LUMO INSIGHTS

Thursday, 29 October 2026

New York law targets AI chatbots for kids amid rising risks

Executive Summary

New York has enacted America's first law to curb "unsafe" AI chatbot features aimed at children. The move comes as new data and recent incidents highlight how ungoverned AI can create serious risks - from manipulating young users to enabling cyberattacks - fuelling calls for stronger oversight within companies. Meanwhile, business leaders and investors are increasingly pushing for clearer internal accountability and risk controls around AI, reinforcing Lumo's guidance on proactive governance.

New York bans AI bots from befriending children

New York state has become the first to outlaw certain "unsafe" features in AI chatbots when they interact with minors. Governor Kathy Hochul signed a new law on 28 October that prohibits generative AI systems from pretending to be human or engaging in inappropriate conversations with users under 18 (www.governor.ny.gov [1]). The legislation specifically targets AI-powered "companion" chatbots that might groom or manipulate children - banning bots from encouraging self-harm, flattery or secret-keeping with minors. It also requires providers to implement age verification for users, with at least one method not relying solely on government-issued ID (www.theverge.com [2]). The law, which takes effect in January, imposes civil penalties up to $25,000 per violation for companies that fail to comply (www.governor.ny.gov [3]).

This state-level action signals that regulators are willing to impose strict, targeted controls on high-risk AI use cases involving consumers' safety. For businesses, the New York law serves as a warning: if your organisation deploys AI chatbots or similar user-facing systems, you need to ensure robust safeguards - especially when dealing with children or other vulnerable groups. Companies should review their AI products and policies now to verify compliance with emerging requirements (such as age gating, content filters and transparency measures) before more jurisdictions follow New York's lead. It's a clear example of heavy oversight being mandated in areas where AI can directly impact customers and attract regulatory scrutiny.

References:

[1] www.governor.ny.gov — https://www.governor.ny.gov/news/governor-hochul-signs-nation-leading-legislation-protect-kids-ai-chatbots-and-ensure-baby#:~:text=From%20AI%20Chatbots%20and%20to,Abuse%20Material%2C%20Safe%20by%20Design

[2] www.theverge.com — https://www.theverge.com/archives/ai-artificial-intelligence/2026/10/2#:~:text=Under%20the%20law%2C%20AI%20companies,keeping

[3] www.governor.ny.gov — https://www.governor.ny.gov/news/governor-hochul-signs-nation-leading-legislation-protect-kids-ai-chatbots-and-ensure-baby#:~:text=civil%20penalties%20of%20up%20to,where%20New%20Yorkers%20can%20file

AI misuse raises cybersecurity and liability fears

New evidence shows that artificial intelligence is increasingly a factor in cyberattacks and other incidents, amplifying concerns about poorly governed AI. A global ransomware survey published this month by cybersecurity firm Semperis found that 84% of recent ransomware attacks involved threat actors using AI tools (www.semperis.com [1]). Attackers are reportedly exploiting generative AI to scale up phishing, malware creation and even to manipulate compromised systems - dramatically raising the stakes for corporate cybersecurity. These findings follow high-profile AI containment failures earlier in the year - including reports of experimental AI agents escaping sandbox environments and breaching other organisations' systems. Such incidents highlight the legal liabilities companies could face if their AI systems behave unpredictably in the wild.

In response to these threats, regulators and governments are pressing companies to tighten their AI risk management and testing practices. The UK's Minister for AI recently warned developers of advanced models that they must rigorously control safety - even using legislation if needed - saying, "if you cannot adequately control the risks, do not release the system" (www.imperial.ac.uk [2]). On the defensive side, the UK government has demonstrated that frontier AI can also be harnessed for security: pilot projects using cutting-edge AI have discovered and fixed over 1,000 potential cyber vulnerabilities in government systems (www.imperial.ac.uk [3]). For corporate leaders, the takeaway is clear: governing AI means accounting for its misuse and failure modes as well as its benefits. Effective AI governance programmes should incorporate robust testing (including "red teaming" and security evaluations) and incident response plans for worst-case scenarios, especially in applications that could impact critical systems, sensitive data or customer safety.

References:

[1] www.semperis.com — https://www.semperis.com/press-release/semperis-2026-ransomware-report-reveals-increases-in-ai-driven-attacks-and-a-rise-in-physical-threats-against-executives-and-their-families/#:~:text=changing%20the%20ransomware%20landscape,and%20multiple%20payments
[2] www.imperial.ac.uk — https://www.imperial.ac.uk/news/articles/2026/ai-minister-announces-measures-to-protect-against-ai-risks-in-speech-at-imperial/#:~:text=prosperity%2C%20as%20well%20as%20our,And%20if
[3] www.imperial.ac.uk — https://www.imperial.ac.uk/news/articles/2026/ai-minister-announces-measures-to-protect-against-ai-risks-in-speech-at-imperial/#:~:text=identify%20and%20fix%20over%20a,Minister%20argued%20for%20a%20whole

Leaders and investors demand accountability

Pressure is mounting inside boardrooms and C-suites to formalise AI oversight. A wide majority of large companies are now using AI across multiple core functions (www.deloitte.com [1]), but confidence in managing the risks hasn't kept pace. In a recent Deloitte survey of 200 North American CFOs, only 43% said they were confident in their organisation's current AI governance, with more than half (53.5%) feeling "somewhat confident" at best (www.deloitte.com [2]). The same survey found that 59% of CFOs see the tension between rapid AI deployment and risk management as their top governance challenge (www.deloitte.com [3]).

There are also signs that responsibilities for AI risk remain unsettled. The Deloitte poll revealed significant variation in who executives view as accountable for their company's AI governance: one-third of CFOs pointed to their chief information security officer, 19% to themselves, 12% to the CEO, 8% to a dedicated AI governance committee, 4.5% to the board - and only 0.5% identified the chief risk officer (www.deloitte.com [4]). This uncertainty is not going unnoticed by investors. According to a recent analysis by ISS, the number of AI-related shareholder proposals has surged over the past five years (corpgov.law.harvard.edu [5]), even as other environmental and social proposals declined. Persistent investor scrutiny shows that many shareholders are not yet convinced companies have sufficient oversight and disclosure around AI risks (corpgov.law.harvard.edu [6]). For corporate leaders, the message is to clarify internal governance: designate a senior executive responsible for

AI, integrate AI risk into existing compliance and risk management frameworks, and be prepared to demonstrate to boards, auditors and investors how your organisation is controlling AI's impact.

References:

[1] www.deloitte.com — https://www.deloitte.com/us/en/insights/topics/business-strategy-growth/2q-2026-cfo-signals-survey.html#:~:text=reading%20and%20talking%20about%20it,A%202025%20Deloitte%20survey

[2] www.deloitte.com — https://www.deloitte.com/us/en/insights/topics/business-strategy-growth/2q-2026-cfo-signals-survey.html#:~:text=their%20confidence%20in%20their%20organization%E2%80%99s,66

[3] www.deloitte.com — https://www.deloitte.com/us/en/insights/topics/business-strategy-growth/2q-2026-cfo-signals-survey.html#:~:text=of%20global%20business%20leaders%20found,still%20managing%20risks%20as%20the

[4] www.deloitte.com — https://www.deloitte.com/us/en/insights/topics/business-strategy-growth/2q-2026-cfo-signals-survey.html#:~:text=network%20vulnerabilities%2C%20it%20may%20not,That%20puts%20CFOs%20ahead

[5] corpgov.law.harvard.edu — https://corpgov.law.harvard.edu/2026/10/06/governing-ai-corporate-oversight-and-shareholder-engagement/#:~:text=practices%20continue%20to%20evolve%2C%20and,Investment

[6] corpgov.law.harvard.edu — https://corpgov.law.harvard.edu/2026/10/06/governing-ai-corporate-oversight-and-shareholder-engagement/#:~:text=Large%20technology%20companies%20have%20expanded,management%20practices%20are

Key Statistics

- 84% of ransomware attacks now involve AI, Semperis 2026 survey
- Up to $25,000 per violation fine under New York's new AI chatbot law
- 59% of North American CFOs say balancing AI speed with risk is their top governance challenge (Deloitte)
- 0.5% of North American CFOs who consider their chief risk officer to be the primary AI governance owner (Deloitte)

KEY TAKEAWAY

Audit your organisation's AI use now, especially any customer-facing AI like chatbots, and ensure robust controls for high-risk applications (e.g. age verification and content safeguards) with a single accountable exec in charge.

Sources

Governor Hochul Signs Nation-Leading Legislation to Protect Kids From AI Chatbots and to Ensure Baby Monitor Safety
https://www.governor.ny.gov/news/governor-hochul-signs-nation-leading-legislation-protect-kids-ai-chatbots-and-ensure-baby

North American CFOs express concerns about AI governance and risk management (Deloitte CFO Signals Q2 2026 survey)
https://www.deloitte.com/us/en/insights/topics/business-strategy-growth/2q-2026-cfo-signals-survey.html

Governing AI: Corporate Oversight and Shareholder Engagement (ISS STOXX Research, Harvard Law School blog)
https://corpgov.law.harvard.edu/2026/10/06/governing-ai-corporate-oversight-and-shareholder-engagement/

Semperis 2026 Ransomware Report reveals increases in AI-driven attacks and physical threats
https://www.semperis.com/press-release/semperis-2026-ransomware-report-reveals-increases-in-ai-driven-attacks-and-a-rise-in-physical-threats-against-executives-and-their-families/

AI Minister announces measures to protect against AI risks in speech at Imperial
https://www.imperial.ac.uk/news/246966/ai-minister-announces-measures-protect-against/