# UK firms lag on AI risk as threats and regulation escalate



Despite rising awareness of AI as a major risk, many UK businesses remain underprepared to manage its challenges, exposing them to security breaches, regulatory penalties and operational disruption. New research from cybersecurity consultancy CyXcel reveals that while nearly a third of UK firms rank AI among their top three risks, a similar proportion lack formal AI governance policies, and many are only just beginning to address the issue.

The study found that 18 percent of UK and US companies are unprepared for threats like data poisoning, where attackers manipulate training data, and 16 percent are vulnerable to deepfakes or identity cloning. These emerging risks underscore the need for stronger oversight and pre-emptive action.

To support businesses, CyXcel has launched a Digital Risk Management platform offering guidance on AI risk identification and governance. Chief Product Officer Megha Kumar said firms want to adopt AI but are held back by the absence of policy frameworks. CEO Edward Lewis highlighted the growing complexity of cybersecurity regulation, including new UK ransomware reporting laws and the EU’s Cyber Resilience Act.

This private sector response complements recent government moves. In November 2024, the UK launched a national AI safety platform, providing tools for impact assessments and bias detection. Science and Technology Secretary Peter Kyle said the initiative supports responsible AI adoption and could unlock a £28 billion fiscal headroom through a projected 5 percent productivity boost.

The UK joins the US and EU in advancing AI regulation, but experts stress that legislation must be backed by public and private investment in computing power and talent to maintain competitiveness. The Social Market Foundation has called for coordinated funding to develop the UK’s AI assurance capabilities.

A government report published this year warns that traditional security methods are inadequate for AI’s complex risk landscape. It maps vulnerabilities across the AI lifecycle and calls for a holistic approach to design, deployment and maintenance.

Market dynamics add another layer of concern. The Competition and Markets Authority has warned about the dominance of six tech giants—Google, Microsoft, Meta, Amazon, Apple and Nvidia—in the AI sector, citing risks to competition and consumer choice. CMA Chief Executive Sarah Cardell stressed the challenge of managing AI’s benefits while curbing harmful market imbalances.

Businesses are being urged to adopt robust governance frameworks that include leadership accountability, risk assessments and staff training. Legal experts also highlight risks around intellectual property and GDPR compliance. The Information Commissioner’s Office has already taken action against firms mishandling personal data in AI systems.

While the UK is building momentum around responsible AI, the gap in business readiness remains a key concern. Closing it will require stronger governance, investment and regulatory agility to turn AI risks into long-term opportunities for economic growth and innovation.

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

## Bibliography

1. <https://dcnnmagazine.com/security/more-than-a-third-of-uk-businesses-unprepared-for-ai-risks/> - Please view link - unable to able to access data
2. <https://www.ft.com/content/8a54932d-d9a9-4a69-969d-89d8b2de149f> - In November 2024, the UK government launched a new AI safety platform to assist businesses in assessing and managing AI risks. The platform offers resources for conducting impact assessments, evaluating AI technologies, and identifying algorithmic biases. Science and Technology Secretary Peter Kyle highlighted the initiative's role in supporting UK businesses to use AI responsibly and positioning the country as a leader in AI assurance expertise. The government aims to integrate AI to boost productivity by 5% and generate £28bn in fiscal headroom. The platform includes a self-assessment tool for small businesses and a partnership with Singapore to advance AI safety research and standards. However, the UK faces global competition, with the US and EU also advancing AI safety measures. Industry advocates emphasize the need for greater investment in computing power and talent to support AI start-ups. The Social Market Foundation has recommended significant public and private sector investment to develop the UK's AI assurance technologies.
3. <https://www.gov.uk/government/publications/research-on-the-cyber-security-of-ai/cyber-security-risks-to-artificial-intelligence> - The UK government's assessment of cyber security risks to artificial intelligence (AI) identifies and maps vulnerabilities across the AI lifecycle, including design, development, deployment, and maintenance. The report highlights that the rapid adoption of AI introduces complex cyber security risks that traditional practices may not sufficiently address. It emphasizes the need for a holistic approach to mitigate vulnerabilities at every stage of the AI lifecycle, thereby bolstering security measures and resilience against evolving cyber threats. The findings underscore the importance of comprehensive risk assessments and the implementation of robust security protocols to safeguard AI systems from potential exploitation and impact.
4. <https://www.theguardian.com/technology/2024/apr/11/uk-has-real-concerns-about-ai-risks-says-competition-regulator> - In April 2024, the UK's Competition and Markets Authority (CMA) expressed concerns about the concentration of power among six major technology companies—Google, Microsoft, Meta, Amazon, Apple, and Nvidia—in the AI sector. The CMA warned that this concentration could lead to anti-competitive dynamics and limit market diversity. Sarah Cardell, CMA's chief executive, emphasized the challenge of harnessing AI's potential while preventing exploitation of market power and unintended consequences. The CMA is committed to applying all legal powers to ensure AI delivers on its promise without compromising competition and consumer choice.
5. <https://dpnetwork.org.uk/ai-risk-and-regulation/> - The Data Protection Network discusses the importance of managing AI use within organisations to ensure efficiency, ethics, and responsibility. Key considerations include establishing senior leadership oversight, identifying key stakeholders, defining roles and responsibilities, understanding existing AI systems, developing appropriate policies and procedures, providing training and AI literacy, conducting risk assessments, and managing suppliers. The article also highlights AI security risks such as vulnerabilities in AI models, data manipulation, malicious attacks targeting training datasets, unauthorised access to sensitive data, and the exploitation of AI by cybercriminals to create sophisticated malware. It underscores the necessity for organisations to adopt a comprehensive governance framework to effectively manage AI risks and harness its benefits safely.
6. <https://www.trowers.com/insights/2023/june/embracing-ai-requires-careful-risk-management> - Trowers & Hamlins law firm advises businesses to carefully consider potential disputes and compliance issues before adopting AI technologies. Key areas of concern include intellectual property rights, conducting comprehensive risk analyses, and data protection. The firm highlights the importance of understanding the sources used within generative AI to avoid copyright infringements and the necessity for thorough risk assessments to identify and mitigate potential exposures. Additionally, the article emphasizes the significance of data protection, noting that personal data used in AI systems is under scrutiny by the Information Commissioner's Office (ICO), which has been issuing fines to companies failing to comply with data protection regulations. The firm recommends that businesses proceed cautiously and ensure they have robust governance structures in place when integrating AI into their operations.
7. <https://www.osborneclarke.com/what-risks-need-be-considered-business-using-artificial-intelligence> - Osborne Clarke outlines the risks businesses should consider when using artificial intelligence (AI), focusing on input risks related to training data and user inputs. The firm emphasizes the importance of understanding the profile of training data to prevent bias and discrimination, as AI systems are only as good as their training data. It also highlights data protection risks, particularly concerning the General Data Protection Regulation (GDPR), noting that if training data includes information about identifiable individuals, it is likely to fall within the scope of GDPR. The article underscores the need for businesses to conduct due diligence on the suitability of AI tools and to ensure compliance with data protection laws to mitigate potential legal and reputational risks.