Podcast Transcript

Risk Never Sleeps
Episode 29
Frank Riccardi

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 discuss the people that are protecting patient care. I'm Ed Gaudet, the host of our program, and today I'm pleased to be joined by Frank Riccardi, cybersecurity and data privacy expert and author of Mobilizing the C-Suite: Waging War Against Cyberattacks. Welcome, Frank.

Frank Riccardi: Thank you. I'm pleased to be here.

Ed Gaudet: Excellent. Excellent. And you've got some really interesting background. Obviously, you're an author. You are a juris doctor, a lawyer, practicing lawyer still, or?

Frank Riccardi: No, I haven't practiced in 25 years since I got into healthcare compliance. I've been in compliance and privacy and internal audit. And by virtue of being chief privacy officer, I got a lot of exposure to data breaches and ransomware attacks, unfortunately. And that's where I built up my experience in cybersecurity.

Ed Gaudet: Excellent. So take us through your background. You've worked at some really impressive hospitals, Cone, and Adventist, and Trinity.

Frank Riccardi: Yeah, so I retired towards the end of 2021 after 25 years in healthcare compliance, and I did stints as a chief compliance and privacy officer for healthcare systems that owned hospitals and physician practices and Medicare Advantage plans. And as I said, by virtue of being chief privacy officer, did a lot of work managing privacy breaches and cybersecurity events and worked very closely with CISOs and cybersecurity staff. When I retired, I wrote a book Mobilizing the C-Suite: Waging War Against Cyberattacks, and I wrote the book because in my career I found that executives understood what compliance was and they understood internal audit they got. That's been around a long time. They got data privacy, but they never quite grasped cybersecurity. They never quite grasped cyber hygiene, some of the basic principles. And I wrote the book to help leaders, C-suite leaders and board members and others not only understand basic cyber hygiene, but to embrace their massive accountability when a data breach is successful, unfortunately, and their accountability in making sure that the CISO is supported and that the cyber security program is effective. And I also wrote the book to help cybersecurity professionals teach the workforce about cyber hygiene. And what inspires me to write and speak about cybersecurity is we continue to have a worldwide epidemic of ransomware. We have daily phishing attacks, we have daily credential stuffing attacks, and we have the most awful kind of cyber attack you can imagine romance scams and people don't think of that as a cyber attack. But it is. And my goal is I want to educate and teach and help people and companies so that they're not victims of cyber attacks. But at the end of the day, if I can help just one person not be the victim of a romance scam or a phishing scam or a ransomware in their personal lives, I feel like I've done my job.

Ed Gaudet: That's terrific. And we're going to unpack the book. But before we do that, how did you get into healthcare?

Frank Riccardi: Kind of by accident. I was a practicing lawyer. I did general practice law. I did matrimonial personal injury. And this was many, many, many, many years ago. Too old to say how long it was. But I decided I wanted to move my career into medical malpractice field because it was very lucrative and it had a lot of colleagues doing well with that. So I started taking courses and eventually I got a degree in clinical laboratory science, and I got the degree towards about maybe 1997 or so, which was about the time of the infamous Operation Lab scam that occurred with the OIG and the Department of Justice.

Frank Riccardi (cont'd): And they were investigating laboratories for fraud and noncompliance. And what ended up happening is I got hired by a laboratory consulting firm to do compliance audits and help laboratories manage that process. And so it accidentally led me to a completely different career. And from the laboratory consulting, I ended up in healthcare.

Ed Gaudet: And you stayed in it for a while.

Frank Riccardi: And I stayed in it for 25 years. I really loved the mission and the values of healthcare organizations, you know, and nothing wrong with working for a company that makes widgets or makes cars. I think that's great. But the mission of patient care is something special. And my first big job was with Trinity Health, which was a faith-based organization, and I just got hooked. And so I stayed in healthcare and I still love healthcare. And anybody that's in healthcare, they're really doing God's work because they're helping people at their most vulnerable time in their life.

Ed Gaudet: Right. And everyone's a patient and everyone knows a patient and everyone has loved ones that are patients. And so it truly is a shared mission. And that.

Frank Riccardi: Absolutely.

Ed Gaudet: Everybody. So I'm a technologist by trade and, you know, healthcare was always that one industry that I just never got into early in my career because they were always behind everyone from a technology perspective. And then when high tech and AHRA hit in 2009, 2010, it just made sense because there was this forklift upgrade now for healthcare from an infrastructure perspective and they were starting to acquire. And applied new technologies. So, and I'm so glad I got into it because now I'll never get out of it.

Frank Riccardi: Yeah, you get hooked. It gets in your blood.

Ed Gaudet: Like you said, you get hooked.

Frank Riccardi: Yeah.

Ed Gaudet: And the relationships are so different, too. And the people are just. I mean, it's not that they're easy, but they're just nicer again because we are working together. Yeah.

Frank Riccardi: And the whole raison d'etre of healthcare is the ultimate customer care. Yeah, really patient care. But it is the ultimate. And you're right, you have really great relationships now. It's like any company. You have your ups and downs, but at the end of the day, you're all going towards a very important mission.

Ed Gaudet: That's right And when cyber surge jumped the other side of the street and became a risk to patient safety, yes, that's when it started to get really interesting and scary, right, and real. And so talk to me about what you learned over just the last five years and how differing it's been since the previous couple decades.

Frank Riccardi: So I would say I'll even go back maybe ten years. I would be in meetings with healthcare organizations and they would ask a question about cybersecurity. And at some point someone would stay up to get up and it'd be a consultant and they would say, Don't worry about it. As big as you are, you're just not big enough for the cyber criminals and gangs. They're looking for these big targets, and now everybody's big enough. They're going after little dermatology practices, 2 or 3 physician dermatology practices. And if they can lock down the patient record with ransomware, they will make a ransom demand. And they don't have to make a big ransom demand. They don't care. So now they're going after everybody. So I think one of the things that's changed is maybe ten years ago, only the big companies were targets. Everybody's a target now. It's unbelievable. The other thing that has changed is I think there's been a sea change since the global pandemic where leaders are now really starting to understand their level of accountability. And the example that I will give you is in 2021, there were three huge cyberattacks that just changed the zeitgeist of the culture in the United States of America, and one was Colonial Pipeline, and it got shut down for ransomware. And so for a week, people on the East Coast of the United States, from Texas to New Jersey, couldn't fill up their gas tank. There was Schreiber Foods, which is a big dairy conglomerate, and ransomware shut down their dairy processes.

Frank Riccardi (cont'd): So there was a cream cheese shortage. In 2021, you couldn't get a schmear on your bagel. And then the other big one was JBS Foods, and they're a Brazilian meatpacking giant, and their processing plants in the United States were shut down and so you couldn't get your turkey sandwich. So what happens is, pre-pandemic people think ransomware is in cyberspace and it's synonymous with data breaches. But because of these three events, people now say, wait a minute, I can't get a shimmer on my bagel, I can't fill up my gas tank, I can't get a ham, and turkey sandwich. It's ransomware actually can physically affect me and my real life. It can come in the physical world. And so what ends up happening is the general public is now buying reading things in the newspaper and watching TV. They're getting more sophisticated and they find out with Colonial Pipeline, what happened is there was a cybercriminal gang called Darkside, and they stole a password from an employee that left the organization. And we think that that stolen password was just a reused password. So the employee was signing in as everybody was working remote in the pandemic. They were signing into Colonial Pipeline systems with a VPN and they were using a password that they probably were using somewhere else. And so Darkside probably bought it on the dark web. They stuffed it into the VPN and it worked. So what the public learns is this one of the tried and true internal control mechanisms in cybersecurity is when somebody quits the organization, you terminate access to their systems. Well, Colonial Penn didn't do that. They didn't terminate that employee's access to the VPN. It was a live VPN. The other thing is you teach your employees don't reuse your passwords. Maybe they didn't do that, but this person looks like they did. The last thing, if that VPN would have been protected by multi-factor authentication.

Ed Gaudet: Exactly.

Frank Riccardi: When Darkside credentials stuff that password into the VPN, they wouldn't have had the one-time numeric code and it would have been thwarted. And the public learns this and they're like, oh my gosh, basic cyber hygiene would have prevented the Colonial Pipeline cyber attack. And now when these attacks happen, and if they're successful because a company didn't patch their systems, didn't use multifactor authentication or maybe a laptop was lost, but they didn't encrypt it, the public is now just as angry at the C-suite leaders as they are at the cybercriminals. It's a sea change in accountability. And so basic cyber hygiene is more important than ever.

Ed Gaudet: That's right. And with the SEC changes now and with what's happening in New York with the new data privacy rule that just hit and their whole cybersecurity strategy, which again, they're trying to lay out for the nation, right?

Frank Riccardi: Yeah.

Ed Gaudet: It's going to start getting really interesting, especially when executives are going to be on the hook for these attacks. Whereas before, like you said, Oh, it's the organization or it's our cyber team or I wrote an article I think a couple of years ago now, Forbes magazine, where I laid out this notion and that boards have to be accountable for cybersecurity, just like you have an audit committee, just like you have a finance committee, just like you have a comm committee. Yeah, Cybersecurity needs its own committee and it needs to be chaired by people that understand cybersecurity. It can't be someone's, you know, uncle, aunt, whatever. Yeah. So we think that will make a huge change as well to the level of understanding and the level of investment and resources that the teams will get moving.

Frank Riccardi: Yeah, I would agree with that. Cybersecurity expertise at the board level is critical and it's no longer going to work. If there is a cyber attack and you fire the CSO, that won't work anymore. Maybe it worked in the past, but it will not work anymore. The C-suite and the board has to be accountable for cybersecurity.

Ed Gaudet: Exactly. So let me go back to something you said earlier about the two provider dermatology office.

Frank Riccardi: Yeah.

Ed Gaudet: What can they do? Because they clearly don't have a CSO on staff. They clearly don't have millions of dollars they can spend on technology. So what would you tell that two-person dermatology office?

Frank Riccardi: If they haven't already gotten bought up by a big healthcare system? I'll give you two answers. If you are a dermatology practice and you are part of a big healthcare system and the healthcare system, CIO or CSO says, Hey, I need to take your information systems and roll it up into my EHR and I need to extend my cybersecurity program to you. You have to let them do it. You don't want to become a shadow IT dermatology department doing your own thing because then you are vulnerable to an attack. So first thing is listen to the health system CSO and do what he or she says. Now the second thing I would say is if you are on your own and you don't have a have a CSO, one of the things you might be able to do is there are some vendors out there that are pretty cost effective that they can set up a cybersecurity program for you. Soup to nuts. Some of them can do your patches, they can teach your staff cyber hygiene, they can help you with multifactor authentication and they can do it on a pretty cost effective basis, especially when they have a lot of clients and that might be your best bang for your buck. Don't try to do it on your own. Try to outsource it to a cybersecurity vendor that will do this for you. If you don't want to do that, then you're going to have to find somebody in your organization or hire somebody that's tech savvy enough that they're going to understand about phishing and how emails can come to your employees and they ask for a survey or click on the link and they upload ransomware. And it's really hard to do. It's not intuitive, but you're going to have to find somebody to help you, whether you hire it or you get a vendor to do it. If you're a small dermatology practice or any kind of small business might need a little bit of help.

Ed Gaudet: Great advice, great points. And to the listeners, I'll also note that there are a number of free guides available through the HHS, the 405 program, as well as CSO, has free assets and documentation and tools you can look at. Obviously Frank was teeing that up for your book, but you didn't. You didn't oh.

Frank Riccardi: Didn't go for it.

Ed Gaudet: You can also mention your book, too.

Frank Riccardi: Now you are talking about this.

Ed Gaudet: Yeah, there it is.

Frank Riccardi: All right. Man, I'm telling you. Thank you for the softball. I am just.

Ed Gaudet: I love that you didn't take it, though. Actually, that even says more. Love that. Okay. Yeah. So take a look at Frank's book if you haven't already. Want to hold it up one more time for folks would love.

Frank Riccardi: To hold it up one more time. And it is going to give you small dermatology people the basics of cyber hygiene so you'll be able to protect your.

Ed Gaudet: I absolutely love the title too. It's so true. Mobilizing the C-suite like we're all in this together. We're stronger together. But we do have to work in concert. It can't be the purview of one department trying to work across all departments.

Frank Riccardi: It works from the top down. Cybersecurity, like everything else, tone at the top.

Ed Gaudet: It does. I often say the fish rots from the head down.

Frank Riccardi: That's a good a good one.

Ed Gaudet: You know, I love your background. Compliance, privacy, security. If you were in front of a C-suite, oftentimes this notion of cybersecurity and privacy and the nuances of the two things gets lost. How would you describe the two and how would you point out the differences?

Frank Riccardi: I love the question. So, as someone who has had experience as chief privacy officer, but I've never been a CSO, but I've worked very closely with CISOs and cybersecurity, and I hear a lot of talk about privacy versus cybersecurity, and I never saw that in my career because every time I had a privacy breach or an incident, it was always a cybersecurity matter, always a cybersecurity incident. And. One of the CSO had a cybersecurity incident was a breach. It was a breach. It was privacy.

Frank Riccardi (cont'd): So I view privacy as being the arm that is educating the workforce on privacy issues. If you're in healthcare, it's on HIPAA. If you're in a different business, it might be a different law. When there's a breach, the privacy team would manage the breach. So they're going to work with your cyber liability carrier, with your attorneys. They're going to work with marketing. They're going to work, get the notices out. They're going to be involved with legal counsel. And fending off any or being involved in shouldn't say in managing any lawsuits. The cyber security team is extremely important because they are going to do the forensic lab work. They are going to tell me, Oh, this is how the attack happened. It was credential stuffing or it was phishing or some kind of social and engineering. Here's what happened. Here's how we stopped the bleeding. We fixed it. They would usually file a police report on it. And then they're deeply involved in the technical pieces because at least in my world, at my level, we had cyber insurance. And the cyber insurance carrier would give you what's called a privacy coach, and then they would also have a forensic team. And I could work with the privacy coach, but I really needed the CISO to work with the forensics team because very often they had to go into their systems and look and see exactly where things happened. So I always saw privacy and security hand in glove, working very closely together. At one side of a coin, they're very close. I could see in the future the two departments being fused because in theory, most organizations I've worked with, the CISO reported to the CIO. Not optimal really to see, so should not report to the CIO. But if you took privacy and cybersecurity put them in a different department, it could roll up to anybody other than the CIO. And then you truly have freedom from any conflicts of interest.

Ed Gaudet: I mean, it'll be interesting to see if that actually ends up happening. No, ATA that's what happened actually. That was peer to the CIO and manage all of those aspects of security, whether it be cyber as well as physical security and privacy in that one one organization. So we're going to switch some topics here and ask you a little bit about you, Frank.

Frank Riccardi: Sure.

Ed Gaudet: You go back in time. Why did you tell your 20 year old self?

Frank Riccardi: My 20 year old self, I would say, Frank, you're no doubt very handsome and smart fellow.

Ed Gaudet: Of course.

Frank Riccardi: But you need to always try to step outside your wheelhouse and find things that you're not good at and dabble in them because that will broaden your horizons. So if you are not good in math, learn to make change. Take an algebra course. If you're not good in public speaking, go to Toastmasters, learn how to do public speaking. And it's advice that all your listeners could take to heart. Because in my own life, when I was in high school, I had a tremendous fear of public speaking. I hated it. And when I got into college, I just said, I'm going to force myself to get out there. And I found that I was funny, I was witty, I liked the back and forth, and I fell in love with public speaking and I ended up going to law school. So, you know, you might think you're bad at something and if you dabble in it, the whole world could open up to you.

Ed Gaudet: That's right. Yeah. No, that's so great. In fact, you know, it's surprising that there's a survey. I guess they ask once a year what people are most afraid of. And public speaking, I think is usually 1 or 2, depending on the year, right? Yeah. Frank, I'd be remiss if I didn't ask you this question because this is the Risk Never Sleeps Podcast. Okay. What's the riskiest thing you've ever done?

Frank Riccardi: So the riskiest thing I ever did was when I was in high school. I lived in upstate New York where it was very cold and snowy and on a really cold, bitter, snowy day, just on a lark. I don't know why I did it. I hopped in my car and I drove to a ski mountain and I went to the ski lodge and I rented skis and poles and I trudged up the mountain. And then I attempted to ski down the mountain without any lessons, without ever having put on skis, without ever having any lessons. And I took the hardest moguls I could find now Ed, I'm not going to tell you, I actually skied down the mountain. I tumbled down the mountain and it was very risky. I could have broke my neck. I could have broke my arm or something. It was really stupid. When I got home later that week, I talked to my Uncle Joe. I told what I did. He thought it was funny. He said, Frank, I'm going to take you out skiing. So he took me out skiing one day.

Frank Riccardi (cont'd): Little did I know and did teach me how to ski, but his real reason was he wanted to teach me how to get up when I fell. And so we went skiing, taught me how to ski. We went skiing. Sure enough, I fell down, could not get up. He comes over, I outreached my hand. He bats it away. So I'm not going to help you get up. I'm going to teach you how to get up. So he told me where to put the skis, how to put them down and angle them just right and with the poles. And if you follow the procedure, you can pop right up.

Ed Gaudet: Yeah.

Frank Riccardi: And sure enough, I popped right up. And after that I had a lot more confidence because I knew if I fell down, I could get up. But it was a very important life lesson that because the thing of it is we're human beings and we're going to fall down. We're going to make mistakes. We're going to do dumb things or people are going to push us down. Maybe they don't like us, maybe they're bullies. But if you know how to get up, you're going to be just fine in life because you're going to fall down and you want to avoid it. But you just got to know how to get up and everything will be good. So riskiest thing was skiing without lessons. But you know, I guess I got a life lesson out of it.

Ed Gaudet: Yeah. No, that's terrific. Terrific story. I love that question because I always get some really interesting stories about people. That's a new one. That's a unique one. I like it. This is where I get to call the Audible because I heard something about you that's not on your LinkedIn page. Okay. I hear you're a vinyl collector.

Frank Riccardi: I am. I'm an.

Ed Gaudet: So let's talk music.

Frank Riccardi: I would love to talk music. Okay. Well, let's let you ask.

Ed Gaudet: Well, I was going to ask I mean, I love music, too. So first off, do you have a high-end system that you listen to?

Frank Riccardi: I do. I have a Peachtree Integrated amplifier, which is sweet and I love it. And it's the greatest integrated amplifier I've ever had. You know, you can spend ten, 20 and more on an integrated...

Ed Gaudet: Hundreds and thousands of dollars. Macintosh systems, and.

Frank Riccardi: It's nuts. Yeah. And this one was thousands of dollars, too. But I will tell you, for the money, it's the best sounding I've ever heard. But the way they designed it, it's the most simple, easiest integrated amplifier. I almost call it the iPhone of integrated amplifiers. It's so simple and fun. I have really good speakers and I have a exactly what you call it, but it's a little device and it's got a test tube. And when I turn it on, it can give the analog sound a test tube warmth to it. So it's really sweet. It's a really nice, subtle wow.

Ed Gaudet: Okay, so what's on your turntable now?

Frank Riccardi: So and what goes great with a coffee cocktail or cold one on a Friday afternoon?

Ed Gaudet: Kind of blue by Miles Davis.

Frank Riccardi: Well, that too.

Ed Gaudet: Oh, pretty close.

Frank Riccardi: Oh, great Link Wray Rumble his greatest hits 1956 to 1962 and.

Ed Gaudet: I love that.

Frank Riccardi: For your listeners. What I'd like to just let them know about this album. I highly recommend it. He had a smash hit in 1959. It was called Rumble and it had three power chords. It's his famous twang, twang, twang, and it was so seductive that the song was banned throughout the United States because people thought it was going to stoke teenage violence and gang wars. But Pete Townshend of The Who as a young man heard the song and he want to say a quote. So Pete Townshend of The Who, if it hadn't been for Link Wray and Rumble, I would never have picked up a guitar. So if it hadn't been for Link Wray, we wouldn't have had The Who one of the greatest rivals.

Ed Gaudet: Oh. Absolutely.

Frank Riccardi: So.

Ed Gaudet: Have you seen The Who in concert?

Frank Riccardi: I've not seen The Who in concert.

Ed Gaudet: Oh. Do you go to shows at all? Do you go to any?

Frank Riccardi: It's been a long time since I've gone to shows. I used to go a lot, many, many years ago. I haven't gone to one in a long time.

Ed Gaudet: So you collect vinyl. So what types of genre, anything really interesting or unique?

Frank Riccardi: I don't know if there's anything really interesting. I like classic rock and I'm going to define that as 50s, 60s, 70s, 80s and 90s.

Ed Gaudet: Okay.

Frank Riccardi: So that's kind of the genre that I like. But I recently came across a hard rock band called Dream Theater. I don't know if you ever heard of that.

Ed Gaudet: I do know them.

Frank Riccardi: Yeah, okay. And I absolutely love Dream Theater and that's one that boy, when I turn up my stereo and I get my test tube going, you can really hear everything. It's just a wonderful, wonderful band. Would love to see them in concert.

Ed Gaudet: Friends of mine, we started at one point during the pandemic just before a vinyl club and which I love. And so I have, you know, I was a collector of albums for many years and then went to CD and I have about, I don't know, 5000 CDs that I've put on a Brennan. Do you know the Brennan device?

Frank Riccardi: No, haven't heard it.

Ed Gaudet: It's basically a Pi device that you can stream all of your CDs from and it's,

Frank Riccardi: Oh wow!

Ed Gaudet: It's got a nice interface and.

Frank Riccardi: Wow.

Ed Gaudet: Yeah. So you can, you know, you're ripping into the device and you get to share them. Whatever. I love the Sound of Music on a vinyl with a nice set of speakers and you can pick up things like, I brought the Ziggy Stardust album.

Frank Riccardi: Oh, nice.

Ed Gaudet: And so in the vinyl club, we play one side of an album, right? And I just remember listening to that and I was like, Wow. Just like opened up things I had never heard before because I didn't have that fidelity. Just incredible. Just incredible.

Frank Riccardi: Yeah. There's something that's wonderful, too, about the imperfection of analog that you put on the vinyl record and cracks and pops and scratches, but it's warm. It's part of the ambience. And there's something I think you lose by the perfection of digital that I can't explain unless you're just listen to the vinyl or just enjoy it.

Ed Gaudet: Yeah, everything feels compressed and pushed together. Yes, Everything is sort of like and you can't make it. It's really difficult to make out those those notes in the imperfections obviously. So I don't often ask this question, but I will to you.

Frank Riccardi: Okay.

Ed Gaudet: On a desert island and you can only bring five albums. No greatest hits.

Frank Riccardi: Okay.

Ed Gaudet: What are the five?

Frank Riccardi: The First Doors album.

Ed Gaudet: Oh

Frank Riccardi: That would be their Sergeant Pepper's Lonely Hearts Club Band.

Ed Gaudet: Wow. Two for two. Okay.

Frank Riccardi: Yep. I would say probably Moody Blues Nights in White Satin. I would say it would be Elton John. And what was the album where he.

Ed Gaudet: Wireweed or.

Frank Riccardi: I'm drawing a Blank on the Elton John album? It was one of the Elton John albums. And then I probably would have a Foo Fighters album because I'm also a big Foo Fighters fan.

Ed Gaudet: Ah, Foo Fighters. Nice. Yeah. Foo Fighters have a great I mean, what a great library of songs.

Frank Riccardi: Oh, by the way, it was Captain Fantastic.

Ed Gaudet: The Brown Dirt Cowboy.

Frank Riccardi: Yes. Elton John.

Ed Gaudet: Someone saved my life tonight.

Frank Riccardi: That was it.

Ed Gaudet: Favorite Songs by Elton John.

Frank Riccardi: You know what? I could not pull that out of my brain.

Ed Gaudet: I love that song. Yeah. No, a friend of mine who actually ended up developing building integrated receivers and amps and things.

Frank Riccardi: Oh, nice.

Ed Gaudet: You ever hear Krull? No, I think it's called Krull. Anyway, they're no longer around. He went to Harman Kardon, too. I remember when we were kids, and I forget how old we were. Probably seven years old. And he brought that album out that for the first time, I'm like, What is this? Yeah, fantastic. All right. Well, that was terrific. Any last parting comments to our listeners, Frank?

Frank Riccardi: I guess the only parting comments, I'm active on LinkedIn, so if anybody's interested in learning about me and what I do, please hop on over to my LinkedIn profile page. And if you want to learn about me, that's probably the best place. But you could also interact with me and you can follow me or you can send me a connection request. I'd be happy to accept it. And next to my smiling face on my LinkedIn page to the right, there's a bell. And if you click on that bell, every time I do a post, you'll get notified of it. And I post on compliance and privacy and cybersecurity. And I even did a post on Link Wray So you can read about Link Wray and you can...

Ed Gaudet: Terrific.

Frank Riccardi: Love him as much as I do.

Ed Gaudet: All right. All right, folks. So that is Frank Riccardi joining us. And again, check out his book, Mobilizing the C-suite: Waging War Against Cyberattacks. This is Ed Gaudet from the Risk Never Sleeps Podcast. If you're on the front lines protecting patient safety, remember to stay vigilant because risk never sleeps. Thanks for listening to Risk Never Sleeps Podcast for the show, notes, resources and more information and how to transform the protection of patient safety. Visit us at censinet.com. That's censinet.com. I'm your host, Ed Gaudet. And until next time, 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