The governance challenges of AI

Transcript

EDNA CONWAY

I think that in the AI context, look, even humans … everybody has their own bias on this, right? I don't think the robots are taken over. I don't think AI is taking over. So we all can disagree on that. I'm putting my money on us, the carbon-based units, baby, every day of the week.

But I do think that we have to change the way we think about things. And so, if you start to think about agentic (AI) … Vic, you and I talked about this … I am hot on getting people to recognize that there's natural language processing and LLMs (large language models). There's traditional ML (machine learning), and then there's agentic. And to me those agents are nothing more than humans. They're new identities and they can learn.

So, as they learn, how do I, to Jennifer's point, govern them? And how do you break what they're going to do so that we can capture in a predictive way where the break is so we can do a break fix model.

And that's where I get to my dream, which is going right back to security and quality by design, period everywhere, all the time with everyone.

VIKRANT RAI

I agree. I mean, I think you brought up a really interesting point about how do you make this more valuable and address the risks that may be out there. And so, when I think about governance, you know, I always think about governance as, it can be done in three parts, right? You can have a centralized governance, which provides a lot more structure in how policies need to be adopted, how regulatory decisions need to be made. So that's centralized.

The exact opposite of it is a decentralized model. We're seeing centralized governance, but a very decentralized operation. That needs to start talking to each other somewhere along the middle lines, where you almost think of it as a federated model.

Obviously these three are … examples that I mentioned are unique in their own perspectives. Well, what I kind of wanted to highlight here is the two examples of how we're seeing centralized governance that needs to be defined and operationalized at the top, but it also needs to flow down, depending on the business use case, right?

So, every organization is different. What works for one may not work for the other, which is why it is important to take a step back and think about the strategy, put in structure in place.

Like in my experience with my clients, I've seen them defining AI policies, for example. From a governance perspective, they'll have part-time responsibilities within a risk function or an IT function or a, or someone who's heading the, the privacy and the data aspect of it. And so, yes, that that's a good starting point, but I think we'll see more evolution down the road where we'll have dedicated AI strategy and an AI governance "house," if you will, that will help make more strategic decisions, in how the technology unfolds itself in the near future.

JENNIFER BISCEGLIE

And I think all those points are spot on. And I would offer to you that this is where, again, from a Grant Thornton standpoint, it gives you the opportunity to elevate the conversation to an executive- and a board-level conversation. Because you don't want to necessarily slow down the use of this advanced technology, but you have to at some level control it so that it doesn't tank the company. And so there has to be some sort of level guardrails.

I mean, this has been going on forever. When we started being allowed to bring your own devices, right? Before, it was you couldn't bring your own device. Now you can bring your own device, and you can hook it to your network because they put security postures on top of it.

But the board and the executive team need to work with, like the folks at Grant Thornton, to understand that this is the business we're in. These are the guardrails that this business is going to be valued against. And then everybody in the organization needs to understand that and adopt it. Because I think the technology advancements, I think we all agree are bottom up. They're just moving so very quickly that if we don't have that control in place … we want the adoption … if we don't have that control in place, we are going to lose.

AYAN PAUL

I mean, I'll just chime in a couple of things. I mean, more along what we've been talking about. I mean, risks, as we know it, will change completely and this will not be an incremental change. It will be a very large change. And it is well-known that if we have more powerful systems coming online, risks obviously increase because they start to proliferate in a way, the risks proliferate, but also the probability of it getting manifested also proliferates. So there's two things that happen.

I don't think we have a clear assessment of all the risks that we are facing right now. Do we need an answer before we adopt these systems? We won't wait. I didn't say the right answer. The right answer is yes, we must wait. But what will really happen is people won't wait. The industry won't wait. The governments won't wait, essentially because they have to compete against the others.

EDNA CONWAY

All right. I have to jump in for a minute. I'm going to take a different approach.

AYAN PAUL

Yes.

EDNA CONWAY

I think it would be a mistake to wait. Here's why. Sometimes you don't figure out what the risk is until you go do it first. So there's a learning opportunity in that.

AYAN PAUL

So, I completely agree with that. And that is fair. Of course, we'll be happy to help in any manner possible. But the bigger question really is that do we have enough guardrails that the risks we are taking don't lead to a catastrophic failure? We don't know. Honestly, we don't know.

VIKRANT RAI

And risk appetite …

AYAN PAUL

Right. Yes, exactly, exactly. And that is an assessment which is usually done with historical knowledge. We know what happens. We know what breaks, we know what, etc., etc. I know you're smiling because we also look forward and try to assess more and more risks. And some people are really putting in a lot of effort into that. But like the machine learning models we train, we are also trained on data, which is historical data, and hence we are, in a certain way, we are within, what do you call them? Blinkers, right? Or the horses wear …? You have blinders. Blinders.

So, what I would ask the experts who are dealing with this to do is go beyond the traditional definitions of risks, go beyond the traditional definitions of what a system is capable of doing. And only then do we understand that where we stand and where we could be standing in five years as far as assessment of all of these things go.