Hey! What’s New? 2025-19

Why Employees Smuggle AI Into Work

An article on the BBC webpage, written by Sean McManus, notes that, according to a survey by Software AG, half of all knowledge workers use personal AI tools. The research defines knowledge workers as "those who primarily work at a desk or computer."

For some, says McManus, “it's because their IT team doesn't offer AI tools, while others said they wanted their own choice of tools. Unauthorized use isn't violating a policy, he adds, “it's just easier than risking a lengthy approvals process, he quotes someone as saying.

The recent release of DeepSeek, a freely available AI model from China, is only likely to expand the AI options, McManus believes. He cites the case of Peter (not his real name), who is a product manager at a data storage company, which offers its people the Google Gemini AI chatbot.

“External AI tools are banned but Peter uses ChatGPT through search tool Kagi. He finds the biggest benefit of AI comes from challenging his thinking when he asks the chatbot to respond to his plans from different customer perspectives. "The AI is not so much giving you answers, as giving you a sparring partner," Peter says. "As a product manager, you have a lot of responsibility and don't have a lot of good outlets to discuss strategy openly. These tools allow that in an unfettered and unlimited capacity."

The version of ChatGPT Peter uses (4o) can analyze video. "You can get summaries of competitors' videos and have a whole conversation [with the AI tool] about the points in the videos and how they overlap with your own products." In a 10-minute ChatGPT conversation he can review material that would take two or three hours watching the videos. He estimates that his increased productivity is equivalent to the company getting a third of an additional person working for free.

The use of unauthorized AI applications is sometimes called “shadow AI.” It's a more specific version of “shadow IT,” which is when someone uses software or services the IT department hasn't approved. Harmonic Security helps to identify shadow AI and to prevent corporate data being entered into AI tools inappropriately. It is tracking more than 10,000 AI apps and has seen more than 5,000 of them in use.

McManus notes that these include custom versions of ChatGPT and business software that has added AI features, such as communications tool Slack. But, he adds,” however popular it is, shadow AI comes with risks.”

He points out that modern AI tools are built by digesting huge amounts of information, in a process called training. Around 30% of the applications Harmonic Security has seen being used train using information entered by the user. “That means the user's information becomes part of the AI tool and could be output to other users in the future.”

Companies may be concerned about their trade secrets being exposed by the AI tool's answers, McManus writes, but notes that Alastair Paterson, CEO and co-founder of Harmonic Security, thinks that's unlikely. "It's pretty hard to get the data straight out of these [AI tools]."

But, McManus adds, “firms will be concerned about their data being stored in AI services they have no control over, no awareness of, and which may be vulnerable to data breaches.” On the other hand, “it will be hard for companies to fight against the use of AI tools, as they can be extremely useful, particularly for younger workers.”

AI “allows you to cram five years' experience into 30 seconds of prompt engineering," says Simon Haighton-Williams, CEO at The Adaptavist Group, a UK-based software services group. "It doesn't wholly replace [experience], but it's a good leg up in the same way that having a good encyclopedia or a calculator lets you do things that you couldn't have done without those tools."

What would he say to companies that discover they have shadow AI use?, asks McManus. Answers Haighton-Williams: "Welcome to the club. I think probably everybody does. Be patient and understand what people are using and why, and figure out how you can embrace it and manage it rather than demand it's shut off. You don't want to be left behind as the organization that hasn't [adopted AI]."

For more, have a look at Why employees smuggle AI into work.