Cyber Resilience Strategies Are Too Inward-Focused



A new report from Zscaler, ***'The Ripple Effect: A Hallmark of Resilient Cybersecurity'***, warns that if an organization's cyber resilience strategy is too internally focused, it leaves businesses dangerously exposed to external shocks.

Key findings

Organizations are starting to understand the importance of creating robust cyber resilience strategies to defend against significant failure scenarios

96% of organizations have updated their cyber resilience strategy in response to external factors in the past 12 months

90% of organizations have increased their cyber resilience investment in last 12 months — an average increase of 19% over 2024

But these strategies are not factoring the entire business infrastructure into their plans

61% of organizations admit their cyber resilience strategies are too inward-looking

60% of respondents having already experienced a significant failure scenario due to a supplier / third party vendor in the past year

63% expecting to experience the same again in next 12 months

Leading to dangerous gaps around their preparedness for emerging threats — with the supply chain becoming a potential exposure point

65% of respondents agree the macroenvironment is driving large levels of volatility within their organization's supply chain

68% agree that their organization has a far higher reliance on contractors and third parties than ever before

40% of organizations have updated their cyber resilience strategy in the past 12 months in response to supply chain volatility; 48% in response to an increase in third-party contractors

AI is viewed as the biggest emerging external threat

56% have taken the step to categorize their data to **prevent data loss via AI tools**

63% of organizations have included agentic AI in their **cyber resilience strategy**

76% of organizations have fully deployed or are testing agentic AI, but **50%** of those have done so without having governance firmly in place

More than half agree that their organization is likely exposing sensitive data due to employee use of

- 56% SHADOW AI
- 56% PUBLIC AI APPS

Quantum computing is becoming an increasing worry for security teams

63% of respondents agree that if data was stolen today and then decrypted by quantum computers in the next 3–5 years it would still pose a risk to their organization

But only

- 44% have factored Post Quantum Cryptography into their cyber security strategy

And just

- 39% have conducted a quantum-readiness assessment

Organizations are grappling with a volatile market and the implications of evolving data sovereignty laws

74% of respondents agree the current macroenvironment is forcing their organization to make quick operational pivots

60% have updated their cyber resilience strategy in the past 12 months for data sovereignty laws

79% of global organizations are evaluating the sovereignty risks of foreign technology dependency

Underlying agility issues are impeding security teams from responding effectively to these threats

59% of respondents agree their organization's IT architecture is unable to keep up with the speed of business change

Many organizations are still heavily relying on legacy systems:

- 28% claiming a critical reliance
- 53% stating a medium reliance



Your next step

To thrive amid uncertainty, organizations must build resilience from the inside out. Done right, that protection ripples outward, reducing the impact of external shockwaves beyond their 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

METHODOLOGY

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

ABOUT ZSCALER

Zscaler accelerates digital transformation so 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 160 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform.

©2026 Zscaler, Inc. All rights reserved.