ChatGPT is creating a legal and compliance headache for business

Over the past few months, ChatGPT has taken the professional world by storm. Its ability to answer almost any question and generate content has led people to use the artificial intelligence-powered chatbot for completing administrative tasks, writing long-form content like letters and essays, creating resumes, and much more.

According to research from Korn Ferry, 46% of professionals are using ChatGPT for finishing tasks in the workplace. Another survey found that 45% of employees see ChatGPT as a means of achieving better results in their roles.

But there seems to be a darker side to artificial intelligence (AI) software that is being overlooked by employees. Many employers fear their staff sharing sensitive corporate information with AI chatbots like ChatGPT, which could end up in the hands of cyber criminals. And there's also a question about copyright when employees use ChatGPT for automatically generating content.

AI tools can even be biased and discriminatory, potentially causing huge problems for companies relying on them for screening potential employees or answering questions from customers. These issues have led many experts to question the security and legal implications of ChatGPT's usage in the workplace.

Increased data security risks

The increased use of generative AI tools in the workplace makes businesses highly vulnerable to serious data leaks, according to Neil Thacker, chief information security officer (CISO) for EMEA and Latin America at Netskope.

He points out that OpenAI, the creator of ChatGPT, uses data and queries stored on its servers for training its models. And should cyber criminals breach OpenAI's systems, they could gain access to "confidential and sensitive data" that would be "damaging" for businesses.

OpenAI has since implemented "opt-out" and "disable history" options in a bid to improve data privacy, but Thacker says users will still need to manually select these.

While laws like the UK's Data Protection and Digital Information Bill and the European Union's proposed AI Act are a step in the right direction regarding the regulation of software like ChatGPT, Thacker says there are "currently few assurances about the way companies whose products use generative AI will process and store data".

Banning AI isn't the solution

Employers concerned about the security and compliance risks of AI services may decide to ban their use in the workplace. But Thacker warns this could backfire.

"Banning AI services from the workplace will not alleviate the problem as it would likely cause 'shadow AI' – the unapproved use of third-party AI services outside of company control," he says.

AI is more valuable when combined with human intelligence**Ingrid Verschuren, Dow Jones**

Ultimately, it is the responsibility of security leaders to ensure that employees use AI tools safely and responsibly. To do this, they need to "know where sensitive information is being stored once fed into third-party systems, who is able to access that data, how they will use it, and how long it will be retained".

Thacker adds: “Companies should realise that employees will be embracing generative AI integration services from trusted enterprise platforms such as Teams, Slack, Zoom and so on. Similarly, employees should be made aware that the default settings when accessing these services could lead to sensitive data being shared with a third-party.”

Using AI tools safely in the workplace

Individuals who use ChatGPT and other AI tools at work could unknowingly commit copyright infringement, meaning their employer may be subjected to costly lawsuits and fines.

Barry Stanton, partner and head of the employment and immigration team at law firm Boyes Turner, explains: “Because ChatGPT generates documents produced from information already stored and held on the internet, some of the material it uses may inevitably be subject to copyright.

“The challenge – and risk – for businesses is that they may not know when employees have infringed another’s copyright, because they can’t check the information source.”

For businesses looking to experiment with AI in a safe and ethical manner, it’s paramount that security and HR teams create and implement “very clear policies specifying when, how and in what circumstances it can be used”.

Stanton says businesses could decide only to use AI “solely for internal purposes” or “in limited external circumstances”. He adds: “When the business has outlined these permissions, the IT security team needs to ensure that it then, so far as technically possible, locks down any other use of ChatGPT.”

The rise of copycat chatbots

With the hype surrounding ChatGPT and generative AI continuing to grow, cyber criminals are taking advantage of this by creating copycat chatbots designed to steal data from unsuspecting users.

Alex Hinchliffe, threat intelligence analyst at Unit 42, Palo Alto Networks, says: “Some of these copycat chatbot applications use their own large language models, while many claim to use the Chat GPT public API. However, these copycat chatbots tend to be pale imitations of ChatGPT or simply malicious fronts to gather sensitive or confidential data.

“The risk of serious incidents linked to these copycat apps is increased when staff start experimenting with these programs on company data. It is also likely that some of these copycat chatbots are manipulated to give wrong answers or promote misleading information.”

To stay one step ahead of spoofed AI applications, Hinchliffe says users should avoid opening ChatGPT-related emails or links that appear to be suspicious and always access ChatGPT via OpenAI’s official website.

CISOs can also mitigate the risk imposed by fake AI services by only allowing employees to access apps via legitimate websites, Hinchliffe recommends. They should also educate employees on the implications of sharing confidential information with AI chatbots.

Hinchliffe says CISOs particularly concerned about the data privacy implications of ChatGPT should consider implementing software such as a cloud access service broker (CASB).

“The key capabilities are having comprehensive app usage visibility for complete monitoring of all software as a service (SaaS) usage activity, including employee use of new and emerging generative AI apps that can put data at risk,” he adds.

“Granular SaaS application controls mean allowing employee access to business-critical applications, while limiting or blocking access to high-risk apps like generative AI. And finally, consider advanced data security that uses machine learning to classify data and detect and stop company secrets being leaked to generative AI apps inadvertently.”

Data reliability implications

In addition to cyber security and copyright implications, another major flaw of ChatGPT is the reliability of the data powering its algorithms. Ingrid Verschuren, head of data strategy at Dow Jones, warns that even “minor flaws will make outputs unreliable”.

She tells Computer Weekly: “As professionals look to leverage AI and chatbots in the workplace, we are hearing growing concerns around auditability and compliance. The application and implementation of these emerging technologies therefore requires careful consideration – particularly when it comes to the source and quality of the data used to train and feed the models.”

Generative AI applications scrape data from across the internet and use this information to answer questions from users. But given that not every piece of internet-based content is accurate, there’s a risk of apps like ChatGPT spreading misinformation.

Verschuren believes the creators of generative AI software should ensure data is only mined from “reputable, licensed and regularly updated sources” to tackle misinformation. “This is why human expertise is so crucial – AI alone cannot determine which sources to use and how to access them,” she adds.

“Our philosophy at Dow Jones is that AI is more valuable when combined with human intelligence. We call this collaboration between machines and humans 'authentic intelligence', which combines the automation potential of the technology with the wider decisive context that only a subject matter expert can bring.”

Using ChatGPT responsibly

Businesses allowing their staff to use ChatGPT and generative AI in the workplace open themselves up to “significant legal, compliance, and security considerations”, according to Craig Jones, vice president of security operations at Ontinue.

However, he says there are a range of steps that firms can take to ensure their employees use this technology responsibly and securely. The first is taking into account data protection regulations.

“Organisations need to comply with regulations such as GDPR or CCPA. They should implement robust data handling practices, including obtaining user consent, minimising data collection, and encrypting sensitive information, “ he says. “For example, a healthcare organisation utilising ChatGPT must handle patient data in compliance with the Data Protection Act to protect patient privacy.”

Second, Jones urges businesses to consider intellectual property rights when it comes to using ChatGPT. This is due to the fact that ChatGPT is essentially a content generation tool. He recommends that firms “establish clear guidelines regarding ownership and usage rights” for proprietary and copyrighted data.

“By defining ownership, organisations can prevent disputes and unauthorised use of intellectual property. For instance, a media company using ChatGPT needs to establish ownership of articles or creative works produced by the AI - this is very much open to interpretation as is,” he says.

“In the context of legal proceedings, organisations may be required to produce ChatGPT-generated content for e-discovery or legal hold purposes. Implementing policies and procedures for data preservation and legal holds is crucial to meet legal obligations. Organisations must ensure that the generated content is discoverable and retained appropriately. For example, a company involved in a lawsuit should have processes in place to retain and produce ChatGPT conversations as part of the e-discovery process.”

Something else to consider is the fact that AI tools often exhibit signs of bias and discrimination, which can cause serious reputational and legal damage to businesses using this software for customer service and hiring. But Jones says there are several techniques businesses can adopt to tackle AI bias, such as holding audits regularly and monitoring the responses provided by chatbots.

He adds: “In addition, organisations need to develop an approach to assessing the output of ChatGPT, ensuring that experienced humans are in the loop to determine the validity of the outputs. This becomes increasingly important if the output of a ChatGPT-based process feeds into a subsequent automated stage. In early adoption phases, we should look at ChatGPT as decision support as opposed to the decision maker.”

Despite the security and legal implications of using ChatGPT at work, AI technologies are still in their infancy and are here to stay. Jake Moore, global cyber security advisor at ESET, concludes: “It must be reminded that we are still in the very early stages of chatbots. But as time goes on, they will supersede traditional search engines and become a part of life. The data generated from our Google searches can be sporadic and generic, but chatbots are already becoming more personal with the human-led conversations in order to seek out more from us.”