

How AI Is Changing Cyber Insurance

As organizations rapidly adopt artificial intelligence (AI) to achieve efficiencies and remain competitive, they may become increasingly vulnerable to cyberattacks, including deepfake fraud and AI-enabled phishing. At the same time, AI's rapid expansion is prompting cyber insurers to reassess whether existing policy frameworks adequately address these risks, as many policies were not originally designed with AI-related exposures in mind. Although the commercial insurance market has yet to reach a consensus on addressing AI-driven threats, many insurers are increasing scrutiny at renewal, which may result in tighter underwriting standards, additional application questions about AI use or more explicit exclusions.

Most Cyber Policies Were Not Built for AI

Traditional cyber insurance policies were drafted before AI became mainstream, meaning many neither clearly affirm nor explicitly exclude coverage for AI-related losses, often referred to as silent AI exposure. While such legacy wording, when read broadly, may suggest that AI-related risks are covered, this ambiguity can create uncertainty. For example, risks such as inaccurate AI-generated outputs and AI system manipulation (e.g., data poisoning) may not cleanly align with traditional cyber policy triggers, potentially creating coverage gaps.

As AI-related claims begin to surface, insurers are gaining a clearer view of how coverage responds in practice, and reliance on broad interpretation may give way to more explicit policy wording and greater underwriting clarity.

Why Insurers are Paying Attention Now

AI is expanding both cyber and liability exposures in ways that are difficult to price. For instance, cybercriminals are using agentic AI to craft sophisticated social engineering scams at scale, while AI-generated voices enable deepfake fraud that is increasingly difficult to distinguish from legitimate communications. Additional exposures include AI-generated errors, regulatory scrutiny and intellectual property concerns. Yet, historical loss data on AI-specific incidents is limited, making it difficult for insurers to assess how frequently such events may occur, their potential severity and the risk of systemic losses.

Regardless, early market responses are already emerging. The Insurance Services Office recently introduced general liability endorsements that carriers can use to exclude losses arising from generative AI, and similar concepts could eventually influence wording changes in cyber and technology errors and omissions (E&O) policies over time.

The Definitional Challenge

Although cyber insurers have generally been slower than some other liability lines to introduce explicit AI-related wording, this is beginning to change. Insurers are taking steps to clarify the extent to which AI-driven events fall within cyber policy triggers, and policy language is evolving to address areas such as deepfake fraud, AI-related regulatory exposure, and IP and copyright risks.

Some insurers are narrowing coverage, while others are introducing affirmative grants for specific AI-related risks, such as data poisoning and liability arising from AI-generated outputs. Additionally, a small number of standalone AI insurance products are entering the market. However, these may overlap with existing cyber and tech E&O coverage, as traditional policies may already cover some AI-related risks (e.g., data misuse and system failures).

What Brokers and Insureds Should Do

Brokers and insureds should work together to carefully review renewal policies and endorsement schedules, paying particular attention to terms such as “machine learning,” “automated output,” and “generative.” They should also coordinate a review of cyber, technology E&O, and management liability policies to identify potential coverage gaps or overlaps. Engaging with carriers to confirm specifically whether AI-related losses are covered, excluded or subject to limitations is essential.

As renewal approaches, organizations should map their AI use to better understand their exposures. They should also document how AI is being used, monitored and controlled, as governance frameworks and risk management practices are becoming increasingly important to underwriters.