# UK faces doubling of AI-enabled cyberattacks as preparedness gaps widen



The advent of artificial intelligence (AI) has revolutionised numerous sectors, but its implications for cybersecurity are both profound and alarming. As businesses increasingly adopt AI technologies, the United Kingdom faces a growing threat landscape characterised by AI-enabled cyberattacks. This shift has prompted stern warnings from cybersecurity experts and governmental agencies alike. The National Cyber Security Centre (NCSC) has indicated that a significant "digital divide" may emerge, distinguishing those organisations that can adapt to rapidly evolving cyber threats from those that cannot.

Research conducted by Absolute Security revealed that 54% of chief information security officers (CISOs) feel ill-equipped to deal with these sophisticated AI-driven threats. Andy Ward, an international senior vice president at Absolute Security, referred to the NCSC's warning as a “wake-up call for all UK organisations.” He emphasised that AI is fundamentally reshaping the cybersecurity landscape, advancing both the speed and sophistication of cyberattacks, a sentiment echoed by other experts in the field.

The numbers tell a grim story. In 2024 alone, the NCSC received nearly 2,000 reports of cyberattacks, nearly doubling from previous years, with 90 classified as significant and 12 as highly severe incidents. Cabinet Office Minister Pat McFadden emphasised the necessity of bolstering cybersecurity efforts in light of these escalating risks, highlighting the recent targeting of major retailers such as Marks & Spencer and Harrods by ransomware attacks, which disrupted operations significantly. McFadden called for a new cybersecurity strategy and legislative measures to enhance the UK's defences against these evolving threats.

Moreover, the situation is exacerbated by the emergence of state-sponsored hacking, with entities from countries like Russia, China, and North Korea utilising AI to enhance their cyber capabilities. Richard Horne, CEO of the NCSC, elaborated on this trend, noting that the sophistication of cyber assaults has dramatically increased. The NCSC reported a threefold rise in severe attacks, which have adversely affected critical infrastructures, including health care facilities.

Survey data illustrates the disparity in preparedness among organisations. While 20% of companies report feeling very well-equipped to face high-volume AI-powered attacks, a substantial segment of the workforce remains sceptical. The Arkose Labs report highlighted that only 42% of cybersecurity professionals fully grasp the role of AI within their organisations, revealing significant gaps in knowledge that must be addressed. Coupled with the fact that nearly 95% of cybersecurity professionals believe that AI can enhance detection and response capabilities illustrates a dual-edged sword; while AI can fortify security measures, it also creates avenues for more sophisticated attacks.

In this evolving landscape, the need for proactive measures cannot be overstated. Organisations must leverage AI both to fortify their defences and to comprehend the complexities of the threats they face. Alarmingly, many businesses still lack formal policies governing the secure use of AI technology that could safeguard against these burgeoning threats. With threats evolving rapidly, it is imperative that cybersecurity strategies are continuously updated to keep pace with advancements in technology and tactics employed by cybercriminals.

The government's forthcoming Cyber Security and Resilience Bill is expected to address some of these challenges, aiming to enhance protections for critical infrastructure and supply chains. However, it is clear that the responsibility to safeguard against AI-enabled attacks must also rest with individual organisations. As the cyber threat landscape continues to morph under the influence of AI, remaining vigilant and proactive in cybersecurity strategies will be crucial for all sectors of the economy.

In conclusion, as countries like the UK brace for a future riddled with AI-enabled cyber dangers, collaboration between public and private sectors becomes vital. Only through collective awareness, investment in technologies, and improved education can we hope to bridge the digital divide and create a resilient cybersecurity framework that can withstand the next wave of threats.

### Reference Map

1. Paragraph 1: [[1]](https://www.uktech.news/ai/are-businesses-ready-for-ai-enabled-cyber-threats-20250513)
2. Paragraph 2: [[1]](https://www.uktech.news/ai/are-businesses-ready-for-ai-enabled-cyber-threats-20250513), [[5]](https://www.securitymagazine.com/articles/101434-78-of-cisos-are-experiencing-impact-from-from-ai-cyber-threats)
3. Paragraph 3: [[2]](https://www.reuters.com/business/retail-consumer/britain-face-more-cyberattacks-ai-adoption-grows-minister-says-2025-05-07/), [[3]](https://www.ft.com/content/6603dac2-1c01-41e7-9925-4042500ccc53)
4. Paragraph 4: [[2]](https://www.reuters.com/business/retail-consumer/britain-face-more-cyberattacks-ai-adoption-grows-minister-says-2025-05-07/), [[6]](https://www.reuters.com/technology/cybersecurity/uk-facing-increased-hostile-activity-cyberspace-security-official-warns-2024-12-03/)
5. Paragraph 5: [[4]](https://www.axios.com/newsletters/axios-codebook-4c6813f0-a5ce-11ef-ad2a-91f707f80b70), [[5]](https://www.securitymagazine.com/articles/101434-78-of-cisos-are-experiencing-impact-from-from-ai-cyber-threats)
6. Paragraph 6: [[3]](https://www.ft.com/content/6603dac2-1c01-41e7-9925-4042500ccc53), [[4]](https://www.axios.com/newsletters/axios-codebook-4c6813f0-a5ce-11ef-ad2a-91f707f80b70)
7. Paragraph 7: [[6]](https://www.reuters.com/technology/cybersecurity/uk-facing-increased-hostile-activity-cyberspace-security-official-warns-2024-12-03/)
8. Paragraph 8: [[7]](https://www.axios.com/2024/11/19/ai-cyberattacks-bots-arkose-labs-survey)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.uktech.news/ai/are-businesses-ready-for-ai-enabled-cyber-threats-20250513> - Please view link - unable to able to access data
2. <https://www.reuters.com/business/retail-consumer/britain-face-more-cyberattacks-ai-adoption-grows-minister-says-2025-05-07/> - As AI technology becomes more widespread, the United Kingdom is expected to face an increase in both the frequency and severity of cyberattacks, according to Cabinet Office Minister Pat McFadden. Speaking at the CyberUK 2025 conference, McFadden announced the declassification of an intelligence assessment revealing that AI will 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 including Marks & Spencer, the Co-op Group, and Harrods, resulting in significant operational disruptions. McFadden emphasized that cybersecurity is a vital necessity, not a luxury, and urged both public and private sectors to strengthen their defenses. The government plans to introduce a new cyber security strategy and legislate new powers under the upcoming Cyber Security and Resilience Bill. NCSC CEO Richard Horne also advocated for ending ransom payments to undermine the attackers' business model.
3. <https://www.ft.com/content/6603dac2-1c01-41e7-9925-4042500ccc53> - The UK's National Cyber Security Centre (NCSC) has reported a significant increase in severe cyber attacks over the past year, warning of a widening gap in the nation's ability to combat such threats. The NCSC observed a tripling of these attacks, affecting key organizations like London hospitals and the British Library. Chief executive Richard Horne emphasized the need for increased efforts to keep up with rapidly advancing cyber threats, particularly those from state-led entities such as Russia, China, and North Korea, as well as sophisticated criminal organizations. The NCSC received nearly 2,000 reports of cyber attacks, with a significant number requiring agency support. The agency highlighted the critical need to improve the cyber security of public infrastructure and supply chains and underscored the importance of basic cyber hygiene and strong password practices to fend off commodity cyber attacks. However, the increasing sophistication and volume of state-led and criminal cyber activities pose a growing challenge exacerbated by the use of AI in cyber operations.
4. <https://www.axios.com/newsletters/axios-codebook-4c6813f0-a5ce-11ef-ad2a-91f707f80b70> - In today's newsletter, Arkose Labs' survey reveals that only 20% of companies feel very prepared to defend against AI-powered attacks, which have increased in frequency and sophistication due to generative AI. The survey highlights a disparity in confidence levels between executives and senior directors/managers regarding AI preparedness. Companies deploying AI security tools feel more confident, but AI also brings more sophisticated threats. CrowdStrike has identified a new China-linked cyber-espionage group, Liminal Panda, targeting telecom networks to spy on communications. This raises concerns about China's aggressive cyber tactics and potential geopolitical ramifications. Microsoft is unveiling new cybersecurity features at its Ignite event, including enhancements to Windows device recovery and changes in how security vendors access the Windows kernel. These updates aim to prevent global outages and improve system resilience. Other industry updates include legal actions by X against California and cybersecurity patches from Palo Alto Networks. Heather "Razzlekhan" Morgan receives an 18-month prison sentence for her role in the 2016 Bitfinex hack.
5. <https://www.securitymagazine.com/articles/101434-78-of-cisos-are-experiencing-impact-from-from-ai-cyber-threats> - The 2025 State of AI Cybersecurity report from Darktrace discusses the shifting role of artificial intelligence (AI) in cybersecurity, featuring insights from more than 1,500 security professionals globally. According to the report, 78% of Chief Information Security Officers (CISOs) are seeing impacts from AI-driven cyber threats. This represents a 5% increase from 2024. Although AI-fueled threats are impacting more CISOs, more than 60% of them feel sufficiently prepared to defend against such threats (nearly a 15% increase year-over-year). 95% of cyber professionals think AI can boost the speed and efficiency of prevention, detection, response and recovery efforts against cyber threats. Still, the report emphasizes that knowledge deficiencies persist. Only 42% completely understand the AI in their organization’s security stack, with notable gaps in understanding between CISOs (60%), IT security administrators (14%), and IT security analysts/operators (10%). To shore up the skills shortage, many organizations intend to leverage AI, with 88% asserting the use of AI is essential for improving proactivity and freeing up time for security teams. 64% report plans to involve AI-driven solutions in organizational security stacks, while only 11% report plans to increase cyber staff in 2025. In terms of AI policies, 95% of respondents state their organization is discussing (50%) or implementing (45%) formal policies for secure AI usage.
6. <https://www.reuters.com/technology/cybersecurity/uk-facing-increased-hostile-activity-cyberspace-security-official-warns-2024-12-03/> - Britain's cyber security chief, Richard Horne, has issued a warning about the rising hostile activities within the UK's cyberspace. The National Cyber Security Centre (NCSC) reported a 16% increase in incidents, with 430 cases in 2024 compared to 371 in the previous year. These incidents have become more frequent, sophisticated, and intense, with 347 involving data exfiltration and 20 involving ransomware. The NCSC, a part of GCHQ, also highlighted the issuance of 542 notifications to organizations, advising them on how to mitigate these threats. The annual review pointed to ransomware as the most immediate threat to critical infrastructure and expressed concerns about AI's potential to facilitate more advanced attacks. Horne emphasized the underestimation of these risks and warned against complacency regarding state-led threats and cybercriminal activities.
7. <https://www.axios.com/2024/11/19/ai-cyberattacks-bots-arkose-labs-survey> - A recent survey by Arkose Labs reveals that only 20% of companies feel very well prepared to combat high-volume AI-powered bot attacks. The threat landscape is rapidly changing due to generative AI, with 56% of respondents noting an increase in cyber threats and sophistication. The report highlights the evolving challenges that companies face in adapting their cybersecurity strategies to the capabilities of AI technology. Interestingly, there is a disparity in confidence levels between executives and employees regarding AI preparedness. Companies already utilizing AI security tools tend to feel more equipped to handle these attacks. However, AI proponents express concern about the security threats posed by the technology. To effectively counteract AI-driven threats, organizations must leverage AI to understand the threat landscape, identify attacks, and stay ahead of emerging tactics.