



ARTIFICIAL INTELLIGENCE

Got Insurance?

If lawyers are looking for comprehensive AI insurance policies, they're out of luck

BY DANIELLE BRAFF

Lawyers have adopted generative artificial intelligence at a rapid pace. According to a February 2024 LexisNexis survey, 43% of the

Am Law 200 firms had a dedicated budget for investing in generative AI tools.

Sure, AI can speed up mundane tasks and reduce lawyer workload. But it also can be unreliable, and it is frequently disparaged for its hallucinations, biases and incomplete responses.

For instance, in the World Economic Forum's *Global Risks Report 2024*, 1,500 global experts and leaders said AI-generated misinformation and disinformation is the biggest tech risk.

Despite dispelling the cautionary tales of law firm AI usage, there is still no grand plan for insurance that would cover law firms and attorneys against any discrepancies that generative AI may be adding to their work.

Nevertheless, there are some steps lawyers and firms can take to make sure they're covered.

Most firms have professional liability insurance, aka malpractice insurance, and many firms have dedicated cyber liability insurance policies, says Lynda Bennett, a partner and the chair of Lowenstein Sandler's insurance recovery group. But "as with all policies, the devil is in the details of the specific terms and conditions of a policy to determine scope of coverage."

Some lawyers may be surprised, after a claim is presented, to learn that coverage for AI-related claims is not explicitly covered by their malpractice policy. Use of AI tools may not satisfy the definition of professional service

or losses flowing from the use of such tools—particularly if lawyers are sanctioned based on the use of the tool, Bennett says.

“Lawyers may find the coverage that they need in their cyber policies, [but] we are still seeing tremendous variation among the terms and conditions of the coverage offered,” Bennett says.

Other policies—particularly property policies including real estate, land and inventory—also are starting to manage AI risks through the use of low sublimits, Bennett says. For example, a loss from a single AI-related claim may be capped at \$500,000 even though the policy has a face amount of \$10 million. There are two ways insurers limit their losses: by exclusions or by limiting the coverage amount, she says.

Dipping a toe in

Kevin Kalinich, the founder of Aon’s Cyber Solutions Group and leader of Aon’s Intangible Assets Global Collaboration, who is currently writing the insurance chapter for the upcoming 4th edition of *The ABA CyberSecurity Handbook*, says the big issue is determining how to make AI policies worthwhile for insurance companies. The potential return on investment for insureds for policies addressing intangible assets often far exceeds that of tangible assets, he says. Translation: If a damaged tangible property was worth \$1 million and costs \$150,000 to insure, but the intangible assets are worth \$1 million and cost \$75,000 to insure, then the ROI for the intangible assets for the insured is twice the return compared with the tangible assets (assuming the same frequency and severity of risk, which is a big assumption), Kalinich says.

That’s because tangible assets have a clear, market-determined replacement value, while intangible assets are harder to value, so coverage limits may be negotiated or capped.

The insurance companies also need to establish the potential frequency and severity of AI losses, and they need to determine whether it’s possible to cover AI overall.

Typically, insurance companies will base their underwriting decisions on 20 to 30 years of actuarial modeling and loss ratio data. They don’t have that amount of data on the frequency and severity of AI-related losses, Kalinich says. Similarly, after gas-powered cars were created in the late 1800s, it took more than 30 years for a state to mandate auto insurance—and insurance wasn’t required in most of the states until about 1970.

While widespread AI insurance solutions are limited, there are some companies taking the first steps in this direction.

Orbital Witness, a London-based company specializing in generative AI-driven due diligence for real estate transactions, collaborated with First Title Insurance to launch an insurance-backed guarantee for its residential property product. If clients want to add the insurance, they pay a few dollars per policy and would be covered if the AI they use makes a mistake, Orbital Witness co-founder Ed Boule says. So far, they have had no claims, and they’re considering an expansion into commercial property transactions.

Meanwhile, Munich Re, a German multinational insurance company, has been writing insurance products to reduce uncertainties with regard to AI adoption since 2018 via its flagship aiSure product. AiSure provides insurance to AI vendors, who can then offer insurance to their clients—with the promise to compensate the client if the AI tool didn’t perform, according to Michael Berger, the Palo Alto, California-based head of Munich Re’s Insure AI team.

In the last two years, the company has seen the nature and adoption of AI changing.

“The very definition of AI underperformance has changed to now include new risks like hallucination, [intellectual property] infringement or systemic discrimination,” he says. “Our team considered it to be critical to respond to this changing risk profile by broadening our product offering to provide insurance coverage to AI users as well.”

Munich Re offers law firms using AI tools insurance coverage for their own financial losses stemming from AI, as well as coverage for third-party liabilities such as lawsuits and associated costs.

Their AI insurance is available across the board—including for law firms—but the individual process to gain coverage includes due diligence on the AI systems used. Once that’s completed, contract details are created based on individual need. Munich Re declined to provide more details and pricing.

Safety first

Before launching AI insurance for law firms, insurance companies should also determine the authentication protocols in place for access to the firm systems and have strong backup systems in place to maintain and secure access to client documents and other sensitive information.

“Insurers expect law firms to engage in constant vigilance in terms of training personnel with respect to the latest cybercrime tactics through security awareness training modules, simulated phishing exercises and multilayer approval processes to make payments with voice confirmation of payment instructions,” Bennett says.

Also, as widespread cyber- and tech-related outages and attacks continue, insurers will remain focused on supply chain issues and may conduct deeper due diligence during the underwriting process into the law firm’s supply chain of vendors to assess interdependence of systems through contractual indemnification and insurance requirements with vendors, she adds.

Finally, when the insurance companies are confident in the supply chain and authentication protocols, they will need to create an AI-related plan that doesn’t overlap with claims covered by cyber liability and intellectual property insurance policies, says Melissa Ventrone, the Chicago-based leader of the Cybersecurity, Data Protection and Privacy practice at Clark Hill. ■