CT-Loop-CISO-Mike-Britton

Sat, Jul 12, 2025 4:43PM 6:49

SUMMARY KEYWORDS

Cybersecurity, AI transformation, risk quantification, business impact, email security, financial risk models, CISO role, organizational governance, emerging threats, AI adoption, data management, regulatory impact, efficiency improvement, resource management, business alignment.

SPEAKERS

Jo Peterson, Mike Britton

M Mike Britton 00:00

So I am currently the CIO for abnormal. Ai, lot of my job is managing our cybersecurity program here our customer trust, which is our GRC program, and our technology. And one of the big tasks in my role is AI, transformation for our internal processes here at abnormal so I'm sure you're going to have some a very interesting lens to answer these questions through. That would be a very exciting project, I think.

J Jo Peterson 00:08

Hey everyone, thanks so much for joining. I'm Jo Peterson. I am the chief analyst at Clear Tech Research, and you're joining for clear tech loop. We're in the know and on the move today. I've got Mike Britton, CIO of abnormal AI with me. Hey, Mike, thanks. Jo, glad to be here. I'm glad you're here too. So in case you're just joining us, clear tech loop is a focus podcast series, and we're delivering sharp, real time insights at the intersection of cybersecurity, cloud and AI security, and this session is part of a series of conversations with it and security leaders that are navigating a new era of risk and responsibility. But it's not just about protection. We ask what they see on horizon and how they're preparing for it through a three question lens. So Mike, before we dig into the questions, tell me a little bit about what you do in your day job? Yeah.

J Jo Peterson 01:33

So let me get on with the first one. From a CISOs perspective and a CIOs perspective, how should the organization and and you guys that are in sort of leadership roles in it be thinking about cyber risk in terms of dollars and business impact?

M Mike Britton 01:50

Yeah, I think it's hard. I'm a big fan of trying to quantitate risk. I'm a big believer in things like fair and trying to assign $1 amount to really make it tangible. I think the problem a lot of times when you're trying to assign risk and understand risk is it's it's always hard to understand the magnitude of an event or the likelihood of its occurrence. One of the nice things with us as a business is we deal with email security, and that's probably one of the easiest risks to quantify. And so you look for the things that are most likely to happen and what that impact could be and and really just it's more of a putting it out there and putting it in visibility of your CFO, your CEO and your key executives, so they know when they make business decisions and when they have business objectives that they can kind of align with where your risk tolerance is and where your risk appetite is as an organization.

J Jo Peterson 02:46

Yeah, and just a plug for your your product. I think it's cool. You're doing some stuff that some other folks maybe aren't, so you're a little bit ahead of the curve there. So there you go. So in your opinion, what is the best way to integrate cyber risk into the business's overall financial risk models?

M Mike Britton 03:07

Yeah, I think they need to be part of the conversation, and that's where it's probably a worn out conversation of where does the CISO sit at the seat of the table? And I feel like the better they understand the business, and I'm a big believer on anytime I've come into an organization or taken on a new role, is really listen a lot and understand how the organization makes money, what their macro risks are, what are risks inside the organization, what's going to keep them from succeeding and from there, layer on, their expertise in cyber and help them understand how cyber events or cyber implications could impact their ability to deliver and I think where security in general, as a function has always been kind of the Office of no and stop and slow things down. I think really you've got to shift and be how can I help you speed up? How can I reduce friction? How can I help you take more risks as an organization without incurring additional risk to the organization?

J Jo Peterson 04:08

That's fair, and you know, it is maybe a tired conversation, but it's still worth having. Yeah, so given the project that you're working on right now, which, again, sounds super fun and cool to me. How should the CISO be thinking about AI adoption in terms of its use to secure emerging threats, but also from that organizational governance perspective?

M Mike Britton 04:37

Yeah, I think it's, it's a couple things. It's understanding how AI is going to be used, and understanding the implications of that use, being able to clearly understand the data going into the system that's using AI, where it's located, what impacts that may have for your customers, your regulators, things like that. I think also it's. It. We're, this is not a fad. I like to say we're in the age of AI. So you better get on board, because your business is absolutely using it. There's a very low barrier to entry for them to use AI in their day to day jobs. And if, if we're going to try to put our heads in the sand or trying to avoid it, or try to be technology Luddites, and we're we're going to find ourselves very, very ineffective, and we're going to be incurring a lot of risk that really we had control over, that, you know, we chose to ignore. So I think that's part of it. I think it's just simply embracing it. There's so many use cases beyond, you know, how do I use it in my sock. How do I use it for better detection? How do I, you know, some of it's just simple. Don't overlook the easy things. And I'm sure most organizations are like me. It's, you know, it's, I don't have enough resources, I have too much work. And so, how can I leverage AI to make my team more effective, more efficient? How can I reduce having to hire 10 people over the next two years, versus leveraging AI and only hiring two new people? And so I think I think part of it is you've got to look at it holistically. I think you need to understand the full breadth and depth and scope that AI can have on your business.

J

Jo Peterson 06:17

That's a great answer. I think it's a really good answer, especially it's firsthand. It's a firsthand response given the project that you're working on internally. So great advice for those listening. Mike, thank you for taking a little bit of time with us today, and I'm sure that our conversation is going to resonate with some folks. Thanks everyone for joining you.