# AI drives new cyber threats as legal risks and regulatory scrutiny intensify



Artificial intelligence is rapidly reshaping the cyber threat landscape, creating new vulnerabilities for organisations across the UK and US. While offering transformative potential, AI is also enabling more sophisticated attacks and amplifying the complexity of securing digital infrastructure.

Internally, the swift adoption of AI tools often outpaces security reviews. Integrating these systems into existing IT environments introduces vulnerabilities—from unpatched software to excessive access permissions—that threat actors can exploit. These risks are magnified by the speed at which AI is being embedded into core business processes.

Externally, attackers are weaponising AI to automate and scale operations. AI enables faster scanning for network weaknesses and launches parallel attacks that outpace traditional defences. Advanced threats now include polymorphic malware that rewrites its code to evade detection, and AI-powered phishing capable of mimicking voices and creating deepfakes. AI is also being used to mine stolen data for targeted fraud and blackmail.

AI systems themselves are also being attacked. Techniques such as prompt injection and training data poisoning can distort AI outputs, leak sensitive information, or degrade performance. The UK’s National Cyber Security Centre warns that advanced “frontier AI” tools will significantly impact cyber resilience by 2027.

Regulators are responding. In the UK, while no AI-specific cybersecurity law exists, obligations under GDPR and the Network and Information Systems Regulations apply. The NCSC has published guidance to help organisations mitigate AI-related risks. Proposed legislation such as the Cyber Resilience Bill suggests a move towards heightened accountability, with senior executives increasingly exposed to personal liability.

The US framework is more fragmented but similarly evolving. Federal agencies including the FTC and SEC are targeting executives over cyber failings, while state-level laws—like California’s AI transparency rules—mandate incident reporting where AI is implicated in cyberattacks. Legal exposure is rising, and litigation over AI-driven security breaches is expected to grow.

The impact is already visible. The NCSC reported a 16% rise in hostile cyber activity in 2024, with AI-enhanced methods playing a central role. Cabinet Office Minister Pat McFadden noted that AI is increasing both the volume and sophistication of attacks, prompting new cybersecurity strategies and regulatory plans.

Business readiness remains a concern. A global Lenovo survey found 65% of IT leaders doubt their defences can counter AI-powered threats such as polymorphic malware and insider misuse. Many organisations lack effective safeguards for AI assets—models, data and prompts—and face challenges linked to legacy systems, limited resources and skills shortages.

The legal consequences for weak cyber governance are growing. UK law allows for regulatory fines, civil claims and, in some cases, criminal prosecution. The Online Safety Act adds further obligations, especially around harmful or misleading AI content.

Legal teams now play a critical role. In-house counsel must map regulatory duties across jurisdictions, educate senior leaders, and ensure governance structures address AI and cyber risk. Policies should mandate cybersecurity reviews for all AI use, while board-level oversight must be documented.

Vendor agreements require scrutiny. Legal teams should confirm that cloud-based AI providers meet recognised security standards and report incidents promptly. Given that no defence is foolproof, liability mitigation strategies—covering vendor obligations, insurance and financial risk planning—are essential.

Experts advise investing in AI-enhanced threat intelligence, advanced detection tools, and network segmentation. For critical infrastructure, innovations such as remote kill switches may become vital. As AI becomes embedded in business operations, organisations that embed robust, legally compliant cybersecurity frameworks will be better positioned to gain customer trust and unlock new opportunities.

AI is both a powerful asset and a complex risk. The legal landscape is moving toward stricter accountability for cybersecurity and AI governance. Organisations that act now to strengthen their defences and compliance frameworks will be best placed to lead in an AI-driven economy.

Created by [Amplify](https://www.hbmadvisory.com/amplify): AI-augmented, human-curated content.

## Bibliography

1. <https://www.jdsupra.com/legalnews/artificial-intelligence-and-cyber-risk-6849871/> - Please view link - unable to able to access data
2. <https://www.reuters.com/technology/cybersecurity/uk-facing-increased-hostile-activity-cyberspace-security-official-warns-2024-12-03/> - In December 2024, Richard Horne, Britain's cyber security chief, warned of a 16% increase in hostile cyber activities within the UK's cyberspace compared to the previous year. The National Cyber Security Centre (NCSC) reported handling 430 incidents in 2024, up from 371 in 2023. These incidents have become more frequent, sophisticated, and intense, with 347 involving data exfiltration and 20 involving ransomware. The NCSC also issued 542 notifications to organizations, advising them on mitigation strategies. Horne emphasized the underestimation of these risks and cautioned against complacency regarding state-led threats and cybercriminal activities.
3. <https://www.reuters.com/business/retail-consumer/britain-face-more-cyberattacks-ai-adoption-grows-minister-says-2025-05-07/> - In May 2025, UK Cabinet Office Minister Pat McFadden announced that the growth of AI would increase both the frequency and sophistication of cyberattacks in Britain. An intelligence assessment revealed that AI would escalate cyber threats in the coming years. In 2024, the National Cyber Security Centre (NCSC) received nearly 2,000 cyberattack reports, with 90 considered significant and 12 classified as highly severe—a threefold increase in major incidents from the previous year. Recent ransomware attacks have targeted notable British retailers, resulting in significant operational disruptions. McFadden emphasized the necessity of robust cybersecurity measures and announced plans for a new cyber security strategy and legislation under the upcoming Cyber Security and Resilience Bill.
4. <https://www.axios.com/2025/01/07/goldilock-agentic-malware-2027-doomsday> - A NATO-backed report by UK cybersecurity startup Goldilock warns that AI-powered cyber weapons, capable of evading current security tools, could become a reality within two years. These agentic malware threats will primarily target critical infrastructure such as energy grids, transportation networks, financial institutions, and healthcare systems. Given the rapid development of AI technology and the limited guardrails in place, companies must start allocating budgets for advanced cyber defenses immediately. Goldilock recommends investing in AI-enhanced threat intelligence, network segmentation tools, and AI-based detection systems. They also advocate for tools like their remote 'kill switch,' which can disconnect servers from critical infrastructure systems when malicious activity is detected.
5. <https://www.techradar.com/pro/security/most-companies-admit-their-current-security-cant-stop-ai-cybercrime> - A Lenovo report surveying 600 global IT leaders reveals that 65% believe their cybersecurity defenses are outdated and cannot counter modern AI-powered cyber threats. Top concerns include external attacks, insider risks, and protecting AI assets themselves, as generative AI enables more rapid, deceptive, and complex attacks, including polymorphic malware, AI-driven phishing, and deepfake impersonation. Alarmingly, 70% of IT leaders are concerned about employees misusing AI, with over 60% viewing AI agents as an emerging class of unmanageable insider threats. Additionally, crucial AI components such as models, training data, and prompts are becoming high-value targets for attackers. Lenovo VP Rakshit Ghura emphasizes the need to combat AI threats using AI itself, advocating for a dual approach that merges enhanced detection and AI integration into existing defense systems. However, challenges like legacy infrastructure, limited budgets, and skill shortages hinder progress. Despite these obstacles, Lenovo argues that securing AI workplaces not only protects organizations but also fosters growth, lowers costs, and boosts productivity. The report concludes that AI is becoming integral to future business success, and those failing to adapt risk falling behind.
6. <https://www.forbessolicitors.co.uk/articles/ai-powered-cyber-threats-navigating-the-legal-and-insurance-challenges> - As artificial intelligence (AI) becomes more integrated into cybercrime, businesses face not only technical challenges but also critical questions of liability, governance, and insurance. AI has enhanced traditional cybercrime tools, enabling more sophisticated phishing attacks, voice cloning, and video deepfakes that have deceived executives into making fraudulent transactions. For instance, AI-generated voice attacks have been used to impersonate senior officials, leading to unauthorized access to sensitive accounts. The consequences of failing to implement adequate safeguards against AI-powered cyber threats are severe and costly. Civil liability may arise under the UK GDPR and the Data Protection Act 2018, where affected individuals can sue for distress or financial loss if their data is compromised. Regulatory fines imposed by the Information Commissioner's Office (ICO) can reach up to £17.5 million or 4% of global turnover. Contractual liability is also a serious risk; breaches of client agreements or data handling protocols may trigger claims for damages and even contract termination. Criminal liability, while less common, is not out of the question. Under extreme circumstances, such as gross negligence in critical infrastructure settings, prosecutions under the Computer Misuse Act or even the Corporate Manslaughter and Corporate Homicide Act could be pursued. The Online Safety Act further adds a layer of statutory obligation. Failure to prevent harmful AI-generated content on your platform, including deepfakes, could lead to regulatory action, including fines and enforcement measures by Ofcom.