Brown & Brown

WHITE PAPER

What Would (A) I Do About AI?
Corporate Cyber and Employment Risk Considerations Surrounding AI with Assistance from ChatGPT

AUTHORED BY:

Jessica Slater
Assistant Vice President

Christopher Keegan
Senior Managing Director

Exponential advancements in the technology and popularity of AI tools such as ChatGPT has led companies to leverage AI for many applications across industry sectors.

As technology evolves, companies are challenged with innovation and integration into their business and how to best anticipate and prevent associated risks. We asked ChatGPT about the risks that ChatGPT poses to companies. Allowing ChatGPT to outline high-level risk considerations (eloquently at that!), real-world examples, and more detailed commentary from the humans on the Brown & Brown Cyber team follows:

Q: "Can you explain the risks of ChatGPT to companies?"

A: As an AI language model, ChatGPT poses certain risks to companies that choose to use it as part of business operations. Here are some of the potential risks:

- Data Privacy and Security: Companies must ensure that the data they feed into ChatGPT is secure and have proper data protection protocols in place. Any data breaches or leaks could result in serious consequences for the company, including legal penalties, reputational damage and loss of customer trust.

- Bias and Discrimination: ChatGPT may have inherent biases in its training data, which could result in discriminatory responses or actions. Companies must mitigate these biases to ensure that their interactions with customers or clients are fair and equitable.

- Lack of Control: Companies using ChatGPT may not have full control over the responses generated by the model. This means inappropriate or inaccurate responses may be generated, which could negatively impact the company's reputation or even result in legal consequences.

- Misuse of Data: Companies must ensure that employees use ChatGPT for its intended purpose and not for malicious activities. For example, employees may use ChatGPT to extract sensitive data or manipulate customers for personal gain.

- Technical Limitations: ChatGPT is not perfect, and technical limitations or errors may arise during its use. Companies must be prepared to handle these situations and have backup plans to ensure that operations are not disrupted.

Overall, the risks associated with ChatGPT are similar to those associated with any new technology. Companies must proactively address these risks and ensure that they have proper protocols in place to mitigate them.

Brown & Brown Commentary on Risk Evaluation and Mitigation:

What do the humans think?

To date, certain companies have restricted or banned the use of AI tools, and one country has blocked ChatGPT specifically due to privacy concerns. Other companies and countries continue supporting and advancing new AI tool applications. One survey revealed customer service purposes as the most popular AI business application used by companies currently.

Regulatory Reverberations

Alongside these innovations, companies can anticipate regulatory action. Where protected information is involved, expect that privacy regulators will focus on the collection, protection and proper storage of that data in accordance with regulations such as GDPR, CCPA, etc. From an employment perspective, the Equal Employment Opportunity Commission (EEOC) has been monitoring this area. In January 2023, they held a public meeting devoted to AI and potential employment discrimination. The EEOC subsequently issued guidance on the use of AI tools and the Americans with Disabilities Act (ADA), indicating company responsibility for biases perpetuated through processes performed by AI tools.

AI Security Threats

Another angle to consider is the risk associated with human use of ChatGPT in furtherance of a nefarious cause. ChatGPT identifies misuse by company

employees as well as the inability of a company to control all model output. Taking that a step further, there are concerns that AI tools can be used to carry out sophisticated attacks. The latest iteration of ChatGPT has reportedlydeveloped ransomware, obfuscating malware and has improved social engineering capabilities compared to the prior version. This could allow motivated attackers to operate at a higher volume and quicker pace, including those without previously required expertise (think simplified ransomware-as-a-service which perpetuated attacks in the past). In direct opposition and on a more positive note, AI can also be used to bolster cybersecurity and fraud management measures.

Go-Forward Vigilance

Companies embracing emerging technologies should be evaluating risks by prudently reviewing company practices, procedures, and compliance. This includes addressing potential mistakes and biases inherent in AI tools. Continued vigilance is critical as the application of AI tools, and its implications develop at such an unpredictably rapid pace. Specific exposures companies face depends upon how AI is used. Risks must be evaluated through tailored analysis of each company's particular operations and AI applications. Based on the risks outlined above, types of insurance that might be implicated by practices utilizing AI could include Cyber Liability, Employment Practice Liability and others. The Brown & Brown team welcomes opportunities to assist in assessing the impacts of AI technology usage on an organization's overall risk profile and evaluating the appropriate insurance coverage.

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving property & casualty program.

B|B Brown & Brown

Find Your Solution at BBrown.com