Heimdal survey: US executives are four times more confident about AI risk than the teams managing it

New research from cybersecurity company Heimdal finds 29% of US executives say AI risk is under control, against 7% of the practitioners running it day to day.

1,000 IT professionals say AI is outpacing the controls meant to manage it.

LONDON, UNITED KINGDOM, June 16, 2026 /EINPresswire.com/ -- Heimdal today published The State of AI Risk Management in 2026, a survey of 1,000 IT professionals across the United Kingdom and the United States.

The report's headline finding is a divide inside the same organizations: the closer a person sits to the day-to-day running of AI, the less confident they are that the risk is contained.

In the US, 29% of C-suite and VP respondents say their organization has AI risk under control, against 7% of the mid-level practitioners managing it.

In the UK the gap runs the same way, 18% to 11%. Both gaps are statistically significant.

AI tools are already present across most IT estates, and most teams run several at once.

The controls have not kept pace. Across both markets, the report finds adoption has outrun security controls by roughly two to one.

The survey also records a counterintuitive pattern: the teams that see their AI use most clearly are the most concerned about it, not the least.

Heimdal's report describes visibility as the diagnosis rather than the cure.

In an incident publicly disclosed in January 2026, the acting director of CISA, the United States cybersecurity agency, uploaded documents marked "For Official Use Only" to public ChatGPT in mid-2025.

The agency's own monitoring flagged the activity within a week, but the use policy had not prevented it.

Key findings

• Executive confidence outruns the frontline. In the US, 29% of executives say AI risk is under control, against 7% of practitioners. In the UK, 18% against 11%.

• AI is already embedded. ChatGPT runs in 72% of UK IT environments and 69% of US environments, and Microsoft Copilot in 68% of UK and 59% of US.

• Readiness lags adoption. Only around 4 in 10 teams rate their security stack as ready for AI-related risk.

• Concern rises with visibility. Among UK teams with full visibility into AI use, 56% flag data leakage as a top concern, against 27% of teams with none. In the US the figure is 59% among teams with full visibility.

• Operational load is high. Nearly three-quarters of IT and security teams lose at least a quarter of their week to repetitive, low-value work, and around one in three lose more than half.

• The most overloaded teams are the most optimistic about AI. 59% of the most overloaded US teams, and 55% in the UK, expect AI to ease the load.

"Misplaced confidence is one of the most dangerous things in security. This data shows executives are far more confident that AI risk is under control than the evidence supports. Most of the conversation right now is about productivity, when the bigger question is how AI can be turned against the business. The report shows the gap between how secure leaders feel and how secure they actually are," said Adam Pilton, Cybersecurity Advisor at Heimdal.

Independent security researcher Rafay Baloch, CEO and Founder of REDSECLABS, added: "The risk that concerns me most is not AI itself but the blind spots it can create. When teams use AI tools without clear oversight, sensitive information, intellectual property, and business data can end up in places leaders never intended. Many organizations believe having an AI policy means they are prepared, but a policy alone does not create visibility. The companies seeing the best results are not the ones trying to restrict AI. They are the ones creating clear guardrails while helping employees use AI responsibly."

The report concludes that organizations should treat AI as part of the core IT estate, applying the

same scrutiny to AI services as to any other critical supplier, including procurement review, contractual data-handling terms, a current inventory of sanctioned and unsanctioned AI tools, and technical controls over access, execution, action chains, and privilege.

The full report is available at https://heimdalsecurity.com/blog/state-ai-risk-management/

About the research
The State of AI Risk Management in 2026 is based on a survey of 1,000 IT professionals (500 UK, 500 US), conducted via Pollfish from 1 to 8 May 2026. The sample spans six seniority tiers from entry-level through C-suite and VP.

About Heimdal
Heimdal is a global cybersecurity provider offering a unified security and compliance platform across endpoint, identity, email, network, and access security. More than 17,000 customers in over 40 countries use its 12-plus integrated products to prevent threats, detect breaches, and automate response.

Danny Mitchell
Heimdal Security
+44 7999 498241
email us here
Visit us on social media:
LinkedIn
YouTube
X