

## Hey! What's New? 2025-107

### Why Leaders at Many Companies Are Scrambling to Outpace Cyber Risks

Steph Brown writes in *FM Financial Management* that “cyber resilience is a work in progress for organizations as executives struggle to close risk readiness gaps. For many leaders, skills shortages are the biggest hurdle to formulating effective, technology-driven risk mitigation strategies.”

According to PwC’s [2026 Global Digital Trust Insights report](#), she writes, “the gap between ambition and capability is also forcing leaders to reconsider their route to resilience.

Respondents noted that knowledge and skills gaps were the top two barriers to progressing AI implementation strategies over the next 12 months.”

PwC surveyed 3,887 business and tech executives across 72 countries.

“As skills shortages delay progress, companies aim to push the use of agentic artificial intelligence (AI) across security practices, and over half of executives (53%) say they are prioritizing AI and machine learning tools to help close capability gaps,” the report said.

Other strategies include exploring security automation tools (48%), cyber tool consolidation systems (47%), and upskilling or reskilling resources (47%).

But, despite those ambitions, Brown learned that “the geopolitical risk landscape is adding further complexity for leaders. Sixty per cent of business and tech leaders place cyber risk investment in their top three strategic priorities, in response to ongoing geopolitical uncertainty. Subsequently, confidence in cyber readiness is nearing a 50–50 split for leaders, and only 6% feel confident across all vulnerabilities surveyed.”

She notes that “these layers of uncertainty are creating blind spots for the C-suite, which is struggling to budget for and deploy proactive strategies. Proactive measures in the report refer to the use of monitoring, assessments, testing, controls, and training tools in preparation for a crisis before it unfolds. The report found that less than one-fourth of leaders (24%) professed to investing significantly more on proactive steps.”

According to the report, “without sufficient protocols in place, companies can become reliant on reactive measures, such as response, customer care, and recovery procedures — principally, two-thirds (67%) of organizations say their proactive/reactive cost ratio is roughly even. However, those measures are less sustainable long term.”

Reactive costs are harder to track and can be dispersed across multiple business functions.

“While proactive spending sits in the security leader’s budget,” the report added, “[reactive costs] include harder-to-quantify costs such as lost opportunities and reputational damage.”

The survey also found that “the power of quantum computing is forcing companies to rethink data encryption. A report published in late 2023 by global consulting firm Protiviti said, ‘The rise of quantum computing has the ability to render obsolete existing cryptography methods.’”

In the PwC report, quantum computing ranks among the top five threats organizations are least prepared to address, yet fewer than 10% prioritize it in budgets and only 3% have implemented all leading quantum-resistant measures surveyed.

What's holding leaders back?, Brown asks. "According to the report, many executives cited minimal understanding around post-quantum risks, combined with limited internal resources and competing demands as top barriers to quantum proficiency."

For organizations progressing in this area, most are still in the piloting and testing stage (29%). However, some are making considerable strides and 22% are already implementing quantum-resistant security measures.

"Although quantum isn't an immediate cyber threat, those who delay the transition to post-quantum cryptography may be exposing their sensitive data, authentication services, and cryptographic systems," the report said. "With implementation timelines stretching into years, establishing the foundations for quantum-resistant security demands early action today to avoid adversarial disruption tomorrow."

Get the report at [2026 Global Digital Trust Insights Survey: PwC](#).