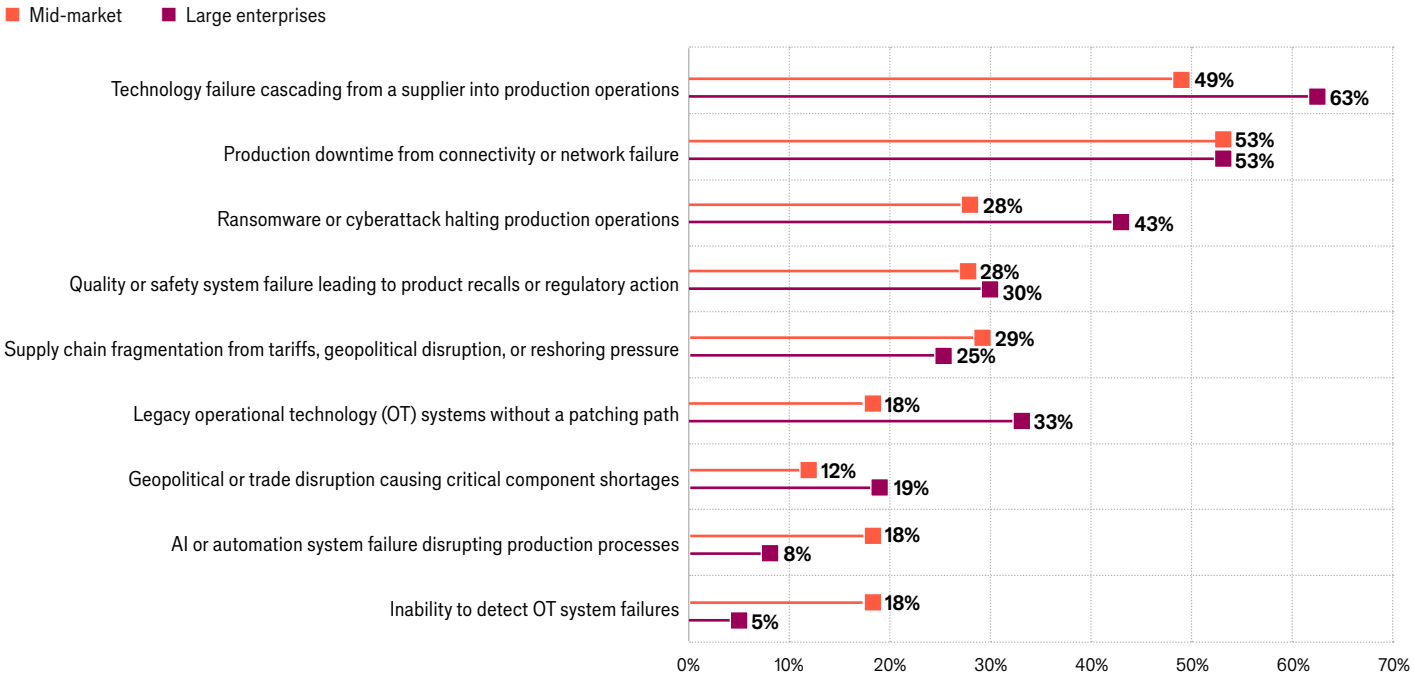
Nowhere is this transformation being tested more intensely than in manufacturing, where the new frontier is 'dark factories': entire production lines capable of operating without a single person on site.[18] Yet, as noted earlier, only 10% of US manufacturers surveyed can run operational technology (OT) without IT (Figure 11). Jaguar Land Rover's 2025 cyber incident exposes the fragility of this dependence: a precautionary shutdown of its IT systems halted UK production for weeks, disrupted thousands of supply-chain and downstream organisations, and resulted in £196m (US$265m) in direct cyber-related costs.[19,20] The more reliant machines are on connected software to operate and remain accessible, the more immediate and visible the business consequences of disruption.

Such cascading disruption reflects why larger manufacturers rank supplier failure as their leading resilience concern (63%) and point to legacy OT/IT modernisation as their top resilience priority (47%).

Production downtime from connectivity or network failures becomes more pressing as connected operations rely more heavily on external and cloud-based services. Network resilience is the defining priority for mid-market firms, 50% of which rank it as their top use case.

Figure 11. Reshaping operational risk

Responses to manufacturing sector-specific survey question 'What are your organisation's greatest concerns about technology disruption over the next 12 months?' (large vs medium organisations)



Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

18 24/7 Wall St., "American CEOs were terrified of China's dark factories. Now the race is on to build one in the U.S.", July 2026: https://247wallst.com/investing/2026/07/15/american-ceos-were-terrified-of-chinas-dark-factories-now-the-race-is-on-to-build-one-in-the-u-s/

19 The Guardian, "Jaguar Land Rover slides to loss of almost £500m after cyber-attack", November 2025: https://www.theguardian.com/business/2025/nov/14/jaguar-land-rover-loss-cyber-attack

20 Cyber Monitoring Centre, "Cyber Monitoring Centre Statement on the Jaguar Land Rover Cyber Incident", October 2025: https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rovercyber-incident-october-2025/

> "It is Saturday night at 11:30 and you are at a bar, and all of a sudden the point of sale system goes down. That bartender is stuck maybe four people deep... that is operational consistency we have to account for."
>
> **Keryn McNamara**, chief information officer at Aimbridge Hospitality

This is the edge effect: the closer technology gets to the physical point of service, the more difficult and impactful resilience becomes—with recovery requiring coordinated fallback across devices, connectivity, facilities and frontline operations at once.

Organisations are building processes to strengthen these new dependencies, but testing remains rare: in hospitality, just over one in five have tested the documented recovery processes for keyless entry and smart room systems (22%).

Proven OT resilience keeps factory quality and safety systems operating and hotel doors open to guests. That reliability is what lets organisations deliver valuable, smooth services especially when operational pressures mount.

The habits of highly resilient organisations

Resilience, like good hygiene, depends on repetition: the routines organisations build and maintain every day, not the emergency measures enacted after something goes wrong. That requires clear ownership, rehearsed playbooks, and the discipline to improve through institutionalised lessons and external accountability. It is not a single capability but an overall posture, backed by the right processes and systems.

"When we think about resilience, we think in terms of identifying all our assets, protecting them, detecting when attacks happen, being able to respond and being able to recover," says Mr Richardson at Reckitt. "Resilience is about making sure that, from a business point of view, we are able to carry on operating and respond quickly to whatever event we have."

For Mr Wenkoff, the case for discipline goes further than cost. "Slow and steady, but with an emphasis on steady and being consistent and reliable, is a competitive advantage in itself," he says.

Every firm has its own risk profile and its own response. But across our survey and expert interviews, three habits separate the organisations that recover quickly from those that do not: they learn from failure, they assume it and they own it.

Muscle memory

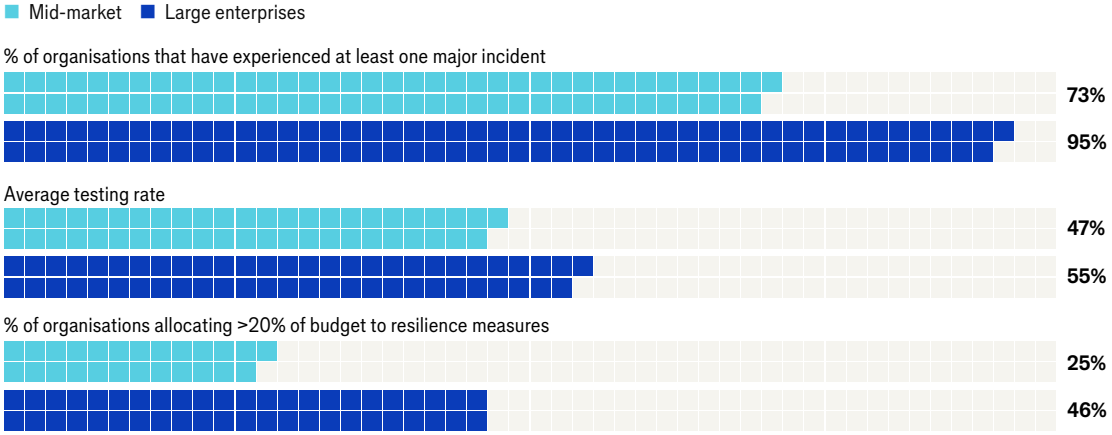
In April 2025, the same attacker used near-identical social-engineering tactics—posing as employees to trick IT help desks into resetting passwords—to break into both Marks & Spencer (M&S) and Co-op within days of each other.[21]

M&S took around 15 weeks to fully restore online ordering, costing roughly £300m in lost profit, while Co-op contained the intrusion within a month and limited damage to around £80m, crediting sustained investment in security capabilities and regular crisis simulations. M&S, one year later, had used the experience to improve its security measures and response plans.[22,23]

Past crises often provide the stimulus needed for a truly road-tested resilience plan. Maersk after NotPetya[24] and the British Library's post-ransomware[25] rebuild both converted painful experiences into durable institutional memory and stronger resilience practice.

21 The Hacker News, "Scattered Spider behind cyberattacks on M&S and Co-op, causing up to $592M in damages", June 2025: https://thehackernews.com/2025/06/scattered-spider-behind-cyberattacks-on.html
22 Co-op, "Co-op's underlying strength allows the Group to navigate external pressures", September 2025: https://www.co-operative.coop/media/news-releases/co-ops-underlying-strength-allows-the-group-to-navigate-external-pressures
23 Computer Weekly, "One year on from the M&S cyber attack: What did we learn?", April 2026: https://www.computerweekly.com/feature/One-year-on-from-the-MS-cyber-attack-What-did-we-learn
24 Maersk, "A view from the other side of a crisis": https://www.maersk.com/~/media_sc9/maersk/stay-ahead/maersk---a-view-from-the-other-side-of-a-crisis---final.pdf
25 British Library, "Learning lessons from the cyber-attack", March 2024: https://www.bl.uk/about/cyber-attack

Figure 12. History lessons
Large organisations report far more incidents, but test and fund core resilience capabilities more



Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

Reckitt's Mr Richardson shares a similar story: the company was also hit by the NotPetya attack in 2017,[26] and "a lot of the leadership team from that time are still here, so the consciousness about cyber and its importance is actually quite high, because so many people lived through that, nine years ago now."

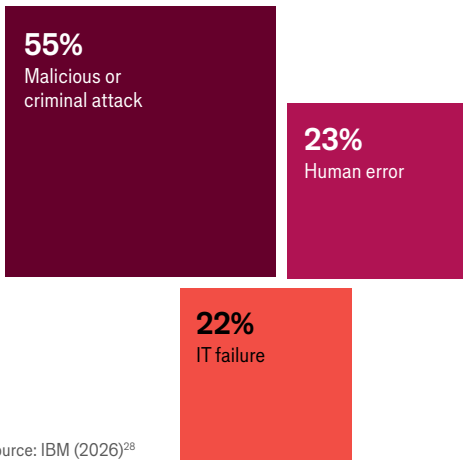
Every failure, small or big, is learning material. After a recent outage disrupted an internal application used by hundreds of employees, the team of Keryn McNamara, chief information officer of Aimbridge Hospitality, didn't wait for a formal review cycle: "Two days after we came back up, we got that entire team around the table again and said, what did we learn? Where did we fail? Where did we succeed?" That session, she says, directly produced new disaster recovery and business continuity playbooks.

The organisations pulling ahead learn from every failure, not only their own but also the experiences of others, through information-sharing groups, insurers' claims patterns and the publicly documented post-mortems of others' disasters. The differentiator is whether they trace incidents back to the decisions that permitted them and change their budgets, architecture and process accordingly.

Assume failure

Resilience failures rarely begin with a sophisticated, never-before-seen technique: almost always, it is a misconfiguration, an unpatched vulnerability, an overlooked control or incomplete security coverage that materially enables an intrusion.[27]

Figure 13. Bad intentions
Root causes of organisation breaches (% of all breached organisations)



Source: IBM (2026)[28]

26 BBC, "Reckitt Benckiser warns of permanent sales hit from cyber-attack", July 2017: https://www.bbc.co.uk/news/business-40517105
27 Palo Alto Networks, "2026 Unit 42 global incident response report", February 2026 : https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report
28 IBM, "Cost of a data breach report 2025", 2025: https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai

The paradox is that the vulnerabilities are often familiar, and the remedies well understood. "It is a combination of some real basic stuff—the hygiene stuff that we're extremely disciplined on—and then being very connected with what's happening, since it's an evolving landscape," explains Mr Richardson.

Resilience requires rehearsal, which gives organisations the confidence to move faster: adopting new technologies, meeting customer and regulatory expectations, and spending less time recovering from failures. Rehearsal builds that confidence more cheaply than real incidents.

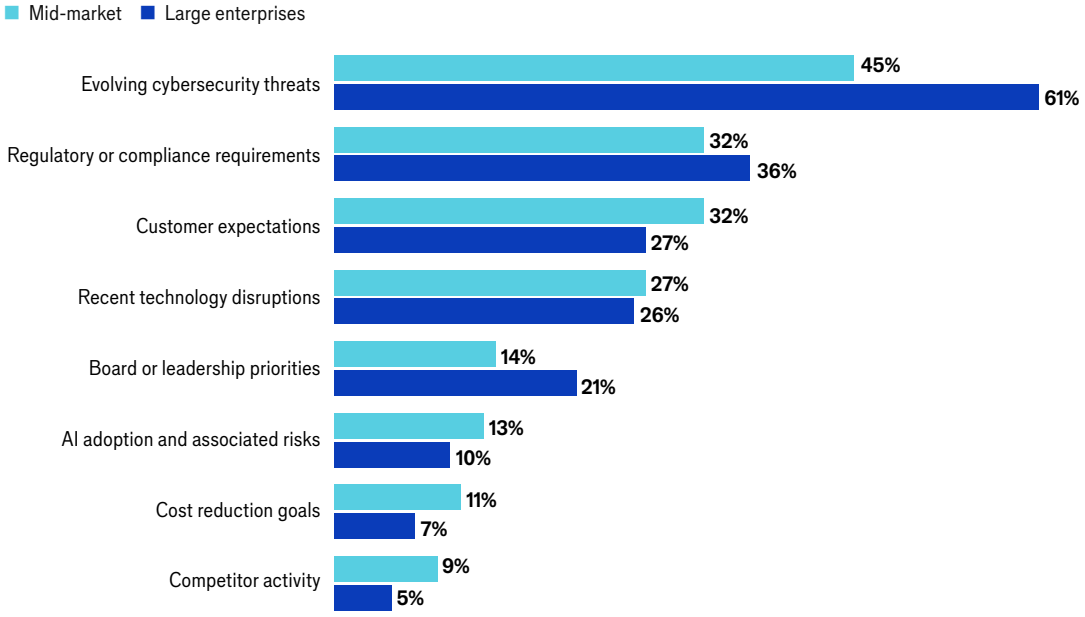
Leadership is unglamorous, adding well-known best-practice controls into system design upfront: "basic chopping wood", as Mr Wenkoff describes it, which, "if you're operating at scale, is critical." For mid-market firms, that goes to the fundamentals: "multi-factor authentication, single sign-on: do you have those in place, and are you holding your employees responsible?", points out AXA XL's Mr Waters. "Sometimes it's a simple thing, particularly on the low end, that becomes more relevant."

Controls still need to be tested before disruption strikes. Mr Richardson advises tabletop exercises, which "allow people to actually experience what would happen in a relatively safe space, where you can stop, ask questions and think through how you'd actually enact the playbook if the worst happened." Tested incident-response plans are among the most effective cost-reduction measures during a data breach, saving firms an average of US$1.49m in 2023.[29]

Increasingly, resilience is being demanded from outside. Compliance requirements and customer expectations rank as the second and third most common drivers of investment in resilience measures, behind only threat response (Figure 14).

Figure 14. Driving resilience

Responses to survey question 'What most commonly drives investment decisions related to keeping your systems secure and operational at your organisation?' (large vs medium organisations)



Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

29 Forbes, "How a security incident response plan saves money in case of a cyberattack", February 2025: "https://www.forbes.com/councils/forbestechcouncil/2025/02/21/how-a-security-incident-response-plan-saves-money-in-case-of-a-cyberattack/

> "There's some real basics: making sure you've got trusted backups, and they're immutable; making sure you've got a good restoration process, and you're testing that you can restore; and then actually running regular full disaster recovery processes. Nothing new there, but having the discipline to make sure those are in place is a really, really important thing."
>
> **Nigel Richardson**, chief information and digitisation officer at Reckitt

That reflects a tightening regulatory environment, especially for sectors where operational failure carries significant human consequences. Ninety-four percent of financial services firms, which are also facing mandated responsibility for their third-party relationships,[30] rate regulatory reporting to be critically or very dependent on technology resilience. For healthcare, 63% believe reporting to be of critical importance for Health Insurance Portability and Accountability Act (HIPAA) compliance. "The leaders are the ones that handle sensitive customer data: healthcare, financial services, software and tech companies," notes Mr Waters. "I do think they are ahead of the curve, frankly, because they have to be."

Insurers are becoming more selective about the risks they are prepared to absorb as cyber threats become more costly and complex.[31] Underwriters increasingly want proof of testing and controls before they write a policy at all, a high bar that more and more organisations are willing to meet: roughly 60-70% of large corporates and 40-50% of mid-market firms carry cyber insurance as of early 2026.[32] "To see [the share of mid-market firms buying cyber insurance] at 50% indicates that there is a shift. And I think it's a positive signal," says Mr Waters.

External scrutiny, in other words, is converging on the same question the best-run organisations already ask themselves: has anyone actually tested the plan?

A champion with clout

"In the end, who's accountable?", asks Mr Menon. "I think in most enterprises that's very clear: it's the CIO and the CISO"—with CISOs increasingly owning cybersecurity strategy, governance and risk management.[33] The harder part, he explains, is that accountability cannot sit with security leaders alone as technology spreads into every function. Resilience becomes a shared responsibility across the business, achieved with a "balance between a degree of control and standardization against the ability to move quickly, which is where the functional areas want to go." That balance matters beyond governance: resilience is increasingly judged on the competitive advantage the business keeps, or gains, as conditions change.[34]

The broader resilience becomes as a business responsibility, the greater the need for clear accountability. Resilience now depends on coordinated action across technology, legal, compliance, finance, HR and operations, making explicit answerability more—not less—of a requirement for both business leaders and boards.[35]

30 Financial Industry Regulatory Authority, "2026 FINRA annual regulatory oversight report: Third-party risk landscape", December 2025: https://www.finra.org/rules-guidance/guidance/reports/2026-finra-annual-regulatory-oversight-report/third-party-risk
31 Reuters, "Cybersecurity costs will shrink AI's profit boost", July 2026: https://www.reuters.com/commentary/breakingviews/cybersecurity-costs-will-shrink-ais-profit-boost-2026-07-14/
32 American Academy of Actuaries, "Cyber Insurance Nears an Inflection Point", February 2026: https://actuary.org/article/cyber-insurance-nears-an-inflection-point/
33 Deloitte, "2026 NASCIO-Deloitte cybersecurity study", April 2026: https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/2026-nascio-deloitte-cybersecurity-study.htm
34 McKinsey & Company, "McKinsey on Risk & Resilience, Number 21", March 2026: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/mckinsey-on-risk
35 National Association of Corporate Directors (NACD), "Principle three: Establish board oversight structures and access to expertise", April 2026: https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/2026-cyber-risk-oversight/cyber-risk-handbook-principles-2026/principle-3-establish-board-oversight-structures-and-access-to-expertise/

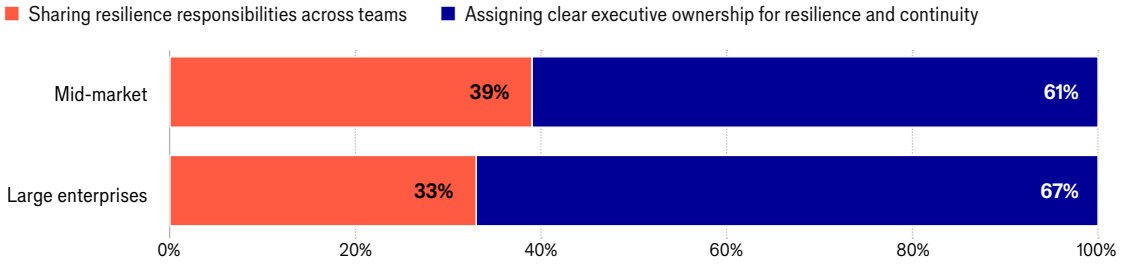
Organisations are moving in the right direction, prioritising assigning clear executive ownership over distributing responsibility more broadly (Figure 15).

Board-level engagement is a differentiator for resilience maturity among larger organisations. "The board members typically sit on other companies' boards too, so they bring outside experience, which is actually really helpful," highlights Mr Richardson. At Reckitt, that perspective feeds into a more structured governance model, with the company strengthening oversight "at every level—board, audit committee, global executive committee—from KPI reporting to make sure we've got the right initiatives in place," alongside strong commitment to funding and resources.

Learned, assumed, owned: the habits are unremarkable individually. What makes them a differentiator is that so few organisations maintain all three.

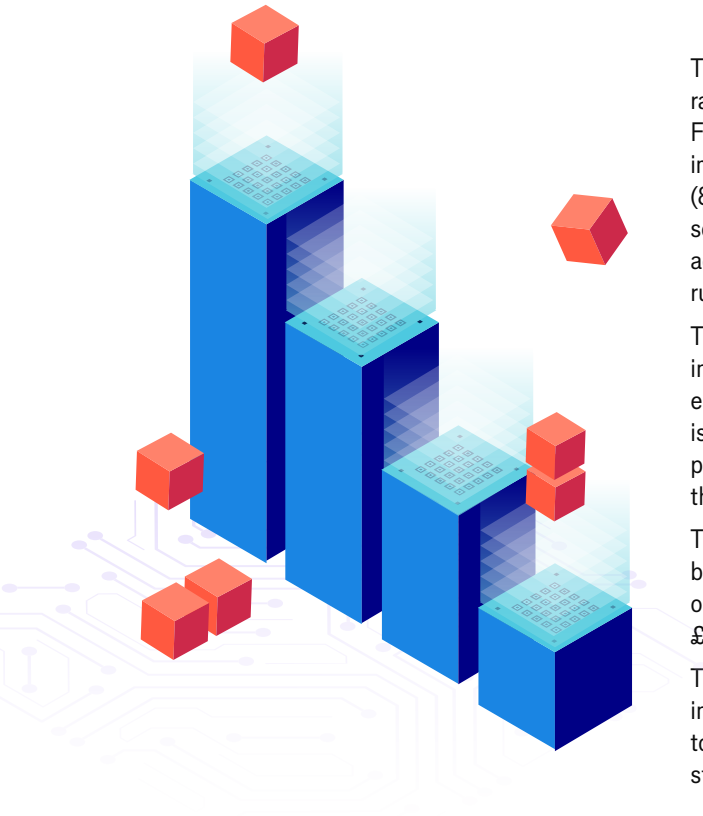
Figure 15. Resilience across the board

Responses to survey question 'Which option does your organisation prioritise more?' (large vs medium organisations)



Source: Economist Enterprise *'Technology Resilience Index'* survey (2026)

Conclusion



The returns on resilience are more than avoided cost. Across sectors, executives rate it as important to client trust and retention more than 80% of the time. Financial services firms flag client retention during market stress as very or critically important 87% of the time. Retailers say the same of customer and brand loyalty (87%), healthcare providers of patient retention and trust (86%), and professional services firms of client work quality and accuracy (96%). "Resilience is a competitive advantage as it fosters trustworthiness: our customers depend on us to be up and running and to be open," concludes Mr Wenkoff.

The outage example that opened this whitepaper took down dozens of services in minutes, from a single point none of the affected companies controlled. In an economy built on deep interconnection, failure travels further and faster than what is immediately visible. No organisation is invincible. Whoever finds their own weak points first will be the one to keep market confidence and to seize the opportunities that ever-present technology disruption creates.

The stakes of resilience became tangible for M&S and Co-op: both were breached by the same attacker using the same tactic within days of each other, but only one had rehearsed. Fifteen weeks and £300m separated them from a month and £80m, all due to how quickly each could adapt once disruption hit.

The organisations that build resilience through better visibility, resilient infrastructure, trusted partners and disciplined operational practices are positioned to recover fast, and to keep innovating, competing and growing while others are still catching up.

ECONOMIST ENTERPRISE

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

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

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

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