Podcast Transcript

# Risk Never Sleeps
# Episode 99
# David Woska

**Ed Gaudet:** Welcome to Risk Never Sleeps, where we meet and get to know the people delivering patient care and protecting patient safety. I'm your host, Ed Gaudet. Welcome to the Risk Never Sleeps Podcast, in which we talk to the folks that are on the front lines protecting patient safety and delivering patient care. And today, I am pleased to be joined by a special guest, Dave Voska, who is the Chief Information Security Officer at Cincinnat. Welcome, Dave.

**David Woska:** Well, thank you so much. And I'm really excited about doing this today.

**Ed Gaudet:** Excellent. So great to have you on the program. Let's start off with your current role and a little bit about what you do at Sensen. A little bit about your current company.

**David Woska:** Yeah, absolutely. So a company I think you know a little bit about. So I wear a couple of hats. I'm responsible for keeping citizens secure. Obviously I also lead a great team which develops risk assessments in the at risk ops platform to help health systems with third party and enterprise risk management.

**Ed Gaudet:** Excellent. And you've been here for months now.

**David Woska:** Four months in just a few days.

**Ed Gaudet:** And you've already added some new elements to the platform through your curation efforts. One of those is the NIST AI RMF assessment type that's in enterprise risk, which is pretty exciting. And you've got a couple of other ones coming soon as well.

**David Woska:** I do. I do. I'm really excited about the new healthcare cybersecurity performance goals that CSA put out a little earlier this year. So we've turned that into a risk assessment that will really help as a template for healthcare systems to benchmark where are they today and where are their opportunities to improve their cybersecurity programs?

**Ed Gaudet:** Excellent. And I think by the time this airs will be already into the benchmark program as well. Yeah. And so customers will be able to utilize that new assessment type that you're building. Oh, I'm.

**David Woska:** Really excited about that. It's a really different feel, you know, coming from a provider space. I've always been very focused on how do we protect our patients, how do we keep our health systems secure. But in the software company, it's a lot different here. It's also about the product that we're selling and the services that we provide. So, you know, doing podcasts like this help marketing and sales, where I have contacts in healthcare and just being able to bring my experience in healthcare, you know, to the things that we do.

**Ed Gaudet:** Yeah, it's quite different. We'll unpack that in a bit. So how did you get into healthcare? You've got a pretty long, uh, experienced career in healthcare. So help our listeners understand how that all started out.

**David Woska:** Oh, yeah. So I've always had a real passion for learning and science and technology and, you know, really I actually thought I was go to med school at one time. I actually started in academia. I have a doctorate in chemistry, where I've done a lot of research and couldn't have multiple publications. I did a multidisciplinary degree in inorganic and physical chemistry, which included work in the laboratory, as well as theoretical work doing molecular simulations of chemical reactions. So that gave me a lot of practical experience running complex Unix systems.

**David Woska (cont'd):** I ended up changing careers, actually, and strangely enough worked for DuPont, a chemical company of all things, managing the enterprise Unix environment. I've always had this idea that healthcare is really important. And like I said, I want you to go to med school. So I was lucky enough to join a long term care facility in New York as a systems manager. And that's kind of where I started my career over 20 years ago in healthcare. But over time, I've also been a CIO of a health system. And before joining Cincinnati, I was the assistant vice president of information security at the largest health system in New York.

**Ed Gaudet:** And that's Northwell. And they're also a customer of Sensenets. Right?

**David Woska:** They are. They are. I was really thrilled to bring in Cincinnati to Northwell Health, and now I'm on the other side of it, having calls with my old colleagues.

**Ed Gaudet:** That's pretty cool. I also believe you know a little bit about quantum mechanics, too. I told you, I told you we were going to go there. I did warn you.

**David Woska:** You did, you did. I had to brush the dust off some of my old textbooks. All right. I actually loved studying quantum mechanics and had an opportunity to teach it a couple of times. Quantum mechanics is a branch of physics that explains how very small particles, like electrons and photons behave. And understanding the math and the physics behind it was something that I enjoyed immensely back during my graduate and my graduate days. And and now more recently, just looking at all the things that are going on around quantum computing is just really fascinating.

**Ed Gaudet:** So if you were at a neighborhood party and someone asked you, Dave, what the hell is quantum mechanics? How would you describe it to someone like myself, the uneducated? How would you describe it?

**David Woska:** How would I describe it? Okay, so I think that, you know, generally folks know that classical computing is all about those ones and zeros bits, while quantum computing is instead of bits, they use something called quantum bits or qubits.

**David Woska (cont'd):** They have very unique properties based on quantum mechanics properties such as superposition and entanglement. I love those words, and I'll give you my analogies in a moment. But at the end of the day, superposition and entanglement are what really allows quantum computer to process information in ways that classical computers just can't do. And it can do these kinds of calculations so much faster as well.

**Ed Gaudet:** Yeah. So in effect simultaneously.

**David Woska:** Yeah, yeah. So superposition is okay. Think of superposition like this okay. In a regular computer you have bits. It's like a light switch. You they're on or it's off. You know, ones or zeros. In quantum computing qubits, they're kind of like a dimmer switch. So they could be on. They're off. They're somewhere in the middle. So essentially you can represent on and off or zero and one at the same time simultaneously. And the ability to be in multiple states at the same time. That's called superposition. It allows for that. The processing of simultaneous possibilities in calculations reminds.

**Ed Gaudet:** Me of my college days.

**David Woska:** I'm sorry.

**Ed Gaudet:** It reminds me of my college days being in multiple states at the same time. Aha. All right. So but seriously, there's obviously constraints in terms of how things are processed or computing Obviously, within the classical context, this notion of logic gates the and or not right whereas quantum does it differently. So they process those calculations in very, very unique ways. And so talk about that and talk about the ability to parallelize that computation in a way that, you know, again is non traditional. And because I want to get to what I want to do is get to the connection of why should we care. And maybe we don't care so much today, but like everything else, tomorrow could be just around the corner for this. And as cyber security leaders, we may at least want to have some indication of what it is and how to get our arms around it quickly. So let's unpack this a bit. Sure.

**David Woska:** So there's this notion of quantum entanglement. That's a fancy term. But what it really means is that imagine you have two qubits okay. So those are those bits that I was talking about. Imagine there like a Paradise. Okay, but these dice are linked in such a way that if you roll one, the other one always shows related value. So no matter how far apart they are, they are aware of each other's state or value. So this connection is called entanglement. Okay. It means that a state in one qubit instantly affects the state of another one. And that enables this much faster and more complex calculations. And where it really will make a difference are in the whole field around cryptography. Obviously, you know, that's one of the most talked about applications in quantum computing today, where you could have that possibility or potential of breaking widely used encryption techniques or methods like RSA or ECC, which rely on factoring very large numbers, solving discrete logarithm problems, something that classic computers don't do well and they take a very long time. So I mean, we've all seen those charts like, well, if you have a four character password, your password can be cracked in, you know, four minutes, three minutes, you know, 30s whatever. With quantum algorithms, it's just exponential. It can crack those codes incredibly fast.

**Ed Gaudet:** Mhm.

**David Woska:** Interesting. Another field is around artificial intelligence. Even, you know, it can enhance machine learning algorithms making it faster and more efficient. And there's one field that's kind of near and dear to my heart really. And that revolves around using quantum computers to simulate molecular interactions at the atomic level for.

**Ed Gaudet:** Drug discovery I bet.

**David Woska:** Yeah. Drug discovery, material science. I mean, it really has the potential to revolutionize these industries that depend on chemical reactions and molecular modeling.

**Ed Gaudet:** Excellent, excellent. And so, you know, as you go back to the encryption problem, what are some of the things that CISOs and others can start to think about. In a world where we have quantum computers readily available and the risk of losing the efficacy of the encryption we currently have is there is real.

**David Woska:** Yeah. So thankfully we're still a little ways off. I mean, you know, companies like Google and IBM, you know, they're making significant progress and they're really at the forefront of quantum computing. But there's still a lot that's still a long way to go, frankly, when it comes to cryptography, I think, you know, where CISOs are probably looking to go, they need to think about what that next level is. You know, passwordless authentication, risk based authentication, where it's less about the password that could be hacked, but using other methodologies that are quite at risk.

**Ed Gaudet:** Mhm. Well, it also probably introduces new Post-quantum cryptographic systems like multivariant, cryptography, and other approaches.

**David Woska:** Now, that's very true. Boy, it's been a while since I've taken multivariate calculus, but. Uh, yeah. I mean, at the end of the day, you know, cryptography, you know, revolves around mathematical algorithms, okay? And, you know, mathematicians are phenomenal at coming up with different ways of creating cryptographic keys and using quantum computing to come up with new ways. New algorithms that are harder and harder to crack are definitely going to be, you know, something that you should be looking at.

**Ed Gaudet:** Yeah. Okay, good. And then obviously, as we get closer to this, what's your prediction in terms of timing, do you think this is in the next five years. Do you think it's less. Do you think it's longer?

**David Woska:** I still think that understanding how to expand the number of qubits that are being used is something that is a challenge that they need to overcome first. Once we hit that, once we're able to get over that barrier, I think things will get progressively more and more, you know, will be able to be done with quantum computers. I think it's going to be a while, frankly. I think that there are just some things that, you know, we need to better understand to figure out. I'm not a betting man. So, you know, I'm not going to say five years, ten years. I'll use a quantum computer to give you some probabilities though. Mhm. Maybe I'll die.

**Ed Gaudet:** There. Yeah. Well there's obviously the compute the physical considerations around qubit stability and the environment that one has to manage, which is a much cooler environment to keep those things stable. Right. So we're obviously not even prepared for that. We've seen how much artificial intelligence has sort of stretched our ability to keep up with the compute demand, if you will, for large language models and the such. So I'm a little more optimistic. I think, five years Viewers on the outset will start to be using quantum for those particular areas that we talked about earlier, which would be exciting.

**David Woska:** It'll be amazing, and I've been following it more and more, especially since my son just graduated with his degree in electrical and computer engineering. So he and I talk about those kinds of things. He actually understands it better than I do.

**Ed Gaudet:** Oh, maybe we should have had him on. Maybe. I'm just kidding. All right. Dave, so you talked about the CPGs. What are some of the other priorities you have over the next 12 months?

**David Woska:** I'm mostly focusing on using my background and experience working in healthcare to help drive better risk outcomes. I think arming security teams with the information they need to drive down risk is really paramount. I think I have a lot of ideas and maybe you'll like some of them and that, you know, we can expand risk ops to add more features and functionality to really bring us to the next level. I think some.

**Ed Gaudet:** Of the things you've been working on, I know you shared your connection with business continuity, business resilience and disaster recovery. Anything you want to share, give people sort of an early, early look at some of the ideas you're thinking about.

**David Woska:** Oh, sure. I think kind of a natural progression if you think about third party risk management, which is one of the things that risk apps does very well. Obviously, having that ecosystem of assets within your catalog and being able to not just do risk assessments from a third party risk perspective, but also being able to look at it from a disaster recovery perspective from a business continuity perspective, even doing business impact analysis as part of the onboarding of a new technology solution, I think is really important.

**David Woska (cont'd):** And that'll help you as an organization understand where that solution should be and what's the criticality and what are the dependencies between that solution and other systems that where the integration exists? I think that there are some very logical steps that make sense. Being able to have incident response plans associated with technology solutions, and being able to run exercises, and having a true understanding of all the things that go into your doctor plan or air plan connected to those assets. I think that there's a true benefit to having that full view of everything that's going on in your catalog.

**Ed Gaudet:** It certainly, I think today more than ever, people are more aware of. It's not a matter of if, it's a matter of when. So therefore I can only do so much given my ability to identify, protect and detect. And so if an event is going to occur, then I better have the ability to respond and recover quickly within the context of running the business and the impact that it can have. If we are down longer than we should be down. So it's good to see that focus shift. And also I think those worlds are coming together, the cybersecurity worlds, if you will, the GRC worlds. Yes. And the business continuity and disaster recovery worlds. Whereas for many years they were separate silos within an organization that, you know, maybe met, but not as frequently as they should and certainly didn't draw the connections as tightly as certainly we know they need to be drawn. That's exciting. And what are some of the things that keep you up at night as a CISO of a smaller tech company? Quite a transition from your previous employer. Yeah, my.

**David Woska:** Budget is a lot smaller.

**Ed Gaudet:** Uh. Oh, you know.

**David Woska:** It's just new challenges. A smaller company definitely has, you know, different and unique challenges. And, you know, a large, complex health system, obviously. But it also isn't as regulated obviously, as well. That offers some advantages. Decisions we make won't impact patient safety. I love that I'm able to really kind of think about security in the context of we need a secure solution, we need a secure environment. But patient safety is at risk, at risk. So that's a big difference in kind of the way I look in.

**Ed Gaudet:** The day to day operations. But yeah, but conversely, you have the ability to make decisions that can affect patient safety on a more global level because you can enable more of those health systems with the tools and the processes and the procedures to do a better job protecting patient safety.

**David Woska:** Arming security teams with the information they need is really, you know, what it's all about.

**Ed Gaudet:** Yeah. All right. Great. You know, if you're outside of this job doing something that you love and you're most passionate of, what would it be? What would it be?

**David Woska:** I love spending time with my family. I make no. I make no apologies for getting away as often as I can, and spending time with my kids and my extended family as well. I'm an avid golfer. I like to say I play golf, but I'd say it's more of, you know, I just go through the motions. Um, I do enjoy it, though. I like it a lot. I love music, I love, you know, a big hobby of mine is woodworking, actually. Right now, I'm building, um, oak end tables for my living room.

**Ed Gaudet:** No. No kidding. Wow. Yeah. Do you use, like, the what do they call those, a dove groove or what? What are the connections that you, uh.

**David Woska:** Dovetail grooves. Dovetail? Dovetail connections? Yeah. I don't I'm not quite up to that level.

**Ed Gaudet:** Um, okay.

**David Woska:** But I do use other types of joints.

**Ed Gaudet:** Okay, interesting.

**David Woska:** Joinery is definitely an interesting part.

**Ed Gaudet:** It's the most complicated piece of woodworking that you've experienced or you've done on your own.

**David Woska:** Probably making these end tables is probably the most advanced. Yeah. There are drawers. There are some complex joinery in it. The legs are tapered. Oh, a lot of routing as well.

**Ed Gaudet:** Nice.

**David Woska:** That sounds like.

**Ed Gaudet:** Sounds like you have a little barn there with some tools to play with. Happy garage? Oh. Yeah, my father did that. He loved making things. We had our first daughter. He immediately, you know, made her bureaus and dressers and all this stuff. We still have them, you know, toy boxes. And he just loved making those things. Yeah.

**David Woska:** I grew up in a family. So my father is an architect, a corporate architect. So I grew up watching his buildings, you know, go up. And interestingly enough, it's not counting censor.net the last three health systems that I worked with, every one of them had an office in one of my father's buildings.

**Ed Gaudet:** Really? Yeah. That's pretty cool.

**David Woska:** That is very cool. Yes. My mother is an interior designer, so she designed those buildings, but she's done some really phenomenal things.

**Ed Gaudet:** That's very cool. That's very cool.

**David Woska:** She worked in Manhattan.

**Ed Gaudet:** I did not know that. Yeah. Uh, did your dad know Frank Lloyd Wright?

**David Woska:** I doubt.

**Ed Gaudet:** That. I don't, I doubt that. That's all I got on the architect side. Yeah. All right, if you could go back in time, what would you tell your 20 year old self?

**David Woska:** Oh, boy. What would I tell my 20 year old self? I think I would say, hang in there.

**Ed Gaudet:** Hang in there, okay.

**David Woska:** Life throws curveballs, but as long as you have family that you can count on, you know it'll all work out.

**Ed Gaudet:** Okay. All right. I would love to see you as a 20 year old kid. So would I. There's going to be a video floating around somewhere, right?

**David Woska:** Yeah. In my 20s, I was finishing up my graduate work, working in laboratories Stories and teaching and.

**Ed Gaudet:** Pretty cool.

**David Woska:** Yep. Yep.

**Ed Gaudet:** Okay, I know you're a really risky guy. What's the riskiest thing you've ever done? Yeah.

**David Woska:** So after years of studying and research in chemistry, changing careers into healthcare information technology. Yeah, that's pretty risky. Riskiest thing I ever did.

**Ed Gaudet:** So in chemistry. Did you ever mix anything, any elements together that were combustible? Uh, yeah, that's pretty risky. That's pretty risky, right? It was controlled. Oh, it was controlled. Okay, okay. All right, fair enough.

**David Woska:** The saying that goes better. Living through chemistry.

**Ed Gaudet:** Better living. All right. Hardest lesson in your career?

**David Woska:** Hardest lesson? The hardest lesson, I think you know is more around. It doesn't always go your way or it doesn't go the way you thought it would. Mhm. Yeah. And having that backup plan.

**Ed Gaudet:** Yeah. And also having the ability to understand that when you're going through it. Mhm. Right. To give you that peace, if you will, a little bit of a Zen moment. Very true. Yeah. All right. You mentioned music earlier. Sure. You're on a desert island. What are the top five records you'd bring with you? Five records. Okay. Because there's a turntable there on the island. So I was going to say.

**David Woska:** Do I do I get to have something that I could play it on?

**Ed Gaudet:** You do? You do? Yeah. All right. All right.

**David Woska:** So I want a good turntable and really good.

**Ed Gaudet:** Oh, it's a great turntable.

**David Woska:** Yeah. All right.

**Ed Gaudet:** So the Macintosh system, it's all fully loaded. You're going to have.

**David Woska:** There we go. Okay.

**Ed Gaudet:** You're gonna have a good time.

**David Woska:** I start with Pink Floyd. Dark side of the moon.

**Ed Gaudet:** Very nice. Okay. Very nice.

**David Woska:** Steely Dan, the royal scam.

**Ed Gaudet:** Very good.

**David Woska:** Both really good albums. Yeah. Led Zeppelin, houses of the Holy.

**Ed Gaudet:** Oh, wow. Look at you. Coming out of the woodwork with LED Zeppelin. Houses of the Holy. I love classic d'yer mak'er. Very good song.

**David Woska:** Yeah, yeah. Over the hills. Far away.

**Ed Gaudet:** Yeah.

**David Woska:** It's a great album. What am I?

**Ed Gaudet:** The rain song, I think is on that. Right? What's what? The rain song is on that too, isn't it? Yes it is.

**David Woska:** Yeah, yeah, that's a great song. Love the doors. Love you, love you. Love the 1967.

**Ed Gaudet:** You love the doors. I did, Dave. I did. How come I didn't know that about you? You never asked. Well, let's talk about.

**David Woska:** His Grateful Dead.

**Ed Gaudet:** But my first band. My first band was the Doors. That's it. Really? Yes. That's my true love. Yeah, that's my origin story that connected me into everything. Writing other bands, the beats, the Beat Generation, which is a gateway into the Grateful Dead and and other things. Yeah, but it was the doors. It was Jim Morrison, actually. It was very cool. Yeah.

**David Woska:** My brother, he's a doctor by day, but he's a musician by night. Oh, he's had a couple of bands for years and years, and I still go back to those days when, you know, listening to him coming home from school and, you know, running to the piano with a new idea or something he wanted to try out or compose. And now I get to see him playing, you know, other venues. That's really.

**Ed Gaudet:** Cool. Does he play? Does he cover doors? The doors?

**David Woska:** Or does he cover the doors? No, he does a lot of yacht rock. He has a jazz band also, which is phenomenal. Nice. Yeah. He's pretty. Musical family.

**Ed Gaudet:** Nice. Very good. All right. All right. That's four albums. What do you got for us?

**David Woska:** I'll go a little bit more modern. How about the Eagles? No.

**Ed Gaudet:** I'm just kidding.

**David Woska:** I like the Eagles.

**Ed Gaudet:** Yeah, Eagles are great. Eagles! Eagles are coming to the sphere. Why don't you go to the sphere, Dave. And see the Eagles.

**David Woska:** I saw them in their farewell tour with Steely Dan. Oh, God.

**Ed Gaudet:** Nice. That's a good show.

**David Woska:** That was a great show. Probably the best show I've ever been to.

**Ed Gaudet:** So, fun fact about Steely Dan. There's a lot of fun facts about Steely Dan where the name came from, I do. Do you know the movie? Just tell me the movie. You don't have to go through the whole Barbarella. Barbarella with Jane Fonda.

**Ed Gaudet (cont'd):** Yeah. Yeah. There's a song. I think it's on. Scam kid. Charlemagne. Is that on scam Charlemagne?

**David Woska:** Absolutely.

**Ed Gaudet:** Do you know that song is about.

**David Woska:** Oh, I did.

**Ed Gaudet:** Augustus Owsley Stanley Right. the. Well, he was the audio engineer for the Grateful Dead, but he also produced a lot of psychedelics. He was the main producer of LSD back in the the early 60s. And that fueled sort of the great American acid tests that Ken Kesey and Timothy Leary had put together. So it's all related. There's this unbelievable relationship with music and writers and culture and artists, and it all kind of comes together, if you dig. It's interesting those those relationships. But Steely Dan, great band. All right.

**David Woska:** I've been going to their concerts as much as I could. Okay.

**Ed Gaudet:** All right. What advice would you have to young professionals trying to break into healthcare and or cybersecurity?

**David Woska:** I think it starts with figuring out which track you want. Okay, so there's obviously the very highly technical security engineering and secops and so forth. That's what most people students tend to lean towards. But there's also a whole other side of cybersecurity around risk management and governance and disaster recovery and security awareness and training. I mean, those are so critical. Most people tend to think of the sexier part of cybersecurity, which is really cool, and I really marvel at the people who do it. I've always gravitated more towards the risk management and governance side of it, but I've always found it more interesting to me and it's just as important. So, you know, when you're in school and you're taking classes, I think, you know, you want to take classes. Obviously you want to understand, you know, computer technology, computer science and more universities than ever are introducing cybersecurity curriculums.

**David Woska (cont'd):** So I think that's fantastic thing because we just don't have enough people in cybersecurity.

**Ed Gaudet:** That's a good point. And I think this notion of the ability to critically think is so important. And I think oftentimes people that are coming out of school and looking at different opportunities get a little constrained by what they believe is required technically to do the job. Whereas the nice thing about things like risk management is you can have varying degrees of technical background and do well. You can come out of school with very little technical background and still be assuming you can critically think, right.

**David Woska:** Yeah, of course you need to be good at problem solving. You've got to be good at.

**Ed Gaudet:** Problem solving, no question. Like that's a jacks to open. But the thing about risk management in general is it's so connected to the business, and you get this opportunity to engage with the business and see much broader aspects, not only of business, but where technology and business intersect, the impact of technology on business positively and negatively. And then you can leverage that and that knowledge as you're building it over time, maybe to go into other areas of cybersecurity that maybe require more, more technical experience, more technical background. And so I always find it interesting that third party risk and enterprise risk management and just general GRC provide a really nice entry point for people coming out of school that want to get into cyber, but, you know, may not have the technical background to go into the SOC, for example, to do Pentesting or to do cryptography or whatever.

**David Woska:** But you could get there. It's a great but you can get there. Yeah, absolutely. I've always loved third party risk management, risk management, security awareness and training. I kind of have this notion, if you will, that the human being is just as important as the technology. You know, you can have the latest and greatest security technologies in place, but at the end of the day, you know, it's a human being that makes the most difference, whether it's that person who spots a phishing email and then says, okay, I see that I'm going to report it, or a security team that exercise an incident response plan so that when something does happen, they know what to do and they're ready. Right. So I feel that the human part of it is just so critical.

**David Woska (cont'd):** I had a really good boss who once said something to the effect of, you know, it's not just your security team, it's every employee in the organization that's part of the security team. So I think that's a really great point.

**Ed Gaudet:** Yeah. No, you're absolutely correct. And I think that gets lost sometimes when we're so focused on either the process or the technology. We sometimes miss the forest through the trees. And and again, one of the hardest connection points often referred to. And I hate this, the weakest link. I hate that, by the way.

**David Woska:** Yes.

**Ed Gaudet:** I always look at it as the strongest opportunity. Right? The strongest opportunity is to enable your workforce, enable people to be your best ability to protect patient safety, patient care data, etc.. Right. But those connection points are so critical and they're so fragile in many ways. And oftentimes we get enamored with the technology or we get enamored with our process and we forget that without the right people and that attitude, which is much more open to transformation and change, because if you're truly going to fix something, you have to change. You have to change something. And oftentimes it's that relationship with a really good tool or a really good process and terrible tool. And if you have a really good process and a bad tool, you're going to get bad outcomes regardless. And it's the people that have to understand that and work towards the end goal, which is change for the better, and making sure that we have the right people, the right process and the right technology working together. And yes, it really is. And it's so obvious. And we all have people process technology, but then people will say it. But actually the hardest part is the application of those three things in a way that literally is driving better outcomes.

**David Woska:** I totally agree. You know, you write a check, you can buy technology. Okay. You know, you have people on your staff that can learn a product and can make it work, configure it properly, etc. but if you don't have good processes behind it, how do you react when you configure a SIM to report something based on a threshold of certain events? Okay, it has to go to the right people.

**David Woska (cont'd):** They have to have the right playbooks and processes in place, and they need to practice it so that they're quick and they can respond and minimize the impact, you know, contain it and remediate it quickly. So it's so important to have all three. It really is.

**Ed Gaudet:** Really a great way to end the show. Thanks Dave for joining me today. This is Ed Gaudet from the Risk Never Sleeps Podcast. And if you're on the front lines protecting patient safety and care delivery, 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