

Hey! What's New? 2024-124

Only 2% Of Businesses Have Implemented Firm-Wide Cyber Resilience

According to new research from PwC, almost four-fifths (77%) of organizations expect their cyber budget to increase over the coming year as organizations cite unpreparedness to an ever-expanding surface of cyber vulnerabilities, according to *PwC's 2025 Global Digital Trust Insights* survey.

The research, which surveyed 4,042 business and tech executives from across 77 countries and territories, finds that only 2% of the companies surveyed have implemented cyber resilience across their organization, even as more than three-fifths (66%) of tech leaders rank cyber as the top risk their organization is prioritizing for mitigation over the next 12 months. This comes as the average cost of a data breach across all respondents is US\$3.3M.

As organizations increasingly operate across digital platforms, two-thirds (67%) note GenAI has increased their attack surface over the last year.

According to Sean Joyce, Global Cyber & Privacy Leader, PwC US, "this year's survey findings highlight that what worries organizations most is what they're least prepared for. The top four cyber threats found most concerning — cloud-related threats (42%), hack-and-leak operations (38%), third-party breaches (35%) and attacks on connected products (33%) — are the same one's security executives feel least prepared to address.

"Cyber resilience is everyone's responsibility, from the boardroom to the employee. We must hold each other accountable and ensure we address emerging risks by leveraging new technology, practicing foundational cybersecurity principles, and investing in resources that will secure the future of the organization."

The research found that, "as companies contend with cyber security concerns, almost four-fifths (78%) of leaders surveyed have ramped up their investment in GenAI over the last 12 months, with 72% increasing their risk management investment in AI governance. This comes as two-thirds (67%) of security leaders note GenAI has expanded the cyber-attack surface over the last year, ahead of other technologies such as cloud technology (66%), connected products (58%), operational technology (54%) and quantum computing (42%). But while leveraging GenAI remains key to cyber resilience strategies, organizations face several challenges when incorporating the technology, notably with existing systems/processes (39%) and a lack of standardized internal policies governing its use (37%)."

Despite the clear threats and a lack of preparedness, the survey findings highlight that organizations are nevertheless taking action. "More than three-quarters (77%) expect their cyber budget to increase over the coming year, with nearly half (48%) of business leaders prioritizing data protection and data trust as the top cyber investment over the next year. Tech leaders, on the other hand, note cloud security (34%) remains their top-priority. Almost one-third (30%) of organizations expect cyber budgets to increase by 6-10% next year, while one-fifth (20%) expect budgets to increase by 11% or more."

There is also a clear cyber security imperative, the survey found. "Organizations cite investment in cybersecurity as a key differentiator for competitive advantage, with 57% citing customer

trust and 49% citing brand integrity and loyalty as primary drivers for such investment. In the backdrop, cyber regulations are also driving investment – with 96% reporting such regulations to have increased their cyber investment in the last 12 months.”

Get the survey at [2025 Global Digital Trust Insights Survey: PwC](#).