Podcast Transcript

Risk Never Sleeps
Episode 71
Rick Doten

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 am pleased to be joined by Rick Dotan, VP of Information Security at Centene Corporation. Hey, Rick.

Rick Doten: Hello. Good to meet you. Happy to be here.

Ed Gaudet: Good to see you. Let's start off with a little bit about Centene and your current role there.

Rick Doten: Centene is a large public healthcare payer. We manage Medicaid, Medicare, and Affordable Care Act in, across the country. And my role is a unique role in that I started almost five years ago as the CISO for the health plan, Medicaid Health Plan here in North Carolina, with the intent that I'm a dotted line report to the head of cybersecurity and corporate. So they referred to me as the neighborhood cat because I'm everywhere, I provide comfort to people, they feed me. I've helped, obviously, work with the global CISO on daily basis and all of his direct reports and with the CTO and head of platform and CIO. So I fit in where as needed to help things out, because I don't have the administrative overhead of the other executives, so I can spend time and ferreting problems or helping teams. So it's a lot of fun. It's like being an internal consultant.

Ed Gaudet: Very cool, very cool. How did you get into health care and IT?

Rick Doten: So two very different questions. IT, was back in the 80s: you get a computer, you get on bulletin boards, you start doing things. I worked in computer stores in college. I worked on internet and government contracts, doing IT stuff that kind of naturally progressed into that. Healthcare, I've gone back and forth in my career being a management consultant. I ran ethical hacking teams for the late 90s to the late 2000s, including forensics into response team and the risk management teams, and going back and forth from being a consultant to virtual CISO to being a CISO for a mid-sized company 12 years ago, to a virtual CISO for five years. And then here, where I am now. In that, I had lots of, particularly when I was a virtual CISO, most recently, I had customers all over the world in every different industry, from gold mining companies to movie studios to conglomerates to every kind of thing you can think of; energy and chemical company in different parts of the world. So everyone needs security. Similarly, what gets you to the need is where the industry comes in. So I'm still going to need to have identity management and configuration management and risk management, and all these different things. But am I measuring against a yardstick for finance or for health care or for payment or for energy, like the being in health care is less relevant about just being a generalist in cybersecurity and understanding all the industries.

Ed Gaudet: No, that makes sense. Absolutely. As you look out over the next couple of years, what are the top three things you're thinking about strategically?

Rick Doten: Are these things, you mean, things that I think are really interesting? Things I think that people should be worried about? Things they think that are opportunities?

Ed Gaudet: Oh, I love all three.

Rick Doten: Okay. Anyone who knows me knows that my big mantra is that we need to remember that even just the United States, we have the Fortune 500 and then 5 million other companies. And there's a huge difference between the capabilities of those. And so I work for a very big company. We have money, we have resources, we have people. Most of, 99% don't.

Rick Doten (cont'd): And so when we talk about security, most of the vendor community, most of the security market is geared towards the Fortune 500 and mid-market and ignoring the rest of them because there's no money in the rest of them. And so I have had a really big, been passionate the last few years, what are we doing for the 99%? I'm the Lorax; I speak for the trees. Because all of them being insecure makes everyone insecure, and they're in the same fight that we do, that we are in. They have same adversaries or similar adversaries, or doing the same things to them as they are to big companies who can successfully defend themselves. So anything that helps them at scale, I'm a big fan of, because that is, we always wonder why we as an industry haven't been secure. We keep seeing there's compromises every single week and ransomware going crazy and all this stuff. But yet we have AI and we have these great tools and we have all this technology. It's like the people who are getting their lunch taken from them can't afford those things and don't have the people. Things to be able to help identify more practitioners get into the industry from non-traditional methods, and get more people to help because they have personality types that can do this. Things that can help the 99% in giving them some capability, and that's not too expensive, that can be managed. And things that then the other thing is going towards the Cloud. It's been a great advantage in the last 10, 14 years that Cloud services and Software As A Service has made these 99% be able to have platforms that they did not have the opportunity to have before because they couldn't afford to build them or didn't have the resources; couldn't afford to buy them, or didn't have the resources to build them. I'm really excited about the opportunity of all of those things for people to be more secure. So what are the things that I worry about? I worry about people, I want to say being misinformed but undereducated and what is really important. I'm on the editorial panel for the CIS critical security controls. And so we've, the controls are in order of importance. And control number one has always been asset management. I can't protect what I don't know about. So we have asset management. We have data protection. We have identity management, configuration management, and vulnerability management. Those are the important things. These are the fundamentals. They're not sexy. There's not like this AI whiz kid thing that is now doing it. There's not some hot box and there's not something that fixes all of this. And there is not some cool acronym or buzzword that we use to be able to do all these basic things. If you're not focusing on that first, don't bother doing the rest of it, because if you could have the best acronym thing, I'm not good at acronyms. If someone says, Oh, what is your thing for CPNTY? I'm like, I don't know, what is that? Tell me what it does.

Rick Doten (cont'd): It's like saying, Hey, do you like the Jerry Lewis sandwich at the deli? I'm like, Just tell me what it is, not the name of it that somebody came up with. Yes, a turkey and cheese on rye. So the, so I think that the focus on not the "Here's the bad actors and here's a threat scenario that you need to worry about" is less more important than if you do the basics well then you're going to be less susceptible. I know what I have, I'm protecting my data, I'm using good passwords, I'm keeping my configuration management date, and I'm managing my vulnerability management. And then while I'm there, let me do some email protections. While I'm there, let me make sure that my users are educated. While I'm there, let me make sure that any tooling and telemetry I have that there is something that is actually logged, configured correctly, logging that people are looking at it, or there's alerts and there is a capability to respond to it. Because when I was a virtual CISO, the two things that I saw missing most in companies universally was one, a governance process that linked the business to technology. Technical people don't make business decisions. If I'm going to do take away everyone's admin rights on their local laptops, that's a business decision, not a technical decision. If I'm going to accept a risk of a certain vulnerability not being patched, that is a business decision, not technical decision. And so having that governance gives the power to the business to be able to make these informed decisions and the role of technology is to inform them. That is what many organizations, not only the 99% but also in some of the Fortune 1000, don't really have. And that's where you still see things where people are saying, Oh, when is management going to finally accept security? When is the board going to finally let us do the things we need to do? Because at the higher end maturity, you're like, What do you mean; they're pushing us. But for the 99%, they may not. And that might be a communication issue. And then the second thing is, that I've seen missing as first being governance, and the second thing being an ... response capability. I never went in to an organization that wasn't well instrumented. They had the best tools. They had the expensive boxes. Their little lights were blinking. They felt like they were really secure, but it wasn't configured. It wasn't logging. There was no alerting when something bad happened, and there was no response capability, like, what do you do when something goes wrong? What do you mean? The box protects me. Not all the time. And that's where I said low-informed because they're following buzzwords, they're following things, they're following, Oh, I need to worry about data leaking over Gen-AI. Like, that is not a new thing. You need to worry about hallucinizations and bad information coming back that you're making business decisions on.

Rick Doten (cont'd): That's more of a business impact. So those kinds of things are what kind of worry me. Obviously, the bad actors are going to be bad actors. They're going to grow, they're going to expand, they're going to get better. But there's a lot of people tracking them. And so the main thing that I tell people, and then I'll finally take a breath and let you ask another question because everyone is like, How long is he going to talk? Is he going to...

Ed Gaudet: No, this is great...

Rick Doten: Find your community. I'm based in Charlotte. We have a very tight CISO community here in Charlotte. I am the Cruise Director for it because I help get dinners organized and events organized and people together and help make sure that we are communicating. And we are a very diverse group of companies, from very big banks down to little manufacturing firms with no regulations. And because we all get together, all of us are better. All of us are mature in our programs because we all share information, and we really need that community because it's a support group. Right? And not all cities have the same level of cohesiveness. And I won't knock other cities, but I could name specific cities, but I won't. I know this because there are groups that come into town every week to take us all to dinner, to have a little summit, to have a little thing, and they constantly say, Wow, you are so tight here in Charlotte. It's not only that you all know each other; you're all good friends, have inside jokes, have things you do, have history, and that is so important in just from personal human connection, but also from helping you in your organization to have a call away from answering any question or knowing, is this a good consulting firm or a bad consulting firm? Is this a tool that's just snake oil, or is it something that's really useful? Or, what do you think is reasonable for me in this particular sense?

Ed Gaudet: Yeah, nicely said. So let's unpack a couple of things. I loved your comment about bringing cybersecurity equity, if you will, to the world. So have you thought about how do you do that at scale? So how do you bring the 99% along in a way that makes sense and actually makes a difference?

Rick Doten: I think it's, community is the first step. I strongly believe, and I've been on other podcasts talking about this, that there needs to be some kind of government intervention, support, whether it's incentives for MSSPs to work with them, discounts on access to tooling, supplements or vouchers or something to be able to help them because we support other industries, oil industry and the farm industry and all these other industries, we supplement them. But what about the people who can't defend themselves? And frankly, we're talking about sometimes nation state actors or proxy actors. That is a much broader thing that will take much longer and a lot more things to be able to deal with, but that is an option. There's other philanthropic ways of doing it, from being allowed to be able to help out in how much can some of the haves help the have-nots? And the have-nots are not like that they don't want to and they don't have the ability to, just this is just a business because you got to make decisions. Because like I said five minutes ago in my rant is: technical people don't make business decisions. And accepting, mitigating or transferring a business risk is a business decision, and choosing not to do certain tooling or processes in cybersecurity is a business decision if it is well-governed, and that they can choose to. And then when something bad happens, the business' like, Yep, my bad. Does insurance cover it? Nope. Okay, we're going to have to hit. But you don't blame the head of security for it because they informed you and the business took a decision. And that's how with all this SEC and going after SolarWinds CISO and going after all these things, if there is governance that can help, in that, you're not the one hung out to dry. And if you do find yourself in that position, then you need to go. We have educated them for first with Joe Sullivan, now with Tim Brown, about things that could go wrong and what we want to do to make sure that doesn't happen to us, and whether it's decisions we make or make sure that things are in contracts and ... Insurance is is up to levels and things like that. And in the community, these are things we talk about all the time. I was on a roundtable at RSA last year talking about like liability. And so it's something that we talk about a lot, and I find it interesting. And these groups who come into town and want to talk to us is, Oh, what do you think about AI, or what do you think about this liability? For example, we've been talking about this for over a year. It's like if you are not in our conversation, then you think it's a new thing.

Ed Gaudet: You think the business hype, if you think about it, the excuse is: It's technology, and we don't understand it. But there are board members that don't understand the details behind audits and finance. And yet, when does it become an excuse that's outlived itself? When does it become?

Ed Gaudet (cont'd): At some level, we all use technology today. It's very few people that you could say live in a cabin somewhere in the woods and don't use technology. So even the largest corporation, the CEO and their staff are, I'm sure, immersed in technology. So when does it become just an overt excuse for not doing the right thing?

Rick Doten: So yes, I agree with you that almost every company is a technology company. We're not just doing everything manually, and consumers as well. And I think the thing that has helped the larger companies mature faster over the last couple of decades is that many board members are on multiple boards, and if you're on a board of a company that just gets hacked and has a very serious thing, and you live through that, all the other companies, you're on board so you say, I don't want that to happen to me again. What are we doing about this? And so that starts propagating. And I was on a panel three years ago, and the moderator is like, When is the board going to step up and agree and understand security? I'm like, What are you talking about? They're pushing us. But that's from my vantage point, my Fortune 500 part of the world. And I still have peers who are still struggling with that. But so the short answer comes back to communication. And the other thing I found as a virtual CISO is I'd go into an organization when the security team is not getting the recognition, they're put into a box of compliance. You do vulnerability scans and respond to incidents. We'll do the engineering, architecture and everything like that is because usually the person who is the director of IT security is like is what I call a tool jockey. And so if they're very technical, then their communication is very technical. And being able to, and that's where governance comes in, being able to understand the business. My three rules of being a CISO are: rule number one, understand what your business does to make money and don't do anything to disrupt it. Number two is: don't make your users your biggest hackers by putting in controls that they have to go around to do their job, right? And number three is: find community, and I already talked about that. So that part of talk, so I'd go in and I'm helping mentor this director of IT security, and we're like, Oh we're doing these things and they're not listening to me because we need this stuff because this bad thing could happen, this thing here, and this then. What does the business do? Do you understand that? Do you know how to make money? Do you understand, like where there, are you making connections with the legal team and the compliance team and the audit team, and as well as the operations of what business does to be able to say like, I am your partner; How can I make it better?

Rick Doten (cont'd): I don't want to be, 15 years ago it was the office of no. Everyone says, even now, Let's not be the office of no. It's like, We stopped that in the 2000s. Of mature group it is, what is it the business process you want to do? How can I then secure it, or make it something that the business is comfortable with the risk that they're accepting while doing it? Because again, I'm not the one who makes the decision, right? It's a business decision. I could say, Here are some options. And they may say, There's too much end user abrasion if you do that; we're going to accept it. Fine. Sign here if you accepted the risk. We suggest as mitigation. Then I will, then I'll work on doing more monitoring then. We're going to accept the risk. I'll do more monitoring and have response capability if something goes wrong; reactive than proactive. That's fine. But the business makes the decision. And then over time, if there's so many things we're doing, they're like, Hey, maybe I should listen to you two years ago and let's put this control in, because we're spending a lot of time with this and that thing; whatever. But you need, it's not going to be perfect the first time, and building that relationship takes the ability to listen to the business and say, How can we make novel solutions to do the things, to manage the risk to the point that the business can take? So going back to your point is, I think it's a breakdown in communication because they don't know how to talk to the leadership in the language that they can talk to and that they need to talk to for them to understand and educating them and doing it in a way. And so that's like what it all boils down to is communication. Because once they understand that IT risk management is not about protecting IT, it's about protecting the business, frankly, from having an IT infrastructure, or else we wouldn't even worry about it.

Ed Gaudet: That's right. Cyber risk is business risk. Just changing topics a little bit. Over the last couple of years's been tough on a lot of folks. What are you most personally or professionally proud of for the last couple of years?

Rick Doten: What am I proud of? What I've done in the last couple of years?

Ed Gaudet: Yeah. Yeah.

Rick Doten: So in the last year I've become my special interest in socializing and talking about neuro divergency within the cybersecurity industry. And I first started a year ago at a security conference here locally. I was asked to do an opening talk and the topic was community. ... I love it when they give me a topic because then I can figure out how to back into it. And I said, I want to dip my toe into neuro divergency, which is things that are neurological things in the brain that you cannot adjust. So things like autism and ADHD and OCD and dyslexia and then other kind of fun ones most people have heard of: dyscalculia which is like dyslexia, but with numbers, and dyspraxia, which is movement things, you get very clumsy and you spill things and stuff like that, and even ... will fit into there. These are things that I've noticed over 25 years of managing people that a lot of people again, ethical hackers, forensics, response people, risk management people, even developers and DBAs I've managed years ago that they are, that they're neurodivergent. They fit into these one thing: autism or ADHD mostly, and then I got really good at keeping them productive. And so this presentation I did a year ago was like, Hey, we talk about community, or community is diverse community, and there are people who think differently, and they think differently because that's how their mind work. And it's not a behavioral thing, and they're not procrastinating because they are lazy; they are procrastinating because they have a disability in their executive function to be able to initiate tasks. And that connection between the back of the brain with all the knowledge and the front of the brain that does things, is not always wired right. It's not disability of knowledge, it's one of performance. And so how can we then get them on task and get them motivated and get them focused to be able to get things done and managing people who we'd had to keep the lights down because there are sensitivity issues, people who didn't communicate well or just isolate, let other people talk for them, people who didn't, who got overstimulated a lot, again, keep them in a separate room and not have people bother them, people who had a hard time starting task will help getting it started, and then they'd finish it, or people who start tasks and they get bored and then can't finish it? Let's work on things to help get them finishing it. And so I took all of this and I said, There has been this, there's a mystique, a negative connotation to neurodivergency. Oh, he's autistic. But there are very high-functioning people who work through this. And there are people who are not. It is a spectrum, as we call it. And if you've seen one person, you've seen one person. And how it affects them is different.

Rick Doten (cont'd): Because in the 11 different executive functions, you may be very good at some and very bad at others. High myopia is one ... where people who are always late and they're missing things, all those kind of things. In others that could be the opposite, where I will never be late for anything and I know exactly how long it's going to take. The superpower goes both ways. So I started socializing that, and I was really nervous: Is this going to be resonating with people? And to the 100 people that were there for that day, I spent two hours afterwards talking to people as they were sharing their stories, telling me how their experience, their kids, their family, their parents, whatever, and that it really resonated. And so I've done it about four more times as keynotes and three podcasts where I've done it, where I talked about this at depth. And again, every single time it comes back as like really resonates with people. And so I'll be speaking on that topic at RSA show this year, and I'm very excited to be able to socialize that. And I'm also very happy to see that there have been a lot of other articles. I even have a slide where I keep adding them. I just added one this morning from a Netflix blog of a couple of their engineers talking about it, and that this is now being more socialized so that we can normalize it, and then we can accept that this is not a function in somebody's behavior, but how their mind works and how do we work with it. How you got here could be a lot of reasons. It could be ADHD or autism or dyslexia; it could be childhood trauma. But let's deal with it. What is the output? What is the trait? And let's work with it. So that is what I've been most proud of, is that every time I bring this up, it resonates so much, and I feel like I'm helping people who finally understand themselves better and, or their partner or their staff, how to manage people. And they're like, This is really great because now I'm not, like, angry at them for not doing something. Oh, I understand; this is something that you have a challenge with. Let's do this little thing by I'll just sit with you while you work on it and you'll get it all done. It's like the mirroring kind of thing. And that has been the most gratifying to me.

Ed Gaudet: That's terrific. I'd love to have you back on and really explore that more at some point, if you're interested. I think I know the answer to this question I'm going to ask anyway. Outside of your current job and health care, what are you most passionate about? What would you be doing if you weren't doing this job?

Rick Doten: One of the things of autism is you have special interests, right? And I do a lot of, I have a lot of special interests. Right now it is this whole neuro divergency. I've been gone through over 50 hours of clinical online training to be a certified clinician in these things. That is a special interest. As opposed to a hyperfocus, which is: you're falling a rabbit hole down some YouTube channel, right? Especially which is longer-term thing. And I've done many things that I will not list all of them here, but this is something that I'm very interested in and can pursuing and getting more education and helping people with, because there's a lot of people who need a lot of help, and particularly for adults with neuro divergency, there's not as many people who can support them as there is with kids. I'm a yoga teacher. Known fact, everybody around me and I teach classes twice a month for my health plan, and that's something I've always been interested: wellness and fitness and things. I used to be a personal trainer and used to teach women self-defense back in the 90s. I did all these crazy things. And it's just really, it's things that I feel that help others, whether it's from a physical standpoint, from a cybersecurity standpoint, because that's my special interest as well, or from now talking about from a mental health standpoint. And that's what really reaches me, is being able to talk and be able to help people, help my industry, help my community. That's the core.

Ed Gaudet: I love that. If you could go back in time, what would you tell your 20-year-old self?

Rick Doten: My 20-year-old self was an arrogant little snot. So I, I was like, Just get over yourself. In five years, you're going to think you were an idiot. In ten years you're going to think, Man, why did he even think that? Is that you grow every single day and I think that you are, I'm embarrassed about things I did even ten years ago that I'm like, Oh, I can't believe I did that. And so just say that it will, you will no more, you will continue to learn more than you thought you could about yourself, the world, the things you're interested in. And you may think you know a lot now, but even now, I bet ten years from now look back like, Man, I was an idiot ten years ago.

Ed Gaudet: Yeah. Amen. I look back on photos and go, Who is that person?

Rick Doten: Yeah, it's really different. Like when you're, I have two adult sons, and when they pass that time frame. And I can remember where they were, where you were at that time, you're like, Oh, man.

Ed Gaudet: Were you better or worse?

Rick Doten: Oh, much worse. It's a generational thing. It's, I was probably more successful. But what does success mean? Was I well-adjusted? Was I happy? Did I have those things are all variable things. But I definitely would not have been able to put up with myself at that point. As an adult, no, I'm going to have to coach you on a lot of things.

Ed Gaudet: Yeah. Risk Never Sleeps Podcast. What's the riskiest thing, Rick, you've ever done?

Rick Doten: Again, the ADHD side of me is always novelty thinking and explore the explorer gene and you have impulse control; is another one of the executive functions. That's not regulated. Oh, I did outdoorsy things of climbing on stuff I shouldn't climb on, going down rapids I shouldn't have gone down, driving in a way that I shouldn't have been driving. Yeah. So there's a lot of, again, that impulse control thing, particularly when you're younger and your executive function is not fully developed. Your prefrontal cortex is not fully developed till you're 25. And I did silly things that were dangerous. And so I had sprained my neck. I had almost broken every bone. I had done all kinds of stuff doing silly things, and was accident-prone by doing those things which part of it's impulse control, part of it's a little bit of just like being accident-prone is one of the features of neuro divergency.

Ed Gaudet: Okay, I typically ask this question. If you're stuck on a desert island, hypothetically, and you could bring either five movies or five records record albums, what would you bring with you?

Rick Doten: Satellite internet.

Ed Gaudet: That solves it. You get everything then.

Rick Doten: Because I would not be able to like, manage with just five things. I would probably create new things. I am not like an avid reader of nonfiction and fiction of genres that are traditional. Even though I've, I have a degree in English literature. But I'm still not.

Ed Gaudet: You do? Me too.

Rick Doten: But my taste in music vary changes because there are things that I like and things I don't. So it's a bad question for me because that's not like how I work. I guess is, my answer is: I would figure out a way to get off the island or not get on the island in the first place. And if I did, I would create a way to get off the island quickly. Not just resolve myself to, I guess I'll be reading these books over and over again.

Ed Gaudet: Oh, I love it. Any advice to folks coming into the profession, either into healthcare or both cybersecurity?

Rick Doten: Yeah, find your passion. Which is like something that's silly, that we always say because, but it's such an important thing because going through the neuro divergency discussion or education that I did, I realized that I'm able to put words to things that I just generally said before. We hire based on personality and aptitude. Now, I can tell you what those traits are. Or I know how to interview somebody who isn't going to talk to me, and now I can explain why and how that works. All those little things. But one of the things that's a big one in that is enthusiasm. And when there is a special interest in getting to something, people that I used to hire as ethical hackers, they would take their clock radio apart when they were, they'd figure out how things work. They would like, mess with things and see how to make it better. And find the things that you naturally want to do. If you like dancing, find things that are like, I'm going to run around all day and I'm going to pull cables. It's like the thing that you are naturally good at, lean into it. The thing that you're naturally in. Because there's a rainbow of roles within cybersecurity, and I've done almost all of them. And so there was something that takes a lot of formal education and no formal education and a lot of problem-solving and no problem-solving and following directions and some things that are exciting and novel and some things that are boring and monotonous. And depending on where you like to do, lean into that and you'll find something that you will like.

Rick Doten (cont'd): And it may not be what you think at first. So in cybersecurity, people come in, want to do ethical hacking, right? And they want to do the Pin testing. And then they're like, Oh, I like this, instant responding is fun because then I get to solve problems like a detective. Or, Oh, I like security architecture because it's like putting a bunch of Legos together. Or, I like doing detection engineering because then I'm taking the things that the detectives find and finding a way to detect it next time. So there are lots of these little things that you may not realize are a thing until you get into it, and then you will naturally evolve to it. Because people in my generation, you didn't go into, you didn't seek to go into cybersecurity; it found you. You have to be the one who solved the problem. And then the next time they say, Hey, can you make this thing not do this thing again? Sure. And then next thing you know, you're the security guy.

Ed Gaudet: Yeah. No, it's great advice. I think Bukowski said, Find what you love and let it kill you, or something like that.

Rick Doten: And it's not what you love that can apply to something that makes you money.

Ed Gaudet: Yeah, yeah.

Rick Doten: In my industry.

Ed Gaudet: Yeah. That's right. Yeah. You know, and that's what I love about cyber. You're right. It's such a broad field that it really can map your personality to the role in a pretty, pretty interesting way and then evolve over time and capture and learn a lot of different things about not just cyber, but also the business because of the access you get from that role, unlike any other role, I think.

Rick Doten: And that's why I love being a consultant, is I got exposed to so many different industries. When I go into, 17 years ago, I go into hospital and they're like, Oh, tell me experience with hospitals. Let me tell you about the auto industry, which is very similar to how hospitals set up and their risks are the same and their challenges are the same. And so because most people don't do cross-industry stuff. It's, you're with, I'm in Charlotte, it's the banking capital of the US. All the bank people hang out with bank people.

Rick Doten (cont'd): But not looking at, Oh, what's the manufacturing doing or what the oil companies are doing? What are the healthcare companies doing relevant to us? Because you're so used to being in this little clique. And so that's why I always encourage, if you have the ability to get into consulting, to get this broad range of what it is that you like, what industry is most interesting to you, which part of the world is most interesting to you, then that gives you that broad sense to bring in. Oh, I saw this problem. I saw this problem working for this manufacturing firm in Mexico. And here's what we did to solve it, because very similar to a thing that we have here.

Ed Gaudet: Yeah. Yeah. Interesting. Great advice, Rick. Really appreciate your time. Thanks for joining us today. This is Ed Gaudet from the Risk Never Sleeps Podcast. If you're on the front lines protecting patient care and delivering 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