# More than a third of IT workers using unauthorised AI tools amid rising security and mental health risks



# The Shadow of AI: Navigating the Risks of Unauthorized Use in the Workplace

As artificial intelligence (AI) increasingly permeates the workplace, concerns about its unregulated use are surfacing with alarming frequency. A recent report has revealed that 38% of IT workers admit to using unauthorized generative AI tools, a practice that poses significant risk to both individual employees and their organizations. The findings underscore the need for comprehensive policies and training to address the burgeoning phenomenon of "shadow AI."

The research, conducted by Ivanti, highlights that despite 44% of companies already integrating AI across multiple departments, a considerable number of employees are resorting to unapproved tools. This discrepancy is primarily driven by inadequate training and support, with nearly half of office workers stating that the AI tools they rely on at work were not provided by their employers. The lack of formal training is a widespread issue; a survey of over 14,000 workers across various regions found that 69% had never received guidance on using generative AI safely and ethically. Such statistics suggest a glaring need for organizations to establish clear frameworks governing AI usage.

Interestingly, one in three workers intentionally conceal their use of these tools from management, often fearing the stigma of incompetence or the threat of redundancy. This behaviour reflects a deepening trust gap between employees and organisations. With 27% of individuals reporting feelings of impostor syndrome related to AI use and 30% expressing concern that their roles may be at stake, the connection between unauthorized AI practices and psychological distress cannot be ignored. Such anxiety is compounded by the pressure to keep up with rapidly advancing technologies, leaving many feeling overwhelmed and underprepared.

The risks associated with this clandestine usage extend beyond the psychological; they also encompass tangible security threats. Unauthorised AI tools can inadvertently leak sensitive data and render existing security protocols ineffective. For instance, a separate survey revealed that 38% of employees share confidential company information with AI tools without their employer’s knowledge, often with younger workers (46% of Generation Z and 43% of Millennials) leading the charge. Such actions heighten the possibility of data breaches and cybercrime—issues that are already concerning 65% of workers familiar with the risks of AI technology.

To mitigate these risks, experts emphasise the necessity for organizations to modernise their approach to AI governance. According to Brooke Johnson, Chief Legal Counsel at Ivanti, companies must develop sustainable AI governance models that prioritise transparency. This also involves not merely enforcing stricter controls, but creating an inclusive environment where employees feel comfortable discussing their AI usage without fear of retribution. Effective policies should focus on security measures, such as robust endpoint protection and Zero Trust Network Access (ZTNA) solutions, to manage and monitor unauthorized tool usage effectively.

Moreover, broader industry data supports this need for comprehensive policy development. An ISACA Pulse Poll found that while 69% of digital trust professionals believe adversaries are effectively leveraging AI, only 28% of organisations have allowed the use of generative AI. This suggests a significant gap in organizational preparedness, one that could potentially widen the skills gap within the workforce and strain mental health resources.

As shadow AI becomes a pressing issue, organisations must act to foster a culture of trust and education around AI technologies. This initiative could not only help bridge the skills gap but also protect against the psychological impacts of rapid technological change. The future of AI in the workplace hinges on a collective effort to streamline its integration responsibly, balancing innovation with security and employee well-being.

## 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.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)
* Paragraph 2 – [[2]](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), [[3]](https://futurumgroup.com/insights/more-than-50-of-workers-admit-to-using-unapproved-generative-ai-tools/)
* Paragraph 3 – [[4]](https://www.forbes.com/sites/torconstantino/2024/10/21/55-of-employees-using-ai-at-work-have-no-training-on-its-risks/), [[7]](https://bizstack.tech/news/38-of-employees-share-sensitive-data-with-ai-posing-security-risks/)
* Paragraph 4 – [[5]](https://www.isaca.org/about-us/newsroom/press-releases/2023/ai-policies-are-low-use-is-high-and-adversaries-are-taking-advantage-says-new-ai-study), [[6]](https://www.itbrew.com/stories/2023/04/26/eight-in-10-security-pros-use-unauthorized-ai-tools-survey-shows)

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.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> - A report by Ivanti reveals that 38% of IT workers use unauthorized generative AI tools, raising concerns about skill gaps and security risks. Despite 44% of companies integrating AI across departments, many employees secretly use unapproved tools due to insufficient training. One-third conceal their AI usage to avoid being perceived as incompetent, with 27% experiencing AI-induced impostor syndrome and 30% fearing job replacement, leading to anxiety and burnout. The study emphasizes the need for organizations to establish clear AI usage policies to address these issues.
3. <https://futurumgroup.com/insights/more-than-50-of-workers-admit-to-using-unapproved-generative-ai-tools/> - A Salesforce survey of over 14,000 workers across North America, Europe, Latin America, and the Middle East found that 55% use unapproved generative AI tools at work. This widespread use poses significant IT and cybersecurity risks, including potential exposure of private company data and trade secrets. The survey also highlighted a lack of training, with 69% of workers globally having never received training on using generative AI safely or ethically. The findings underscore the need for organizations to implement clear policies and training programs for AI usage.
4. <https://www.forbes.com/sites/torconstantino/2024/10/21/55-of-employees-using-ai-at-work-have-no-training-on-its-risks/> - Research from the National Cybersecurity Alliance indicates that 55% of employees using AI at work have not received training on its risks. Despite this, 65% express concern about AI-related cybercrime, and 38% admit to sharing confidential work information with AI tools without employer knowledge. The highest incidences of unauthorized sharing occur among younger workers—46% of Generation Z and 43% of Millennials. The study highlights the need for organizations to establish clear AI usage policies and provide comprehensive training to mitigate potential risks.
5. <https://www.isaca.org/about-us/newsroom/press-releases/2023/ai-policies-are-low-use-is-high-and-adversaries-are-taking-advantage-says-new-ai-study> - An ISACA Pulse Poll reveals that 69% of digital trust professionals believe adversaries are using AI as successfully or more successfully than digital trust professionals. Despite this, only 28% of organizations have expressly permitted the use of generative AI, and only 10% have a formal comprehensive policy in place. Over 40% of employees are using generative AI regardless of policies, indicating a significant gap in organizational preparedness to manage AI-related risks.
6. <https://www.itbrew.com/stories/2023/04/26/eight-in-10-security-pros-use-unauthorized-ai-tools-survey-shows> - A survey commissioned by cloud security platform Devo found that 80% of 200 IT security professionals have used AI tools without authorization at work, and 23% are aware of colleagues doing so. Despite this, 78% believe their organization would request they cease using such tools if discovered. The survey highlights widespread dissatisfaction with the state of automation in security operations centers and the need for organizations to address the risks associated with unauthorized AI tool usage.
7. <https://bizstack.tech/news/38-of-employees-share-sensitive-data-with-ai-posing-security-risks/> - A survey by the National Cybersecurity Alliance reveals that 38% of employees share sensitive work information with AI tools without employer permission. This behavior is particularly prevalent among younger workers, with 46% of Generation Z and 43% of Millennials admitting to such actions. Experts warn of serious security risks associated with this behavior, including unintended sharing of personal information and potential data breaches. The study emphasizes the need for organizations to establish clear AI usage policies and provide secure alternatives for employees.