

Hey! What's New? 2025-118

59% of Employees Use Unapproved AI Tools at Work

Cybernews conducted a survey on employees in the U.S. to figure out how they use AI tools at work. "The findings were quite surprising, revealing that the vast majority of respondents used AI tools that were not approved by their employers," the report says

The study shows that "there's still a lot of miscommunication (or overall lack of communication) between employees and employers when it comes to AI tools. Many companies lack any official policy on the use of AI, and employees admit to sharing sensitive information with AI tools. Since many of these AI tools end up leaking customer data, thousands of businesses may be at risk. Additionally, IBM recently revealed that shadow AI (the use of unapproved AI tools at work) can increase the cost of a data breach by an average of \$670K."

Key survey findings included:

- 59% of employees use AI tools that their employer has not approved.
- 75% of employees who use unapproved AI tools shared possibly sensitive information with them.
- Executives and senior managers are most likely to use unapproved AI tools at work.
- 89% of employees understand the risks associated with AI tools.
- 23% of employers don't have any kind of policy related to AI use at work.

The survey points out that 59% of employees admit to using AI tools that haven't been approved by their employers. "More interestingly, out of those using unapproved tools, 57% claim that their direct managers are OK with it and support it, and 16% claim their direct manager doesn't care. This shows that companies are not putting enough effort into raising awareness on the risks of irresponsible AI use."

According to Mantas Sabeckis, Security Researcher at *Cybernews*, "if employees use unapproved AI tools for work, there's no way to know what kind of information is shared with them. Since tools like ChatGPT feel like you're chatting with a friend, people forget that this data is actually shared with the company behind the chatbot. As it turns out, many managers quietly give a thumbs-up to using these tools, even if they're not officially approved. That creates a gray zone where employees feel encouraged to use AI, but companies lose oversight of how and where sensitive information is being shared."

The survey report says that "the biggest risk of unapproved AI tool usage at work is that employees will end up sharing sensitive data with them. As it turns out, 75% of employees using unapproved AI tools admit to sharing potentially sensitive information with them. Most commonly, they admitted to sharing employee data, customer data and internal documents."

Interestingly, the overall share of employees (including both those using and not using unapproved tools) sharing sensitive data with AI tools was 44%. "This means that employees using unapproved tools are much more likely to use them irresponsibly."

"When employees paste sensitive data into unapproved AI tools, there's no guarantee of where that data will end up," says Žilvinas Girėnas, head of product at nexos.ai, an all-in-one AI platform for enterprises. "It might be stored, used to train someone else's model, exposed in

logs, or even sold to third parties. That means customer details, contracts, or internal documents can quietly leak outside the company without anyone noticing. “Once sensitive data enters an unsecured AI tool, you lose control. It can be stored, reused, or exposed in ways you’ll never know about. That’s why companies need secure, approved tools to keep critical information protected and traceable.”

93% of executives and senior managers admitted to using unapproved AI tools at work., the survey found. “Managers, team leaders and supervisors also used unapproved AI tools surprisingly often. This creates an interesting paradox – those who are supposed to set an example and prioritize company security seem to be the most irresponsible when it comes to AI use at work.”

Despite the threats associated with AI tools and their widespread use among employees, nearly a quarter of companies don’t have any kind of official policy regarding the use of personal AI tools at work. “Shadow AI thrives in silence,” adds Girénas. “When managers turn a blind eye and there’s no clear policy, employees assume it’s fine to use whatever tool gets the job done. That’s how sensitive data ends up in places it should never be. AI use in the workplace should never live in a gray zone, and leaders need to set clear rules and give employees secure options before the shortcuts turn into breaches.”

For more on the research and findings, see [59% of employees use unapproved AI tools at work – most of them also share sensitive data with them | Cybernews.](#)