NEWS RELEASE

Splunk Report: Agentic AI Takes Center Stage in CISOs' Path to Digital Resilience

2026-02-24

- ***Nearly all CISOs Report They Are Now Responsible for AI Governance and Risk Management, Cite the Growing Sophistication of Threat Actor Capabilities as Their Greatest Risk***
- ***Vast Majority Say AI Enables More Security Events to be Reviewed***

SAN JOSE, Calif., Feb. 24, 2026 /PRNewswire/ -- Cisco today announced the release of Splunk's annual report, *The CISO Report: From Risk to Resilience in the AI Era*, surveying 650 global Chief Information Security Officers (CISOs). The report highlights CISOs' rapidly expanding role, their strategic approach to AI adoption, and a steadfast commitment to human talent as they confront an increasingly complex landscape.

"CISOs operate in the eye of the storm, at the center of constant transformation. Role responsibilities expand, threats evolve, and AI accelerates everything," said Michael Fanning, CISO, Splunk, a Cisco Company. "This expanded mandate brings an exceptional level of pressure and personal accountability. We are not just managing technology. We are managing risk, talent, and the digital resilience that drives critical business outcomes."

The AI Imperative
AI is recognized as a powerful business imperative and productivity powerhouse for security teams, including agentic AI. The survey highlights:

- 95% of CISOs cite the growing sophistication of threat actor capabilities as their greatest risk. Ninety-two percent of CISOs say that improving threat detection and response capabilities is a top priority, followed by strengthening identity and access management (78%), and investing in AI cybersecurity capabilities (68%).
- 92% of CISOs say AI enables their teams to review more security events.
- 89% report improved data correlation with AI.
- 39% of CISOs who have partially or fully adopted agentic AI strongly agree it has increased their teams' reporting speed by more than double the rate of those who are still exploring (18%).
- 82% of CISOs believe agentic AI will increase the amount of data reviewed and 82% say it will

increase correlation and response speeds.

While CISOs' approach AI with cautious optimism, 86% fear agentic AI will increase the sophistication of social engineering attacks, and 82% worry it will increase deployment speed and complexity of persistence mechanisms. Ultimately, AI is seen as essential for combating advanced threats and delivering significant business advantages.

Expanded Mandate and Personal Stakes
CISOs are operating at the leading edge of digital transformation, with nearly four out of five reporting their role has become significantly more complex. More than three quarters of CISOs are now worried about personal liability for security incidents, a sharp jump from last year, when just over half expressed similar fears, underscoring the high stakes involved. Nearly all respondents now report that CISOs responsibilities include AI governance and risk management, with more than four out of five also overseeing secure software development (DevSecOps).

Talent Over Tech in Closing Gaps
Despite the rise of AI, CISOs are prioritizing human capital to address critical skills gaps. Their main strategies include upskilling current workforces, hiring new full-time employees, and engaging contractors. This reflects a belief that human intelligence and creativity remain security's most powerful tools, especially for nuanced tasks like threat hunting.

Security is a Team Sport
Shared ownership is proving critical for stronger cybersecurity outcomes. Joint accountability drives the most value for key security initiatives (62%), security budget and funding (55%), and access to security-relevant data (49%), indicating that collaboration across the C-suite is a force multiplier for resilience.

Burnout and the Quest for Clarity
The report reveals a significant challenge in workforce retention, with nearly two-thirds of security teams experiencing moderate to significant burnout. Leading stressors include:

- High alert volumes (98%)
- False alerts (94%)
- Tool fatigue (79%)

To address these issues, CISOs are consolidating security data into a single view and using data-driven narratives to translate technical nuances into clear business imperatives for non-technical leadership. However, challenges to improving cross-departmental data sharing persist, such as:

- Data privacy concerns (91%)
- High storage costs (76%)
- Lack of shared data views (70%)

Reframing Security as a Business Enabler
CISOs are increasingly focused on translating cybersecurity's value into clear business outcomes. Incident reduction, improved Mean Time to Detect (MTTD), and Mean Time to Respond (MTTR) are the top metrics used to communicate ROI to leadership. Collaboration with C-suite peers, especially on budgeting and key initiatives, is crucial for success.

The CISO Report highlights the transformation of the CISO role into a strategic leader. The report demonstrates how these executives are effectively navigating complex challenges by championing data-driven strategies, fostering human-centric leadership, and thoughtfully integrating AI. Through these approaches, CISOs are strengthening digital resilience and empowering their organizations to thrive in an ever-evolving threat landscape.

To download the 2026 CISO Report, please visit the Splunk website.

Methodology
Oxford Economics researchers surveyed 650 Chief Information Security Officers (CISOs) in July and August of 2025. Respondents resided in Australia, France, Germany, India, Japan, New Zealand, Singapore, the United Kingdom, and the United States. They represented nine industry groups: manufacturing, telecommunications, media and communications, financial services, public sector, energy and utilities, transportation and logistics, retail and consumer goods, healthcare and life sciences, and information services and technology.

About Cisco
Cisco (NASDAQ: CSCO) is the worldwide technology leader that is revolutionizing the way organizations connect and protect in the AI era. For more than 40 years, Cisco has securely connected the world. With its industry leading AI-powered solutions and services, Cisco enables its customers, partners and communities to unlock innovation, enhance productivity and strengthen digital resilience. With purpose at its core, Cisco remains committed to creating a more connected and inclusive future for all. Discover more on The Newsroom and follow us on X at @Cisco.

About Splunk LLC
Splunk, a Cisco company, helps build a safer and more resilient digital world. Organizations trust Splunk to prevent security, infrastructure and application issues from becoming major incidents, absorb shocks from digital disruptions, and accelerate digital transformation.

View original content to download multimedia:https://www.prnewswire.com/news-releases/splunk-report-agentic-ai-takes-center-stage-in-cisos-path-to-digital-resilience-302695047.html

SOURCE Cisco Systems, Inc.