Podcast Transcript

Risk Never Sleeps
Episode 55
Kevin Tambascio

Ed Gaudet: Welcome to the Risk Never Sleeps Podcast, in which we learn about the people that are on the front lines, delivering and protecting patient care. I'm Ed Gaudet, the host of our program, and today, I'm pleased to be joined by Kevin Tambascio, Director of Cybersecurity Data and Application Protection at the Cleveland Clinic. How are you, Kevin?

Kevin Tambascio: Doing great. Thank you for having me as a guest here.

Ed Gaudet: Awesome. Yeah. No, I'm glad you're able to join us. So, tell us about your role and your current organization.

Kevin Tambascio: My role is overseeing a team that is responsible for the protection of our data, both structured and unstructured data, that our organization uses on a day-to-day basis. We also protect the applications everything from on-prem applications to new-generation cloud applications that our developers are creating. So we protect anything, both custom-developed. We have a significant number of developers doing custom develop software as well as well as the multitude of commercial applications that support all of our different clinical operations.

Ed Gaudet: Wow. So, a small job.

Kevin Tambascio: Yeah, a small job.

Ed Gaudet: How many applications do you currently have in your custom inventory roughly?

Kevin Tambascio: Custom somewhere in the low hundreds of custom software. So it could be things that it could be everything from applications we've developed to glue different commercial applications together, maybe fill some gaps or in some cases, things that we just had a need and we went out and built the software that we need for our operations.

Ed Gaudet: Okay, cool. And when you look at the risk of those applications, you treat them as third-party vendors, like a third-party vendor would be treated. Or do you treat them differently?

Kevin Tambascio: Yeah. So, our team manages a secure software development life cycle. And so we've been bringing in policies and procedures to basically enact security from the beginning. And we're starting to work more with our development teams as they start in the process, make sure they have the security requirements as well as the privacy requirements that they need. For example, on application is going to be external facing that has patient health information, stringent set of requirements on both privacy and security as there should be. And so we work with those teams to understand those requirements, develop threat modeling processes, and execute those as they go through the journey of building their software, static code analysis, operational protection of those applications as well. And we have also a 24 over seven security monitoring operation here as well. So we bring all that together for them, make it easy for them to understand their requirements and build their software in that way and then support it throughout its lifetime.

Ed Gaudet: Oh good. Okay. So you're monitoring it on a regular basis?

Kevin Tambascio: Absolutely, absolutely.

Ed Gaudet: What happens? I mean, does it ever occur internally where maybe the scope, the original scope, changes over time? And how do you deal with that from a risk perspective?

Kevin Tambascio: The original scope of an application, you mean?

Ed Gaudet: Yeah, the scope maybe of the usage or maybe the use case changes. So maybe initially it wasn't going to you weren't going to put Phi in it. But then over time, there was an opportunity to put Phi in it. So how do you ensure that you're not just doing a one-and-done assessment, you're actually monitoring it on a regular basis? Do you have processes in place for that?

Kevin Tambascio: Yeah, I think it's always important to work with teams who are building things new from the start, but also making sure that when they look at major feature changes, new additions, new scope enhancements, as you're talking about, make sure those processes work in both those cases because certainly, the scope of these applications can change. It's going to change the risk just as much as we're also tracking the outside privacy landscape. So much change happening with states enacting different privacy laws and things. We have a hospital in London, and so London brings us into GDPR and things like that as well. Yeah. So we're constantly keeping track of the cybersecurity threat landscape, of course. Right? I usually talk about cybersecurity protections having almost a half-life. Right. They degrade over time and you have to continuously invest in that space. So, looking at how does that landscape change? How do we want to push new requirements to our teams? How's the privacy landscape changing how we should focus on these applications? And it also marrying that with the changes they want to bring to the market as well, and trying to paint that picture for them so they know what is the target, what are the expectations they need to hit.

Ed Gaudet: You know, your team's currently looking at AI or beginning to bring AI into applications, either new ones that are developing or existing ones that have already been developed.

Kevin Tambascio: Yeah, probably all the above. So it's interesting, the explosion of AI this year, the past 12 months or so, and how much that's come into the daily lives of people here in cybersecurity. We have everything from application owners that want to bring AI to vendors who are trying to add it to every single product that we have, just adding new AI-enabled features, which, of course, brings a whole host of questions.

Kevin Tambascio (cont'd): And then we also, I'm part of an AI task force that is reviewing a lot of the clinical or institutional research that we're doing, and certainly, a lot of interests in our researchers to look at how they can use machine learning to solve some really interesting clinical questions, and applying some of the same research techniques they use in the past, and now bringing it into the fold with machine learning. And so a lot of different areas. AI is interesting in the sense like it. We think of it as a new problem or a new thing we have to worry about. But there's also things like we know how to manage some of the basics of AI, like AI requires servers to be patched, or we have to keep track of data leaving the organization if they're using an AI service, that's maybe cloud-hosted, for example, but those are really similar problems or problems we've already had, right? We also have to look at how are they using that AI from a biased perspective, a fairness perspective, how the data is being pushed out, what kind of data they're sharing. Those are some of the new areas to look at or prompt engineering in some cases. So it's a fascinating space. I think with everything it has positive things. It has potentially negative implications. I was speaking to a group of college students last week, and one of them was talking about wanting to be a red teamer but looking at it from an AI perspective. So imagine someone that's not really using the traditional hacking tools. More thinking like how do I employ AI as my hacking tool?

Ed Gaudet: Interesting. Yeah.

Kevin Tambascio: And so that was he was all excited about that kind of stuff. And so lots of different good, negative, different ways to look at AI. It's really fascinating.

Ed Gaudet: Any advice to listeners that are just embarking down that path with AI, maybe from learnings that you had?

Kevin Tambascio: Sure. I think it's first and foremost it's something that if you're at a position like I am, figure out how your organization can embrace it and support it. It's not going to be a simple like website you can block or something. It's something where you really have to understand it and understand. And how do you empower your people? In our case, clinicians people who don't necessarily have a technical background. How do we provide guidelines to them in order for them to be able to use it for good but avoid some of the problems?

Kevin Tambascio (cont'd): So I think you really have to understand the business owners; just like everything in cybersecurity, you have to really understand the customers and the use cases on what they want to do. And you have to be in a position to provide guidance in a way that's going to help them achieve without providing the roadblocks or getting in their way because it is a powerful tool for innovation. We want to make sure our customers can embrace it. We looked at policies and things like that early on, created internal policies or guidelines on like, what can you use this for? What are situations you can't use this for, and try and provide really clear guidelines to those clinical users so that they understand because there's obviously a huge amount of interest in this space. And so, providing clear guidance to them was really important. Have that dialogue; start that dialogue now. So you're in a position to really help them.

Ed Gaudet: Great. That's excellent. All right. So, let's change gears a little bit and talk more about your background. How did you get into healthcare and cybersecurity in particular?

Kevin Tambascio: So yeah. Um, it's I'm coming up on my five-year anniversary here at Cleveland Clinic. And it's been a tremendous journey. I started actually in the industrial control system space. So, I've spent over 18 years working at Rockwell Automation. It's a major industrial control system vendor. I started there when I was in college. I started as a software engineer. So my background is not cybersecurity. It's not IT. So, I was a product engineer for about 18 years in my career. I got into I had different roles in industrial control systems, from a software engineer to an architect, and then I got into product cybersecurity. So, working with a team of people to formulate requirements and processes and things to how we build security into PLCs and things like that. And so, after about five years, I just happened to be recruited by someone who was working for the Cleveland Clinic and took a chance. And I was a new challenge. I lived in Cleveland all my life. I know this place well, but it's an institution of the highest regard here on the city of Cleveland. And so I felt really called to serve almost more than just taking a job. I just felt like a tremendous opportunity to help my community, help all the patients, the millions of patients that we serve every year. And it's been a tremendous ride.

Ed Gaudet: Yeah. No. Excellent. And coming into healthcare from Rockwell, what did you notice? Did you notice that shared mission that everyone talks about, and what did that mean to you?

Kevin Tambascio: I think the shared mission here is tremendous. We all feel a responsibility for the weight on our shoulders of protecting the information. Patients come to us at the most vulnerable points in their lives. They travel from around the world to come here for heart surgeries and things, and the last thing I want them to be worried about is, are these devices going to harm them. Is their information going to get stolen, right? Our critical service is going to be available to support the care. And I think we all see that. We all feel that. I think having spent so, so many years in the vendor side and the vendor side, you have similar responsibilities. But at the end of the day, you're also handing off responsibilities to the customer and asking them, hey, go and implement this product in a secure way at your factory or wherever you're deploying that product here in healthcare, it's we're at the end of the line, right? There is nobody else to protect. There is nobody to transfer the risk to to somebody else. And so we all feel that pressure and that responsibility. But we also feel, I feel, tremendous amount of satisfaction when we're able to make change here when we're able to reduce risk here by some of the actions that my team and other teams take. It's a challenging environments, availability, just like in manufacturing and availability of health care is 24/7. We don't close the Starbucks on our main campus. Hospital never closes. There's no doors to it because it's open 24 seven. And it is as a metaphor, if that's what like being in healthcare, just pumping caffeine through everybody.

Ed Gaudet: Plug for Starbucks there.

Kevin Tambascio: Yeah. So it's not to say I didn't feel that sense of mission back in industrial control space because we were supporting many customers working in a number of critical infrastructure industries, pharmaceuticals, food and beverage, places like that. But I feel like it's even more here. My own. My family goes to the clinic, I go to the clinic, all my information. All my data as a patient is in these servers that my team protects now. So tremendous responsibility you feel being in healthcare.

Ed Gaudet: Yeah, that's great. That's great. Yeah. We're all customers right at the end of the day. Or we know customers at the end of the day. As you look out over the next 12 to 24 months, what are your top three priorities?

Kevin Tambascio: Top three priorities. Certainly. Always. Let's see. I'd say always understanding the perimeter. So I always think about the knowns and the unknown. Unknown unknowns. The famous Donald Rumsfeld quote. Right.

Ed Gaudet: Yeah.

Kevin Tambascio: Just what is out there? What holes do we have in our perimeter? Because, you know, part of my team is looking at all of the exposed applications, and it only takes one little opening, right, for someone to do something right, ensuring that we have complete visibility of our data, always knowing where our Phi and our intellectual property live, if it's protected, if it's the right people of the right level of permissions, things like that, and then being able to really support our customers, building great applications in the cloud, on-prem, being able to support these services and really being an enabler for the innovation that we want to do, always being aware of the perimeter, always understanding our data and where it is and how it's protected, and ensuring our we're not losing this information through like email, data loss prevention, things like that, and then making sure we're really helping our customers succeed.

Ed Gaudet: That's great. What keeps you up at night?

Kevin Tambascio: What keeps me up at night? It's the fear of the unknown. I think we always try to look at, like, hey, do we have a certain coverage of our organization? Do we have 100% coverage of our perimeter? Do we know where 100% of our data is? It's something our CISO really drills into us to make sure that we're thinking that way. It's not just, hey, these five servers are protected. Well, that's great. What about all the other stuff or the handful of web applications? So I often think about how do we know we've really wrapped our arms around the whole problem. How do we know that we've really secured 100% of our applications or secured or identified 100% of our data? So I'm always fearful of the blind spots. What do I not know? What do we not have control of at this point? Because that's where I feel like, hey, we're going to get caught here. And so I think that's why I wake up thinking about sometimes.

Ed Gaudet: Yeah. No, I hear you. Tough couple of years with the pandemic and everything. What are you most personally and professionally proud of?

Kevin Tambascio: Wow, that's a great question. I think professionally, I'm very proud of our organization and how, through the darkest days of the pandemic, we rallied together to solve really tough problems in a much-compressed timeline than we typically can operate in. We were we went from, hey, next week or a couple weeks from now, we might have some more VPN users as people start to work from home. And we, I think, three days later, all started working from home and we scrambled to make sure, hey, do we have a VPN capacity, support a quarter of our caregivers working remotely? We had to move from Skype, which we had on-prem Skype at the time. We moved to Teams in like a month, which is pretty fast for us to push out a change to 80,000 caregivers and be able to drive that change in a way because we knew we needed to happen. We couldn't scale the current platform without we hosted a presidential debate in the middle of pandemic. Yeah. So.

Ed Gaudet: Yeah, I forgot about that.

Kevin Tambascio: Pandemic. Debate. That was held at our medical school on our main campus hospital, and we spent months setting up networks, pen testing networks, things like that to make sure that the security was ready for that event as well. Just I could go on and on with stories, how we work to get iPads as a get them. We you can't just take an iPad and make it something you could deliver care on. We had to go through software evaluations and things to make sure that we could use certain software on iPads to have political conversations, but being able to have doctors talk to patients virtually, or patients being able to have the availability of devices to talk to their family if they're isolated on a COVID unit just over and over again. This organization does tremendous things logistically, and the way we came together to all those small projects added up to a lot of big difference for the larger organization.

Ed Gaudet: Did you work the debate directly?

Kevin Tambascio: Yeah, yeah.

Ed Gaudet: What was that like?

Kevin Tambascio: In cybersecurity, a bunch of us were there, a lot of us were at home supporting it. Yeah, it was it was interesting. I think from a security perspective, it was kind of quiet. We were all just sitting at home watching all of our tools, just waiting because, you know, you get this feeling like, hey, we've got this target on our back, we're in the news, and there's this media, and everybody from around the world there. And, you know, we're watching all the tools. And it was pretty quiet. The debate itself was nuts, but the cyber perspective was relatively quiet, though it was overall a good experience.

Ed Gaudet: That's good. So outside of healthcare and cyber, what would you be doing? What are you most passionate about?

Kevin Tambascio: Yeah. So a couple of things I really enjoy personal fitness. So I've been a crossfitter for a number of years, since about 2015. I'd say I do it now as much for the physical side as the mental side. And I talk to like when I was talking to that student group last week, talking about, hey, listen, cyber is tough. It's tough to work in this field. We deal a lot of unpleasant things. And that mental health aspect is really important as well. I look at CrossFit and I also like to do road biking and stuff on my on the weekends and stuff.

Ed Gaudet: Nice.

Kevin Tambascio: That's a good mental as much as a physical benefit. Um, my son, I love playing video games. We love doing family cooking homemade pizza and movies and stuff together as a family.

Ed Gaudet: Nice. Nice. What kind of video games?

Kevin Tambascio: Star Wars, Lego video games. My son loves Minecraft and Roblox, and we'll play a bunch of things like that.

Ed Gaudet: Did you play D&D as a kid?

Kevin Tambascio: No, no, I never played that as a kid.

Ed Gaudet: No. Okay, okay. All right. Excellent. If you could go back in time. Speaking of kids, what would you tell your 20-year-old self?

Kevin Tambascio: Well, the funny answer I came up with is buying Bitcoin like this when it first came out. Like minded. Buy it, whatever it be, don't be the guy who bought the pizzas with like 100 bitcoins or something.

Ed Gaudet: Yeah, right. That's. Don't be that guy.

Kevin Tambascio: Exactly. But yeah, on a more serious note, I think about just making sure you enjoy the journey that your career is. I think I was always a forward-looking person looking ahead at the next project, the next job, the next whatever, and just spend some more time just focusing on the present. I think that's some a flaw of mine that I try to control now a little better than I did before. And I think also just, I don't know, I feel like a lot of people or you go into a career at that age thinking like, hey, I'm going to be a programmer for my whole life. And that's what I thought for a long time. And I didn't really broaden out what I was doing for a number of years. I was just basically wrote C plus code for 14 years straight and just embracing like, hey, career, things are going to come from left and right, or different turns in the road are going to happen. And yeah, not to be afraid of it. And I think once I stopped being afraid, that's when I started moving into product security and then going from control systems to healthcare and embracing that change where I think before initially I was hesitant of that. So I think definitely learning like, hey, the career is going to take you in different places you don't expect. And looking back 20, 25 years, I would have never thought I'm doing cybersecurity health care.

Kevin Tambascio (cont'd): So the crazy, crazy idea I originally went to college expecting go to med school. And so I started in college as a pre-med major. I was going to major in biology and go to med school and everything, and then all the people around me were just computer science majors and in my dorm and stuff, and I just was drawn to computer science even more, changed my major, and then next thing you know, and I'm now working in healthcare, which in hindsight is good because I found out later I don't like blood and other things like that. So, but may not have been the best career choice at age 20, I think I was going to go to med school.

Ed Gaudet: Um, I don't like blood either, by the way.

Kevin Tambascio: Yeah, yeah. Uh, you know, I get a flu shot. I gotta look away. Right? You just. Hey, enjoying the journey and trusting that things are going to work out. I think I was always looking forward or wanting to know where I was going to go next. And so, yeah, next thing, I'm working for the hospital.

Ed Gaudet: So that's great advice. Those are great. Yeah, that's really good. So I'd have to ask you this question because it's the Risk Never Sleeps Podcast. What's the riskiest thing you've ever done?

Kevin Tambascio: So, riskiest thing I've ever done. I'm going to go with moving to healthcare. Going from industrial control. What I was just talking about leaving it. Hey, I can make that change. Um, I think when I joined the Cleveland Clinic five years ago, I didn't know. Hey, are all my skills going to translate over? Can I be successful? Like, Rockwell's a product engineering company. I'd never been in IT. I'd never been in a cyber security department before. I mean, I'd always been surrounded by software engineers. And it's a different world. Are the skills and abilities and things that I had going to translate to success in healthcare? Um, and I didn't know I took a chance. So I think at some level I could look at that as a risk that I took to move to an industry. Obviously, I didn't know about the pandemic and the presidential debate and quantum computer that we have on our main campus that, uh, all these like big, huge things that have been huge challenges here or AI falling directly into what my team does.

Kevin Tambascio (cont'd): I didn't know if I could be successful. So looking back, I'm like, wow, I did take a risk. But it's obviously worked out well and it's been incredibly rewarding to be in healthcare for the past five years.

Ed Gaudet: Yeah, that's what I love about the combination of healthcare and cyber. You can. There's so many ways to enter in. Um, I know lawyers, developers, architects, product people. You can come at it from so many different ways. And, um.

Kevin Tambascio: Yeah. And I always tell, like the group of students last week, I was, I think a lot of students to think like, hey, I've got to be a hacker to be in cybersecurity. And like, I mean, that's great if that's what you want to do. Right? But I talked to them about, hey, some people are more offensive in nature, some are more defensive, some are more technical. And then I talk about, hey, we've got folks that work in GRC and they're more in the business side of things and more customer-facing roles and stuff. Right? So there's room for a lot of different types of people in cybersecurity in different ways to come in. Certainly, we have a lot of folks that have started a help desk and kind of work their way through.

Ed Gaudet: Right.

Kevin Tambascio: But yeah, I was a developer. I never worked at a help desk or anything like that before, and I can be a part of cybersecurity as well.

Ed Gaudet: Yeah, awesome. Music or movies. I don't know if you saw that question on the.

Kevin Tambascio: I did, yeah.

Ed Gaudet: So music or movies, you're on a desert island.

Kevin Tambascio: I was talking to my I was talking to my son about this question and we were both like, well, it's kind of silly. If you're on a desert island, you should bring something to hunt with, something to make fire with, something to collect water with, but something you've got, all that stuff.

Ed Gaudet: You got all that covered.

Kevin Tambascio: This is got all that covered. You can bring some movies and stuff to keep you entertained, right?

Ed Gaudet: Yeah. So movies. Okay, good. What are your top five movies?

Kevin Tambascio: Well, I'll throw out a couple movies in an album. Uh, I a big Marvel fan, I have to say End Game, Infinity Wars, some of my favorite movies. Top favorite movies. I don't know, I almost can't watch one without the other. Like, gotta agree together, right? Just a five-hour marathon.

Ed Gaudet: You're on an island. You've got plenty of time.

Kevin Tambascio: Exactly. And then music, I'd have to say. And justice for all Metallica. That's the album that got me into that kind of music a long time ago. So I'll go with that one.

Ed Gaudet: Nice. You listen to Pantera too, and, uh.

Kevin Tambascio: I have, I've seen them in concert. Yes.

Ed Gaudet: What's your what was your favorite concert?

Kevin Tambascio: My favorite concert of all time.

Ed Gaudet: Any band?

Kevin Tambascio: Probably in 1995, I saw Pantera, White Zombie.

Ed Gaudet: Oh, White Zombie. Yeah.

Kevin Tambascio: No, that's a crazy show. And we have this, like, outdoor amphitheater that has great concerts and stuff. And I never thought an outdoor concert could make the ground shake, but Pantera managed to cause the ground to shake there. That was a tremendous show, and it was like 20 bucks back in like 1995, right? Yeah, like concert tickets are like 150 bucks now, right? So I'm really getting more a lot more active.

Ed Gaudet: And where you sit.

Kevin Tambascio: Yeah, yeah. This is like 20 bucks. It was a long ticket. And I was like, man, I can't believe like, the ground is shaking like this. So I'll go. Well.

Ed Gaudet: That's so cool. Excellent. All right. Well Kevin, thanks so much. This has been terrific. This is Ed Gaudet from the Risk Never Sleeps Podcast. If you're on the front lines protecting patient safety and patient care, remember to stay vigilant because risk never sleeps.

CENSINET®

Censinet RiskOps™ Demo Request

Do you want to revolutionize the way your healthcare organization manages third-party and enterprise risk while also saving time, money, and increasing data security? It's time for RiskOps.

SCHEDULE DEMO

www.Censinet.com