# Nearly half of workers secretly using unauthorised AI tools, exposing firms to security risks



## The Rising Challenge of Shadow AI: Understanding the Risks and Implications

As artificial intelligence (AI) continues to weave its way into the fabric of the modern workplace, organisations are grappling with the implications of its adoption. A recent report from Ivanti shed light on a troubling phenomenon: the covert use of unauthorized generative AI tools among IT and office workers. Alarmingly, nearly 40% of IT professionals confess to employing these tools without their employer's approval, with the rate climbing to 46% among general office workers. This trend, referred to as "shadow AI," raises serious concerns about skill gaps and security vulnerabilities.

The allure of unauthorized AI usage stems from inadequate training and the lingering fear of job redundancy, as many employees worry that their roles could be replaced by AI technologies. This uncertainty often leads to what has been termed “impostor syndrome,” where one in three workers feel a need to conceal their AI usage to avoid appearing incompetent. Nearly a third of those surveyed in the Ivanti report admitted to keeping their AI activities secret from management, suggesting a significant disconnect in workplace culture regarding technology adoption.

Interestingly, while 44% of organisations have already integrated AI solutions across various departments, a substantial number of employees resort to using unsanctioned tools. This behaviour is not merely a reflection of individual choice; it points to a broader systemic issue within companies—namely, unclear policies surrounding AI use. Brooke Johnson, Ivanti’s Chief Legal Counsel, advocates for a comprehensive governance model that prioritises transparency and inclusivity in AI policies to address this discrepancy.

The concerns associated with shadow AI extend well beyond mere employee choices. A lack of oversight can lead to severe security risks, including data leaks and system vulnerabilities. Unauthorized tools have the potential to bypass existing security protocols, particularly when accessed by those with elevated permissions. Cybersecurity experts warn that the absence of stringent governance frameworks can expose organisations to cyberattacks and data breaches, particularly as insecure APIs and patchy compliance controls come into play.

The rising popularity of tools such as China's DeepSeek, which have attracted scrutiny from agencies like the Pentagon and the U.S. Navy due to data privacy fears, exemplifies the potential risks. Security experts caution that employees using such tools may inadvertently introduce vulnerabilities by inputting sensitive corporate data into unsecured models. As reported, companies often operate with an astonishing array of AI tools—typically 67—of which 90% are unlicensed or unapproved. This underscores the urgency for organisations to pivot from outright bans of these tools to a focus on effective governance and risk management strategies.

To tackle these multifaceted challenges, organisations must start by modernising their IT policies. This involves implementing secure infrastructures that prioritise endpoint protection and stringent access controls through Zero Trust Network Access (ZTNA) solutions. The call for proactive measures is echoed by numerous cybersecurity firms, advocating for a shift in focus from policing usage to fostering an environment where AI can be used safely and effectively.

As employers and IT departments navigate this delicate balance, it is paramount that they acknowledge the human factor at play. Acknowledging the mental stress associated with evolving workplace environments—where nearly a third of workers report anxiety and burnout related to AI usage—is also critical. Clear, supportive policies not only mitigate risks but also empower employees to harness AI’s potential responsibly.

In conclusion, as shadow AI continues to proliferate, its implications—ranging from skill degradation to severe data security breaches—must not be underestimated. Organizations stand at a pivotal crossroads, where establishing clear and inclusive AI governance policies could mean the difference between leveraging AI as a strategic advantage or risking significant operational vulnerabilities.

## Reference Map:

* Paragraph 1 – [[1]](https://www.techradar.com/computing/artificial-intelligence/naughty-naughty-more-than-a-third-of-it-workers-are-using-unauthorised-ai-as-the-risks-of-shadow-tech-loom-large), [[2]](https://www.axios.com/newsletters/axios-codebook-38f09de0-e257-11ef-8ac2-05372d4f3eec)
* Paragraph 2 – [[1]](https://www.techradar.com/computing/artificial-intelligence/naughty-naughty-more-than-a-third-of-it-workers-are-using-unauthorised-ai-as-the-risks-of-shadow-tech-loom-large), [[4]](https://www.axios.com/2024/04/03/ai-security-employers-workers)
* Paragraph 3 – [[1]](https://www.techradar.com/computing/artificial-intelligence/naughty-naughty-more-than-a-third-of-it-workers-are-using-unauthorised-ai-as-the-risks-of-shadow-tech-loom-large), [[2]](https://www.axios.com/newsletters/axios-codebook-38f09de0-e257-11ef-8ac2-05372d4f3eec), [[5]](https://blog.k7computing.com/perils-of-shadow-ai-in-organizations/)
* Paragraph 4 – [[3]](https://www.axios.com/2025/02/04/shadow-ai-cybersecurity-enterprise-software-deepseek), [[6]](https://www.grammarly.com/business/learn/shadow-ai/)
* Paragraph 5 – [[3]](https://www.axios.com/2025/02/04/shadow-ai-cybersecurity-enterprise-software-deepseek), [[5]](https://blog.k7computing.com/perils-of-shadow-ai-in-organizations/)
* Paragraph 6 – [[1]](https://www.techradar.com/computing/artificial-intelligence/naughty-naughty-more-than-a-third-of-it-workers-are-using-unauthorised-ai-as-the-risks-of-shadow-tech-loom-large), [[2]](https://www.axios.com/newsletters/axios-codebook-38f09de0-e257-11ef-8ac2-05372d4f3eec), [[4]](https://www.axios.com/2024/04/03/ai-security-employers-workers)

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

## Bibliography

1. <https://www.techradar.com/computing/artificial-intelligence/naughty-naughty-more-than-a-third-of-it-workers-are-using-unauthorised-ai-as-the-risks-of-shadow-tech-loom-large> - Please view link - unable to able to access data
2. <https://www.axios.com/newsletters/axios-codebook-38f09de0-e257-11ef-8ac2-05372d4f3eec> - This Axios newsletter discusses the rise of 'shadow AI,' where employees use unauthorized AI tools, posing data security risks. IT teams are focusing on governing AI use rather than banning tools outright. The emergence of China's DeepSeek AI tool has raised concerns, leading to its ban by the Pentagon and U.S. Navy. Cybersecurity vendors are developing solutions to monitor and mitigate risks associated with shadow AI. The newsletter emphasizes the importance of governance in maintaining security in an AI-driven environment.
3. <https://www.axios.com/2025/02/04/shadow-ai-cybersecurity-enterprise-software-deepseek> - This Axios article highlights the challenges IT teams face due to unauthorized AI tools, known as shadow AI. The rise of China-based DeepSeek has sparked concerns over data privacy and security, with security executives warning that employees could input corporate data into its open-source model. Studies reveal that companies typically operate with 67 AI tools, 90% of which are unlicensed or not approved. Banning these tools has proven ineffective, shifting the focus towards better governance of AI use.
4. <https://www.axios.com/2024/04/03/ai-security-employers-workers> - A survey by cybersecurity firm 1Password indicates a growing conflict between employees and employers over AI app usage. 22% of 1,500 North American workers, including 500 IT security professionals, admit to knowingly breaking workplace rules regarding generative AI use. This trend highlights the tension between IT departments trying to secure networks and workers wanting to use their preferred tools. Many existing IT security policies were designed for office networks and company devices, leading to friction as employees seek more convenient tools.
5. <https://blog.k7computing.com/perils-of-shadow-ai-in-organizations/> - This blog post discusses the hidden dangers of shadow AI, emphasizing security risks such as data exposure, weak security controls, model exploitation, and unsecured APIs. It also highlights compliance issues, lack of audit trails, and cross-border risks associated with unauthorized AI tools. The article underscores the importance of organizations being aware of these risks and taking proactive measures to mitigate them.
6. <https://www.grammarly.com/business/learn/shadow-ai/> - This article from Grammarly Business outlines the risks associated with shadow AI, including security vulnerabilities, compliance issues, and data integrity concerns. It emphasizes that unauthorized use of AI tools can lead to data breaches, exposing sensitive information to potential cyberattacks. The piece also discusses the challenges organizations face in managing these risks and the importance of establishing clear policies and governance structures.
7. <https://www.atharvgyan.com/2024/09/shadow-ai-use-of-unauthorized-ai-tools.html> - This article defines shadow AI as the use of unsanctioned or unauthorized AI tools by employees without the knowledge or approval of their organization's IT departments. It discusses key concerns such as data security risks, regulatory and compliance issues, and the potential for unauthorized AI to influence business decisions. The piece highlights the importance of organizations being aware of these risks and taking proactive measures to mitigate them.