Podcast Transcript

Risk Never Sleeps
Episode 50
Aaron Weismann

Ed Gaudet: Welcome to the Risk Never Sleeps Podcast, in which we learn about the people that are on the front lines, delivering and protecting patient care. I'm Ed Gaudet, I'm the host of our program, and today I'm pleased to be joined by Aaron Weissman, the CISO of Main Line Health in Pennsylvania.

Aaron Weismann: Yeah. Thank you for having me.

Ed Gaudet: Yeah. You bet. Welcome to the show. And you've got a really interesting background, so let's just dive right into it. Tell us about your current role and a little bit about the health system.

Aaron Weismann: Yeah. So, in my current role I'm CISO for Health system in the suburbs of Pennsylvania. We're about 15,000 staff, five hospitals, a number of different ambulatory centers, again serving the population of the Main Line and New Jersey, Delaware, etc. I've been here for about three and a half years. Prior to that, I was the CSO over at Commonwealth of Massachusetts Executive Office of Health and Human Services, which was fun. I love that gig. It was great. And then, prior to that was an attorney.

Ed Gaudet: That's the interesting part of your background, the attorney.

Aaron Weismann: Yeah. It's not very common, but there are dozens of us, so.

Ed Gaudet: Oh yeah, but how does that uniquely set you up to be a CISO? Because you either come the technology path or maybe you come compliance. Very few of you come the attorney path.

Aaron Weismann: Yeah. No. And so I was one of two attorneys embedded with our IT department. Our CIO, gosh, over a decade ago, had asked for attorneys specifically dedicated to IT to help with a lot of contracting needs, compliance needs, privacy and security needs. So, I ended up being the attorney. I sat literally next door to our CISO and ended up consulting with him quite a bit, and then, over time, sort of became closer and closer to that part of it. And then we had some turnover in the space. And after a bit of a tumultuous staffing process, I finally just went to the CIO and said, hey, you're not going to do worse than me. Here's my three-year plan. Let's see if this works out for you. And true to form, I stayed for my three years, and then this opportunity here at Main Line Health came up, and I had to jump on it. My wife is from Philadelphia and wanted to be closer to her parents. It seemed like a match made in heaven. And three and a half years later, I can say it absolutely is.

Ed Gaudet: Now. Are you from Boston? Are you a Boston native or?

Aaron Weismann: I spent about a decade in Boston. I'm actually from Saint Louis and moved to Boston right after the legal market collapsed in 2008 - 2009. Oh yeah, which was great. I mean, just absolutely wonderful time to be an attorney. And I made my way into finance and then government healthcare, and the rest is history.

Ed Gaudet: Now, I saw you worked at State Street, I think, right?

Aaron Weismann: Yep.

Ed Gaudet: Yeah. In Boston or Quincy?

Aaron Weismann: Uh, Boston.

Ed Gaudet: Okay. Yeah. Excellent. My wife's first job was at State Street. Yeah.

Aaron Weismann: No. And the Quincy back offices are wonderful. I mean, it's a gigantic complex, as I'm sure you're well aware.

Ed Gaudet: Yeah, I think it was called the Frank Russell Fund. Is that ring a bell? Is that right? Did I get that right or I was just. The memory is such a fickle thing.

Aaron Weismann: Yeah, State Street has a ton of funds that they run. I think that's one of them. I don't know sort of where it sits as far as fund size.

Ed Gaudet: But were you there when Tom Quinn was there? Do you know Tom? Tom Quinn?

Aaron Weismann: Not. The name sounds familiar, but not off the top of my head.

Ed Gaudet: No, he was a CISO at Goldman Sachs, and then he went to State Street. Um, there for a while. Yeah.

Aaron Weismann: I wasn't really in with our technology department at State Street, so I was working on fund management from the legal side. So supporting that part of the business and didn't really interact with technology very much while I was there, unfortunately.

Ed Gaudet: Got it. So how did you get into healthcare in particular, given the background?

Aaron Weismann: I got into healthcare through technology, right? So, I was a technology attorney with Health and Human Services. Health and Human Services obviously does healthcare. It's an umbrella organization in Massachusetts over six different obviously health and human services groups. Right. The state Office of Medicaid MassHealth.

Aaron Weismann (cont'd): So a bit on the payer side there, Snap benefits and job placement through the Department of Transitional Assistance and then through our public health and mental health departments, got into the public health and mental health healthcare provision. Right? And what I really liked about that is all of our clinicians were pretty much there because they wanted to help the public and because they wanted to do really cool things with respect to public health. And I was sort of enamored with the work that they were doing from a legal and security side, wanted to try and support that as much as possible, and eventually, I mean, became so interested in it that I went to a health system. Yeah. And one of the things that drew me to Main Line health, actually, is their dedication to public health as well, and the dedication to the community and how involved they are with the community. So I really love that, and I really love the passion for the mission that creates. And everyone I've run into here is just incredibly passionate about the work.

Ed Gaudet: I love that about healthcare, that shared mission that you don't necessarily see in other industries, right? When you look at your next 12 months - 24 months, what are the top three priorities that you're focused on?

Aaron Weismann: I think it's probably the top three priorities everybody else is focused on, which is, you know, trying to get our heads around AI and large language models, generative learning models, etc., how we're going to manage that, how we're going to incorporate it into what we do. Network Microsegmentation is another big one. So trying to figure out for the devices on our network that we can patch that we aren't able to manage very well, how do we at least put them in their own sandbox so that they're not impacting other devices and sort of our production network at large, and then identity governance, really trying to get a lot more sophisticated about how we handle identity management, how we build roles, responsibilities, etc. within that.

Ed Gaudet: Those are top three priorities for most CISOs these days. When you think about the last couple of years, been tough for many people going through the pandemic, how do you think we're doing as an industry overall.

Aaron Weismann: As a security industry or healthcare industry?

Ed Gaudet: Healthcare.

Aaron Weismann: Yeah, I mean, I think healthcare's handling it very well. COVID was obviously very hard on hospital bottom lines. It was hard on our clinical staff from a technology standpoint. I think it was hard on technology teams because we went from, I don't want to say uniquely because a lot of organizations had an on-premises presence, but sort of this unique on-premises presence where we can't operate without our physical facilities, especially given that we're a health system with hospitals. Right? I mean, ambulatory, you could probably do telemedicine. Someone needs a gallbladder removed. You can't do that over telemedicine. Right? You must do that on-premise. Right? So we went from this very heavily focused practice for sort of this on-prem security and safeguards to this more distributed model, where we now have people reading remotely. We have people doing telemedicine; we have administrative staff working from home. And so we now have this very distributed environment, and that is completely new to healthcare in a lot of ways, where it isn't necessarily for other industries. So, one of the things we had to do was grapple very quickly with those new realities. I think we did a pretty good job as an organization. I know other organizations did a great job as well, and there's a lot to be learned from that, both from how are you going to operate as an IT and security team and also how are you going to contribute to patient safety and preserve patient dignity and prevent those breaches with, again without impacting the care that needs to happen on a day to day basis. So, lots of lessons learned there. But I think we've risen to the challenge and done pretty well as an organization.

Ed Gaudet: What are some of the things you change on the cybersecurity side to adapt to that?

Aaron Weismann: Yeah. So, one of the biggest changes was we had hardware-based EDR. So, we had EDR appliances and network closets. We got rid of those were entirely software-based EDR now because, really, the threats aren't going to happen just on premises. We now have computers everywhere. That that was one of the main changes how we've conceptualized of some of our other services. Again, shifting more to cloud services. So we're not operating physical facilities on-prem.

Aaron Weismann (cont'd): We have SaaS solutions that are communicating with our PCs and hopefully doing a lot of the processing, at least as vendors promise right off-prem to free up some of the capacity for our PCs, make that home use experience a lot easier, etc., so a lot of changes like that. And then obviously we have to think about, okay, how are we safeguarding our endpoints in an environment that is inherently insecure that we can't secure.

Ed Gaudet: The home?

Aaron Weismann: Yeah, exactly. Exactly. And I think some of those challenges are also going to come up in the home healthcare conversations that we're having, hospital at home, etc. A lot of the lessons learned from what we did with staff, we're now going to be able to apply to medical devices in the home as well, and hopefully support patient experience more robustly that eay.

Ed Gaudet: Sort of a benefit, if you will, of having to learn how to manage remotely. How about from a team perspective? I know there's not a lot of teams going into the office any longer. How do you manage the culture? How do you manage that? The team collaboration when folks are remote from a cyber perspective.

Aaron Weismann: My team could not be happier that they are working from home. Their perspective is everything we do is virtual and remote anyway. Like we're not actually, we're using a computer, but we're not actually physically interacting with any of our security infrastructure because we don't have any security infrastructure, all of its off-prem. So they're thrilled about that. As far as sort of promoting that team collegiality, the getting people to sort of actually think as a team on a monthly basis. We do bring folks in to sort of have a lunch and learn meeting where we check in as a team, talk about what we're doing, have a couple of presentations on topics, and we bring lunch as well. So we order from a local pizza place or local Italian place, something like that. And the team loves it.

Ed Gaudet: Are you still doing tabletop exercises physically in a physical setting or a live setting?

Aaron Weismann: Yeah, so we do that and we had a tabletop exercise recently for our IT department in a live setting. We're going to be doing an enterprise tabletop as a follow-up to that, some of the conversations is, hey, we would have done this on-prem. Do we, in fact, do this over teams or Zoom or something like that? Right? Where we bring a core group in person to have sort of the main conversation, and then everybody else is distributed, the idea being that our hospital command centers are all going to be remote. They're they're going to be in the hospitals. They're not going to be at our corporate offices, but our corporate folks are going to be at the corporate offices. So when we want a more closely simulate that, now we have that sort of distributed model as well. So, I think it'll be interesting to see how that works out. It's the first time we're doing it that way. But I think overall, it's going to provide a more realistic model of what's going on and what we're doing.

Ed Gaudet: That's a really great point where you do have that mixed mode of operation. Better to do it in what it would be like if, in fact, it was alive. A real exercise versus a tabletop? No, I think that's really good. So getting back to pandemic, tough year for a lot of folks. What are you most personally or professionally proud of over the last couple of years?

Aaron Weismann: I came in June of 2020, so I started the job like at the beginning of the pandemic, and I always half-heartedly joke with people if there's another pandemic. My lesson learned is do not move, right? Don't buy a new house, and move across states.

Ed Gaudet: Yeah, but you didn't know, I mean, right?

Aaron Weismann: No, there was no way to know. But terrible experience. But the thing I'm most proud of, other than sort of managing that move, is when I first came to Main Line Health, we had a relatively small security team, and like I said, we had a very on-prem mindset. Since then, we've been able to justify a pretty significant expansion in both security team and our infrastructure. My goal coming in was we're going to build a world-leading cybersecurity program. I think we're on track for that. I don't want to say, hey, like, we're the best, because I don't think anybody can really lay claim to that necessarily, other than maybe like the Microsoft's or the Amazons or the Googles of the world.

Aaron Weismann (cont'd): But I think with the resources we have and the strategy we've put together, we're doing a pretty fantastic job. And a lot of that strategy is developed by the team. It's not just me; it's not just my managers. It's everybody involved in figuring out the direction we're going to go in. I think we had a few unique opportunities that gave rise to that, but it also helped solidify the ownership, right, that everybody has over our security program because, in large part, they are the owners of it right there. Because of them, we were able to implement X, Y, and Z, for example. Right?

Ed Gaudet: Is security a rate limiter to AI adoption?

Aaron Weismann: We're taking a very forward perspective to that. So as long as it's HIPAA compliant, like we want to see it, we want AI in place. We're looking at generative models for threat detection and our own environment. We are very much encouraging the use of AI. Unfortunately, because of the data we use, we can't just say, hey, go over to ChatGPT and have it write a bunch of letters for your providers. Although we are an Epic shop and Epic is deploying their version of a large language model, and I think it's going to be fantastic as far as helping physicians take notes, helping them chart, helping them communicate with patients. I mean, I think it's just going to be a huge boon for them.

Ed Gaudet: Yeah, no, that's a great point. And, of course, it'll evolve quickly. Like AI has evolved quickly over the last 12 months. So outside of outside of your day job, what are you most passionate about?

Aaron Weismann: I have four young kids, a seven-year-old, a five-year-old, a four-year-old, and a two-year-old. So by default, I'm very passionate about them. I love all of them to death. I mean, they're absolutely wonderful, but outside of work, they're my entire life. Yeah.

Ed Gaudet: Those are great ages. I have three daughters. They're much older. But yeah, those are the formative years.

Aaron Weismann: Yeah. No, everybody keeps telling me, enjoy this while you can because you're gonna miss it. And as my kids age. Absolutely. It's just it's crazy.

Ed Gaudet: Yeah. You blink and you're looking at a 30-year-old. How did that happen? Wait, that would make me hold on.

Aaron Weismann: I'm not going to say it.

Ed Gaudet: I'm not. I'm still 18 in my head. What happened? Okay, I'm asking you for advice. What's going on? Speaking of 18-year-old, what if you go back in time, what would you tell your 20-year-old self?

Aaron Weismann: That's a really good question. I think I'd tell my 20 year old self, persevere, right? Life is challenging. Career paths are challenging. Not a whole lot of guidance in the space. Right? To your point, just I'm still asking questions like how do I do X? How do I get Y? Just be upbeat about it and persevere.

Ed Gaudet: I felt much smarter at 20 than I do now.

Aaron Weismann: Oh, 100%, yeah.

Ed Gaudet: But yeah, but the patience aspect is and persevere. And yeah, it's going to get easier. And yeah, those are really that's great insight. I have to ask you this question. This is the Risk Never Sleeps Podcast. What is the riskiest thing you've ever done, Aaron?

Aaron Weismann: I probably jump into cybersecurity.

Ed Gaudet: During a pandemic?

Aaron Weismann: Yeah, exactly. So I jumped into moving during a pandemic. But no, I jumped into cybersecurity full-time in 2017.

Aaron Weismann (cont'd): I sort of dabbled in it before then and helped cover between CISO transitions because of where I was. But one of the things they really ingrained in you in law school is if you decide to leave the law at any point, you're going to have a lot of difficulty getting back in. And it's the same for any profession. But law school, again, it's a special school for this. The teachers started to talk about, okay, the longer you're away from the law, the less facile you are with it, the less knowledgeable you are of current jurisprudence, etc., and you sort of lose your ability to practice. I find that to be sort of accurate. I still sort of keep a toe in contract negotiations and as part of our cybersecurity efforts, a lot of that is becoming legally driven now, a lot of really interesting upcoming regulations, a lot of really interesting regulations in existence. Now I dabble in it, but again, could I go back into the law full-time and do contract negotiation and transactional practice? No, there's no way. So I think at the time I had a really difficult decision. Do I go into this? Do I not go into this? And I really struggled with it the year before I went into it because there were some conversations about potentially doing that. I just had my first son and I wasn't prepared at all. The year after, I'm like, hey, maybe I could do this. So I took the jump. And honestly, it's the best decision I've ever made. I have a passion for technology and a passion for cybersecurity, and really, it's one of those cases where when you work in your passion, you're able to make it very fun, very successful, etc. That's not always the case, but it is absolutely the case for this for me.

Ed Gaudet: Absolutely agree with that. No, it's so true. I mean, you got to get up every morning. You better be passionate about it. Otherwise, it's hard enough to get up these days.

Aaron Weismann: Yeah, exactly.

Ed Gaudet: Any cultural interests? Music, Arts? Painting, poetry?

Aaron Weismann: I like art, I'm a terrible artist, but I like doing the art. A lot of digital artwork. I'm really getting into AI artwork, and I think it's just incredibly fascinating. I'd like to be better at it, but again, I'm not music. I used to play clarinet and flute. I have not kept up with that. But yeah, I mean just practically any kind of music. I absolutely love.

Ed Gaudet: Ian Anderson, Jethro Tull.

Aaron Weismann: Yeah. So actually, it's funny, my college roommate loved Jethro Tull, had Jethro Tull posters.

Ed Gaudet: Mine too. Mine too, by the way.

Aaron Weismann: It was awesome. So it's definitely one of those you really have to be of a certain mindset to like it.

Ed Gaudet: Acquired taste.

Aaron Weismann: Yeah, exactly.

Ed Gaudet: Yeah yeah. He's still they still play. They're still active. Yeah a couple of them I'm not sure if Ian Anderson is still alive, but I know that a couple of the bandmates still play. So actually my college roommates going this weekend I think to to a show in Connecticut.

Aaron Weismann: Oh, fantastic.

Ed Gaudet: Yeah. All right. Any last advice to folks that are either maybe moving from legal to cyber or starting off in cyber and just getting their bearings?

Aaron Weismann: Yeah. So my advice for legal practitioners who want to move into cyber is absolutely do it. I know a ton of people who've made the switch at not a ton like five, but five people who've made the switch. And they absolutely love it. I mean, they're but again, they're very passionate about technology. They're passionate about cybersecurity. And I think the legal degree helps. So if it's in your wheelhouse, I definitely recommend it. As far as new practitioners, I'd say learn as much as you possibly can, get certifications, learn new technologies. Really make sure that you're keeping up to date with current developments in cybersecurity because it's developing so, so quickly. It's so easy for your skills to get rusty. And if you don't have that educational component, you will get rusty and you will fall behind the times, right? So that would be my sort of advice.

Ed Gaudet: Okay. Excellent. We've been speaking with Aaron Weissman, the CISO at Main Line Health. Appreciate your insight for listeners today. A lot to unpack and think about there, especially if you're thinking about joining either healthcare or a cybersecurity team coming out of the legal profession. So thank you for that. This is Ed Gaudet from the Risk Never Sleeps Podcast. For those of you 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