Brown & Brown

PROPERTY & CASUALTY

AI Risk Part II

A Risk Manager's Guide: Uncovering the Risks

By, Christopher Keegan

After understanding the essentials of AI, the next step for a risk manager is to apply that knowledge to their company's efforts to employ AI in its business and identify and assess the resultant risks. Because some surveys claim that more than 75% of people are using AI without their company's authorization, it's clear that many companies may not have a strong grasp on what AI exposures they may be facing.[1]

Surveys also indicate that many companies are not providing clear guidance around AI usage, and some employees see AI as a helpful tool when they have a large volume of work and are pressed for time. With the partnership of other company stakeholders, risk managers can create a process to better analyze and quantify AI risk.

Risks will differ from company to company depending upon the type and size of the business, technology being used, databases, outsourcing and depth of AI implementation. Each type of AI has specific use cases that are more appropriate, meaning risks will differ depending upon the use. For example, generative AI is best focused on content generation and conversational user interfaces (UI) where humans are kept in the loop. Conversely, AI math skills, for example, are only at a formative stage and usually are not sufficiently mature enough to be relied upon.

Potentially positive use cases for Generative AI

- Content generation: text, image and video generation; synthetic data creation; coding
- Conversational user interfaces: virtual assistants and chatbots
- Data extraction: positionless optical character reading

Potentially undesirable use cases for Generative AI

- Prediction and forecasting
- Automated decision-making
- Recommendation engines
- Classification and segmentation

1. 2024 Work Trend Report, Microsoft and LinkedIn 5/24. 75% of people are already using AI at work; 46% of them started within the last 6 months; 78% of them are using their own tools (80% in small and medium-sized companies) Over 50% of them are reluctant to admit using it for important tasks.

For an organization to uncover the uses of AI and to understand what exposures the company may be subject to, groups should review appropriate uses and keep track of them. Risk managers should be organizing or taking part in creating simple and lightweight vetting processes to capture the following:

- Business intent of AI product utilization, identifying how and where a person is in the loop
- Type of technology, including the vendor, product and how it is used
- Data being used to build, test and execute the AI solution
- Potential risks and mitigations that have been identified

Entities should seek to incorporate the vetting process into existing processes where possible. These might include:

- Third-party risk management and risk identification initiatives
- Project approval procedures
- Software development lifecycle tools
- Business as usual (BAU) processes followed by analysts and data scientists
- Enterprise risk management frameworks and processes

Specific workshops can be created to bring businesses into the AI risk identification process. Ideally, these workshops would cover some of the following matters on the agenda.

1. AI overviews, training and examples around the art of the possible
2. Identifying pain points, opportunities and solutions leveraging AI to share with a broader group
3. Value and complexity of each solution and prioritization for implementation

Controls for Generative AI Use

- Develop clear usage policies and establish organizational guidelines that outline the acceptable use of ChatGPT and similar AI tools. Employees should be aware of these policies and trained on secure and responsible usage practices.
- Existing policy awareness and enforcement programs should be used to prevent sensitive information from being transferred into AI tools.
- Access to ChatGPT and other AI systems should be restricted to authorized or approved personnel only and subject to robust authentication methods, such as multi-factor authentication.
- All communication between users and AI models should be encrypted to safeguard against potential man-in-the-middle attacks.
- Usage should be regularly reviewed and monitored to detect suspicious activity or potential abuse.
- Create a culture of openness and accountability where employees feel comfortable reporting security concerns or incidents involving ChatGPT or other AI tools.
- Continuously educate your organization on the latest developments in AI security and collaborate with industry peers to share best practices and stay informed about emerging threats.[2]

Insurance implications and coverage

AI risk can create new risks that impact different lines of insurance. To date, most insurers have not made exclusionary changes to their policies to address AI developments. This is likely because AI operations lawsuits have been few and largely focused on copyright in training models, which is not a risk faced by most companies.

How We Can Help

Risk managers looking to ensure their insurance programs are optimized for the new world of AI risk should take steps to assess and identify its use within the entity. At Brown & Brown, we believe that AI-related risks will evolve rapidly, and impacts will be individual depending upon the implementing entity, applications created, controls developed and technology being used. The Brown & Brown team can provide guidance in measuring the impact of technology, cyber and AI on organizations and analyzing insurance programs to align coverage to a company's risk appetite. Our cyber risk models can encompass AI risk scenarios to evaluate individual exposures. Please contact your Brown & Brown representative to further understand our capabilities.

2. For more information on steps that can be implemented see Artificial Intelligence Risk Management Framework (AI RMF 1.0) and the NIST AI RMF Playbook

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 program.

Brown & Brown

Find Your Solution at BBrown.com