Podcast Transcript

Risk Never Sleeps
Episode 52
Steven Ramirez

Ed Gaudet: Welcome to the Risk Never Sleeps Podcast, in which we learn about the people protecting patient safety and delivering patient care. I'm Ed Gaudet, I'm the host today, and I am pleased to be joined by Steven Ramirez, the Chief Information Security and Technology Officer at Renown Health. Steven, welcome.

Steven Ramirez: Thank you. Glad to be here.

Ed Gaudet: Yeah, welcome to the show. Excited to have you here and learn more about you and your background. So why don't we start there? How did you get into healthcare, technology, and security specifically? Give us the short version.

Steven Ramirez: Well, both my parents are in the field. My dad's a primary care physician, still practicing now, and my mom's a respiratory therapist. So quickly, when I got into college and realized that I was better at computer science and biology, I think that was my natural track to really see where I could go into things. But my first job was Georgetown Health, so I think that was really the onset of that worked with CHI back in 2011, really, when they were just building up to where they are now with Commonspirit and being one of the biggest not-for-profit health systems. Worked with McKesson as well as IBM Watson. So, really, on what they were doing on the Medicare-Medicaid side of the House. Was doing security for that, so very different vantage point. And then started up my official CISO duties at UofL Health and transitioned over to Renown.

Steven Ramirez (cont'd): So just kind of been dabbling in healthcare, which is very interesting and dynamic. So we know we're part of that critical infrastructure and definitely have our own ways of doing things versus other industries.

Ed Gaudet: Right. That's right. Yeah. Very different in that shared mission is unique to healthcare. What does that mean to you?

Steven Ramirez: Well, it's definitely, everything we do translates back to patient care supporting our care providers, and supporting our community. So our team takes that personally, on what we do on a day-to-day basis, really making sure that we are supporting our care providers and, I really make sure that I emphasize that, again, we are a support service. So we're here to say no, of course, when we need to. But more likely, yes, and then seeing how we can kind of mitigate risks. So, really being a champion of the people because they're the ones on the front lines, and they've been short-staffed across the board since COVID. So just really trying to be good partners to our clinical teams.

Ed Gaudet: Yeah, that's been challenging for everyone. Tell us a little bit about your health system.

Steven Ramirez: So Renown Health is out in the Reno, Nevada, area. Such a beautiful area, a great system. We are a hospital system. We have a plethora of services. So we're the area trauma center, children's hospital, and cancer center. We also have a recent affiliation with UNR. It is still in its infancy stages, almost going on two years. It was going on bright as I started. So really excited about that partnership in our academic research. And really, as we're transitioning to support our Healthy Nevada project and a lot of the opportunities with the university. So from a security professional, that's awesome because we get to do kind of the things the right way up front versus a lot of older academic medical centers. It's kind of playing catch-up. So it's awesome to be able to have that partnership and be able to lay the groundwork.

Ed Gaudet: Absolutely. And when you think about the last year, in the next 24 months for you, what are your top three priorities that you're working on?

Steven Ramirez: Access and third-party risk management. So being a casino town on what happened down in with MGM. So we really took a lot of lessons learned. We're seeing social engineering, the way they're getting in. So, really, making an emphasis on the front door. So you know gotten our access provisioning, our service desks, etc., a lot of the lessons learned from them, and then really targeting. I know a lot of people, there's a lot of buzzwords on zero trust and, you know, minimally necessary access, but actually operationalizing that. So I think that's where I have the unique role as that CISO, both the security officer and the technology officer, to influence that. My team, security is always at the table. So we're really making sure we're doing security first. Not that we're going to be 100% patch compliant, but again, just making sure that we're there and can kind of have those dialogues that run. So that really enables us to have quick action and make sure that we're keeping risk, cyber front, and center of a lot of what we're doing. So that's going to be our biggest focus point. And also a third-party risk, as I mentioned. We saw movement, and we had a lot of those high-profile instances. So as we continue to see everyone moving to the digital transformation and sassy-based products, how do we better protect ourselves from not just doing the Hunter questionnaires but real-time monitoring, better language to better protect ourselves contractually, etc., liability? So, looking at that whole spectrum of what we're doing, we're actually looking at implementing the room framework. So it's really a good way to have that holistic vantage point and then really help educate our various partners and critical stakeholders on their part in third-party risk. It's more than just the security assessment. So we really are enjoying our journey as we're getting to do that, to do things the right way, starting with getting our monitoring, real-time monitoring, you know, our more meaningful assessments, I like to say. So, making sure that we're doing the inventory of what players are doing, working smarter, not harder. And we're actually a recent client of you guys. Partnering with Certified Health to do that. So it's like we're really going on looking what's going on in the market, and it really makes sense with how important this is to outsource that and use that tool that does a lot of that for us. So, I know Eric Decker and some other higher-profile CISO colleagues really speak highly of the tools. So that's looped us in here. So they do tell me I had to say that I was just coming out. We're excited to start our journey.

Ed Gaudet: I typically don't bring up Censinet specifically on these podcasts. But since you did, Steven.

Steven Ramirez: Yeah. Yeah. No, but that's front-and-center at Censinet because that's the biggest way that people are getting in. I was out at Becker's this week, and also the emphasis on AD security. So really making a focal point on how we're better protecting our Active Directory. If you're able to protect that and also recover that quicker, we feel like we'll be farther ahead than a lot of other organizations on that.

Ed Gaudet: That's right. And so when you're thinking about your overall strategy for third-party risk, how do you involve the business differently now as you think through automation, bringing in automation and continuous monitoring of those third parties?

Steven Ramirez: Well, just making sure they have a seat at the table. So, we've made a big emphasis on our review process. So we have a, so it's a technical estimation committee. So it's really on AB net new technology that comes in. They review that to really see the necessity, the interconnections, etc. So that's the perfect focal point not only for security assessment but to look at all these other integrations for the whole ecosystem. Make sure that you're speaking with the business about what's going on, but also for really the intent, because these discussions are happening at our President's Council to really have an understanding and a pulse on where the organization's strategy is. You know, as we talked about earlier, you know, staffing challenges, we're looking at different opportunities and technologies that can supplement staffing on those opportunities. So when looking at that, just really making sure that we do look at the risk perspective and how we do supplement the business to make sure that those contracts have the right language, that we're making sure that we're working with some solid partners that have good security, posture, etc. so.

Ed Gaudet: That's great. And since you've just gone through this process, there are oftentimes we run into peers of yours and others who struggle with getting the commitment from the clinical side of the house on the process. What advice would you give them, specifically? Oftentimes, the clinician will go off and purchase a system and just say, Okay, we've bought this, go ahead and do a risk assessment on it now.

Steven Ramirez: Yeah, that's that age-old. It's really on having those strategic partners and supply chains. There are a lot of front doors to see what is and isn't being purchased. So that's where you need to educate them on anything technology needs to be routed to us. So when they say it takes the village, it does take a village—also working with your TMO or transformational management office and our PMO. So it's them looking at anything that's strategic-wise coming in. Obviously, with AI being the big buzz, making sure that we have a grasp on all of this, kind of backchanneling, and relationship building—really making sure that they're able to bundle things by you because that's the best time to catch it upfront before you have any contracts signed and all of that. But from a clinical perspective, the CISO job has evolved to be part of the business. So, we really take advantage of our GRC, our governance, risk, and compliance committee. We have stakeholders from every workstream across the board, and so making them in the loop, in third-party risk, is so important that we're building our framework for our GRC committee around the room that we just think that those different buckets of building that out, because again, as a support service, we need to treat our business the same as we're assessing risk. So really having those stakeholders, your chief nursing officer, your chief medical officer, supply chain, legal, and really everybody at the table so that you can just have those discussions on what's not only going on in the industry but where are we going as an organization to make sure that we're mixing in risk mitigation where needed?

Ed Gaudet: Excellent, excellent. So, other than access and third-party risk, what else keeps you up at night?

Steven Ramirez: Now that I've taken over the technology side, a lot of things. So operational, it's just really everything. Like, if security wasn't enough. But I think that's a question that a lot of CISOs get. I think that if you just do security 101, well, your team puts in their best effort. You're never going to be 100% bulletproof. There's no silver bullet to any specific technology or anything like that. So it's really just about trying to do the basics very well and just be prepared. So nothing should really keep you up at night if you're doing the right process, incident response, and doing everything like that. Because again, you just got to be resilient as an organization. Just knowing that it's a matter of time when the punch is coming. So just do your part to train and train your organization from all the multitude.

Steven Ramirez (cont'd): Guys, remember, and of course, take advantage of Cyber Awareness Month this month. Everybody's role in, you know, social engineering, the technology is just a small piece to what we're doing. But even third-party risk management, access management, you know, really tying that in and educating people to the 'why'. Customizing policy, you know, making sure that we are doing the right thing by the business, the business, the bolts. As AI and ChatGPT and all this stuff come in. If that's something that makes sense for our business, we're going to adapt and see how we can mitigate risk and or utilize it in a way that protects our organization. So, you know, really, hospitals never sleep. So, you know, we're just making sure that we do put in just good policy and practice to support them so we can get a few hours of sleep every now and then.

Ed Gaudet: That's great. And tell us about your training program. So, what are you doing for phishing training as well as? Are you doing a lot of table talk exercises with your teams?

Steven Ramirez: So, we actually went to a managed service partner to help us with phishing. So it's so important that we know formerly the onset of people reporting phishing to what happens after they do that. So a lot of times, it goes to that black hole of you reported it, and IT is looking at it. So we took the approach of having a response back to them. So now, one of our managed service partners actually responds to the email to give an educational verb to, This is phishing, this is spam, or now this is a clear message to go through. So we've really seen having that interaction with the end user really going a long way for them to be able to better spot things that they need to do. Also, looking at what's going on in the industry. We've seen that QR codes are a huge emerging risk. As I was out at Becker's last week, and that was something I brought up there. We were seeing kind of the early stages of that coming out, because it's easier to get through email blocking, usually looking for a link or different attachments. So now there's a QR code in a method that's kind of going through that and requiring that technology adjusts to start to look at embedded messaging as well. So it's really about just remembering to educate your users. We're not going to ever send you any of these. We're not going to ask you to buy us gift cards. We're not going to ask you to click on a link about your passwords. We're not going to send you QR codes to send this unless it's coming from myself, from a method that you know is secure and vetted, to really just be mindful. But again, we're spoofing, you know, everybody's doing their due diligence on I mean, the threat actors are from doing very targeted and almost flawless social engineering at this point.

Steven Ramirez (cont'd): So that's, if anything, keeping me up at night, just the capabilities of how sophisticated they are getting. It's just an ongoing basis that our tools are going to continue to have to evolve because it's just an ongoing battle.

Ed Gaudet: Yeah. So, been a tough couple of years for folks, specifically in healthcare. What are you most proud of personally and professionally?

Steven Ramirez: Healthcare, in general, has come together. I said earlier on that we're very unique. I think that each healthcare system is very embedded and wants to do the right thing for our patients and our community. So, really, they are coming together, doing more with less. The CISOs I think are, some of that, healthcare CISOs are more willing to share lessons learned than anything on that. So just the partnership, friendship, and a lot of what other organizations are willing to share on what they're doing, what's working well, what isn't. I've really kind of seen that consortium and partnership and collaboration, with H-ISAC or FID and other methods like that. It's just been phenomenal how we're able to get back to one another. So that's really as good as our weakest link. And we know that we're all in this together. So, security is all about information sharing. And I've seen that just really, really skyrocket since Covid. I have a lot of different group chats, you know, different memberships. We have Slack and all that with H-ISAC, you know, 4 or 5 D, all of this other stuff. So it's really a great way for, you know, us as a healthcare community to kind of come together and make sure that we're information sharing and really trying to stay ahead of the bad guys.

Ed Gaudet: Excellent. Excellent. So, if you could go back in time, what would you tell your 20-year-old self?

Steven Ramirez: That is a great question. I would probably my 20-year-old self thought I was going to be an attorney, so I would have said, good job on that. Going to law school and really taking that, and staying on the path that I did because it's been awesome. I would have never dreamed that I would have been in cybersecurity when I was going through school, it kind of just happened upon me having a Facebook account and IT Risk really kind of got to the center hold in the millennial aspect. So it's never a boring day.

Steven Ramirez (cont'd): I know we have a lot of shortages in our industry. So I mean, if I could go back, I would try to educate others that they're a step outside of these mainstream jobs. And you really the importance of what we do on a day-to-day basis, especially in healthcare cybersecurity. So just to really champion a lot of what we're doing. So that's where, you know, going and doing different speaking events, and if I have an opportunity to speak to students that it's, this is a very flourishing field. So, I don't know that I directly answered that question.

Ed Gaudet: No, that's good. No, it's good. Yeah, no. There's no right answer. So hardest lesson in your career?

Steven Ramirez: Hardest lesson. That there's not necessarily always, don't be scared to fail. So that's one of my early mentors who said, You're never going to be perfect. There's never going to be; we can't mitigate all risks. So there's always tomorrow, too. So we know we need to work hard. It's an ongoing battle. But again, you need to make sure you take care of yourself and that you know you're never going to mitigate all risk. So, thinking outside of the box, having a strong team that trusts you, trusting your team, and it'll all work itself out because those are the guys you're going to have to work with if there's an event, an incident anyway. So building that trust collaboration with your team and partners is just paramount.

Ed Gaudet: Absolutely. If you weren't doing this job, what would you be doing? Where do you spend your time outside of this job? What's your passion?

Steven Ramirez: Well, I am a newer dog dad. So I love to go outdoors, do some hiking, and try to stay up with them. But no, I love what I do. I wanted to originally be a cop or a firefighter. So I guess it's, you know, in a way of being able to give back. But I guess if I could get better at golf, if anyone has that silver bullet, that would be really cool in life.

Ed Gaudet: Practice, practice, practice.

Steven Ramirez: Oh, yeah. Yeah. That's the only thing that keeps me up at night. That I have a golf trip. And we're so busy doing what we're doing in security that my golf handicap. So I have to tell all my friends and finance and other stuff that I said, Yeah, you guys have it easy. You get to play golf all the time. We have to go keep the lights on.

Ed Gaudet: Are you going somewhere in the States or outside of the country, or?

Steven Ramirez: We're going to the Dominican Republic in February. I'm so excited that we have a big group of guys that we go on an annual golf trip, and I lose a lot more balls than anybody. So if anyone that's in the ball-picking industry and wants to go check around the Dominican in February, I'm your guy, so.

Ed Gaudet: What's the best course you've played?

Steven Ramirez: Oh, that is.

Ed Gaudet: Scotland or Ireland?

Steven Ramirez: I haven't played it. I've played it a few, like the island courses and beach courses, but I really loved the Cabo courses.

Ed Gaudet: Oh, nice, yeah.

Steven Ramirez: I would've sold, so that's probably one of my favorite on that ocean course. And I would definitely have to do this.

Ed Gaudet: You definitely have to play Pebble Beach. You'll have to play Pebble Beach at some point. Oh yeah.

Steven Ramirez: Oh yeah. And ocean reef, so yeah. Got to play that earlier on in February. That was a cool course as well. So I just love beach courses. Played some cool mountain courses as well. But yeah.

Ed Gaudet: Excellent. So I would be remiss if I didn't ask this question because this is the Risk Never Sleeps Podcast. Steven, what's the riskiest thing you've ever done?

Steven Ramirez: Okay. Work or personal?

Ed Gaudet: It could be anything.

Steven Ramirez: I'm very risk-averse. So I think that's why I sit into this job really well.

Ed Gaudet: I like people saying that, and then they say something like, completely crazy. I'm usually risk-averse.

Steven Ramirez: Well, I've wanted to do, like, some skydiving. The fact that I've made it through football and helmets were as advanced as they are now that I guess that contact sports to where they are today must be crazy.

Ed Gaudet: Did you play? What position?

Steven Ramirez: I was free safety.

Ed Gaudet: Oh, nice, yeah.

Steven Ramirez: Yeah, a lot of head contact, I'm sure.

Ed Gaudet: Yeah. Okay. So skydiving. Are you going to do that, or are you just thinking about it?

Steven Ramirez: I would love to do something like that. But again, I'm just so chicken. I'm not doing a lot of stuff like that. So, just like thinking the Reuben Feffer in me on what's risky and what isn't is always kind of been there.

Ed Gaudet: Great skydiving in Nevada. There's a lot of interesting things you can do. Never hike any crazy terrains?

Steven Ramirez: Oh, I have on that, but it's, yeah, I have generally good balance. I guess my big five-foot-ten frame that I'm closer to the ground. So I've been lucky on any kind of hiking. I've just started mountain biking. So maybe if you asked me that question in a year, once I graduate up to the difficult level of the courses

Ed Gaudet: Okay. Any last advice to folks who are thinking about getting into cybersecurity or maybe a couple of years in? Could be some knowledge-based advice or leadership advice.

Steven Ramirez: Don't ever be scared to fail, like I said before. And that's if you're looking for just an ever-changing, exciting field to be in; it's never a boring day in cybersecurity. Like anyone you would talk to, you always want to be working on strategy. And a lot of, you know, how we could be tactical, but it's always like this happened, and you're like, well, how the heck did that happen? Or, you know, you hear on this news story, I'm like, this happened down at MGM. And they're like, well, are we doing the right thing? So it's like, you know, it's just continual wash and repeat on making sure that you're keeping the perimeter up. And just a very exciting and purposeful, especially in the healthcare side. Just a great field to be in.

Ed Gaudet: When the MGM event happened, did you do anything differently or did you give that so close to home, was there anything in there?

Steven Ramirez: Well, we definitely do not, being a casino town, as well as being in right now, we just used that being the tail end to October for Cyber Awareness Month. So we made our theme Don't Gamble on Cyber Security. So it's kind of using that as a use case and really the vigilance of what we're doing. So, of course, there's a lot for what we have seen in social engineering.

Steven Ramirez (cont'd): So make sure that our service desk partners and people with privileged access are doing the right thing, and then look at ways that you can verify end users. So that's the ongoing battle of making sure that the user is who they say they are. So just always getting some creative ways of doing that.

Ed Gaudet: All right. Well, we've been talking to Steven Ramirez on today from Renown Health. This is Ed Gaudet from the Risk Never Sleeps Podcast. And if you're on the front lines protecting patient safety and delivering 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