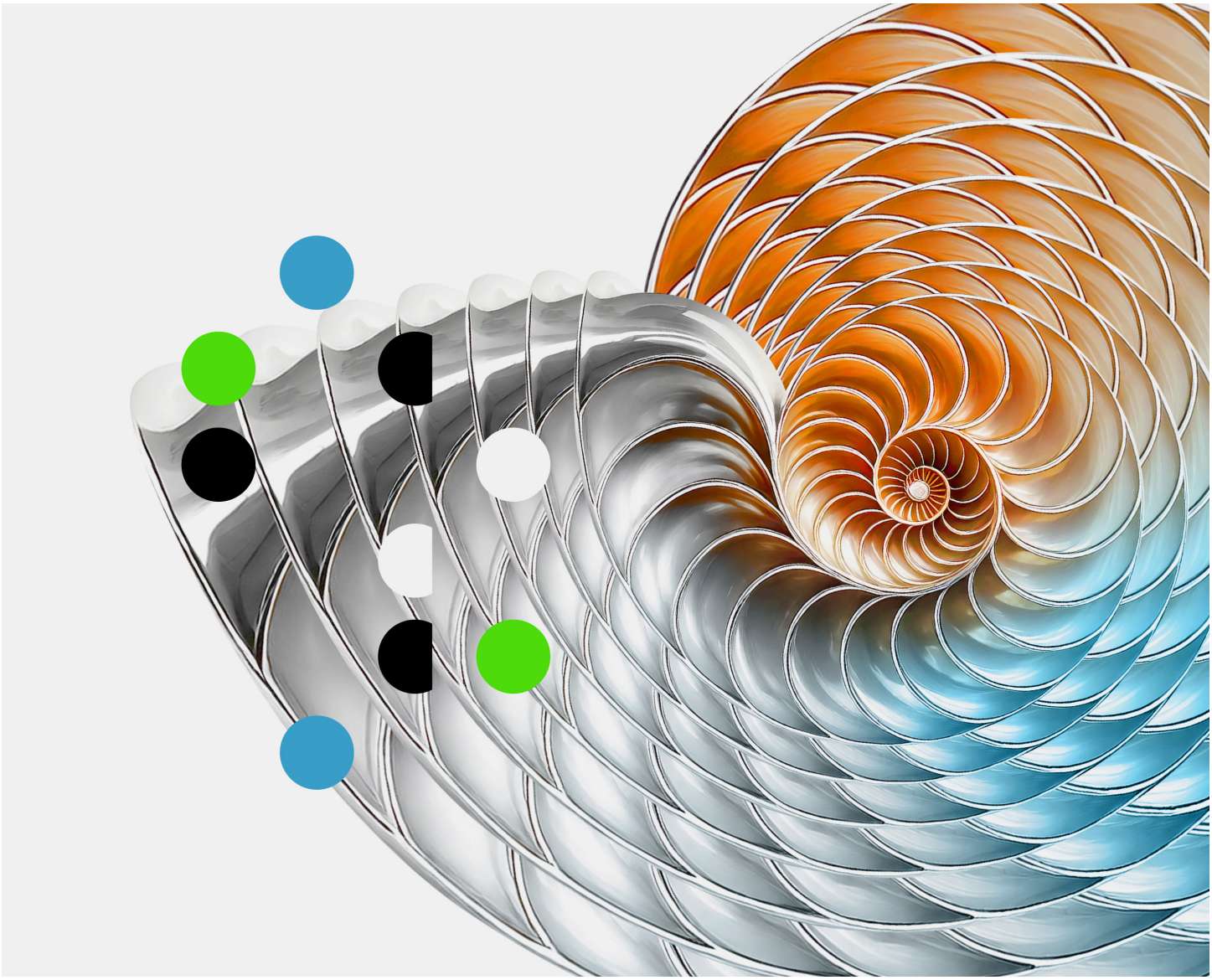
Deloitte.
Together makes progress



Global Tech Trends 2026 | Deloitte Insights

UK perspective: Securing and leveraging AI for cyber defence

AI is a force multiplier for UK organisations, unlocking new value but also amplifying cyber threats.

For UK CIOs, AI is not just another wave of digital transformation, it's a force multiplier that's reshaping both the scale of opportunity and the nature of risk. The same algorithms that can unlock new value for organisations are also being weaponised by adversaries, creating a rapidly shifting battleground.

AI-driven innovation is transforming business models and operations, but it also enables attackers to scale threats and exploit vulnerabilities faster than ever. In the UK, specific considerations such as data sovereignty, regulatory obligations, and evolving guidance from bodies such as the NCSC make this balance particularly critical.

For CIOs, the challenge is clear: maximise AI's benefits while staying ahead of its risks.

A challenging landscape for CIOs

AI brings a host of challenges, from keeping up with the rate of change to data quality, ethical concerns, and talent shortages. As organisations embrace AI, they must also address a range of cyber threats that are becoming more sophisticated and harder to manage.

1. **Data concentration and sovereignty:** LLMs and other AI systems aggregate vast amounts of data into centralised environments, often hosted outside of the UK. This raises material challenges around data sovereignty, GDPR compliance, and cross-border data exposure.
2. **AI model risk:** Vulnerabilities in model design, training data, or validation processes can introduce new attack vectors.
3. **AI application:** Interfaces and integrations expose models to users and third parties, increasing the risk of exploitation through prompts, APIs, or compromised workflows.
4. **AI infrastructure:** The hardware, networks and platforms supporting AI systems create additional dependencies and attack surfaces.

Strategic priorities for CIOs

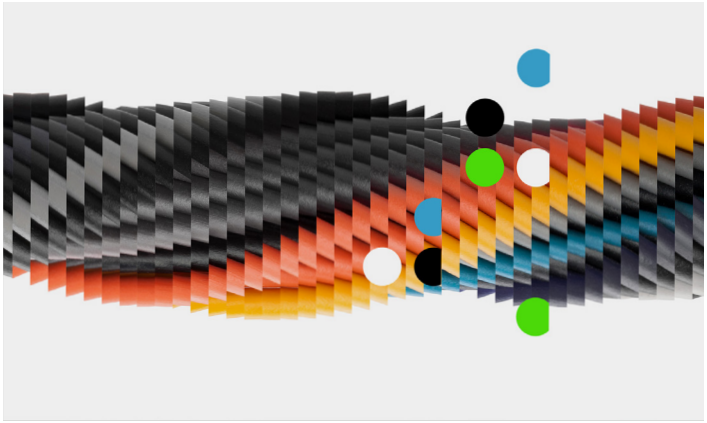
1. CIOs must understand their complete AI footprint, tracking all AI usage across the organisation, including shadow AI, embedded capabilities within SaaS platforms, and token consumption. Uncontrolled adoption introduces unseen risk.
2. There is a pace mismatch between technology and governance. Introduce agile frameworks that allow rapid adoption without limiting progress. Embed security early in design, development and vendor onboarding to keep pace with innovation.
3. AI economics are unpredictable as AI introduces variable, usage-based costs (e.g. token-based consumption) that are difficult to forecast. CIOs must assess value relative to spend, and implement governance to manage this uncertainty.
4. Apply human oversight where it adds value as it can become ineffective if treated as a control point alone. CIOs must define where human judgement is critical and design operating models where humans augment, rather than bottleneck, automated decision-making.

The tech trajectory also suggests the move from agentic to physical AI isn't as far away as we might think, and it's a vital area that CIOs must monitor. It will undoubtedly create more complex and material risks that require progressively sophisticated solutions. And responses will have to match the speed of attack.

AI-enabled defence strategies

While AI can introduce vulnerabilities, it can also provide defensive capabilities. CIOs should consider how AI can be harnessed to strengthen their cyber posture:

1. **Signal enrichment and decision support:** Enhance analysts' ability to interpret events, reduce false positives, and prioritise response.



2. **Response automation:** Streamline elements of response playbooks, enabling faster and more consistent remediation with human oversight.
3. **Risk and compliance intelligence:** Interpret regulatory requirements and risk data, supporting continuous compliance and decision-making. This should also include monitoring token spend to understand the scale of AI usage across the organisation, using consumption patterns as an indicator of where the potential attack surface may be growing.
4. **AI system assurance:** Organisations deploying AI must test models and applications for robustness, resilience, and misuse.

Do we need to redefine trust?

This issue taps into something fundamentally human: trust.

In this agentic era, upholding trust can be complex. With regulation moving slower than the tech itself, how much should you share?

Security cannot be an add on, it must be integral to AI development from day one. Adoption must be supported and encouraged, rather than just implemented, with robust access controls, model isolation, and data sovereignty considerations as mitigation strategies.

Cyber defence priorities

1. Zero-trust remains foundational but must evolve to address AI-driven threats such as identity compromise through highly convincing phishing and synthetic content.
2. Detection, response and remediation at scale is critical, requiring architectures capable of identifying anomalies across users, systems, and modalities, reacting to them at machine speed and recommending actions to reduce their recurrence in a virtuous circle of improvement.
3. Supply chain transparency matters more than ever, with CIOs needing visibility of underlying providers and dependencies in AI ecosystems.

Keep humans in the loop

Human oversight remains essential but must be applied deliberately. CIOs must define where human judgement is required. Invest in skills

to support effective oversight, and design operating models where humans augment, not bottleneck, machine-speed decision-making.

As AI evolves, individuals' responsibilities and capabilities will need to increase exponentially, and it will spark further debate around education provision and workplace skills. It could also broaden the CIO's responsibility to include human capital strategy. That means managing the impact of AI on the workforce and ensuring adaptable teams by focusing on upskilling, talent retention and fostering an environment where human ingenuity and AI capabilities combine.

Where CIOs should prioritise: Securing tomorrow's opportunity

We cannot slow innovation; we must keep up. So, the question remains: how do CIOs realise AI value, like cost reductions, new business opportunities, and productivity gains, while safeguarding company defences? How do you ensure resilience in an AI-native environment?

1. Make sure innovation and safety go hand-in-hand. Skipping security fundamentals can create vulnerabilities that compromise an organisation's competitive position.
2. Invest in AI-enabled cyber capabilities, particularly where they enhance decision-making, response, and risk management.
3. Develop adaptable security architectures to help build organisational resilience as the threat landscape changes.
4. Invest now in 'no regret' foundational capabilities, such as data quality, identity and access management, and scalable infrastructure, to enable secure AI adoption, regardless of how the threat landscape evolves.

By acting decisively, CIOs can shape the future rather than wait for events to unfold. The organisations that pioneer and protect, uphold trust, and recognise the critical role people play will have the advantage.

Learn more

This UK perspective explores one of the key trends featured in our Global Tech Trends report: *The AI dilemma: Securing and leveraging AI for cyber defence.* Read the full trend here.

Key contacts



WIL ROCKALL
Cyber Partner
Technology & Transformation
wrockall@deloitte.co.uk



DMITRY DUDOROV
Cyber Director
Technology & Transformation
ddudorov@deloitte.co.uk

Deloitte.

This article contains general information only and Deloitte is not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this article.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2026 Deloitte Development LLC. All rights reserved.