EINPRESSWIRE

1/3 of US organizations surveyed lack trust in third-party vendors to manage critical risks, new CyXcel research finds

Supply chain risk strategies undermined by internal blind spots, mounting complexity, and over-reliance on unvetted vendors

ATLANTA, GA, UNITED STATES, July 16, 2025 / EINPresswire.com/ -- New research from CyXcel, a global cybersecurity consultancy, reveals a critical shortfall in the US's digital risk landscape: a third of US risk managers surveyed (33%) report they don't have enough trust in third-party vendors to confidently manage their most critical threats, increasing their risk factors and threatening their businesses.

This trust gap is both a vendor problem and a visibility problem. CyXcel's research highlights that nearly a third (31%) of US respondents do not fully understand the risks they're responsible for managing, making it nearly impossible to assess whether vendors are fit for purpose. As organizations continue to outsource key areas such as cyber incident response (23%), AI adoption (22%), and geopolitical risk management (21%), the lack of both trusted partners and internal clarity creates a fragile risk posture.

Layered onto this is the intensifying convergence of threats, AI-driven attacks, rising geopolitical instability, and increasingly sophisticated cybercriminal tactics. These forces demand far more than robust contracts and a one-time vendor review. They require intelligence-led, continuously validated partnerships, supported by internal systems that can assess, question, and course-correct in real time.

“Organizations are stuck between needing external support and not having enough partners they truly trust,” said Megha Kumar, Chief Product Officer and Head of Geopolitical Risk at CyXcel. “It's a tension we're seeing across sectors, and it's leaving risk ecosystems fragmented and vulnerable. Without stronger internal understanding, risk leaders are flying blind, placing responsibility in the hands of vendors they can't fully vet. What's needed now is a shift toward integrated intelligence, not just compliance checklists. Businesses must empower their teams to assess threats clearly and select partners confidently.”

Despite investing, on average, between $85,000 - $120,000 in risk management tools and strategies annually, many organizations are still unsure whether these investments are effective. Just over one in four risk managers (26%) say they feel overwhelmed by the volume and complexity of threats they're tasked with navigating. This growing pressure is prompting critical questions: Are organizations outsourcing because it's strategic or because they don't understand the risk well enough to manage it themselves?

"We see this pattern again and again," said Ngaire Guzzetti, Technical Director – Supply Chain at CyXcel. "Organizations are handing over the keys to their digital resilience, but don't have the internal visibility to know if those partners are steering in the right direction. Risk managers are drowning in complexity, yet leaving the handling of the lifeboat to vendors they barely trust. Resilience doesn't start with spend; it starts with clarity. The more you understand the threat, the better equipped you are to evaluate who should be helping you manage it."

In response to this growing risk fragmentation, CyXcel offers its Digital Risk Management (DRM) platform, which provides organizations with insight into evolving AI risks across all major sectors, regardless of business size. The DRM helps organizations identify risk and implement the right policies and governance to mitigate them. Unlike conventional offerings, CyXcel's DRM uniquely brings together cyber, legal, technical and strategic expertise that has been developed over decades working with companies across numerous sectors, and follows best practices.

The DRM also supports real-time vendor assurance and remediation services, helping organizations continuously validate the integrity of their third-parties, rather than relying on assumptions or outdated reviews. At a time when supply chain attacks are on the rise and regulators are scrutinizing third-party oversight, CyXcel's DRM helps organizations move from reactive to resilient.

About CyXcel
CyXcel enables companies to achieve digital resilience through our comprehensive suite of proactive and reactive services, all backed by a NCSC, ISO and CREST-accredited provider. We enable our clients to understand their digital risks, design and achieve peak resilience, and retain that state even as their external environment changes – especially during a cyber incident.

Research Methodology
The research was conducted by Censuswide, among a sample of 400 cybersecurity workers, who have a good understanding of their company's risk management process (aged 18+) across the UK and US (200 respondents respectively). The data was collected between 05.28.2025 and 06.02.2025. Censuswide abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Censuswide is also a member of the British Polling Council.

###

Sarah Hawley
Origin Communications
+1 480-292-4640
email us here
Visit us on social media:
LinkedIn