RISK INSIGHTS

ChatGPT and the Emerging AI Risk Landscape

Artificial intelligence (AI) chatbot ChatGPT has recently made waves for producing human-like text and communications from user inputs. Accessible to anyone with a computer and internet connection, ChatGPT produces usable written material on a wide range of topics and helps make decisions. These functions are leading many employers to consider ways to incorporate this technology into their organizations to enhance workflows, streamline operations and improve customer experience.

This technology is available to employers of all sizes and presents an opportunity for those that strategically leverage it. However, AI tools have certain limitations and potential risks that employers need to consider. Even if organizations don't plan on incorporating AI technology into their business operations, it's still wise to understand these tools and their limitations because employees may use them without their employers' knowledge or permission.

This article explains what ChatGPT is and outlines emerging risk considerations for using AI technology in the workplace.

What Is ChatGPT?

ChatGPT is a natural language chatbot, meaning it uses a natural language processing system to respond in a conversational manner to user inputs. This allows it to imitate human dialogue and decision-making. ChatGPT is capable of performing or helping with a variety of tasks. For example, ChatGPT can write articles, poems and songs; perform calculations; compose computer code and legal contracts; explain difficult concepts and subjects; automate tasks; and converse with users. This technology is advancing quickly and could have a major impact on how employers run and structure their organizations.

ChatGPT is a network machine learning model trained using data sets to generate human-like text on various subjects. The chatbot is trained from books, websites and articles to create questions, answers, summaries, translations, calculations, code, conversations and more. Its knowledge is limited to information that was available when it was trained, and it's unable to access new information.

Workplace Applications of AI Tools

The significance of AI technology for employers cannot be understated, as it could change almost every aspect of how organizations operate and conduct business. Many employers, especially larger ones, have been using this technology for years; however, ChatGPT is not only making this technology readily available to employers of all sizes but also more accepted than in the past.

Incorporating AI technology can enable employers to run more efficiently and economically by automating many tasks currently performed by employees. AI can not only

This Risk Insights is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.

automate and streamline manual, error-prone tasks but also augment how employees work, which could allow them to focus on higher-value tasks. Instead of replacing employees' jobs, tools like ChatGPT will likely alter the work employees do and the value they offer their employers. Nearly every facet of an organization—including HR, marketing, accounting, legal and software engineering—could be impacted by AI technology.

Additionally, organizations can use this technology to help create employment policies and handbooks and calculate payroll deductions. Some AI technology can provide organizations with real-time insights into market trends and customer behavior by conducting research and data analysis.

Risk Considerations

While ChatGPT and other AI chatbots can replicate many human-like behaviors and capabilities, they have limitations that can expose organizations to a variety of risks.

By being aware of the following risks, employers can evaluate and determine whether to implement AI technology in their workplaces:

- **Errors and outdated information**—Technology like ChatGPT creates the impression that it can do more or is more reliable than it is. AI's knowledge is limited since it's based only on the information used to train it. Therefore, the information AI tools provide users may be low quality or outdated, or it may contain errors. As a result, employers cannot be certain that the information this technology provides or what it produces is accurate. In some cases, AI-generated errors can be costly, subjecting organizations to liability, government audits, fines and penalties. Employers would be wise to verify the information produced by AI tools before using it.

- **Privacy concerns**—This technology can create potential privacy issues for organizations. For example, employees may share proprietary, confidential or trade secret information with ChatGPT (or a similar AI chatbot) which will then become part of its database and could be included in responses to other parties' prompts. Additionally, chatbots like ChatGPT are internet-based tools, so security can never be guaranteed. Before using AI technology, employers should consider reviewing and updating their confidentiality and trade secret policies to ensure they cover third-party AI tools.

- **Intellectual property (IP) infringement**—AI-generated content can also potentially violate IP infringement laws. For example, if the chatbot generates content similar to existing copyrighted or trademarked material, the organization using that content could be held liable for infringement. Organizations can train employees on potential copyright, trademark and IP infringement issues or restrict access to AI tools to reduce legal risks.

- **Cybersecurity concerns**—Technology like ChatGPT is likely to be embraced by cybercriminals—particularly those who are not native English speakers—to carry out social engineering attacks, such as crafting legitimate-sounding phishing emails to steal data from organizations. In addition, this technology may have the ability to help cybercriminals write malicious code, allowing less-skilled threat actors to effortlessly launch cyberattacks. Given the potential cybersecurity risks posed by this AI technology, employers should be diligent in updating and maintaining their data security measures and train employees to follow cybersecurity best practices.

- **Inherent bias issues**—Since the information an AI chatbot like ChatGPT provides is dependent upon the information from which it was trained, and the humans who decided what information the chatbot received, there is the possibility of inherent bias issues. For example, if an organization consults an AI chatbot regarding employment decisions, this bias could potentially lead to claims of discrimination. Compliance issues may also come up depending on state and local laws that require notice of AI use in certain employment decisions. Due to the risk of inherent bias, employers should craft policies limiting or prohibiting its use in connection with employment decisions.

Conclusion

While AI tools like ChatGPT are still relatively new, they will likely continue to improve and become more reliable over time. As such, savvy employers must closely monitor AI technology's developments and potential issues to minimize the risks associated with them.

For more risk management guidance, contact us today.