Transcript

The Community Asks Trish: Cyber Security

Question

Helene Mann: I'd be interested in learning more about how to manage some of the risks in order to make this happen. And so the two [risks] that come to mind are privacy and then also cyber security.

Answer

Trish: Yeah that's a really great question both in terms of data as well as the technology platforms to your point.

So, privacy, one of the things we talked about today in the Summit was being able to put an advisory board together as far as governance and privacy and ethical practices concerned. Because we need to have an understanding of the different populations that are involved and the different data are involved, so we can make the right decisions according to what we decide as an organization we want to have, as our ethical practice, as our... that are going to drive our privacy guidelines. And make sure that we're within compliance and regulatory, depending on what industry we are in, what sector we are in, wherever we are in the world and what populations we are applying data analytics to.

As far as technology is concerned, the same idea around the technology and what often comes up actually when we are talking about technology, and of course what has been in the news a lot lately, has to do with things like fairness and making sure things are not biased in things like artificial intelligence.

So those are also areas that we have to participate in. These are not conversations that can happen outside of us as learning leaders. We need to be engaged in even driving those conversations within our organizations, because, what is bias?

And of course there are a bunch of known different types of biases that can be introduced into artificial intelligence. What are they? in a particulate initiative we are working on, what are the ones most likely to happen. What is the team that you are working with in order to develop the AI technology or to develop those algorithms that are being mediated by AI. What are the potential biases that might apply or show up or be at risk in that particular initiative or that particular project. Because that is a broad scope.

And as much as we make think that bias and fairness in our minds is the same as everybody. That it's a common understanding. It's not. And of course we are going to have some practices that vary in different parts of the world. So, we really need to be not only participating in these conversations, but leading those conversations.

As far as the cyber security is concerned, there are two things that are happening in cyber security right now. The first thing is that it's going to happen, and its going to escalate. So the problem is that our technology systems are vulnerable. We can see that are technology breaches happening in the headlines every day. We just had the Equifax challenge that just came to pass.

So again, this is another area where we can't just sit back and say, "Well this is someone else's problem." We have to expect that there's risk there, and that we need to have a risk strategy that is addressing this specific thing we are trying to do with the technologies that we are trying to leverage, the technologies that we're trying to use.

The second piece on that is that the number one risk in any cyber security strategy is people.You can have the best system in the world, but if you have human beings that are clever in the way that it is they do work around, or somebody has information that they've accidentally given away, either with intent or unknowingly. That's a problem.

And so, then part of that goes back to education and training and people having a level of awareness across your organization at all levels of your organization of what their responsibilities are in being able to keep everyone safe.

What does that look like?

What does that mean?

How is that practiced?

That is the number one vulnerability in cyber security today. And if we as the people side of the business pay attention to the people and how do we make sure that we are on message and that we are providing people with experiences that help them connect with why that really matters and how that's important in keeping ourselves and the organization safe. Then that's a way of really being able to compel people to action to mitigate against those risks.