Deloitte AI360 Podcast

Jim Rowan, Head of Applied AI
Kieran Norton, Cyber AI Leader

Title: Navigating the rapidly-evolving intersection of AI and cybersecurity

Description: AI and cyber lead Kieran Norton discusses the impact of AI, urging early team engagement and strong governance to manage risks and drive innovation.

Duration: 9:14

Jim Rowan: Hey Kieran, how's it going? Welcome to the AI 360 podcast. Excited to have you here today.

Kieran Norton: Right on. Thanks for having me.

Jim Rowan: Let's dive in for a second. Kieran, why don't you tell us a little bit about what your role is at Deloitte and what you're working on?

Kieran Norton: Sure. I'll try and make a long background short. I've been in IT and cyber for over 30 years. I largely use a lot of history and experience as a guide to what's happening in the future and how the tech landscape is shifting, so that's where I spend a lot of my time. For the last 10 years plus, I've been building practices to address the changing tech landscape—mobile, cloud, etc.—and surprisingly, most recently, AI. I spent about a year and a half as the Cyber AI leader for the firm, have been both building systems for the use of AI internally and transforming the way we deliver service to our clients, but also building solutions for clients. I've spent a lot of time over the last 18 months with data science teams and others, and just recently switched to become the Innovation and Assets leader. So basically, I'm putting our money where our mouth is in the AI space.

Jim Rowan: I love it. And I think people think the AI leaders are really busy, but I've got to imagine that AI and cyber leaders are two or three times busier than everyone else in the world because it's got to be super complex for all the things you're dealing with! So, thanks for carving out some time for us. Maybe we can just dive in on some key questions we've got for you. When we think about the AI supply chain—how we get our solutions organized and get them out to the market—what are some things you're seeing in that space, as we think about the regulatory environment and the cyber environment?

Kieran Norton: Yeah, so I think there's obviously a lot going on, and it's different for every company because they're in different stages of their AI journey. So you've got some companies who are farther along, where they're looking at how do they address the risks they're concerned about—both some of the traditional cybersecurity things we've been worried about for a long time, but also some of the nuances associated with specific use of AI technologies—and then getting to a space where historically the cyber team has not really focused, which has a lot to do with toxicity and bias and what we would traditionally look at as data science. It's the combination of both those fields coming together and moving forward together. Again, there's a big difference between where companies are on the journey along the way.

Jim Rowan: One of the things I hear a lot when I talk to clients about scaling their AI solutions, you want to get these things into production and you're tired of doing all these POCs [proofs of concept], but then I hear this conversation about governance and cyber. How do we

think about those elements to help these solutions go from initial use cases and design all the way into production? How do you think about that, and what advice do you have for clients in that space?

Kieran Norton: First off, make sure your cyber team is involved in the innovation journey. They need to be a partner from the outset. That does require cyber teams to think differently than they previously had. It has to be focused on how to get to "yes," not just default to "no" because it's scary. And I've been in the business for a long time, so I can point the finger at myself as I say that. But it's really working together from the outset because otherwise you will see problems down the line. You're going to get into a POC, you're going to build something, it'll be released, you'll have it for internal use only, and then the wheels are going to grind to a halt because you don't know how to deploy that to customers and others in a secure fashion and address the risk because you basically skipped all those things along the way. So, it's a balance between integrating cyber early on so you're building the right foundation, but not slowing the process down based on, let's just say, a historic way of thinking about software development.

Jim Rowan: That's helpful. I also would imagine there are some tools available for the cyber function itself that are AI-enabled to help with this, right? Are people looking at that as a way to help match the speed of software development and the speed of cyber together?

Kieran Norton: Absolutely. So, generally—and I used this phraseology previously—you're going to fight fire with fire in this case. The threats are becoming more intense. You're seeing a lot of things around use case, phishing, deepfakes, and so forth. It's going to expand. The only way to combat that is going to be by using AI. So, as we talk about AI—you've heard me say this many times—we think about how do you use cyber to protect AI and we also think about how do you use AI in the business of cyber. And you really should be contemplating both because they're connected from a strategic perspective, and you're not going to have success with one without the other.

Jim Rowan: As we think about these threats, what are some of emerging things? I've heard of prompt injection. I mean, I know we're not a deepfake right now, but that's got to be a thing out there. What are some other things out there? Could you explain some of those to us?

Kieran Norton: Neither of us are interesting enough to be deepfakes! [laughs]

Jim Rowan: Perfect! [laughs]

Kieran Norton: That's not a defense, but… There are a lot of nuances associated with AI technologies that are new. So you do need to think about prompt injection. But you can also look back to what we've been doing for a long time. These are not actually overall new risks to us, from a cyber perspective. We've had injection techniques against applications—web applications—for a long time; we've been dealing with them for decades. So, you can look back to what we've been doing and you can look forward to say, well, we're going to have to enhance what we do to address what's nuanced and different related to AI. But you're not rebuilding your entire program. So a lot times, I ask people to focus on that because it reframes it from, "Hey, we have to build this whole new thing" to "No, we're doing some things well. We need to figure out where we need to make improvements and then have to go after those. Don't have to start all over." So certainly that's one way I think about it.

Jim Rowan: The other thing I'm wondering, too, is how are organizations thinking about their headcount on this team. Is it humans plus AI is enough to beat the threats coming in? Should people be staffing up? How are you thinking about it? How are your clients thinking about it?

Kieran Norton: I'm a consultant on this answer. I'm going to say it depends! [laughs] No, really, again, it depends on where you are in the journey. So, for some periods of time, you might have to staff up with humans in order to address a gap that you can't fill with technology. But ultimately, you should be thinking about control, design, implementation, automation in such a way as you're building into the natural process. That's what's going to get you that efficiency and speed and effectiveness later on. Speaking as an example we talk about at Deloitte, something we built for ourselves was a digital analyst—it's a level 1 SOC analyst. It looks at all the inbound alerts and events, triages them quickly based on history specific to that client, that environment, technologies, and what's happened before, and it comes back with the answer of "Hey, what this looks like to me, and by the way, here are all the steps I think we should take to remediate it." That's taken triage from 22 minutes to two minutes.

Jim Rowan: Wow.

Kieran Norton: So, you're really looking for those acceleration points that you can leverage AI basically and automation to narrow that gap and make yourselves more efficient and more effective.

Jim Rowan: Makes a lot of sense, Kieran. To wrap it up, what's the big piece of advice you want folks to leave with as they continue their AI journey and be very cyber aware? What would you suggest?

Kieran Norton: Number one, start early, start often. Engage the cyber team early on. You have to have some conversations and set the tone. This is about innovation and progress, etc. and we need to enable that. Then start to think about how do you approach that innovation in a way that lets you accelerate outcomes. Rather than trying to build AI systems in the middle of your userland network, put them in an enclave. You have an opportunity to protect them from the rest of the technical environment as well as use a different set of controls and capabilities within a smaller environmental space to accelerate. You think about a trusted architecture: It's going to morph over time, but if you have everyone building toward that trusted architecture, then ultimately you're going to get speed. Because you're going to be building to known patterns, etc. and using common tools and services and so forth. The last one I would make is if you're just in the early part of the journey, you need to define governance, you need to say what's OK and what's not OK in your environment relative to the use of AI and AI solutions, and you need visibility. If you don't know what's going on in your environment, know who's

using it, how they're using it, etc., there's no way you're going to manage the risk associated with it. So, if you're at the outset, think governance and visibility—that will inform what you need to go do next.

Jim Rowan: Kieran, this has been great. We could have done an "AI 720" here because there's clearly a ton of things to unpack. Really appreciate your time today. Thanks for joining us on AI 360. Appreciate it.

Kieran Norton: Thanks for having me. All right, talk soon.

Jim Rowan: Take care. Bye.

Visit the AI360 library
www.deloitte.com/us/AI360