opentext™ Cybersecurity

AI threats undermine growing ransomware confidence

OpenText Cybersecurity 2025 Ransomware survey

OpenText™ Cybersecurity releases new findings from its fourth annual Global Ransomware Survey which highlights increased ransomware readiness but finds AI is intensifying recovery challenges worldwide.

Spotlight findings

Confidence builds, but AI-driven threats test resilience

The majority of respondents express confidence in their organization's ability to recover from a ransomware attack, signaling progress in overall preparedness...

... yet recovery remains limited, with only 15% of attacked organizations fully restoring their data.

Even with increased confidence in recovery, half of respondents are more worried about ransomware attacks as AI evolves.

Preparedness improves, while AI challenges organizations to balance innovation and risk

88% Signaling a major shift in workplace AI adoption, most organizations allow employees to use GenAI tools...

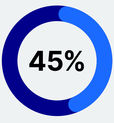
48% ...yet nearly half of those organizations do not have a formal AI use policy in place.

52% As AI adoption grows, more than half of respondents have reported increased phishing or ransomware due to AI.

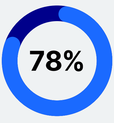
With AI use expanding among both employees and attackers, organizations are increasingly wary of the risks. The greatest AI-related concerns include:

Silent vulnerabilities: Supply chain risks persiste despite AI focus

Forty percent of companies faced a ransomware attack in the past year, and nearly half of these organizations were attacked multiple times.



Ransomware payouts remain a major burden, with 45% of victims paying and 30% paying $250K or more.



The majority of organizations now evaluate supplier cybersecurity, with 82% implementing patch management.

Executive teams elevate cybersecurity from IT issue to strategic imperative

Cybersecurity is moving from the IT department into the boardroom, as AI and the spread of ransomware across critical business systems put it firmly in the spotlight.

What was once seen as a technical concern is now recognized as a core strategic priority for executive teams.

71% of respondents say their executive team sees ransomware as a top three business risk

64% have been asked by customers or partners about ransomware readiness in the past year

In 2026, companies plan to invest in these areas:
- Cloud security (**58%**)
- Backup technologies (**52%**)
- User training (**52%**)

Security training is now common practice, with **77%** of respondents conducting regular security awareness or phishing simulations

Survey methodology

In September 2025, OpenText Cybersecurity surveyed 1,773 C-level executives, security professionals, and security and technical directors from SMBs and enterprises in the United States, Canada, the United Kingdom, Australia, France, and Germany. Respondents represented multiple industries including technology, financial services, retail, manufacturing, healthcare, education, and more.

About OpenText Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified, end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high-efficacy products, a compliant experience and simplified security to help manage business risk.

opentext™ Cybersecurity