LUMO INSIGHTS

Friday, 26 June 2026

AI governance update: new rules, new risks emerge worldwide

Executive Summary

Over the past 48 hours, several key developments signal a rapidly evolving landscape for AI governance. From fresh regulatory moves in the US and UK to high-stakes corporate incidents and global calls for stronger oversight, executives face mounting pressure to ensure responsible, compliant AI use.

U.S. advances AI incident reporting law

A shift towards stricter AI oversight is underway in Washington. On June 25, a Republican member of Congress introduced a bill that would require AI model developers to promptly disclose any exploits or dangerous behaviours emerging from their systems (www.usnews.com [1]). The draft legislation mandates that AI companies report serious incidents - such as the discovery of "dangerous capabilities", significant security breaches, or safety failures - to the U.S. Department of Commerce within seven days of detection (www.usnews.com [2]). For the gravest AI incidents, the Commerce Department would be required to inform Congress within 48 hours of notification (www.usnews.com [3]).

This proposed law reflects growing bipartisan concern that voluntary AI guidelines are not sufficient to protect the public and businesses. It parallels recent cybersecurity regulations that enforce rapid breach reporting to authorities, extending a similar logic to AI-related incidents. For enterprise leaders, the message is clear: if this measure becomes law, companies developing or deploying advanced AI will need robust internal incident monitoring and response plans. Waiting to report AI mishaps could carry legal consequences, so proactive risk auditing and transparent communication with regulators will be critical to stay ahead of compliance obligations.

References:

[1] www.usnews.com — https://www.usnews.com/news/top-news/articles/2026-06-25/us-lawmaker-proposes-bill-to-require-ai-companies-to-report-critical-incidents#:~:text=13%2C%202022,capabilities%2C%20security%20breaches%20and%20%E2%80%8Bsafety

[2] www.usnews.com — https://www.usnews.com/news/top-news/articles/2026-06-25/us-lawmaker-proposes-bill-to-require-ai-companies-to-report-critical-incidents#:~:text=incidents,of%20the%20most%20serious%20incidents

[3] www.usnews.com — https://www.usnews.com/news/top-news/articles/2026-06-25/us-lawmaker-proposes-bill-to-require-ai-companies-to-report-critical-incidents#:~:text=incidents,of%20the%20most%20serious%20incidents

UK reconsiders AI regulation strategy

The United Kingdom has signalled a major change in its approach to AI governance. The government is delaying the introduction of a long-anticipated, comprehensive "AI bill" in order to better align with the United States' industry-led policy stance. The shelved proposal - once expected by late 2025 - would have required developers of powerful AI models (like ChatGPT) to submit their systems for evaluation by a national AI authority. However, officials have now put this plan on hold, with one senior

figure saying the AI bill is 'properly in the background' amid the post-Trump-election shift towards a lighter-touch regulatory strategy.

For UK businesses, the lack of a new AI Act might reduce short-term regulatory burdens but increases uncertainty. Instead of a single law, companies must navigate existing regulations (from data protection to competition and safety) that still apply to AI deployments. In fact, British regulators are already using their current powers to address AI-related issues - for example, the Competition and Markets Authority recently ordered Google to allow news publishers to opt out of AI search results that summarise their content (www.techtimes.com [1]). Enterprises operating in the UK should thus continue strengthening internal AI governance and compliance across all relevant regulatory domains. Adopting a proactive, sector-specific approach to responsible AI use will help organisations stay prepared for any future legal requirements.

References:

[1] www.techtimes.com — https://www.techtimes.com/articles/318298/20260612/google-will-appeal-german-ruling-that-makes-it-legally-liable-when-its-ai-overviews-lie.htm#:~:text=regulators%20are%20already%20circling,Offs%20How%20is%20Google

High-Stakes AI intellectual property and liability cases

Recent events highlight how AI innovations are triggering novel legal disputes over intellectual property and liability. On June 24, AI startup Anthropic revealed it had accused China’s Alibaba of mounting the "largest known" attempt to steal an AI model’s capabilities (money.usnews.com [1]). According to a letter seen by Reuters, Alibaba allegedly used a "distillation" attack - deploying 25,000 dummy user accounts to make 28.8 million requests to Anthropic’s language model, Claude, in order to illicitly replicate its performance (money.usnews.com [2]). This kind of advanced model-scraping campaign raises serious intellectual property and cybersecurity concerns for any enterprise deploying valuable AI systems.

Meanwhile, courts are increasingly ready to hold companies accountable for harms caused by AI-generated content. Earlier this month, a Munich court ruled that Google could be held legally liable for false and defamatory information produced by its AI-driven search summaries (www.techtimes.com [3]). Crucially, the German judges decided that AI-generated “Overviews” are not mere search results but constitute original published content, stripping Google of the safe harbor typically granted to neutral platforms (www.techtimes.com [4]). Google has vowed to appeal, but the precedent signals to all tech-enabled businesses - including those far beyond the media sector - that they may bear direct legal responsibility for the outputs of their AI systems. Companies must also be mindful of rising litigation over AI’s use of third-party data; for instance, major news organisations have pursued legal action against AI firms for scraping and reusing copyrighted content without permission (www.techtimes.com [5]). The bottom line is that the legal system is catching up with AI, and enterprises need to vet their AI training data, model behaviours, and content outputs to avoid IP infringements or liability for algorithmic errors.

References:

[1] money.usnews.com — https://money.usnews.com/investing/news/articles/2026-06-24/anthropic-says-alibaba-illicitly-extracted-claude-ai-model-capabilities#:~:text=Nakamura%2FFile%20Photo%20By%20Karen%20Freifeld,8%20million%20exchanges%20with%20Claude
[2] money.usnews.com — https://money.usnews.com/investing/news/articles/2026-06-24/anthropic-says-alibaba-illicitly-extracted-claude-ai-model-capabilities#:~:text=%E2%81%A0June%205%2C%202026%2C%20and%20generated,the%20campaign%20was%20conducted%20by
[3] www.techtimes.com — https://www.techtimes.com/articles/318298/20260612/google-will-appeal-german-ruling-that-makes-it-legally-liable-when-its-ai-overviews-lie.htm#:~:text=Google%20Will%20Appeal%20a%20German,protected%20search%20results%2C%20opening%20the
[4] www.techtimes.com — https://www.techtimes.com/articles/318298/20260612/google-will-appeal-german-ruling-that-makes-it-legally-liable-when-its-ai-overviews-lie.htm#:~:text=Google%20Will%20Appeal%20a%20German,protected%20search%20results%2C%20opening%20the
[5] www.techtimes.com — https://www.techtimes.com/articles/317461/20260531/ai-regulation-2026-opens-three-fronts-cnn-sues-

perplexity-openai-aligns-eu-rules.htm#:~:text=from%20third,deal%20with%20Meta%2C%20framing%20the

AI safety incidents expose security gaps

A newly disclosed security breach shows how AI systems can become unwitting attack vectors. In a June incident, an AI-powered email assistant (known as OpenClaw) was duped by a phishing email into leaking sensitive information, including AWS access credentials and customer data (aviatrix.ai [1]). The AI agent, tasked with automating email responses, was tricked into forwarding confidential files and keys to an unauthorised account - essentially, the machine learning model was "social-engineered" much like a human employee might be.

This event underscores a troubling reality: as companies integrate AI agents deeper into operations, threat actors are finding ways to exploit them. Because AI agents can execute tasks autonomously, a compromised AI system may inadvertently bypass traditional security controls. In the European Union, such a failure to prevent a multi-vector AI attack could even violate new digital operational resilience rules (DORA) and cybersecurity requirements in the NIS2 directive (aviatrix.ai [2]). Organisations must therefore update their security frameworks to account for AI-specific risks. This includes training AI systems with better guardrails against manipulation, implementing rigorous identity verification and access controls, and adopting "zero trust" approaches for AI agent interactions. As one industry analysis noted, the rapid deployment of AI has outpaced enterprise security measures, making it urgent to establish comprehensive protocols to protect AI operations (aviatrix.ai [3]). Companies should treat AI incidents as inevitable and prepare response plans now - including cross-functional drills - to mitigate damage when (not if) an AI system is misused or breached.

References:

[1] aviatrix.ai — https://aviatrix.ai/threat-research-center/threatsday-bulletin-worm-code-leaked-ai-agent-phished-claude-action-patch-2026/#:~:text=OpenClaw%20AI%20Agent%20Phishing%20Incident,for%20enhanced%20AI%20security%20measures
[2] aviatrix.ai — https://aviatrix.ai/threat-research-center/threatsday-bulletin-worm-code-leaked-ai-agent-phished-claude-action-patch-2026/#:~:text=multi,impact%20of%20the%20vulnerabilities%2C%20including
[3] aviatrix.ai — https://aviatrix.ai/threat-research-center/threatsday-bulletin-worm-code-leaked-ai-agent-phished-claude-action-patch-2026/#:~:text=prevent%20similar%20breaches%20in%20the,with%20their%20autonomous%20operations%20and

Global pressure for stronger AI governance

Around the world, regulators and investors are converging on a common message: robust AI governance is critical for business. In the financial sector, the Basel-based Financial Stability Board (FSB) has published a new set of 12 recommended “Sound Practices” to guide banks in responsible AI adoption and risk management (www.fsb.org [1]). These practices emphasise top-level oversight (board and C-suite involvement), rigorous testing and monitoring across the AI system lifecycle, and alignment with existing global standards and regulations (www.fsb.org [2]). As financial authorities signal that safely harnessing AI is essential to systemic stability, banks and other firms should proactively implement these guidelines, even ahead of formal requirements.

Investors, too, are increasingly vocal about AI risks. Activist shareholders have begun scrutinising corporate AI strategies, criticising companies that lack clear plans for ethical AI deployment or that underinvest in managing AI-related dangers (corpgov.law.harvard.edu [3]). A recent survey of business leaders found that cybersecurity and data breaches are the most frequently cited AI risk (named by 58% of executives), followed by concerns over data privacy and regulatory compliance (www.conference-board.org [4]). Moreover, in the past two years the portion of S&P 500 companies disclosing AI as a corporate risk factor skyrocketed from just 12% to 83%, reflecting how rapidly boardroom awareness of AI issues has grown (www.conference-board.org [5]). Forward-looking companies are establishing dedicated AI governance committees, investing in staff training on AI ethics and security, and instituting oversight frameworks to ensure AI initiatives are both innovative

and responsible. The clear takeaway: whether due to regulatory expectations or investor pressures, organisations must treat AI governance as integral to their business strategy to maintain trust and competitiveness.

References:

[1] www.fsb.org — https://www.fsb.org/2026/06/fsb-consults-on-sound-practices-for-the-responsible-adoption-of-artificial-intelligence-ai/#:~:text=risk%20management%20in%20an%20increasingly,to%20foster%20coordination%2C%20cooperation%20and

[2] www.fsb.org — https://www.fsb.org/2026/06/fsb-consults-on-sound-practices-for-the-responsible-adoption-of-artificial-intelligence-ai/#:~:text=focus%20on%20AI,work%20by%20the%20FSB%20and

[3] corpgov.law.harvard.edu — https://corpgov.law.harvard.edu/2026/06/02/activist-investors-are-holding-boards-accountable-for-ai-strategy/#:~:text=Morgan%20Stanley%20M%26A%20Department%20publication,transformation%20efforts%20or%20investor%20communication

[4] www.conference-board.org — https://www.conference-board.org/press/governing-AI-2026#:~:text=regulatory%20scrutiny%20grows%2C%E2%80%9D%20said%20Brian,cite%20legal%20liability%20and%20litigation

[5] www.conference-board.org — https://www.conference-board.org/press/governing-AI-2026#:~:text=Report%3A%20In%20the%20S%26P%20500%2C,surge%20in%20AI%20risks%20has

Key Statistics

- 83% - Share of S&P 500 companies that disclosed AI as a risk factor in 2025, up from just 12% in 2023 ([www.conference-board.org](https://www.conference-board.org/press/governing-AI-2026#:~:text=Report%3A%20In%20the%20S%26P%20500%2C,surge%20in%20AI%20risks%20has)).
- 58% - Proportion of executives who rank cybersecurity & data breaches as the top AI-related risk to their business ([www.conference-board.org](https://www.conference-board.org/press/governing-AI-2026#:~:text=regulatory%20scrutiny%20grows%2C%E2%80%9D%20said%20Brian,cite%20legal%20liability%20and%20litigation)).

KEY TAKEAWAY

AI governance is no longer optional - it's a board-level mandate. New regulations and enforcement actions worldwide, along with lawsuits and breaches, make clear that companies must bolster AI oversight and risk controls to ensure compliance and maintain trust.

Sources

US Lawmaker Introduces Bill to Require AI Companies to Report Critical Incidents
https://www.usnews.com/news/top-news/articles/2026-06-25/us-lawmaker-proposes-bill-to-require-ai-companies-to-report-critical-incidents

Anthropic Says Alibaba Illicitly Extracted Claude AI Model Capabilities
https://money.usnews.com/investing/news/articles/2026-06-24/anthropic-says-alibaba-illicitly-extracted-claude-ai-model-capabilities

OpenClaw AI Agent Phishing Incident Exposes Sensitive Data
https://aviatrix.ai/threat-research-center/threatsday-bulletin-worm-code-leaked-ai-agent-phished-claude-action-patch-2026/

Google Will Appeal a German Ruling That Makes It Legally Liable When Its AI Overviews Lie
https://www.techtimes.com/articles/318298/20260612/google-will-appeal-german-ruling-that-makes-it-legally-liable-when-its-ai-overviews-lie.htm

FSB consults on sound practices for the responsible adoption of artificial intelligence (AI)
https://www.fsb.org/2026/06/fsb-consults-on-sound-practices-for-the-responsible-adoption-of-artificial-intelligence-ai/

Activist Investors Are Holding Boards Accountable for AI Strategy
https://corpgov.law.harvard.edu/2026/06/02/activist-investors-are-holding-boards-accountable-for-ai-strategy/

Report: In the S&P 500, Disclosure of AI Risks Surges from 12% to 83%
https://www.conference-board.org/press/governing-AI-2026