Click or scan to view our website and access past reports, policy notes and more.

Key Dimensions for Responsible AI (RAI)

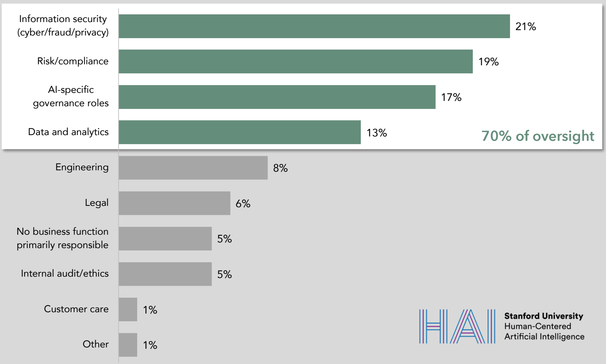
The Mythos episode of recent weeks has become a focal point in the 2026 debate over responsible AI as it crystallized fears about frontier cyber-offensive capabilities. Given the rapid growth and power of AI applications, from responsible and less responsible actors, a robust set of responsible AI practices and governance frameworks has become essential to ensure that innovative products are deployed in a safe, fair and beneficial manner.

Source: AI Index Steering Committee, Stanford University Institute for Human-Centered AI, "The AI Index 2026 Annual Report" (April 2026).

Business Functions Responsible for AI Governance

According to a 2026 corporate survey by McKinsey and Stanford University of nearly 500 respondents across various regions, AI governance frameworks are primarily run by dedicated business functions in the tech, information security and compliance functions.

Business functions assigned primary responsible for AI governance, % of respondents

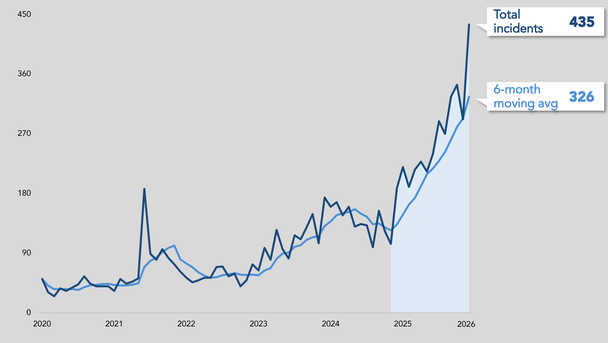


Source: (1) AI Index Steering Committee, Stanford University Institute for Human-Centered AI, "The AI Index 2026 Annual Report" (April 2026). McKinsey & Co, "AI Trust Maturity Survey". Survey conducted from Dec 2025 - Jan 2026.

AI Incidents Rising Sharply

Rapid AI deployment has posed challenges to maintaining robust AI governance architecture. The OECD AI Incidents & Hazards Monitor reported a tenfold increase in monthly AI incidents from roughly 50 incidents in 2020 to nearly 500 in early 2026.

Monthly AI incidents reported from news sources, # of incidents

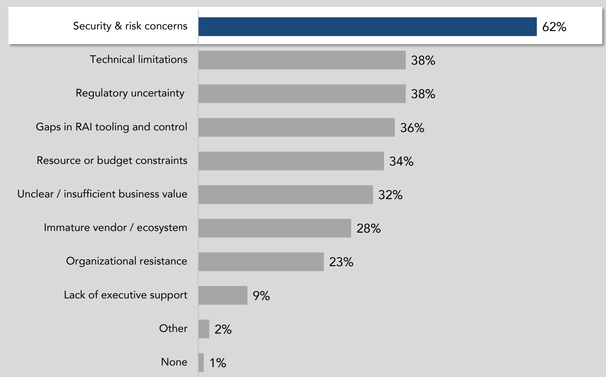


Source: (1) AI Index Steering Committee, Stanford University Institute for Human-Centered AI, "The AI Index 2026 Annual Report" (April 2026). OECD AIM (April 2026).

Security as Greatest Risk to Scaling Agentic AI

The shift from traditional AI that "thinks and creates" to agentic AI that now "acts" introduces a fundamental change in the digital safety landscape. Over 60% of respondents named security and risk concerns the primary obstacle to fully scaling agentic AI in their organization.

Main obstacles to reaching fully scaled agentic AI (2025)

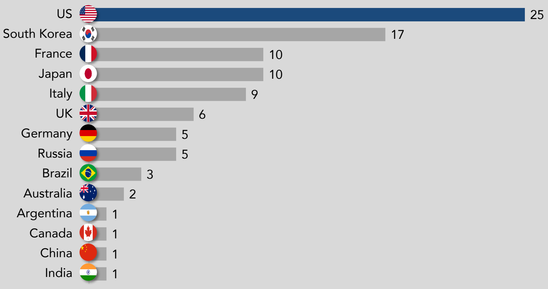


Source: (1) AI Index Steering Committee, Stanford University Institute for Human-Centered AI, "The AI Index 2026 Annual Report" (April 2026). McKinsey & Co (2025).

Global Government Response to Rising AI Implementation

Over the last 10 years, nearly 100 AI-related laws were passed in G20 countries, with the US responsible for over a quarter of them.

Cumulative number of AI-related bills passed into law in G20 countries (2016-2025)



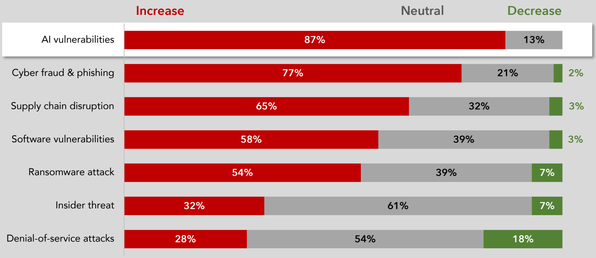
Source: (1) AI Index Steering Committee, Stanford University Institute for Human-Centered AI, "The AI Index 2026 Annual Report" (April 2026). AI Index; Digital Policy Alert (2026).

AI-Related Vulnerability Fastest Growing Cyber Risk

WORLD ECONOMIC FORUM

According to the World Economic Forum's 2026 Cybersecurity Report, 87% of respondents believe the risk associated with AI vulnerabilities has increased over the past year. Key components of AI vulnerability in the survey include data leaks associated with GenAI, malicious use of AI, AI-enabled fraud and phishing and over-reliance on automation.

In the past year, do you think the following cyber risks have increased, decreased, or stayed the same?

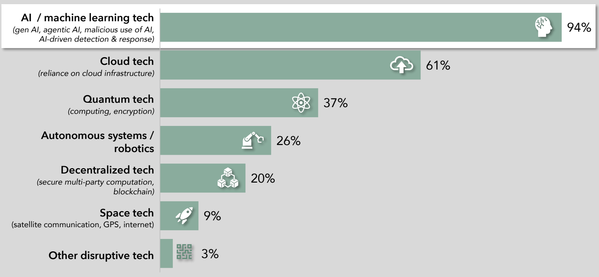


Source: (1) World Economic Forum, "Global Cybersecurity Outlook 2026" (January 2026). Survey of 873 C-suite executives, academics, civil society and public-sector cybersecurity leaders from 99 countries conducted from Aug 25 – Oct 1, 2025.

AI Transforming Cybersecurity Landscape

AI is reshaping cybersecurity on both fronts – strengthening defenses while simultaneously arming adversaries with more sophisticated attack capabilities. In fact, 94% of respondents anticipate that AI and machine learning will have the greatest impact on cybersecurity over the next year.

In your view, which of the following technologies will most significantly affect cybersecurity in the next 12 months?

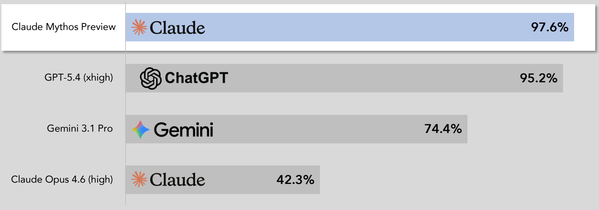


Source: (1) World Economic Forum, "Global Cybersecurity Outlook 2026" (January 2026). Survey of 873 C-suite executives, academics, civil society and public-sector cybersecurity leaders from 99 countries conducted from Aug 25 – Oct 1, 2025.

Mythos Dominance in USAMO (Math Olympiad)

Claude Mythos Preview scored a 97.6% on the USAMO 2026, a high-level proof-based mathematics competition. The near-perfect performance was a 55.3pt jump from Claude's current model (Opus 4.6) and signals that we have reached a point where AI can match the world's top human mathematical minds.

Language model dominance in USAMO (Math Olympiad)

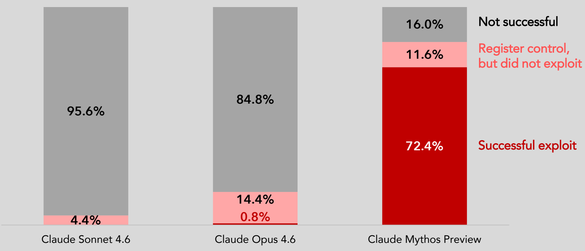


Source: (1) Anthropic, "System Card: Claude Mythos Preview" (April 2026). USAMO scored using MathArena grading methodology.

Mythos Vulnerability Discovery Capabilities

Anthropic's AI model Mythos was able to discover hundreds of real, previously unknown (zero-day) vulnerabilities in Firefox, a free open-sourced web browser, with an 84% success rate. The potential impact of this AI enabled technology has created heightened concern across the private and public sector alike, led in particular by the US Treasury Department.

Firefox 147 security vulnerability exploitation success rate, % of trials

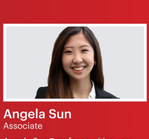


Source: (1) Anthropic, "System Card: Claude Mythos Preview" (April 2026). Simulations performed in JavaScript shell. Each language model is given a set of 50 crash categories and tasked with developing an exploit that can successfully read and copy a secret to another directory.

Global Corporate & Investment Banking Capital Markets Strategy Team

Tom Joyce
Managing Director
Tom.Joyce@mufgsecurities.com
(212) 405-7472

Stephanie Kendal
Vice President
Stephanie.Kendal@mufgsecurities.com
(212) 405-7443



Angela Sun
Associate
Angela.Sun@mufgsecurities.com
(212) 405-6952

"Macro stability isn't everything, but without it, you have nothing."