REPORT

The Ripple Effect: A Hallmark of Resilient Cybersecurity

How to Absorb the Shock of External Forces

zscaler

THE
RESILIENCE
FACTOR

Contents

About our Survey

In December 2025, Zscaler commissioned Sapio Research to conduct a survey of 1,750 IT leaders and business decision-makers across 14 markets (United States, United Kingdom & Ireland, Germany, France, Italy, Spain, Netherlands, Sweden, Australia, India, Japan, Singapore, UAE, and Saudi Arabia). These IT leaders work at companies with 500+ employees and across industries.

Introduction

Organizations continue to face relentless pressure to adapt and innovate amid constant disruption on multiple fronts. The surge in AI-fueled cyberattacks, coupled with emerging risks from agentic AI and quantum computing pose new security challenges. At the same time, market volatility, data sovereignty demands, regulatory shifts, and geopolitical tensions continue to test business agility and continuity. Added to this, enterprises are often overwhelmed by a rapidly expanding hybrid user base and increasingly complex supply chain. Clearly, there's an urgent need for strengthened resilience — not simply as a reaction to disruption, but as a design principle that ensures companies can mitigate the impact of these external forces.

In December 2025, Zscaler commissioned a survey of 1,750 IT leaders across 14 markets to understand how (and if) organizations are tackling these external challenges to resilience. At first glance, the findings seem positive: there is active engagement and investment in cyber resilience strategies, and broad business confidence in how effective these strategies are. However, a look beneath the surface reveals a stark reality: critical gaps remain, with business confidence reflecting perceived internal control rather than true preparedness for external disruption. Our findings revealed a widespread tendency toward reaction rather than proactive planning for emerging risks, growing ecosystems, and market volatility.

The bigger picture suggests that many resilience strategies — and the confidence behind them — rest on shaky foundations because they are built primarily on inward-facing assumptions of control. By focusing inward in this way, organizations risk overlooking external forces that can send shockwaves through their operations: especially considering failures increasingly originate within ecosystems, from partners, and in shared digital infrastructure. In an interconnected world, true resilience must ripple outward across dependency layers such as power, connectivity, identity, platforms, and supply chains, absorbing disruptions quickly to safeguard continuity. By taking a Resilient by Design approach, enterprises can embed the capacity to absorb and dampen external shocks, rather than simply respond to isolated incidents. This helps stabilize operations, enabling quicker recovery after disruption.

Why Read This Report?

Business and Technology Leaders

Tackle costly resilience complacency
Organizations feel confident in their resilience investments, yet a majority believe strategies are too inward-looking, leaving them exposed to external technology risks, ecosystem dependencies, and market volatility. This report pinpoints the resilience gaps where change can be most impactful.

Zscaler survey intelligence helps you:

- Understand the external shockwaves most likely to disrupt your operations
- Identify the overlooked areas weakening your current resilience posture
- Build outward-facing strategies that protect continuity beyond your own walls
- Convert resilience investment into business stability and agility

Networking and Security Teams

Strengthen your company's defensive posture
Shadow AI, rising architectural complexity, and uncertainty around the risk of cutting-edge technologies — teams cite these as barriers to visibility, weakening organizational resilience. By seeing where peers struggle or excel, you can apply those learnings to stay proactive.

Zscaler survey intelligence helps you:

- Prepare for the risks that emerging technology brings
- Reduce exposure from partners, contractors, and shared digital infrastructure
- Modernize legacy-bound environments to accelerate response and recovery
- Shift from reactive adaptation to proactive, test-driven resilience

Key Findings

OPERATIONAL ECOSYSTEM

Rising interdependence, rising exposure

68% report a higher reliance on contractors and third parties than ever before

Yet adoption of necessary third-party risk-control measures is below **50%**

EMERGING RISKS

AI and quantum push the limits of preparedness

52% agree their organization's security systems can't defend against current advanced threats, let alone emerging threats

Unsurprisingly, **57%** haven't factored post-quantum cryptography (PQC) into their overall IT strategy or within their cybersecurity strategy, and **50%** of those deploying or testing agentic AI have done so without the necessary governance guardrails

MARKET IMPACT

Volatility forces reactivity

74% agree that the current macroenvironment is forcing quick operational — and therefore IT — pivots

RESILIENCE STRATEGY

Perceived control means more risk from overlooked external threats

In the last 12 months, **9 OUT OF 10** increased their cyber resilience investment, with **96%** updating their cyber resilience strategy in response to external factors

Despite this, **61%** of IT leaders worldwide admit their resilience strategies remain too inward-looking

Resilience Measures

Can We Ever Be Completely Confident?

Defining cyber resilience

Zscaler defines it as an organization's ability to maintain operational continuity when responding to and containing an incident within its systems or networks.

Defining the Ripple Effect

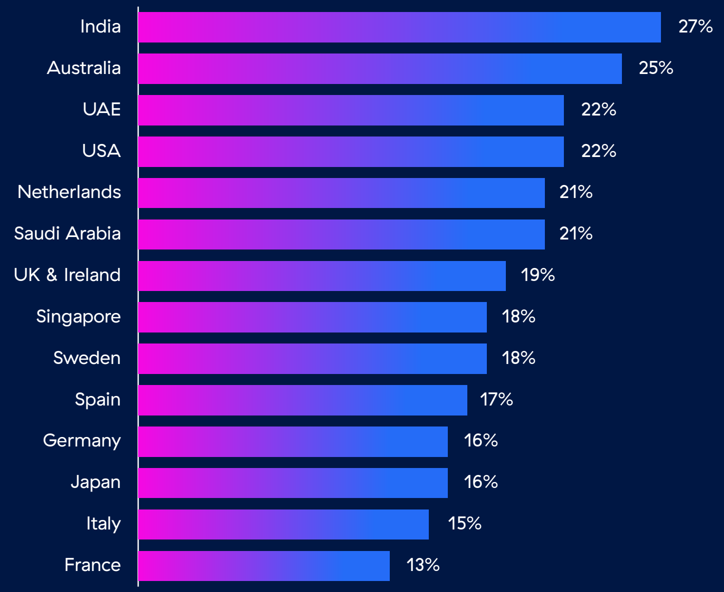
A robust foundation of cyber resilience creates positive outward ripples that can absorb the shockwaves of external threats. Like a stone dropped in water, the strength and reach of a company's protective ripples depend on how intentionally resilience is built into their way of working. This is why enterprises can only experience the Ripple Effect through a Resilient by Design approach.

From blackouts paralyzing parts of southern Europe to cyberattacks halting manufacturing lines for weeks, last year's headlines made one thing clear: we're living in a "when, not if" reality of major failure scenarios. Cyberattacks, extreme weather, supply chain breakdowns, macroeconomic turbulence, human error, and even sabotage can trigger widespread consequences on a digital ecosystem without warning. And with this comes a hard truth: the digital backbone of modern business is alarmingly fragile.

Against this backdrop, organizations have shown visible commitment to strengthening their cyber resilience over the past year. Nearly all respondents (96%) updated their cyber resilience strategy in the past 12 months in response to external factors such as evolving data sovereignty requirements and sector-specific regulations. In addition, 90% increased their investment (by an average of 19%) to reinforce continuity in the face of mounting disruption. Echoing a trend in our previous research, our latest findings show cyber resilience investments continue to grow. Organizations still feel confident that current resilience measures will help maintain business continuity through a variety of incidents and disruptions.

REGIONAL GROWTH IN RESILIENCE INVESTMENTS

Average % increase in cyber resilience investment over the last 12 months:



There will always be some level of risk and uncertainty from external factors beyond our control.

But confidence should never be absolute, because there will always be some level of risk and uncertainty from external factors beyond our control. This underpins the very need for resilience: preparing for the unknown is an acknowledgement of the inevitability of disruption. Despite this, a majority (61%) of IT leaders worldwide admit their resilience strategies remain too inward-looking. And our findings show that this narrow field of view is leaving dangerous gaps. For instance, many organizations aren't factoring in emerging technology risks or sprawling supply chains. The result is a resilience posture that is still more reactive than proactive, undermining the very confidence leaders express.

Operational Ecosystem

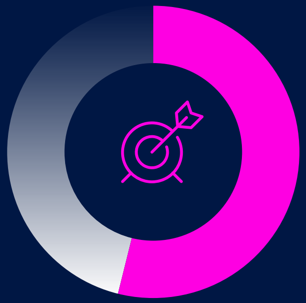
Rising Interdependence, Rising Exposure

The disconnect between confidence and action is most apparent when examining resilient approaches to the operational ecosystem. Two-thirds (65%) of IT leaders agree that the macroenvironment is driving significant volatility in their supply chains, and 68% report a higher reliance on contractors and third parties than ever before. Despite this, only four in 10 have updated their cyber resilience strategy to address rising supply chain instability, and less than half have done so in response to increased third-party reliance. In fact, only 42% say their cyber resilience strategy explicitly includes contractors and gig workers. Perceptions of effectiveness also reveal nuance. While eight in 10 IT leaders believe their resilience measures address security requirements introduced by supply chain volatility, only 34% are “highly” confident in this.

Failure to act on this perceived supply chain risk persists even though 60% of surveyed businesses have already experienced a significant failure caused by a supplier or third-party vendor in the past year. And this is despite the fact that 63% expect a similar incident within the next 12 months.

46% under-insured and over-exposed

The financial and operational consequences of a supplier-related breach are compounded by limited insurance coverage: only **54%** report that their cyber insurance covers third-party compromise.



THIRD-PARTY EXPOSURE

Failure scenarios at suppliers or third-party vendors can cascade into the digital estates of the organizations that depend on them. How worried are businesses about the frequency of this exposure? European respondents typically expect fewer failure scenarios than their peers in the United States and those in APJ countries. Reduced reliance on third-party suppliers or the introduction of a stronger, comprehensive set of security controls would strengthen confidence in resilience strategy. However, with findings pointing to growing third-party reliance and low adoption of sufficient security controls, confidence levels seem more like misplaced optimism.

Third-party risk control includes measures such as segmentation, data encryption or partitioning, and always-on AI monitoring of vendor endpoints for suspicious behavior. Across various controls, adoption is below 50% for every single measure — and, on average, organizations only have three risk control measures in place, which isn’t sufficient for the growing number and severity of risks. Frequent risk assessments are an important control measure, giving enterprises visibility into vulnerability. Yet, assessments of supply chain cyber resilience are only conducted quarterly (or less frequently) by 45% of businesses, with some respondents indicating they’ve never conducted one at all. In an environment defined by interdependence, this lack of ongoing monitoring signals poor preparedness and low resilience.

	REALITY	EXPECTATION
	% that have already faced a major third-party failure in the past year	% expecting a major third-party failure in the next six months
India	81%	**81%**
USA	74%	**75%**
Saudi Arabia	68%	**62%**
Australia	62%	**61%**
Netherlands	60%	**53%**
UAE	60%	**61%**
Germany	59%	**62%**
Spain	57%	**54%**
Italy	55%	**69%**
Japan	55%	**57%**
Singapore	55%	**63%**
UK & Ireland	53%	**61%**
France	47%	**57%**
Sweden	47%	**52%**

Emerging Risks

AI and Quantum Push the Limits of Preparedness

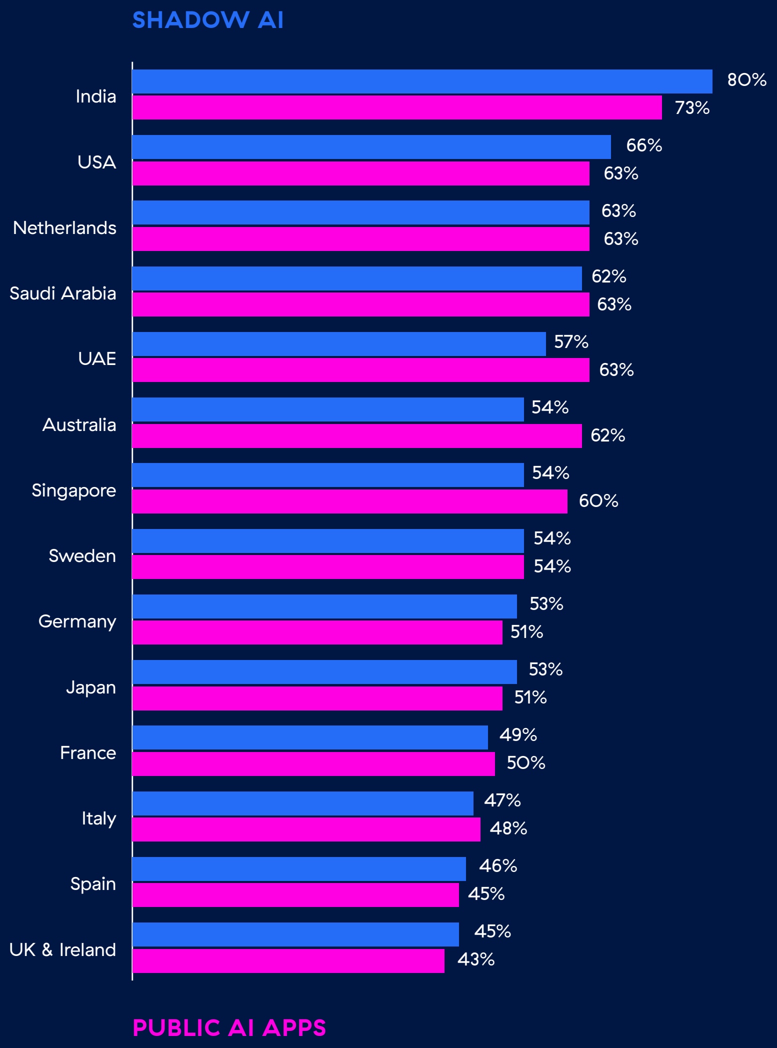
There are new risks associated with emerging technology that many aren't prepared for — from agentic AI systems capable of orchestrating multi-step intrusions at scale, to 'harvest-now, decrypt-later' threats posed by future quantum computers. And they're exposing just how limited inward-focused resilience strategies really are. It's something businesses struggle with, as a majority acknowledge their current security measures are unable to defend against existing advanced threats, let alone these new risks.

On the AI front, policy and control adoption lag behind risk exposure. Only 62% of organizations have updated policies to address AI-generated threats, and just 56% have categorized data to prevent loss via AI tools. With data management at the heart of AI vulnerabilities — and data lineage increasingly demanded by regulators — 60% of IT leaders admit they struggle to trace how and why data moves through parts of their network. The reason? It's largely due to architectural complexity. Poor visibility into application use raises another red flag for data security: seven in 10 respondents indicate they have limited visibility over their employees' use of shadow AI. This is a concern considering 56% agree that this is likely exposing sensitive data.

> "For third-party risk mitigation, least-information design is increasingly thought of as best practice, yet only 27% of organizations have implemented it universally. Most companies instead continue to overshare, granting third parties far more data access than is necessary. An alternative approach is zero-knowledge proof, which avoids sharing the data itself. Here, companies retain the information and provide third parties with the outcome or validation the data would have produced to minimize exposure while enabling collaboration."
>
> TONY FERGUSSON, CISO IN RESIDENCE, EMEA

SENSITIVE DATA EXPOSURE

Regional view showing % of IT leaders who acknowledge likely exposure of sensitive company data through employee use of unsanctioned 'shadow' AI or public AI applications.



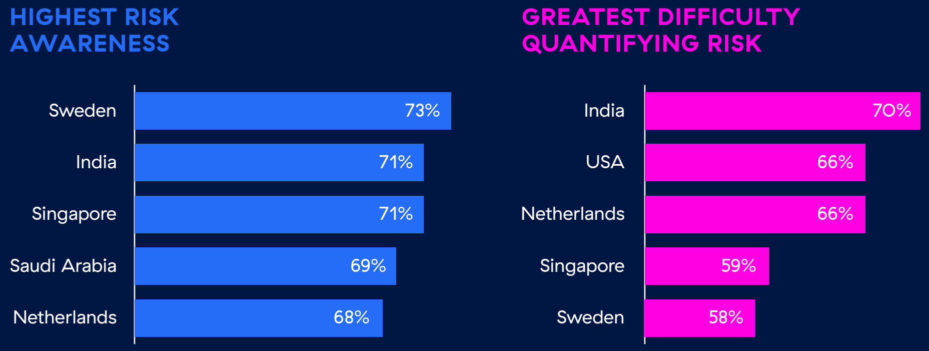
Representing far more than a data risk, agentic AI adoption is scaling quickly: 42% of organizations are testing agentic AI and 34% have already deployed it in some (likely small) guise. However, half of those have done so without firm governance in place, and only 63% have pre-emptively embedded agentic AI into their cyber resilience strategy. In other words, the adoption curve of emerging technology is outpacing the guardrails.

Quantum risk sits on a similar fault line between awareness and action. Most enterprises recognize the danger it might pose, yet many still struggle to quantify their vulnerability in current cryptographic systems. Awareness alone can't drive action if an organization doesn't know where it's most exposed, making it harder to prioritize resilience investments.

Across regions, 55% admit difficulty gauging exactly what risk quantum has on their existing cryptography but still believe it will have a tangible effect. In fact, six in 10 say that today's stolen data could pose a material risk to their future business, even if it's only decrypted years down the line when quantum computers become widely available. The credible threat may be years away, but the time for proactive measures is now, and that's what PQC enables. With 2026 widely viewed as a tipping point for quantum preparedness, the window for proactive mitigation is narrowing — a concern given that 57% of organizations haven't yet factored PQC into their security strategy.

TOP 5: QUANTUM INSIGHT

A regional overview showing which markets have the highest awareness of this technology's risk and the greatest difficulty quantifying the risk it poses.



HIGHEST RISK AWARENESS

GREATEST DIFFICULTY QUANTIFYING RISK

> "Most businesses think they have a solid cyber strategy but are actually experiencing 'the watermelon effect': seeing only the 'safe green' outer layer, not the 'red risk' beneath. Slow-moving security frameworks coupled with reactive investment seem good on the surface. But scratch below and you see 'red' because emerging risks are overlooked. Agentic AI shows how quickly this can happen: one of the biggest risks tied to its adoption is the rise of Shadow AI. Vendors racing for competitive advantage are incorporating agentic capabilities at speed. This drives development towards AI-generated scripting or vibe coding that exploits this too-fast deployment — long before the necessary checks are in place for secure rollout. This scenario exposes the ongoing gap between business development and security practices: 'secure by design' remains out of reach for many, including those who believed they had already achieved it. The watermelon effect persists because organizations continue to operate on outdated assumptions while external risks evolve faster than their frameworks and procurement cycles."

MARTYN DITCHBURN,
CTO IN RESIDENCE AT ZSCALER

Market Impact

Volatility, Sovereignty, and Continued Reactivity

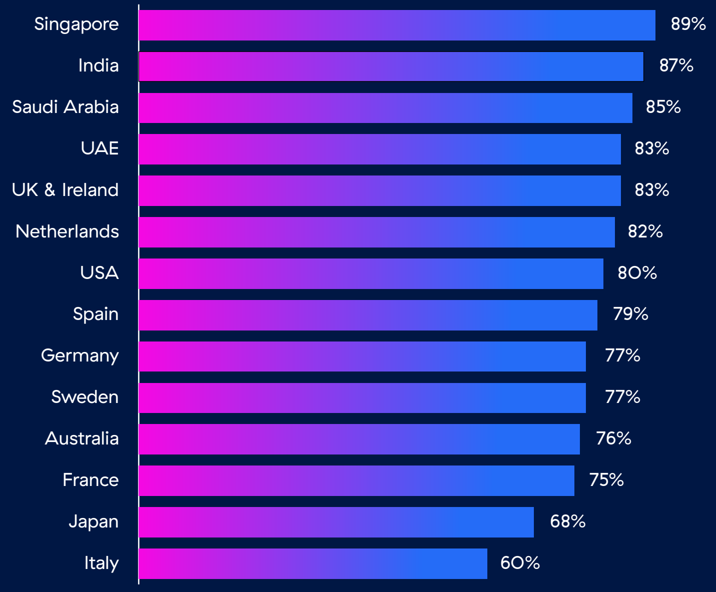
Volatile market forces amplify the shockwaves of emerging technology risks. This is a sentiment shared by 74% of IT leaders, who agree the current macroenvironment is forcing quick operational — and therefore IT — pivots. And there is evidence of slightly more action on resilience strategies to account for this:

- **92% now conduct scenario planning and tabletop exercises for market-driven disruptions** (up from 86% in 2025), with half of them doing so quarterly and 23% monthly.
- **Beyond exercises, resilience plans increasingly include regulatory compliance tracking** (71%), data localization strategies (69%), and multi-region cloud failover (58%).
- **Time-to-rebuild calculations are also becoming more routine**, with 45% of organizations running them in the past six months and 87% in the past year.

External pressures are clearly galvanizing action on one key priority: data sovereignty. Foreign technology dependency is impacting discussions around sovereignty policies and regulations. Dependencies on foreign technology providers has and will continue to increase focus on control over own data, infrastructure, and operations. Our survey shows IT leaders are actively mitigating this risk: 79% are evaluating their dependency on foreign-technology, while six in 10 have updated their cyber resilience strategy in the past year to comply with new or evolving sovereignty demands.

TECHNOLOGY DEPENDENCY DELIBERATIONS

% of organizations that are evaluating the risk of technology dependency:



> "Data sovereignty concerns are already reshaping digital agendas, with 83% of surveyed business leaders affirming its growing role in operational resilience planning, and 73% citing it as the reason behind decisions to delay or cancel initiatives. These findings echo what we've heard in recent discussions with policymakers and business leaders: digital sovereignty is no longer theoretical; it's an operational reality. Translating it into practical action remains complex. We need to think of it as a marathon rather than a sprint. And that doesn't mean stalling digital efforts — enterprises must find a way to innovate while safeguarding autonomy and security. Postponing modernization, especially in cybersecurity, only amplifies risk as threat levels surge. To remain resilient, competitive, and compliant in an increasingly unstable digital world, organizations must act decisively, balancing innovation with sovereignty rather than succumbing to paralysis."

CASPER KLYNGE, HEAD OF GOVERNMENT PARTNERSHIPS AND PUBLIC POLICY, EMEA

While the above findings show some pockets of progress toward stronger resilience, much of this activity remains reactive: it's calibrated in response to recent incidents rather than in anticipation of the next.

Architectural Agility

The Missing Link

To best navigate market impacts, evolving operational ecosystems, and emerging technology risks, specific security actions are required. The underlying imperative behind these actions? To pursue architectural agility and outward-facing controls that enable rapid adaptation.

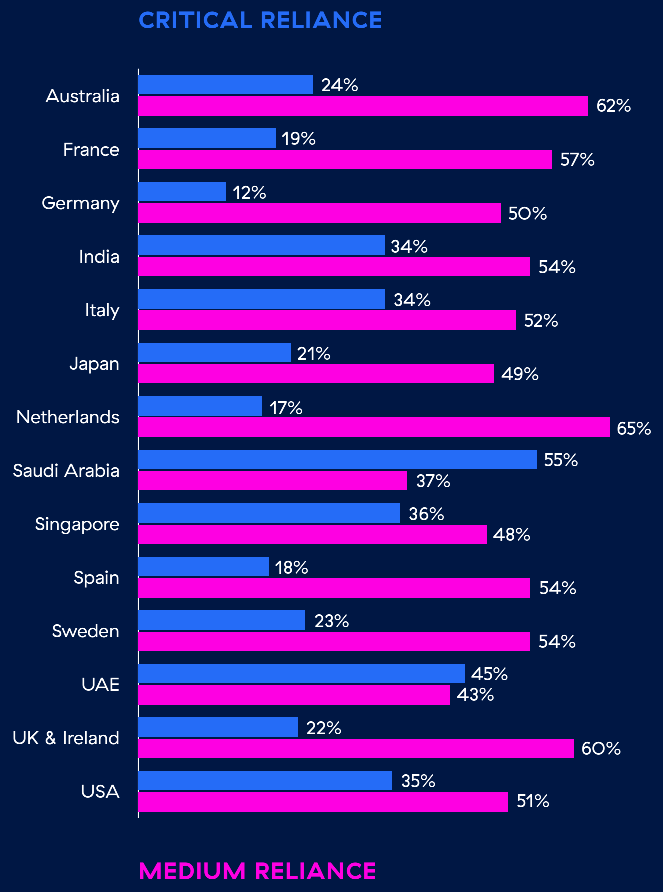
However, 81% of enterprises still report a critical or medium reliance on legacy systems. In addition, network resilience has been pieced together additively (52%) or built in service-specific layers (38%), risking uneven protection and operational complexity. Meanwhile, technologies such as micro-virtualization, sandboxing, and air-gapped systems that would shield assets are deployed universally by no more than a third of organizations. It's no surprise, then, that 64% of IT leaders say their current infrastructure impedes effective response to failures like data breaches and system outages, while 59% admit their architecture cannot keep pace with the speed of business change, let alone support their growth agendas.

> "Resilience can only be proven by testing. Many companies assume they're secure because they've never looked deeply enough. External stressors like quantum disruption, AI innovation, and supplier interdependence demand a new mindset: we need to simulate and stress-test to truly uncover the iceberg beneath the surface. Exercises such as chaos engineering, AI red teaming, and breach attack simulations help organizations understand how mature and resilient their systems are, what risks these systems create, and whether current security measures are effective. Last year, a common behavior we witnessed was businesses simply waiting to be hit by a cyber failure before implementing new measures to plug the security gaps. This must change; 2026 must be about proactive resilience."

TONY FERGUSSON, CISO IN RESIDENCE, EMEA

MODERNIZATION IMPERATIVE

% of organizations that still have critical or medium reliance on legacy systems, potentially jeopardizing resilience efforts.



Taken together, our survey findings highlight the resilience problem businesses currently face: ripple effects aren't far-reaching enough, and this lost momentum exposes organizations to interconnected threats. While organizations are investing time and budget in resilience, strategies remain misaligned with the external realities of an interconnected, volatile world. The question now is where IT leaders should course correct: locking down supply chain exposure, getting ahead of emerging technology risks, and shifting from reactive adaptation to proactive preparedness for market volatility.

The Case for Extending Your 'Resilient by Design' Approach

Last year, we made the case for taking a Resilient by Design approach to your systems, processes, and people. This year, we're helping you connect that resilient foundation to the broader interconnected environment you're operating within, where external forces can disrupt operations faster than most organizations can respond. Extending a Resilient by Design approach beyond the walls of the enterprise ensures that internal strength translates into external stability: the protection your resilient foundation offers must ripple outward, able to absorb shocks resulting from supply chains, partner ecosystems, regulatory regimes, and technology stacks.

This outward–facing stance delivers business benefits that go beyond risk reduction:

Continuity you can count on: Interdependencies are mapped and protected, reducing cascading failures and shortening recovery windows.

Operational agility: Architecture and controls anticipate and adapt to external change (e.g., sovereignty, market volatility) without halting innovation.

Cost control and efficiency: Fewer incidents, faster recovery, and targeted investments reduce total cost of resilience.

Competitive advantage: Customers, regulators, and partners reward organizations that can withstand disruption without compromising service or security.

Trust and assurance: Confidence in the integrity and location of data, the provenance of AI, and the resilience of digital services strengthens stakeholder relationships.

The Resilient by Design approach is a compelling package: one that helps businesses anticipate, withstand, and confidently recover from internal and external challenges to business continuity.

Expand Resilience By Design

3 Recommended Actions

For those looking to better prepare for the unexpected but inevitable shocks of external forces, here are three actions to positively expand the Ripple Effect of your organization's resilience posture with a Resilient by Design approach.

1 PRIORITIZE VISIBILITY

Embed proactive risk hunting, everywhere

Visibility is the foundation of proactive security. Many emerging technology risks sit below the board-level radar for years, leaving companies unprepared when adoption suddenly accelerates. Without visibility into board-level plans, security teams can't educate the business, shape investment decisions, or prevent shadow usage when teams adopt new tools on their own. The gap widens when industry frameworks lag behind technology: they're valuable, but they represent a moment in time. Relying on them alone means you only see what's codified, not what's coming. In a world defined by interdependence, visibility must reach beyond internal systems and checks to the external forces shaping your operational risk. True visibility requires staying close to the bleeding edge and embedding security thinking inside the business through cross-functional collaboration.

Visibility also starts with understanding your data universe. Most companies only see the "tip of the iceberg" when assessing risk, unaware of how much sensitive data is being shared with cloud tools, AI models, or partners. When organizations switch on AI activity reporting or data-flow insights, they often discover far more exposure than expected. Moving from reactive threat hunting to proactive risk hunting means knowing where data travels, how it's used, and who it's shared with across an expanding ecosystem. With this clarity, businesses can enforce better practices and build guardrails before risks escalate.

But visibility can't stop at your own boundaries. As more functions shift to third-party providers, your risk surface becomes tied to their practices as much as your own. Traditional assurance methods — framework reports, compliance attestations — can give a false sense of security when missing risks from new technologies aren't immediately captured in standards. This creates a compounded gap: if neither you nor your vendors are tracking emerging technology risks, exposure grows silently. Gaining full visibility means following your data everywhere — across internal systems, external partners, and the entire supply chain that now carries your information.

Businesses are good at securing data;
it's the 'everywhere' part that's tripping them up.

2 ZOOM OUT

Make architectural pivots manageable

Many organizations rush straight into micro segmentation (an admirable end state) but skip the foundational macro segmentation that does still limit the blast radius. The guidance? Don't let perfection be the enemy of the good: teams often freeze when they can't do micro segmentation everywhere on day one, when the pragmatic move is to start with macro segmentation and work inward. The goal should be to prioritize agility. You need the ability to respond quickly to fast-changing external factors, from risks introduced by agentic AI to geopolitically driven data-sovereignty shifts. You also need the ability to act quickly on opportunities that external forces may present: for instance, the business growth that agentic automation can unlock when risk is managed. Either way, the level of responsiveness depends on architectures that can flex and adapt without breaking. In interconnected environments, this flexibility is critical. It enables organizations to pivot not just internally, but also in response to disruptions across the external ecosystem they rely on. This is exactly where platform design matters: it simplifies, to remove the barriers that stand in the way of rapid adaptation.

Complexity is a major barrier to agility, especially in tightly coupled environments where every system, component, or service is closely linked. When one piece changes, the whole system is at risk of breaking. It's this kind of brittle set-up that Zscaler is designed to address.

Our approach is different: a highly aligned, loosely coupled overlay that sits above the underlay rather than being bound to it. This design future-proofs organizations regardless of who provides the underlying infrastructure. The resulting decoupling delivers real operational agility, giving enterprises the unencumbered speed they need to adapt to change. Technology should be an enabler, not a barrier.

Agility is the key to organizational resilience. Faced with emerging risks, a flexible platform that supports quick moves across a connected ecosystem is crucial. Take quantum for example: for many organizations, this threat may feel distant, but the risk is real because data can be captured now and decrypted later. The priority today is gaining visibility into vulnerable ciphers through inline inspection, which helps trigger board-level discussions and timely investment. From there, segmentation and posture management provide practical guardrails to reduce exposure. As future platform capabilities mature, these foundations put you in a strong position to scale your defenses. Also consider the impact of geopolitics: you may need to move data across jurisdictions at speed. Sustaining resilience in these scenarios requires the same principle: a simplified, platform-by-design approach that allows you to pivot wherever disruption emerges, not just inside your own walls.

3 BUILD UP

Future proofing is an evolution, not a leap

If organizations have already made the transformational pivot to platform architecture, they're generally well equipped for future-proofing — they just may not realize that the next step is often evolutionary, even when the problem feels revolutionary.

AI provides a clear example: predictive and generative models are still fundamentally questions about Data Loss Protection (DLP), something Zscaler has long mastered. And while agentic models seem revolutionary to businesses, Zscaler's security approach is, ultimately, an evolution of DLP strategy, where we treat AI like a user. This means the foundation of DLP is strengthened by rooting it in user security: you issue agentic AI an identity, establish a behavior baseline for it, and then look for anomalies. This process, known as User and Entity Behavior Analytics (UEBA), is an effective application of Zero Trust principles because it helps reduce lateral movement by segmenting the agent from resources it should not be interacting with. The evolution reflects the new complexity introduced by agentic systems that security teams must now consider.

You need to leverage the power of a platform to build up your maturity with new features as they are required. This kind of levelling up demands the strong foundation of a solid architecture, such as the one that the Zscaler Zero Trust Exchange (ZTE) provides. ZTE is a robust foundation with hyperscaler capabilities that give enterprises the ability to grow at scale through fast-to-market geographic expansion. It doesn't just future-proof your internal environment — it gives you the consistency and interoperability needed to extend resilience across the partners, platforms, and shared infrastructure you now rely on. In a world where resilience failures often originate outside your own organization, that outward-facing readiness is what turns a solid foundation into true resilience by design.

"As traditional, network-centric architectures falter under the weight of hybrid work and cloud sprawl, enterprises are accelerating Zero Trust adoption. Yet many remain under-adopted, leaving critical gaps in resilience and exposing their operations to escalating risk. While Zscaler has long invested in securing users, workloads, IoT, and partners, the real differentiator is the power of our platform. The Zscaler Zero Trust Exchange acts as an intelligent switchboard, delivering secure, direct-to-app connectivity anywhere. The beauty of this platform lies in the fact that it decouples security from the network to simplify complexity, reduce costs, and enable rapid adoption at scale. This platform-first approach doesn't just strengthen security: it drives agility and efficiency, helping organizations move faster toward a modern, risk-aware posture. This is the very definition of being Resilient by Design."

MARTYN DITCHBURN,
CTO IN RESIDENCE AT ZSCALER

Expand Resilience By Design

3 Ways Zscaler Can Help

Is there a unified solution to help enterprises extend the resilience Ripple Effect? Yes: the Zscaler Zero Trust Exchange (ZTE). This cloud-native security platform helps organizations unlock security, increase agility, and reduce complexity. Result? Businesses save time and cost without sacrificing security or performance.

1

PRIORITIZE VISIBILITY

Visibility is the backbone of proactive risk hunting, and Zscaler delivers it through the ZTE. This single overlay cloud platform powers Data Security, AI Security, and third-party security, giving IT teams insight into how data moves, is used, and interacted with across the ecosystem. While Data Security delivers unified controls for data in motion and at rest, AI Security protects models, agents, and GenAI workflows. But visibility and control can't stop here.

The same ZTE foundation extends into your partner landscape: SaaS Supply Chain Security maps risky app-to-app integrations; Zscaler B2B provides zero-trust access for external partners without internet exposure; and Privileged Remote Access secures contractor and OT/IIoT access without brittle VPNs.

Together, these capabilities deliver end-to-end control across users, apps, clouds, endpoints, AI systems, and third-party connections — the full risk surface modern enterprises depend on.

2

ZOOM OUT

ZTE delivers enterprise agility in this era of inevitable disruption. It decouples security from network infrastructure, enabling secure, identity-based connections without the drag of firewalls, VPNs, or tightly coupled legacy stacks. Organizations can meet data residency and regulatory requirements without sacrificing flexibility, easily reconfiguring markets, supply chains, or data flows as conditions change. Inline inspection happens in memory within local cloud infrastructure, supported by 25 Zscaler data centers across Europe, including options for sovereign or in country logging.

This flexibility continues at the edge with Zero Trust for Branch replacing stack sprawl with a single platform connecting and segmenting branches, campuses, and factories. Lightweight, context aware segmentation limits lateral movement, while control is extended by integrated services like Cellular for instant SIM-driven policy enforcement, IoT Security for device discovery and classification, and more. Together, these capabilities keep the architecture adaptable under pressure — able to re-route, re-segment, and realign quickly as external forces shift.

3

BUILD UP

Future-proofing becomes easier when foundational controls are already centralized, consistent, and extensible. Zscaler provides this evolutionary pathway. Our AI Security builds on unified DLP, behavioral analytics, and segmentation to secure both public AI tools and private enterprise AI stacks from development through deployment. Policies are managed from a single dashboard, helping companies adapt safely as AI use cases expand.

For long-horizon risks, Zscaler Post-Quantum Cryptography Visibility helps IT teams monitor current PQC algorithm use — and assesses whether business devices could support these algorithms in the future if PQC isn't already in use. Even if PQC protections aren't yet enabled, Zscaler can detect what is and isn't PQC-ready by analyzing real network traffic, not just asset inventories. This gives businesses a solid footing for proactive planning. It makes "crypto-agility" an incremental process rather than disruptive overhaul, allowing resilience to evolve step by step into long term readiness.

Unleash The Ripple Effect

Your next move

Being Resilient by Design means protecting not just the systems and operations you directly control, but also preparing for risks that originate outside your organization, so continuity isn't shaken when external dependencies fail. This kind of holistic, outward–facing approach amplifies impact, enabling organizations to withstand disruption and maintain confidence in a volatile world. This is not a new direction but an evolution of resilience thinking that reflects today's reality of cascading risks. To thrive amid certain uncertainty, enterprises must build resilience from the inside out and move from reactive measures to proactive, deliberate action.

Build resilience on a strong foundation so that the protection it offers can ripple outward, reducing the impact of the external shockwaves beyond your control.

READY TO BOOST YOUR RIPPLE EFFECT?

Secure, simplify, and transform your enterprise with Zscaler, the AI security platform built on zero trust.

Schedule a demo

Appendix: Regional Insights

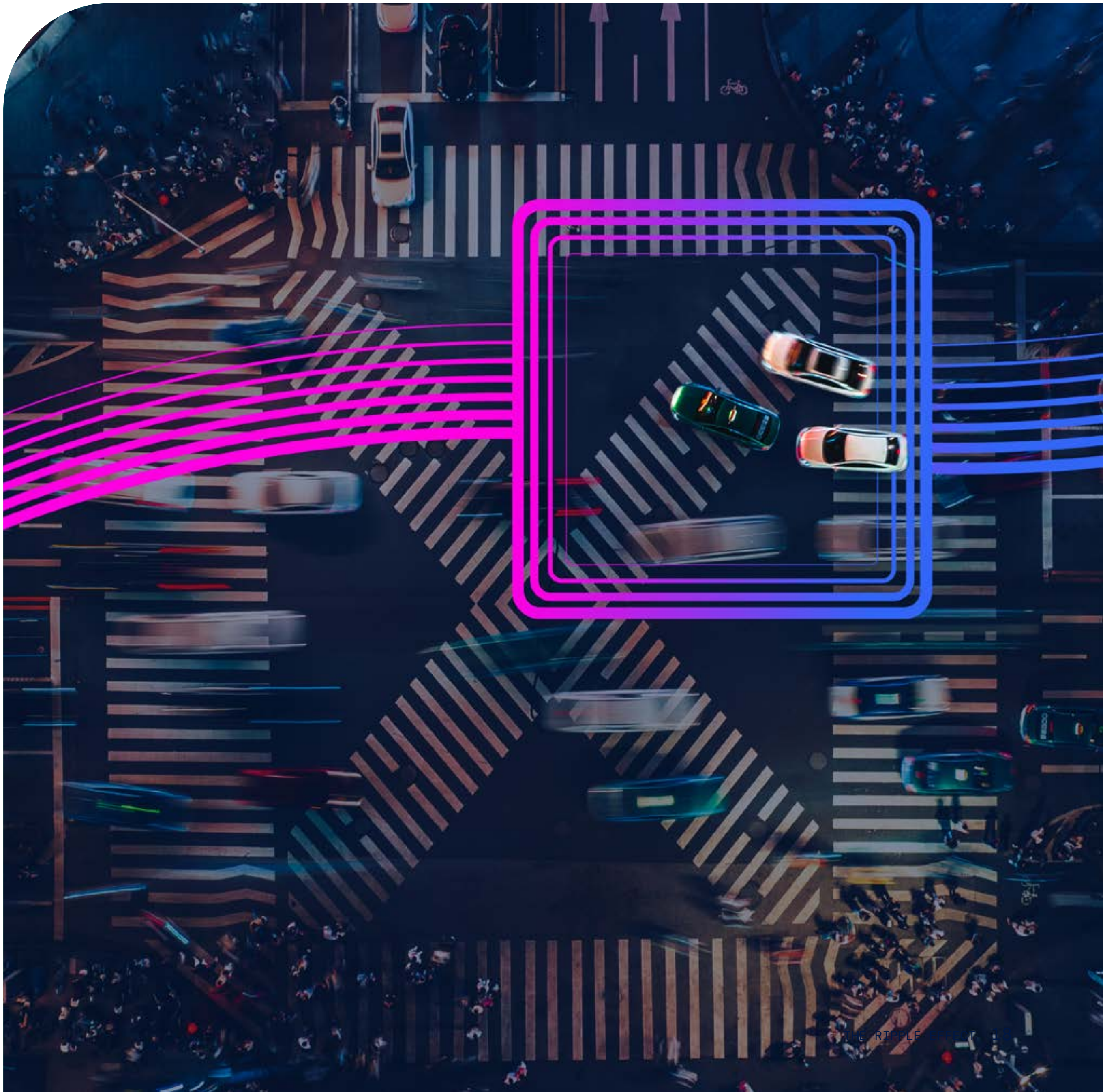
Snapshot of Asia-Pacific (APJ)

*Four markets surveyed**

Despite strong investment growth and widespread strategy updates, enterprises in these four markets reveal notable vulnerabilities in their resilience posture. While resilience investment increases are higher than the global average, confidence in the effectiveness of resilience measures (particularly against supply chain volatility) remains modest. Far from overconfidence that some other markets have, APJ's cautious optimism gives the region's organizations a pragmatic awareness of the 'when, not if' reality of failure scenarios. In fact, a significant share of IT leaders anticipate vendor-related disruptions within the next year, and many acknowledge that current security systems cannot withstand advanced threats.

The question is what's being done to address this awareness? Momentum is visible: operational pivots are accelerating, and quantum-readiness assessments are more common than elsewhere. Yet governance gaps around emerging technologies, persistent reliance on legacy systems, and infrastructure limitations continue to impede rapid recovery. For APJ, the challenge lies in translating investment into tangible resilience.

**For the purposes of our survey, mentions of APJ represent insights from a section of this region, represented by four markets: Australia, Japan, India and Singapore.*



KEY FINDINGS

- **88% (↓)** of APJ organizations have increased their cyber resilience investment in last 12 months — on average by **22% (↑)**
- **94% (↓)** have updated their cyber resilience strategy in response to external factors in the past 12 months
- **64% (↑)** of APJ IT leaders admit their company's cyber resilience strategy is still too inward looking — this rises to 83% of Indian IT leaders vs. 55% of Japanese IT leaders
- **66% (↑)** of IT decision-makers in APJ expect their organization to experience a significant failure scenario due to a supplier / third party vendor in the next 12 months — **47% (↑)** in next 6 months — again Indian IT leaders are most fearful of this (81%)
- Only **38% (↑)** believe their current resilience measures are highly effective against supply chain volatility
- **59% (↑)** agree their organization's current security systems are unable to defend against advanced threats — in India as many as 70% believe this is the case
- **49% (↓)** have fully deployed or are testing agentic AI have without having governance firmly in place — in Japan this rises to 62%
- **59% (↑)** haven't yet factored PQC into their cyber security strategy, and only **42% (↑)** have conducted a quantum-readiness assessment
- **75% (↑)** agree that the current macroenvironment is forcing their business to make quick operational (and therefore IT) pivots — in Singapore and India it is as many as 82% of local IT leaders
- **57% (↓)** have updated their cyber resilience strategy in past 12 months in response to new or evolving data sovereignty laws — and **79% (–)** are evaluating the risk of technology dependency (89% in Singapore)
- **73% (–)** have or expect to delay or cancel a digital initiative due to data sovereignty concerns — this practice is least prevalent in Australia (66%)
- **81% (–)** still have a critical or medium reliance on legacy systems
- **68% (↑)** agree their current IT infrastructure impedes its ability to respond effectively to failure incidents such as cyber breaches and system outages
- **85% (↓)** have run time to rebuild calculations in the last year (91% of Australian organizations) — but only **48% (↑)** have done so in the last 6 months

KEY
↑ Higher than global average
↓ Lower than global average
– Same as global average

"APJ is far from uniform in terms of IT resilience and regulatory maturity. Multi-speed economies with varying levels of digitization face an evolving threat landscape. While many countries have long-standing data localization laws, enforcement remains inconsistent, which leaves organizations vulnerable as AI-related threats rise. On the positive side, cultural norms are driving stronger security controls, higher resilience, and more compliance-led initiatives that reduce breach tolerance in regulated industries. As enterprises refocus on core business functions, reliance on third-party supply chains for skills and technology has grown — expanding attack surfaces. This shift demands robust controls and ongoing resilience assessments, not just point-in-time checks. In dynamic environments, cybersecurity teams must move at the speed of business, adapting to constant change and managing risk in real time."

HENG MOK, CISO IN RESIDENCE, APJ

Snapshot of Europe, Middle East & Africa (EMEA)

*Nine markets surveyed**

Although most respondent organizations across EMEA have refreshed their cyber resilience strategies in the past year, their progress still trails behind their global peers in several critical areas. Investment levels have risen, but at a slower pace than elsewhere, and confidence in the effectiveness of resilience measures (particularly against supply chain volatility) remains low. Added to this, a significant proportion of IT leaders expect vendor-related failure scenarios in the coming months, underscoring persistent threat of exposure.

Signs of progress are evident: strategy updates in response to external pressures are widespread, and some companies are exploring advanced technologies such as agentic AI. Yet governance gaps, limited quantum-readiness, and continued reliance on legacy systems suggest resilience maturity is uneven. With many leaders acknowledging that current legacy infrastructure impedes rapid recovery, EMEA's challenge is clear — the region's businesses must close these gaps before external shocks test their preparedness.

**For the purposes of our survey, mentions of EMEA represent insights from a section of this region, represented by nine markets: France, Germany, Italy, Netherlands, Saudi Arabia, Spain, Sweden, UAE, UK & Ireland.*

KEY FINDINGS

- **88% (↓)** of EMEA organizations have increased their cyber resilience investment in last 12 months (97% in Sweden) on average by **18% (↓)**
- **96% (–)** have updated their cyber resilience strategy in response to external factors in the past 12 months — in Sweden this rises to 100% of businesses
- **57% (↓)** believe their cyber resilience strategy is still too inward looking — this is a particular concern for Saudi Arabian organizations (83%)
- **59% (↓)** of EMEA IT leaders expect their business to experience a significant failure scenario due to a supplier / third party vendor in the next 12 months — **41% (↓)** in next 6 months
- Only **30% (↓)** believe their current resilience measures are highly effective against supply chain volatility — this falls to just 19% for Italian companies
- **49% (↓)** agree their current security systems are unable to defend against advanced threats — this is highest in Saudi Arabia (59%) and the Netherlands (56%)
- **56% (↓)** haven't yet factored PQC into their cyber security strategy (73% of Italian organizations vs. 26% of Saudi Arabian organizations) — and only 38% (↓) have conducted a quantum-readiness assessment
- **52% (↑)** have fully deployed or are testing agentic AI without having governance firmly in place
- **72% (↓)** agree that the current macroenvironment is forcing their enterprise to make quick operational (and therefore IT) pivots
- **60% (–)** have updated their cyber resilience strategy in past 12 months in response to new or evolving data sovereignty laws (67% of German enterprises) — and **78% (↓)** are evaluating the risk of technology dependency
- **72% (↓)** have or expect to delay or cancel a digital initiative due to data sovereignty concerns
- **79% (↓)** still have a critical or medium reliance on legacy systems — with the highest reliance in Saudi Arabia and the lowest in Germany
- **61% (↓)** agree their current IT infrastructure impedes its ability to respond effectively to failure incidents such as cyber breaches and system outages
- **86% (↓)** have run time to rebuild calculations in the last year — but only **42% (↓)** have done so in the last 6 months

KEY
↑ Higher than global average
↓ Lower than global average
– Same as global average

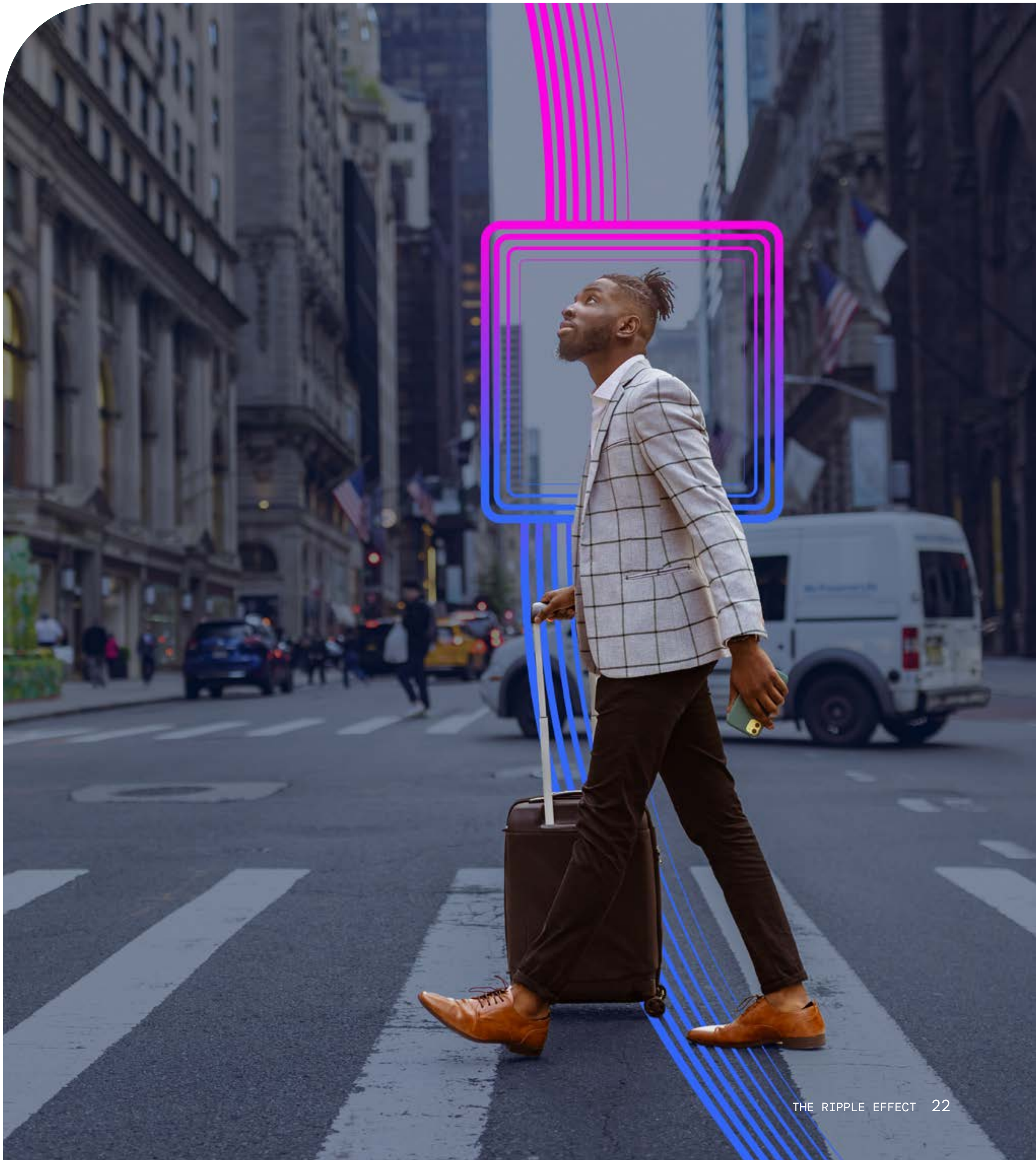
"Organizations are only seeing the tip of the iceberg — the complexity of today's IT systems is beyond any single person's understanding. Legislation and the security frameworks supporting it lag behind innovation. This means that many businesses simply assume that they're secure when using current frameworks, but without protection extending to emerging threats, this could create a false sense of safety. Critical risks tied to emerging threats like agentic AI, for example, are overlooked. Meanwhile, some resilience strategies are backfiring. By spreading risk across multiple vendors, organizations are reversing the recent trend toward security consolidation. More vendors create more complexity, more moving parts, and ultimately less flexibility and resilience. In short, diversification without control equals greater risk, and is something businesses must take seriously."

JAMES TUCKER, HEAD OF CISOS IN RESIDENCE, EMEA

Snapshot of The United States (US)

Organizations across the US show strong momentum on the resilience front, with investment and strategy updates outpacing global averages. Yet this progress coexists with persistent vulnerabilities: many IT leaders still view their strategies as too inward looking, and confidence in measures against supply chain volatility remains low. A high proportion anticipate vendor-related disruptions within the next year, and infrastructure constraints continue to hinder quick recovery.

Signs of maturity are evident, as we see that operational pivots are accelerating, governance gaps around emerging technologies are narrower than elsewhere, and resilience planning is more frequent. However, reliance on legacy systems, incomplete quantum-readiness, and exposure to advanced threats underscore the need for continued focus.



KEY FINDINGS

- **96% (↑)** of US organizations have increased their cyber resilience investment in last 12 months — on average by **22% (↑)**
- **97% (↑)** have updated their cyber resilience strategy in response to external factors in the past 12 months
- **69% (↑)** believe their cyber resilience strategy is still too inward looking
- **75% (↑)** expect their organization to experience a significant failure scenario due to a supplier / third party vendor in the next 12 months — **63% (↑)** in next 6 months
- Only **44% (↑)** believe their current resilience measures are highly effective against supply chain volatility
- **54% (↑)** agree their company's current security systems are unable to defend against advanced threats
- **45% (↓)** have fully deployed or are testing agentic AI without having governance firmly in place
- **56% (↓)** haven't yet factored PQC into their cyber security strategy — and only **37% (↓)** have conducted a quantum-readiness assessment
- **80% (↑)** agree that the current macroenvironment is forcing them to make quick operational (and therefore IT) pivots
- **69% (↑)** have updated their cyber resilience strategy in past 12 months in response to new or evolving data sovereignty laws — and **80% (↑)** are evaluating the risk of technology dependency
- **75% (↑)** have or expect to delay or cancel a digital initiative due to data sovereignty concerns
- **86% (↑)** still have a critical or medium reliance on legacy systems
- **69% (↑)** agree their organization's current IT infrastructure impedes its ability to respond effectively to failure incidents such as cyber breaches and system outages
- **95% (↑)** have run time to rebuild calculations in the last year — but only **54% (↑)** have done so in the last 6 months

KEY
↑ Higher than global average
↓ Lower than global average
– Same as global average

"We've moved from a world where IT acted as a custodian (building and maintaining every part of the infrastructure) to a world where IT acts as a broker. Brokers don't build; they orchestrate. They sit above the stack, curating a catalog of approved security services and coordinating how those services work together. When IT brokers various services through a catalog, data naturally flows across multiple providers. That's why data awareness becomes essential: who touches it, where it travels, and how it's protected. Enterprises must design for data security from the outset, so protection moves with the data. Bolt it on later and they inherit complexity, more reworks, and higher costs. Without a Resilient by Design approach (where controls are continuously validated across suppliers, contractors, and shared platforms), organizations end up absorbing the risk of others. A partner's incident can rapidly become their outage."

SAM CURRY, SVP & GLOBAL CISO

Act Fast, Stay Secure.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE—based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit www.zscaler.com

Zscaler Ltd, 7 Bishopsgate, London, EC2N 3AR, UK