The hidden risks of shadow AI

Understanding why staff use unapproved AI tools is key to managing the security challenges they can create.

Over the past few years, the use of artificial intelligence (AI) has grown rapidly in many workplaces with employees increasingly exploring how such tools can be incorporated into their jobs.

AI can help people complete tasks more quickly, improve decision-making, save costs and increase productivity.

However, organisations' policies and guidance, which should reflect and manage the risks associated with using these new technologies, have not always developed at the same pace.

Rather than preventing them from using AI, this can mean employees turn to using AI tools that have not been approved by their organisation, introducing new cyber security risks that can be hard to identify.

What is shadow AI?

Shadow AI describes the use of AI technology which isn't captured in an organisation's approved systems and processes. It is a form of shadow IT (or 'grey IT').

Recent research suggests that using shadow AI is widespread, with one study finding that nearly three-quarters of employees (71%) reported using AI tools that have not been approved by their employer.

Where cyber security policies cannot meet business needs, organisations are likely to continue seeing their employees adopt new AI services before they have had time to assess them and provide approved alternatives. This trend is likely to be reinforced as AI capabilities become increasingly affordable and readily available.

What are the cyber security risks of shadow AI?

The use of shadow AI can create risks that organisations may struggle to identify and in turn manage, potentially resulting in breaches and security incidents. For example:

- **Sensitive information may be exposed**

Providing shadow AI access to company or customer data likely increases the risk of data breaches, intellectual property loss and failure to meet regulatory requirements.

- **Organisations can lose visibility and control of data**

Employees who transfer sensitive or proprietary information to consumer AI services will likely reduce the organisation's visibility and control over that information. This is because that information may be stored, retained or used to improve the service – outside established security and governance arrangements – unless specific privacy controls are in place.

- **New opportunities for attackers**

AI agents are complex pieces of software that can have critical security vulnerabilities. If an attacker successfully exploits a vulnerability, they can gain access to the same data, services, and privileges that the agent has legitimate access to.

Attackers are highly likely to use agents with looser guardrails to exploit any vulnerabilities or misconfigurations in the wider corporate IT system.

Encourage staff to choose wisely

The NCSC is not recommending that individuals stop using AI – but when turning to these tools for assistance with a work task, think carefully about which apps and services you are using before you share data.

It may feel natural to stick with using the same AI service that you are familiar with from your personal life – but using systems that are not corporately approved can present real problems for your employer.

Focus on reducing the risk

For organisations, the challenge is ensuring that employees have access to AI tools that meet their needs while managing cyber risk appropriately.

The use of shadow AI is unlikely to disappear completely. As with shadow IT more broadly, the goal should be to reduce risk rather than assume it can be eliminated. To do this, organisations should:

- adopt a positive cyber security culture. Encouraging open communication about cyber security issues means employees are much less likely to turn to shadow IT services, including shadow AI. Organisations that understand why people are using shadow AI are better placed to identify risks, provide secure alternatives and support innovation safely
- securely integrate AI systems into the workplace. Refer to the NCSC and international partners' guidance on careful adoption of agentic AI services

You cannot manage what you do not know. By raising awareness of the risks of shadow AI use within your organisation and understanding the needs of employees, you can help them get the benefits of new technologies while using them securely.

Further reading

The NCSC's cyber security culture principles.

An NCSC blog on thinking carefully before adopting agentic AI.

Simon B

Senior Cloud Researcher

WRITTEN BY

Simon B
Senior Cloud Researcher

PUBLISHED

7 September 2026

WRITTEN FOR

Cyber security professionals

Large organisations

PART OF BLOG

NCSC publications