LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# How GCs Can Leverage AI And Mitigate Risks

By **Sue Reisinger**

*Law360 (March 27, 2024, 4:49 PM EDT)* -- Experts at a cybersecurity summit for in-house counsel this week agreed that the best governance strategies for using artificial intelligence should balance the company's business and ethical culture with its tolerance for risk.

While there are legal and other risks in using AI, they said, there also is great risk in not using it and being left behind by competitors.

The Association of Corporate Counsel Foundation hosted the eighth annual Cybersecurity Summit on Monday and Tuesday at the UCLA campus, bringing together law firms, corporations and government officials to discuss preventing and responding to data breaches.

"In-house counsel and law firms play an integral role in preventing, preparing for, and responding to a cyber incident, and this summit aims to provide them with the specific information they need," said Jennifer Chen, executive director of the ACC Foundation. "Summit speakers made it perfectly clear that the threats posed by cybercriminals are only intensifying in scope and innovation, and that we must all remain ... as prepared as possible. This of course includes a greater focus on the current and future impacts of artificial intelligence."

At a session called "GenAI and Cybersecurity — Integrating Cyber Risk into Your AI Governance Strategy," the moderator was Jennie VonCannon, a litigation partner at Crowell & Moring LLP, which sponsored the program. VonCannon spelled out the differences between cyber threats and cyber risks.

"Cyber threats are essentially the particular dangers that can create potential for cyber risks," she said, such as phishing attacks, malware and deepfakes. VonCannon previously served as the deputy chief of the cyber and intellectual property crimes section of the National Security Division of the U.S. Attorney's Office for the Central District of California.

Cyber risk, on the other hand, "is the potential for business losses from all sectors, such as financial loss, reputational loss, operational loss and productivity loss that happens in the digital domain," she explained.

Generative AI, VonCannon said, has "essentially supercharged cybersecurity in terms of the risk and the threat."

Jonathan Duffie, senior legal counsel and North America AI legal lead for Capgemini, agreed that generative AI has given bad actors valuable new tools and has accelerated their opportunities to attack. Capgemini is a giant business tech consultant, headquartered in Paris.

Kristie Weber, director of privacy at software company Elastic, stressed the foundational privacy issues of generative AI. "You still want to make sure that you don't use more data than you need, and that you disclose how you are using it," Weber said.

Asked about how to choose an AI model, Duffie said to begin by defining the business problem you want to solve.

"I probably sit on six AI calls a week with a diverse group of individuals," he said. "It's like, is this technology useful? What are we trying to solve? And that's a really key component."

For example, Duffie said if one only wants to keep the company's LinkedIn page updated, it can use a small model of AI. But if it needs to translate its policies into 15 different languages, it will likely need a model with larger parameters.

"Starting from there, you'll build out and adapt and align the model to your company, and to a particular use case."

Donna Wilkinson, general counsel of healthcare tech company ChartSpan in South Carolina, shared the mistakes her team made in choosing an AI model.

She described moving through the various phases of using AI — identifying the problem, gathering the data, cleaning and inputting the data, and assessing the outcome.

"What was coming out for us was really no outcomes that we could use," Wilkinson said. "The business hated it. ... We had to go back to step one because we didn't [accurately] assess what the problem was we were trying to solve."

She explained that the commercial AI model they chose was "spitting out [solutions with] too much bias for us because we are in the healthcare space. We deal with a population that is elderly, [and] this was not working for us."

VonCannon talked of three types of AI bias — bias in the data sets that train the models; algorithmic bias placed there by people with their own biases who are programming the algorithms; and cognitive bias, such as Americans who usually use U.S. data sets and lose out on a global perspective.

Duffie talked about the importance of "inclusion," of bringing people with diverse backgrounds to the table to assess the problem and talk about governance issues.

"You need everyone at the table considering the potential uses of this technology and how to mitigate risk," he said. "Because I don't think anybody wants to be the Harvard use case study because you didn't consider the things that you needed to."

VonCannon said having the right number and mix of stakeholders at the table "is core to developing a robust and effective AI governance strategy that's going to address all the risks. ... I see the main pillars as legal, technical and business. And all three pillars need to be at the table."

The panelists then talked about all the laws and regulations being discussed globally as well as in various states, and how companies should move forward despite the uncertainties.

Weber warned of "analysis paralysis" when trying to digest too many laws and regulations and striving to be 100% compliant. She suggested being practical by first complying with laws in the areas where one does the most business.

As for laws in the pipeline now, Wilkinson said, "We already know what regulators will likely want. They're going to want transparency, they're going to want explainability, and they're going to want risk-based governance. I know they're going to want those three things. So, no, I don't have a law in front of me, but I'm going to start building my framework from there."

She also mentioned that some federal agencies have issued AI "playbooks," including the Department of Health and Human Services. "They are not law, but they are really helpful," she said.

--Editing by Rich Mills.