



## Lowenstein Sandler's "In the Know" Series Video 37

### AI is Changing Cyber Risk—Is Your Insurance Keeping Up?

By [Heather Weaver](#) and [Bryan Sterba](#)

NOVEMBER 2025

---

**Heather Weaver:** Welcome, everyone. I'm Heather Weaver, counsel in Lowenstein Sandler's [Insurance Recovery Group](#), where I help policyholders secure coverage for complex cyber and technology related claims. I'm excited to be joined today by two fantastic colleagues: [Dave Anderson](#), vice president of cyber at Woodruff Sawyer, and Bryan Sterba, a partner in Lowenstein's [AI](#) and [technology](#) practices.

Today, we're diving into a question that every organization is facing: AI is changing cyber risk, but do current insurance policies actually keep up? And if not, what can businesses do to close those gaps?

AI is transforming how companies work faster, smarter, and more efficiently, but it's also creating entirely new kinds of risk. Hackers are using AI to write incredibly convincing phishing emails, create deepfake videos that sound like real executives, and spot security weaknesses in seconds. But it's not just hackers—sometimes the AI tools themselves cause problems, like chatbots that accidentally share sensitive information, automated systems that make costly mistakes in pricing, or algorithms that make biased or inaccurate decisions that spark regulatory scrutiny.

So, Dave, a big question becomes when something goes wrong because of AI, will your existing cyber insurance actually cover it?

**David Anderson:** The answer is "sometimes," but only if your policy language is broad enough. Older cyber policies were written for traditional attacks—things like network breaches, malware, or data theft. But with AI, the system might never technically be hacked; a chatbot might just give away private data because of a clever prompt. No malware, no breach. And under old policies, insurers might say that's not covered.

The good news is that coverage is evolving. Newer policies are expanding how they define a computer system to include AI platforms, cloud-based large language models, and third-party AI services. Some now treat AI-related incidents as security failures and extend business interruption coverage to outages or corrupted outputs from AI vendors, not just your own systems. But those updates don't happen automatically,

and you have to ask for them and negotiate to make sure your policy reflects how your business actually uses AI.

**Heather Weaver:** Absolutely. And these risks don't sit neatly in one box; AI isn't just a cyber or IoT issue, it's now a business issue, a deal issue, and a governance issue. Even the strongest coverage can fall short if the company's contracts or risk controls are aligned.

Bryan, you're seeing this from the deal and technology side every day. Where are you seeing the biggest risks emerge?

**Bryan Sterba:** Honestly, everywhere—I see it in acquisitions, licensing, product development, and day-to-day operations. Companies are looking for any way to unlock efficiencies by embedding AI into anything and everything in their business. But of course, the quicker you move and the more areas AI touches, the bigger the business impact can be.

When an AI tool makes a mistake or is used improperly, AI-generated content could lead to defamation or IP claims if it influences hiring or compensation decisions. Well, that opens the door to regulatory scrutiny or even discrimination lawsuits. Even without making a mistake, if an AI system is given too much autonomy, it could overutilize, compute, and power resources on unnecessary workflows. So in deals, buyers are now digging further into AI due diligence. They're asking questions like, "Where does your training data come from? If you're scraping data, how are you doing it? What controls do you have on your employees' usage of AI tools, and how do you mitigate risks of models producing biased or inaccurate results? If a company can't answer those questions confidently, it can quickly become a red flag from a board or investor standpoint.

We're also seeing a rise in what's being called "AI washing"—companies talking up their AI capabilities in earnings calls and marketing materials, even when the technology isn't fully developed. If the reality doesn't live up to the hype, well, that can create DNA exposure fast. So these aren't just theoretical risks, they're directly affecting contracts, compliance, reputation, and deal value.

**Heather Weaver:** Exactly, and it's all converging. The same documentation that satisfies a buyer in diligence can also help your broker or underwriter extend broader coverage.

So, Dave, let's connect those dots. One of the fastest growing threats we've seen this year is deepfake fraud. Picture this: someone impersonates a CFO on a Zoom call, directs an urgent wire transfer, and the team approves it because the video and voice were completely real. Twenty minutes later, the money's gone. Why do these kinds of claims still fall into an insurance "gray zone?"

**David Anderson:** It really comes down to outdated policy language. Many older crime policies were written long before deepfakes existed; they only cover

fraudulent instructions sent by email or in writing. So if the scam happens live over Zoom, Teams, or WhatsApp, insurers often say that's not covered or they keep it under a small social engineering supplement. But that's starting to change.

Underwriters are moving away from checkbox questionnaires and focusing on real tested controls like out-of-band payment verification, dual approvals for transfers, and phishing-resistant MFA. If you can show these controls are in place, insurers are much more willing to expand coverage, raise limits, or even offer deepfake-specific endorsements.

The coverage is out there, you just need to demonstrate operational maturity.

**Heather Weaver:** And that same theme—governance and accountability—run straight through tech info coverage, too. Those policies protect companies when their technology or services cause harm to a customer. But with AI, it gets complicated—the act might come from the model itself, not a person.

So if an AI tool gives a customer bad advice or makes a faulty recommendation that causes financial loss, the policy needs to treat that output as your act. Stronger policies are already doing that, and it's critical. Without that clarity, you could have the technology driving your business, but no coverage when it fails.

Bryan, how is this playing out in your world of contracts and deals?

**Bryan Sterba:** This is going to be a huge issue in how companies define and deliver their services and work with their employees. The “canary in the coalmine” for me is how often we're now being asked for AI policies. We draft to emphasize each employee's personal responsibility for AI usage, often spending much of the document reminding employees that they need to review and own any work product they produce using AI.

And I'm negotiating contracts or advising on transactions--it's more of a mixed bag. Depending on the technology, many businesses want to look right past the risks of using AI and focus on the risk of being left behind. But regardless of what side of the deal we're on, I always want to clarify who takes the risk. You can't just say the algorithm did it and, you know, make the problem go away, somebody is going to need to take responsibility. So the contract just needs to reflect that.

It's also showing up constantly in M&A and venture deals. Buyers are expecting more detail on AI usage, where data comes from, whether it's legally sourced, what rights have been cleared. If those answers aren't solid, it can slow down diligence or affect valuation. So much of the real risk management starts at the contracting stage.

The companies that are thinking about this early baking AI risk allocation strategy into their commercial deals, they're going to be much better positioned as these issues start to unfold.

**Heather Weaver:** So, Dave, as coverage evolves, what do underwriters actually want to see from companies that are using AI?

**David Anderson:** Underwriters want transparency and controls. They want to know how you're using your AI. Is it internal or customer facing? Is it built in-house or through a vendor? Does it touch sensitive or regulated data? Then they look for governance or legal, security, privacy and product teams involved. Do you test models before deployment? Do you monitor for drift or bad outputs? Do you have the ability to roll back or disable AI if something goes wrong? If the answer is "yes," you will get better coverage, stronger terms, and often lower premiums. If not, you'll see more exclusions and supplements.

**Heather Weaver:** So the bottom line: AI is reshaping cyber and liability risk faster than most policies were built to handle. But with the right mix of coverage, contracts, and controls, businesses can stay protected and even negotiate stronger terms than before.

Dave, Bryan, thank you both for sharing your insight, and thanks to everyone for joining us. If you have any questions about AI risk, insurance strategy, or how to align governance, contracts, and coverage, we're always here to help.