OpenText Cybersecurity 2025 Global Ransomware Survey: Rising Confidence Meets a Growing AI Threat

2025-10-23

While 95% of organizations are confident in their ransomware recovery, AI-driven attacks and limited data governance are undermining that certainty

WATERLOO, ON, Oct. 23, 2025 /PRNewswire/ -- **OpenText™** (NASDAQ: OTEX) (TSX: OTEX), a global leader in secure information management for AI, today released the findings of its fourth annual Global Ransomware Survey. The survey of almost 1,800 security practitioners and business leaders highlighted a rising tension between confidence and risk: confidence in ransomware readiness is rising yet concern over AI-driven attacks and third-party vulnerabilities are growing just as fast.

Organizations believe they're ready to bounce back from ransomware—but AI is rapidly changing the threat landscape. New attack methods, weak governance, and supply chain vulnerabilities are exposing critical gaps between preparation and performance, creating a higher-stakes environment for defenders and leaders alike. This is especially true for SMBs that have fewer formal AI policies.

"Organizations are right to be confident in their progress in security posture, but they can't afford to be complacent," said Muhi Majzoub, Executive Vice President, Security Products, OpenText. "AI fuels productivity while also heightening risk through insufficient governance and its expanding use in attacks. Managing information securely and intelligently is essential to building resilience in organizations of any size."

Key survey findings include:

False Sense of Confidence Grows, as AI raises the Stakes

Organizations feel more prepared than ever to recover from ransomware attacks, but AI introduces a growing layer of complexity that's causing unease. While internal GenAI use is rising, so are external AI-powered threats. Organizations are navigating a high-stake balancing act to enable innovation while managing risk.

- Ninety-five percent of respondents are confident in their ability to recover from a ransomware attack, but only 15% of those attacked fully recovered their data.

- Eighty-eight percent allow employees to use GenAI tools, yet less than half (48%) have a formal AI use policy.
- Enterprises lead AI governance (52%) compared to SMBs (43%) by having a formal AI policy in place.
- Fifty-two percent report increased phishing or ransomware due to AI; 44% have seen deepfake-style impersonation attempts.
- Top AI-related concerns among respondents include data leakage (29%), AI-enabled attacks (27%), and deepfakes (16%).

Unmanaged Supply Chain Pathways Create Hidden Risks

While much of the ransomware conversation centers on AI, supply chain and third-party risks remain a quiet but dangerous threat. Attacks are both more frequent and distributed, often entering through vendors, partners, or unmanaged digital pathways.

- Two in five companies (40%) experienced a ransomware attack in the past year; nearly half of those were hit more than once.
- Forty-five percent of victims paid a ransom; 30% paid $250K or more.
- Only 15% of those hit fully recovered their data; 2% recovered nothing.
- Twenty-five percent experienced ransomware attacks originating from a software vendor.
- Over three-quarters (78%) of organizations now assess software supplier cybersecurity; 82% have patch management in place.

Sophistication of Ransomware Attacks Raises Awareness

The rise of AI and the spread of ransomware across critical business systems have pushed cybersecurity into the spotlight. What was once seen as an IT issue is now recognized as a core strategic concern for boards and executive teams.

- Seventy-one percent of respondents say their executive team sees ransomware as a top three business risk.
- Nearly two-thirds (64%) have been asked by customers or partners about ransomware readiness in the past year.
- 2026 investment priorities include cloud security (58%), backup technologies (52%), and user training (52%).
- A majority (77%) conduct regular security awareness training; only 4% offer none.

For additional findings from the OpenText Cybersecurity 2025 Global Ransomware survey, view the **infographic**.

Protecting against ransomware now depends not just on internal defenses, but also on how effectively organizations, partners, and technology providers work together to close security gaps before they're exploited. To learn more about our enterprise solutions, explore **OpenText Cybersecurity Cloud**. To learn more about our offerings for SMBs, click **here**.

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.

About OpenText

OpenText™ is a leading Cloud and AI company that provides organizations around the world with a comprehensive suite of Business AI, Business Clouds, and Business Technology. We help organizations grow, innovate, become more efficient and effective, and do so in a trusted and secure way – through Information Management. For more information about OpenText (NASDAQ/TSX: OTEX), please visit us at **www.opentext.com.**

Connect with us:

OpenText Executive Thought Leadership blog
Twitter | **LinkedIn**

Certain statements in this press release may contain words considered forward-looking statements or information under applicable securities laws. These statements are based on OpenText's current expectations, estimates, forecasts and projections about the operating environment, economies and markets in which the company operates. These statements are subject to important assumptions, risks and uncertainties that are difficult to predict, and the actual outcome may be materially different. OpenText's assumptions, although considered reasonable by the company at the date of this press release, may prove to be inaccurate and consequently its actual results could differ materially from the expectations set out herein. For additional information with respect to risks and other factors which could occur, see OpenText's Annual Report on Form 10-K, Quarterly Reports on Form 10-Q and other securities filings with the SEC and other securities regulators. Readers are cautioned not to place undue reliance upon any such forward-looking statements, which speak only as of the date made. Unless

otherwise required by applicable securities laws, OpenText disclaims any intention or obligations to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise. Further, readers should note that we may announce information using our website, press releases, securities law filings, public conference calls, webcasts and the social media channels identified on the Investors section of our website (**https://investors.opentext.com**). Such social media channels may include the Company's or our CEO's blog, Twitter account or LinkedIn account. The information posted through such channels may be material. Accordingly, readers should monitor such channels in addition to our other forms of communication.

OTEX-G

View original content to download multimedia:**https://www.prnewswire.com/news-releases/opentext-cybersecurity-2025-global-ransomware-survey-rising-confidence-meets-a-growing-ai-threat-302592473.html**

SOURCE Open Text Corporation