# How cybersecurity and AI risk management intersect

## Transcript

SPEAKERS:

Johnny Lee, Risk Advisory Services Principal, Grant Thornton Advisors LLC

Ethan Rojhani, Risk Advisory Services Principal, Grant Thornton Advisors LLC

JOHNNY LEE: I think, admitting the bias as a cyberpractitioner, I think there are a lot of analogies between both management's efforts to manage risk around cyber and management's efforts to manage risk around AI. And the same analogy applies at the board level in that, properly managed, both are categories of enterprise risk. Meaning you bring a multidisciplinary team to the table. You have an HR representative to speak to those concerns. You have a finance representative to speak to those data sets and those concerns, those risks. Likewise with legal and operations and compliance and IT.

So that's the bedrock. You have those multidisciplinary perspectives brought to bear. And then you consult niche expertise where you don't have it in house. You hire specialists. For example, IP attorneys who can speak to the rather draconian responses the courts have when you don't pay attention to the guardrails we mentioned earlier. There are cases out there that now speak to complete disgorgement of products that are developed with AI where those earlier risk management concerns were not properly contemplated.

So not only do you lose the IP, you lose the product and have to dismantle the whole thing you've built. So it's a setback in more than one way. And I think those risks, while drastic, are sort of the starting place for that.

There are real risks and adoption is a real thing. So the question is, do you know what your organization is doing? Are they behind a walled garden? Is their experimentation protected and safe from these drastic results in that your IP is protected, the privacy aspects, the consent issues are addressed?

And the things that are allowed to publish to the models or interact with the models are things that are contemplated and approved, not the sort of surprises that you have to deal with reactively.

ETHAN ROJHANI: I like that a lot. I think you covered most of it. I would say one of the very tactical things that boards can do is to ask management about the disaster recovery and contingency plans that are in place. So most organizations have a disaster recovery and business continuity plan that they have to put in place for many reasons, right? Systems go down. Factories are inoperable. Whatever the case may be. I would ask how AI is being integrated into that plan.

And hopefully there is a plan for them to integrate it into. Otherwise the board has bigger questions to be asking management. I would say taking that very tactical approach is an easy way for boards to get started in thinking about how is the organization thinking about contingencies for potential misuse of AI.

JOHNNY LEE: That's a really great point that I want to tag onto, because like cyber, disaster recovery is an enterprise category of risk, right? And you bring these practitioners to a place where they're able to force rank the prioritization of systems that are critical to the business and in which sequence they're brought back in the event of a catastrophe. You can't do that unless you're having an open dialogue with this multidisciplinary team where the personnel on the employee side are considered, where the customers are considered, where the shareholders are considered. It's a great illustration of that earlier point that properly managed you're getting these multiple perspectives so that you're having a fully risk-informed conversation, and the board can pressure test that.