



OpenText and Ponemon Institute Survey of CIOs Finds Lack of Information Readiness Threatens AI Success

2025-08-27

New research of almost 1,900 CIOs, CISOs, and other IT leaders shows they are under pressure to ensure sensitive information is secure and compliant without hindering growth

WATERLOO, ON, Aug. 27, 2025 /PRNewswire/ -- OpenText™ (NASDAQ: OTEX) (TSX: OTEX) today released a new global report, **"The Challenges to Ensuring Information Is Secure, Compliant and Ready for AI,"** revealing that while enterprise IT leaders recognize the transformative potential of AI, a gap in information readiness is causing their organizations to struggle in securing, governing, and aligning AI initiatives across business.

Developed in partnership with the Ponemon Institute -- a leading, independent research firm focused on information security and privacy management -- the study revealed almost three-quarters (73%) of CIOs, CISOs, and other IT leaders believe reducing information complexity is key to AI readiness.

"This research confirms what we're hearing from CIOs every day. AI is mission-critical, but most organizations aren't ready to support it," said Shannon Bell, Chief Digital Officer, OpenText. "Without trusted, well-governed information, AI can't deliver on its promise. At OpenText, we're helping IT and security leaders close that gap by simplifying information complexity, strengthening governance, and ensuring the right information is secure and actionable across the enterprise."

Information Readiness Is the Missing Link in AI Success

While AI is a high priority, the research underscores a key gap, that most organizations lack the information readiness to deploy AI securely or effectively. The report also found that while IT and security leaders remain confident in the ROI of AI, it is difficult to adopt, secure, and govern.

As this gap widens, information management is becoming the connective tissue between enabling innovation and maintaining trust. OpenText helps close that gap, by equipping leaders with the tools to simplify complexity, confidently govern data, and operationalize AI responsibly.

- Information complexity impedes readiness: 73% say reducing complexity is essential (23%), very important (23%) and important (27%) for a strong security posture, with unstructured data (44%) among the top contributors to complexity.
- Data governance is the first line of defense: To address data security risks in AI, nearly half (46%) of respondents say they are developing a data security program and practice.
- Confidence is lagging: Just 43% are very or highly confident in their ability to measure ROI on securing and managing information assets.

The AI Paradox: High Confidence in ROI, Low Readiness in Execution

Leaders are optimistic about the value AI can deliver, but readiness is low. Many organizations still lack the security, governance, and alignment needed to deploy AI responsibly.

- 57% of respondents rate AI adoption as a top priority, and 54% are confident they can demonstrate ROI from AI initiatives. However, 53% say it is "very difficult" or "extremely difficult" to reduce AI security and legal risks.
- Fewer than half (47%) say IT and security goals are aligned with those driving AI strategy, even though 50% of respondents say their organizations have hired or are considering hiring a chief AI officer or a chief digital officer to lead AI strategy.
- GenAI is gaining traction, with 32% having adopted it, and another 26% planning to in the next six months. Top GenAI use cases include security operations (39%), employee productivity (36%), and software development (34%).
- Yet only 19% of organizations have adopted agentic AI and 16% will adopt it in the next six months. Just 31% of those rate agentic AI as highly important to their business strategy.

Improving Information and AI Readiness

The research also revealed best practices for achieving AI readiness based on responses from the organizations that have invested in AI. These include:

- Protect sensitive data exposure: Organizations should know where sensitive data resides, who can access it, and how it is used. Strong access controls, clear data classification policies and anomaly detection tools can help reduce exposure.

- Implement responsible AI practices: A comprehensive approach includes data cleansing and governance, validating AI inputs and outputs, employee training, and regular model bias checks to ensure AI is used safely and ethically.
- Strengthen encryption: Encryption should be applied to data in storage, transit and during AI processing. This ensures that sensitive information remains protected throughout the AI lifecycle.

The full report also reveals additional pressures from insider risk, proving ROI of AI and IT investments, and managing security complexity.

Survey Methodology

The Ponemon Institute independently surveyed 1,896 senior IT and security leaders across North America, the United Kingdom, France, Germany, Australia, and India. The study captured input from organizations of varying sizes and industries, including financial services, healthcare, technology, and manufacturing. The research was conducted in May 2025. Respondents included CIOs, CISOs, IT and cybersecurity executives, and decision-makers responsible for AI and security strategy.

Additional Resources

- Read the full report for more on broader AI and IT priorities, security trends, and investments: **Click here**

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 Thought Leadership

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.

Copyright © 2025 OpenText. All Rights Reserved. Trademarks owned by OpenText. One or more patents may cover this product(s). For more information, please visit <https://www.opentext.com/patents>.

OTEX-G

View original content to download multimedia:<https://www.prnewswire.com/news-releases/opentext-and-ponemon-institute-survey-of-cios-finds-lack-of-information-readiness-threatens-ai-success-302539676.html>

SOURCE Open Text Corporation