Lowenstein Sandler's Cybersecurity Awareness Series

Session 14 – Agentic AI is Knocking on your Company's Door: Are you Prepared to Deploy It?

By Ken Fishkin and Diane Moss

JUNE 2025

Ken Fishkin: Hello, and welcome to another episode of Lowenstein Sandler Cybersecurity Awareness video series. I'm Ken Fishkin, Senior Manager of Information Security for the firm, and today with me is Diane Moss, counsel in the ECVC group, who focuses primarily on AI governance, IP, and Commercial Contracts. And for today's topic, I thought we'd talk about the risks of dealing with agentic AI.

Diane Moss: Thank you, Ken. I'm excited to have this conversation to raise awareness around agentic AI.

Ken Fishkin: So we all know what ChatGPT is, where we have to give a prompt to the tool and we get a response back. But with agentic AI, it's a little different. It's more like having a personal assistant where we tell that assistant what the overall goal is to be without giving them the individual steps they need to take to achieve that goal.

Diane Moss: Yeah, and I think what's so exciting about agentic AI is this workflow efficiency it brings to the table. But we have to keep in mind with that benefit, there are associated risks.

Ken Fishkin: One of the biggest ones that I see deals with ethics—and the issue really is like, let's say, for example, since these tools don't have any ethics, somebody could easily just say, "I want to find the lowest price of this particular rare toy," and the next thing you know, the tool goes out and finds a wholesaler and tries to blackmail them to get the lowest price for the toy.

Diane Moss: Right, and it's funny because when we mention the word "ethics," I think people immediately think of a human quality. But, you know, programming of these tools is just high-tech, and I really look to, actually, developers at this stage to implement some guardrails around ethics that align at a general, basic level with business concerns and business models. And then from there, deployers have the ability to build upon those protections. But everybody starts with something because, look, hackers will take advantage of all vulnerabilities.

So what else do you see in addition to the ethics?

Ken Fishkin: One other issue that I see deals with AI governance. So imagine if you had a tool that had no governance around it—so, nobody would be accountable, anybody could take advantage of that tool at a company.

Diane Moss: AI governance 101 speaks to visibility and that visibility includes human oversight, having a human in the loop to catch errors at a certain level. But it also involves narrow permissions for the tool, giving it a narrow scope of activity.

And then I think the third prong of that, which is very compatible, is to also have behavioral testing of the tool. So you're not only going to look into what the tool accomplished and how it executed its task, but the manner in which it executed the task. Because one of these things that hinges on the ethics concern is it may complete the task, but not in line with the ethical considerations involved. And that's very important to think about.

Ken Fishkin: When you create these AI agents to run these tests, if you don't adequately define the scope, you could run into a lot of issues. For example, let's say you're a pharmaceutical company that invented an anti-anxiety drug, and you asked it to maximize the coverage to all the potential customers. You could potentially see something where it is spamming customers on a regular basis and trying to manipulate them to buy the product.

Diane Moss: There are fraud protection tools, which I think should also be employed in these instances for additional protection, which minimize the vulnerability of agents to hackers and scammers. So that would be the perfect scenario where a fraud protection tool could catch that and avoid that danger. I really like the idea of including contractual provisions which address the liability in the event an agent does go rogue and acts outside of its permissions.

Ken Fishkin: How does one start the process of mitigating these risks?

Diane Moss: I really like the idea of a shared responsibility model. In this model, developers contain the ethics, deployers contain the scope utilization. And I think when there's that collaborative effort, it's a win from all perspectives.

And then on the other side, in-house with the deployers, you can also internally build a cross team of people involved and engaged in the containing of these risks, and players on that team usually include people from IT, people at a managerial level with enough knowledge and authority regarding the use of these tools, and your counsel. So I think together, if everybody has a hand in this, there's more protection.

Ken Fishkin: Thank you for joining us for another episode of Lowenstein Sandler Cybersecurity Awareness video series.