Podcast Transcript

Risk Never Sleeps
Episode 37
Errol Weiss

Ed Gaudet: Welcome to the Risk Never Sleeps Podcast, in which we learn about the people who are at the front lines, protecting patient safety and delivering patient care. I'm Ed Gaudet, the host of our show, and today I am welcomed to be joined by Errol Weiss, the Chief Security Officer for the Health-ISAC. Welcome, Errol.

Errol Weiss: Thanks, Ed. It's great to be here with you.

Ed Gaudet: It's great to see you, too. We've been working a lot together recently, so this has been, this will be a real pleasure for me to get a chance to know you a little better, and our listeners to get a chance to hear more about the H-ISAC and, and what, what you're doing there. So let's start there. Tell us about your role and your organization.

Errol Weiss: Yeah. So, so I've been with Health-ISAC now for a little bit over four years. The role as Chief Security Officer, I don't have, I'd say, the typical CSO job, very member-facing. If you know what an ISAC does, and maybe we can get a chance to talk about that, everything that we do in terms of providing information, intelligence, services, training, I've got responsibility from, like, a technical content and delivery standpoint. That's what really helps keep us busy. So it gives me a chance to speak with our members, work with the community, work with other partners, and whatnot, and make sure we're delivering what we should be for our members to help them stay secure and resilient.

Ed Gaudet: Excellent, excellent. And I took a look at your background, obviously, before the call. I kind of knew this anyway, but. You know, you were in finance before you went into healthcare? And so how has that helped you?

Errol Weiss: The jobs are, I say, closely related, and I was in the banking finance sector for 13 years between Citibank and Bank of America, and during that time, I was, most of that time, between the two. I was running cyber threat intelligence for those organizations and I was heavily involved with Financial Services ISAC. Very well established, they've been around since October 1st of 1999, and very well established, very mature. ISAC, lots of different services, tremendous user base membership, lots of support through the partners and vendors that they have that are part of that organization, and lots of great services. The benefit here is, coming to Health-ISAC, and taking what I thought was working well and trying to replicate and improve upon that, and then ditching what didn't work so well and not even going down that path, learning from all of those mistakes, and providing a lot of those kinds of services for our members. The scary part for me, really, was after a long time in financial services and supporting financial services in various ways was really making the leap to an entirely new sector, right? So many, my healthcare experiences was just going to the doctor, and, and that was really it. So I had a lot to learn when I got here. But, in one case, cyber or cyber. So that's my strong point and that's what I can bring to the table here. But I was just, I've been fascinated by the med device space and have been learning a lot and learning how much I don't know about it as well.

Ed Gaudet: And tell us about the shared mission that's different in healthcare than it is probably in any other industry. I don't know if you've had the same thing in finance as we do in here.

Errol Weiss: Yeah, like, in terms of, like, information sharing and the level of collaboration that was happening across the banks, very robust, very good, lots of good information-sharing networks. During my time there, I learned a lot by participating in the information-sharing networks. I talk about, like, the benefits of info-sharing, thinking about how to protect your own organization, and learning about the latest attacks and things out there. But it's also, there's an aspect of personal growth to it as well. It's you can learn a lot by participating in those networks. But there's also the soft skills too, like learning how to, I'll say, behave during an incident, right?

Errol Weiss (cont'd): You see people under fire and how they're responding to that from a personal standpoint, and what that's like. And I'm watching some of these people thinking, My gosh, the world is burning around them, yet they're calm and collected. I hope I can be that way one day. And learning things like that. So really great robust environment. But when I got here four years ago, I'm going to say the spirit of information-sharing and the level of collaboration in the health sector is even better than what I saw happening in finance. So that's the good news.

Ed Gaudet: Any particular area where that's different?

Errol Weiss: I guess the issue a lot of people think about like information-sharing and why would competitors want to share and things of that sort. And I've been, again, in info-sharing for a long time and the old adage in the banking finance sector was that bad security for one bank is bad security for them all, right? If the public reads about an incident happening at a bank, it not only erodes the trust that that individual might have in that one banking institution, it really could question the whole network, really. And I think that that also serves us well here in the health sector, where I think that there's much more collaboration, even between the partners that's happening today, and that sense of wanting to, you know, ensure that the weakest link is protected is there as well. So I think people have that, that mindset that if I have the ability, I can share and help somebody be more secure, I'm going to do that because ultimately it impacts my own security.

Ed Gaudet: Yeah, that's a great point. What's interesting is you don't see many instances of ransomware attacks in finance. You see a lot of data breach, but you don't see a lot of ransomware. Why do you think it's different in healthcare?

Errol Weiss: I think that there's a few pieces to that story. I think one is, hey, I think we all would agree that the level of resource investment in cybersecurity and healthcare is not where it should be, that in the 1980s, 1990s, the emphasis was really being on HIPAA compliant and a lot of money was spent on being compliant. And compliance does not equal security. One of my favorite stories is when I was at NSA doing penetration testing. We just got done ripping a network apart.

Errol Weiss (cont'd): And during the outbreak, when we told them how bad things were, they said, How could that be possible? We just passed compliance last week! And I'm like, To explain to you the difference between compliance and security. So I think again, the resources aren't where they should be. So that's one part of it. And so, therefore, yeah, healthcare organizations are getting broken into, unfortunately. And they're not as well prepared to respond to a ransomware event as they should be. The other part of it that I really want to get out there too, is with Health-ISAC for the last three years, we've been collecting all the ransomware incidents that we can get our hands on. We've got 12,000 events in our database right now. Only 5% involve healthcare.

Ed Gaudet: Wow. No kidding.

Errol Weiss: So how about that? Now, if you read the newspaper every day, you wouldn't think that, right?

Ed Gaudet: Right. That's right. Yeah.

Errol Weiss: Every single one of these ransomware events seems to be impacting a hospital. We never read about ransomware elsewhere, but I will tell you that every single other, every other sector is being impacted by this. I'm watching the ransomware reports, so who's getting impacted by this. And it's everybody.

Ed Gaudet: Wow, that's incredible.

Errol Weiss: And I think we're reading about it, right, because when a hospital gets impacted, when patients have to be diverted to another hospital to receive emergency treatment, hey, that's big news. That affects me and you and our loved ones. And it's the last thing that I want to see happening when I need some urgent care, is that the hospital responsible.

Ed Gaudet: Ransomware is personal at that point. Yeah. No question. I'd like to unpack the, I love your comment about compliance doesn't equal security.

Errol Weiss: I'm getting in trouble for that. The compliance...

Ed Gaudet: No, but I think it's true. But I think more it's the education of why. So why is it different? And it really helps people think about the relationship of those two things and the perspective. Obviously we don't get ourselves in trouble. What are some of the things you could share with listeners?

Errol Weiss: Yeah, yeah. In all seriousness, it's, it's one of the pieces to the puzzle, right? There's certainly a strong element, strong reason to support compliance culture but I think the mindset on security, I think the way I would sum it up really just comes down to the way the environment has been implemented might not represent the way it was meant to be implemented. And that's where the security checks come in, where penetration testers are so successful is because somebody made a configuration mistake or somebody made a goof, or somebody hasn't applied a patch yet that has nothing to do with compliance, but yet leaves a gaping hole. And I think that's the part there. That's why you need that compliance culture. You need those, those checklists, let's say, to make sure that we've got everything set up the way it should be. And then, we also need that security mindset to go back and make sure that the way, that way it's been implemented in production matches up with our expectations.

Ed Gaudet: Yeah. Also think there's a temporal notion at work too, right, where as compliance tends to be a lot of work to get somewhere and then we wait, and, versus security, which tends to be much more of a real time effort. Any thoughts there?

Errol Weiss: No, I think that you're spot on there. And again, I would say that it's because of the dynamic nature of networks. Things are constantly changing. And then, of course, new vulnerabilities and threats are popping up all the time, right?

Ed Gaudet: Which is where H-ISAC comes into play, right?

Errol Weiss: Yeah, certainly. I mean, I think one of the ones that we're still dealing with today is, is the MOVEit vulnerability that happened a few months ago. And I know it took a lot of people by surprise who either had, didn't even know it was in their environment, or didn't realize what exposures can result if through that particular piece of software, if something went bad. And then of course, the other piece there too is the third-party impacts that happen to all these other third parties that they relied on were using MOVEit as well, and suddenly their data was at risk because of that, that product.

Ed Gaudet: Was there any analysis based on your data set that you've looked at where the factor of exposure based on third parties? So if had it inside, it was worse by a factor of four with my supply chain or... third parties.

Errol Weiss: Yeah, you know, good question. I don't know the answer to that. I do, like, we had a good chunk of our membership that was impacted by that.

Ed Gaudet: Yeah.

Errol Weiss: Yeah.

Ed Gaudet: What are some, so if we look at what you're doing with the H-ISAC, what are some of the strategic priorities for you over the next 12 to 24 months?

Errol Weiss: Besides, sort of, you know, continuously improving on our services in general across the board, really on the threat intelligence side, for example, some of the things that I'm really excited about are what we're going to be rolling out in the medical device security space here. Last year, we hired Phil Englert, who's a luminary in the medical device.

Ed Gaudet: Just talked to him today!

Errol Weiss: Awesome! He's in medical device security space and a welcome addition to the team. As I alluded to earlier, when I realized how much I didn't know about med devices and med device security, and I needed some help. With Phil coming on board, one of the things that we're working on is, is an SBOM repository. We want to be able to offer, essentially a centralized repository for med device manufacturers to provide us their SBOMs and a way for health delivery organizations, whether they're an H-ISAC member or not, to be able to get to that repository and to use it, as, I'd say, almost like a single source. So the whole idea is that singular hospital, who has hundreds of med device manufacturers and thousands of different products, not having to keep going to all these different websites to get the answers that they need. They could potentially just come to us, that singular repository. So we'll have more to say about that in a month but that's going to be definitely a big focus for us in 2024. Super excited about that. And then, like, the growth side, it's going to be expansion for us in Europe and then Asia Pacific as well. So this past year, we've, during this past year, we've hired another Threat Intel Analyst in Europe, one based in Brussels, and then a director of ISAC European operations who's based in Poland. And he's actually moving to Greece in the next few months, but really, to help with us in terms of representing Health-ISAC in Europe, working with our existing members, working with the European Union, European governments, Enisa, and others to really get the word out there about what Health-ISAC is doing and helping on the expansion there.

Ed Gaudet: Oh, that's terrific. Yeah, I'm looking forward to hearing more about that. Let me ask you, how do you think we're doing as an industry post-pandemic?

Errol Weiss: From a cybersecurity standpoint, I think, we've certainly learned plenty during the pandemic, and part of that is the issue with remote work, remote telework, cybersecurity professionals that many of whom, during the pandemic, were now working from home. I think that part of the post-Covid learnings here is going to be that dynamic of return to office, right? Even literally right now, we're hearing about places like Amazon and Google and others that want people to come back to the office. So we're going to see how that's going to work out. I mean, we know the shortage of talent that we see in this space. I think it's going to contribute to the dynamic of people, organizations are insistent upon people returning to the office.

Errol Weiss (cont'd): They may face some turnover because some other organizations might be more suited to remote work and encourage that kind of, of an environment. So, to play the favor. So we'll see how that all works out.

Ed Gaudet: Yeah. And you joined just before the pandemic, right?

Errol Weiss: I did, yeah, yeah. I've been ... remote work for a long time. So I'm very used to this.

Ed Gaudet: Getting good at this. So given that, that tough couple of years we've all had, we've all faced, what are you most proud of personally or professionally?

Errol Weiss: During that time frame, I think that it was certainly scary, right? We were hearing about all the cutbacks that were happening, and certainly risk of losing members as a result of financial stress caused throughout the healthcare sector, for example. When things started to slow down, I think we were also, from Health-ISAC's standpoint, we were pretty quick to recognize that was happening, that dynamic was happening, and we were able to, I'd say, really start tapping the brakes on some of the spending that we have planned, right? And so, we slowed down hiring, and then we really also immediately cut out some of the other expenses associated with regional events and conferences and things of that sort. So we were able to really maintain cost control over, over what we were doing from the Health-ISAC's standpoint. And we really, we weathered through it. I mean, we did great through it. We actually, we grew through that in terms of membership, and we were gaining members during that time frame. And so, it was pretty neat to see that happening. And I think we adapted to it pretty well. Most of us were already remote anyway during that time frame, but I think we were really on top of the game in terms of looking at what the dynamics were happening, what's the cybersecurity issues were at the time. Early days of Covid, we were doing a Friday afternoons, sort of, the social hours, but then also trying to really cater to an environment where we had discussions on what were some of the challenges that organizations were dealing with. We had plenty of companies that went from zero remote work to 100% overnight. Did they have a VPN set up? Do all those remote workers have company-issued laptops, for example? Are really going to remote in? Like, plenty of companies that were dealing with that in an order of days, had to solve that problem.

Errol Weiss (cont'd): And so being able to have those Friday afternoon conversation calls with our members and all the challenges like that and others that we just kept building upon, it was pretty neat.

Ed Gaudet: Yeah, that speaks volumes to the value for your service that providers find and your customers find. So it's a real testament to that. If you can weather a pandemic and come out stronger and better, actually, it's again, it speaks a lot about the value you're providing. Let's go back in time. Maybe, maybe ten years for you, right? What would you tell your 20-year-old self?

Errol Weiss: Is it ten years? That might be a little more than that.

Ed Gaudet: You're still doing the math. That's great.

Errol Weiss: Yeah. Stuck on that. So, I think, so the advice is, and this is great because that's the question you ask when you're giving this advice to anybody really, and I think, for me, it would be, find something that you like, something that you're passionate about. You know, you want to wake up in the morning and be excited to go to work. The old adage, If you love your job, whatever it is.

Ed Gaudet: It's not really a job, if you love it.

Errol Weiss: You never work, right? You never work. Something like that, yeah. That to me, is really important. I think there have been multiple times in my career where I'm sitting down at the desk thinking, I love what I'm doing. Now the secret is, How long can I ride this out before something comes and screws this up? So that's the big one. The other part is really, soak up the experiences along the way. Learn the things that you like to do, but on the flip side, as fast as possible, try to figure out the things that you don't like to do, get that over quick and move on. And I think it's even, if you're in, still in college right now, going to university, try to nail that intern job down. I think it's so important to do something like that. Of all things, between my junior and senior year, I interned at a nuclear power plant. Go figure. How did that apply to? I'm sure if I sat down here long enough, I could think about how that helped me in my career. And it was a great experience. But, obviously, I had nothing to do with cybersecurity at the time. But it taught me things I don't want to do.

Ed Gaudet: Yeah, you don't want to be doing that.

Errol Weiss: Yeah, I don't want to do that. So that's important. And then the third thing is on the mentor and coaches. So important. Get a mentor. Get a coach that you can help, use to constantly challenge yourself with. And the other trick I learned along the way is, if you can get a mentor/coach that's in your company, near you, maybe somebody a little senior to you in your position, that's good. Let's check that box. The second one is if you can also get another mentor who maybe, if you're a career person, you want to stay where you are forever, if you can find a coach or mentor that used to be at your company, so that person knows the ins and outs of your organization, all the bureaucracy, hierarchy, issues, and politics, let's say, that would be great also. But I definitely encourage that other, another, at least another person to be external to the company just so that you can get some fresh perspectives, not be so constrained about where you are there today.

Ed Gaudet: I love that.

Errol Weiss: And I think it's important because we're constantly learning. I still do it today. I meet with my coaches, my mentors, on a regular basis. Especially now, literally, I'm sitting here, I'm meeting with my team next week on an offsite to start talking about pen to paper on what our 2024 goals and objectives are. So I want, I want to stretch. I want to keep going, and I want to figure out how can we challenge all of our, all of us, the whole team and me? And this is part of the updates I'll do with my coaches in terms of what should I be doing? What's next? Right? How do I stretch myself and come up with some goals like that? So I think those are the big three for me.

Ed Gaudet: It's really good, really good. If you weren't doing this job, what are you most passionate about outside of, outside of the job?

Errol Weiss: So, so yeah. So outside the job. I'm living in Florida. I've been here just about ten years or so. And so, I really enjoy the chance to get outside, stay active. So every day, I would say, I'm on my bike, whether it's. I've got a road bike and I've got a hybrid bike that I do also. So, some days.

Ed Gaudet: Are you East Coast or West Coast?

Errol Weiss: I'm off the coast to Jacksonville. So East coast. Yeah. So I'm on the road a couple of days a week doing a road bike. And then the other few days a week I'm doing a path bike through woods over tree roots and rocks and stuff. And yeah, it gets exciting.

Ed Gaudet: Yeah. Be careful.

Errol Weiss: But, but, yes, sir. But it's, it's important to get out, stay active. It's a great way to, to kind of clear the head mentally and get some alone time, get away from all of this stuff because it's a little stressful some days. And so, it's important to get the me time in there. And that's part of it.

Ed Gaudet: Absolutely. No, you're so right. I've just embarked back on that journey of, in the bike riding and on an elliptical last week. So I'm trying to get back into it because, like you said, you're remote now and you're sort of you're chained to your desk and you get up maybe three, four times a day and, and then you're so worn out, you just go to bed, and I got to break that cycle. It's awful. This is the Risk Never Sleeps Podcast. So I have to ask you this question. What is the riskiest thing you've ever done?

Errol Weiss: I wish I had my great parachuting, rock climbing, cliff diving story, I don't. I.

Ed Gaudet: So many people start off with that, and then they tell me like, something completely crazy.

Errol Weiss: Yeah, but I'm not going to. I don't have anything like that. That's like in the physical, kinetic world. I think just the thing that's, it's so boring and so cliche, I feel like at this point. But I kind of alluded to it earlier. To me, the scariest thing I've done recently was this move to healthcare. I told you, I felt very comfortable in the finance sector. I knew a lot of people had a huge network there, and I'm thinking, What am I doing moving here? I don't know anybody.

Errol Weiss (cont'd): And again, back to the we all, I even knew coming here, right, that the cybersecurity resources weren't what they should be. So why am I doing this? What's, what am I hoping to gain by it? Little scary.

Ed Gaudet: What are the 4, 5 most stressful things in life, right? Job change? House, baby, right? Death. I mean that's a big, that's a big change. And oftentimes people will say that, just talked to Samantha Jacques today, and she brought up a very similar, yeah, her change in jobs and location. Quite frankly huge risk. Yeah.

Errol Weiss: I could be the other side of this too. Like, I had a similar experience or really earlier in my career when I was at NSA. I moved from the spy side of the House to the defensive side of the House, and that's where I started on penetration testing. And I was really questioning that move when I moved from one to the other, because, again, the resources, the amount of money that we spent on the spy side, as you guys can imagine, is huge. When I go to the defensive side, I'm walking down the hall, I'm looking at the carpets all worn out, the walls, they're all dirty. I'm thinking, What have I done?

Ed Gaudet: I bet you they're getting more investment these days.

Errol Weiss: I think so, isn't that right? There's a little, it wasn't pretty back then, literally, but it was one of the best moves I made.

Ed Gaudet: Cool. Any final thoughts or advice to folks that are maybe embarking on a journey into cyber or healthcare?

Errol Weiss: When I'm starting to use in my talks right now is when I ... the talk-up, in the beginning, what I'm going to say is, In the next hour that we're spending here together, 3604 PHI records will be breached. So what can you do to help us slow that down, stop that from happening? And those are real stats off the, the HHS OCR website from the past 13-plus years. Add them all up, divide by the number of days, and then come down to hours; that's what we get. It's crazy. So we've got to do something about, again, better protecting the entire healthcare sector.

Errol Weiss (cont'd): It's not just about breach records that I'm looking at here right now. It's everything that we've talked about here today. We've got to do a better job. We need more resources. We need more people, etc.

Ed Gaudet: So if you're thinking about joining, getting into cyber, or joining a company in healthcare, jump right in because we need the, we need the help, whether it's full-time or an intern even.

Errol Weiss: And there's plenty to do. And that's one of the things I love about the job. I get to pick the things I work on. Essentially, there's lots to do.

Ed Gaudet: Yeah, great. Errol, thanks so much for your time today. It's been a pleasure talking to you and getting to learn more about your background.

Errol Weiss: Same here. I really appreciate the time with you and looking forward to more collaboration.

Ed Gaudet: Yeah, you bet. And this is Ed Gaudet from the Risk Never Sleeps Podcast. If you're on the front lines of patient care and patient safety, 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