Lowenstein Sandler's Cybersecurity Awareness Series

Session 15 – Insurance and the Evolving AI Landscape

By Jeremy M. King and Ken Fishkn, CISSP, CIPP/US, CIPM, CIPT

DECEMBER 2025

Ken Fishkin: Hello and welcome to another episode of Lowenstein Sandler's Cybersecurity Awareness series. I'm Ken Fishkin, associate director of the Information Security, and with me today is Jeremy King, partner for the Insurance Recovery Group.

How does AI impact the cyber insurance business with all the challenges that it brings?

Jeremy M. King: AI creates much more complexity and sophistication in what are already threats that can fall within cyber insurance terms. And that means that companies' use of AI is going to be subject to much more scrutiny during underwriting. Underwriters are going to want to look to see that people are being safe and that there's some guardrails around the use, such that there's not increased risks.

AI can create very sophisticated phishing attacks designed specifically for their target. AI can create deepfake videos and trick people into thinking that they're having conversations that they're not really having and can result in the transfer of funds through what insurance calls "social engineering," where it's really just a fake. It's a fraud. But it's all perpetrated by the AI.

There are also new risk vectors that insurers are going to have to be concerned about, like prompt injection attacks and other ways to try to disclose private information, which should trigger typical cyber insurance coverage but wouldn't result from a typical hacking situation. So, it creates a concern about how those policies are going to apply in those situations.

Ken Fishkin: "Prompt injection" is one of those terms that some people don't know about, so I thought maybe we can talk a little bit about what that actually means.

Jeremy M. King: Well, my understanding is that a prompt injection attack is a clever way to probe and query the AI to try to cause it to give answers that typically would be out of the bounds and outside of its training that it's told not to.

So, it's a way to get around safety systems that are in the eye and get information that it has access to that it's not supposed to disclose.

That's where a policyholder needs to be very worried about particularly protected private information getting released—for instance, if you're in the health care industry, and you can trick an AI into giving away people's social security numbers or medical information.

Ken Fishkin: What are some of the recommendations you have for companies to protect themselves against these types of attacks?

Jeremy M. King: Certainly a robust cybersecurity protocol and training and awareness would be important for a company. But from where I sit in insurance, it's certainly understanding the uses that the company has so that when you go to the underwriters, you can buy coverage that's tailored to the specific risks that your company faces. You don't want to try to get just off-the-shelf, cookie-cutter language—you want to make sure that you're working with your broker to have the insurance policy language apply to the technology that your company is going to employ. That way, you can get the best and most comprehensive coverage from the process.

Companies should also be aware of sub-limited coverage. Not all limits in the policy apply to everything and often there are lower limits for certain kinds of things like social engineering, and a company should just be aware about how that works.

Ken Fishkin: And with the recent hack with Anthropic, where AI kind of took over everything and started attacking systems autonomously, what can cyber insurance do as far as that's concerned, since it's so brand new?

Jeremy M. King: The agentic attack on Anthropic is terrifying from a cybersecurity standpoint. Typical cyber insurance policies, we in the Insurance Recovery Group would argue, would cover that because the trigger for the hacking and security breach coverage isn't necessarily a human agent actor. However, you do want to make sure that in your cyber security policy, you are covered for that security breach or access to your systems. That then would cause either disruption and a loss of information or might cause a business interruption that you would put in and apply for under the policy and have covered.

Ken Fishkin: So are there new products that are out now to help people deal with these AI attacks?

Jeremy M. King: Yes. Insurers are releasing new products almost monthly at this point to try to address some of these problems. I would warn folks to look carefully at any kind of AI endorsements that are put on policies just to make sure they really function to expand coverage rather than to restrict or exclude AI-caused events, but you also have some companies that are out now offering products that purport to cover false information from AI or the AI hallucinations or business interruptions that might be caused by a reliance on AI systems and when they shut down or malfunction.

Ken Fishkin: For the hallucination mistakes that the AI models produce, can insurance cover that as well?

Jeremy M. King: Like everything in insurance, the answer always lies in the specific and particular policy terms, so you'd have to analyze the policy very closely.

An agentic hacking attack certainly indicates that we're traveling down the road to where AI can do more and more on its own without the intervention of human agency.

Ken Fishkin: Scary times indeed. Well, thank you, everyone, for joining us for another episode of Lowenstein Sandler Cybersecurity Awareness series.