Podcast Transcript

Risk Never Sleeps
Episode 84
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, the host of our program, and today I am pleased to be joined by Aaron Weismann, the Chief Information Security Officer at Main Line Health. Welcome, Aaron.

Aaron Weismann: Thank you so much for having me. I really appreciate it.

Ed Gaudet: Back again. So you couldn't get enough the first time. I'm sure a lot's changed since we last spoke.

Aaron Weismann: Yeah. It's crazy how much has changed and how much has stayed the same.

Ed Gaudet: We're gonna, I think we're gonna explore both sides. So let's just remind listeners your current role and a little bit about your organization.

Aaron Weismann: Yeah. So I'm the Chief Information Security Officer of Main Line Health. I'm responsible for enterprise information security. Anything touches our network, I'm responsible for securing it. We're a health system in the Philly suburbs. Five hospitals, five ambulatory sites, a number of different clinical practices across the greater Philadelphia area.

Ed Gaudet: Awesome. So maybe let's start with Change Healthcare in the debacle. How did you make out, what learnings can you share with listeners? What learnings do you think we got as an industry? What can we take away?

Aaron Weismann: Yeah, so we were incredibly lucky not to be severely impacted by Change Healthcare. I don't think there's a single health care organization that wasn't impacted by Change Healthcare. And a lot of the impacts weren't necessarily direct impacts. Some people use Change Healthcare as their clearinghouse, as a payment processor, as even their own revenue cycle. And I think those folks were very significantly impacted. Other folks used vendors that use change as a payment processor clearinghouse, what have you. I think it's definitely eye-opening for the industry to see how interconnected and interlinked things are. It was crazy to see sprawling impact of that across the board.

Ed Gaudet: The ability to collect millions of dollars a week that some of these health systems, hundreds of millions was a real deal, was a real impact. And I think you're right, the indication of their tendrils throughout the organization, I think, was the big aha, the big wake up call for folks.

Aaron Weismann: Yeah, absolutely. And I think ultimately I thought I saw numbers around the bottom line. But it's billions upon billions of dollars in at risk claims that are still being worked through, right, because they were down for the better part of two months. So, you know, I think that's going to be a long tail issue that people are dealing with. And we'll see what comes out of that.

Ed Gaudet: I'm interested to see it. Yeah. Now, obviously not directly affected, but did you take anything back into your program? Did you make any changes or adjustments to your process?

Aaron Weismann: Yeah. One of the conversations we're having internally is trying to figure out, Okay, if we have one of these major contagion events, right, an industry contagion event hitting us and we're impacted significantly by it, how are we going to operate effectively? How are we going to provide the patient care we need to do? How are we going to make sure our revenue cycle is up and running, etc.?

Aaron Weismann (cont'd): So a lot of conversations around that internally and a lot of thought where we have single points of failure, trying to figure out how we build redundancy around those. And there's only so much you can do. There are some players in the market that just are irreplaceable or there isn't a fallback to it. So we're really trying to be mindful of the business realities of the situation, but also try and build that resilience within our organization.

Ed Gaudet: Yeah, and build that hygiene. That's really good. And we'll get back to resilience in a second. Have you been following the Ascension incident as well? The breach?

Aaron Weismann: Yeah, I mean it's hard not to. They're the second biggest nonprofit health system in the US, right?

Ed Gaudet: Any takeaways, any learnings so far for listeners?

Aaron Weismann: There's a lot of conjecture and speculation. So based on conjecture and speculation it's: do normal hygiene things. Make sure you're protecting your endpoints appropriately. Make sure you have backups that you can rely on and bring into play quickly. Make sure your downtime drills. I saw an article yesterday about chaos in some of their hospitals. I don't think that's too far-fetched, right? I think when there is a large-scale ransomware attack like that, even if you have downtime drills, even if you drill on them, it is catastrophic. And that sort of plays out with patient care impacts, with inability to provide that care or patients are still coming through the door. So I definitely feel for those folks.

Ed Gaudet: Yeah, yeah, it's never fun. But what is fun is, gaming is fun. And the gamification of cybersecurity and cyber resiliency. I loved your post on that. And I love the game called Don't Roll the Dice. Is that what it's called?

Aaron Weismann: Yes. Yeah.

Ed Gaudet: And is that an actual game that Epic created or is it commercialized or?

Aaron Weismann: It's not commercialized. So Caitlin Bellrose, who's the disaster recovery expert over at Epic, sought to create this fun, gamified way of handling the incident response lifecycle. There had been a lot of requests for Epic to do that. This was the first foray into that, and I'm really proud that I got to participate. It was absolutely fantastic. I've joked that it's the pinnacle of my career, but honestly, it mixes two of my loves, right? Tabletop, role-playing games, and technology. By doing that, it created this thing that is not only approachable, but also is meaningful when it comes to mitigating threats along that response lifecycle.

Ed Gaudet: Yeah, I'm a former D&D player, so it looked a little like D&D. I saw some hit points, references to hit points and.

Aaron Weismann: Yeah, so it hospital points instead of hit points. Right? It was a little more collaborative. Yeah. No, it was cute. So what we were tracking throughout the entire incident was what are the impacts to reputation, what are the impacts to our revenue cycle, and then what are the impacts to our ability to maintain uptime throughout. It was really thoughtfully done and it was based off a d20 system, right? So it was literally rolling the dice to simulate these different pivot points. And when we have tabletop exercises, usually you'll walk through the pivot points and you'll say, Okay, we have an interjection here. What do you do? If we don't have the interjection, what do you do? And I think it was a much more entertaining and approachable way of handling that. And I'd love to be able to say that I'm going to incorporate that into the next set of incident response tabletops we have internally. I'm probably looking at calendar year 25 for that, but I thought it was just an absolutely inspired, it was fantastic.

Ed Gaudet: And what type of roles other than IT roles were participating? Were there any other?

Aaron Weismann: It was very heavily Epic-focused. So Epic is IT. And then you look at the chief medical information officer role as well.

Ed Gaudet: Okay. Good, good.

Aaron Weismann: Yeah. So they had CISO role, desktop tech role, someone who's on the Epic application side, and then CMIO for the organization. And I think from end-to-end, we really simulated the clinical impacts and the IT impacts. The focus again, was on that triage and recovery in the incident response life cycle, not necessarily the operational resilience on the hospital side, although I could definitely see expansion into that.

Ed Gaudet: Yeah. Now, did anyone invoke the cloak of invisibility when that went down?

Aaron Weismann: No, fortunately not. We, in practice sessions we talked about, Hey, if this were to happen, there are likely some roles that would be changed as a result of whatever's going on, given anecdotal evidence. But yeah, no, for the actual exercise, it was really, the equipment was different pieces of technology that one could use to recover. So solid EDR, having really good visibility for your environment, having good backups that are tested, stuff like that. The reinforcement and encouragement obviously being do all these really great industry-leading practices that are going to get you up and running as quickly as possible, you'll avoid the chaos of being down.

Ed Gaudet: Yeah, interesting. Let's talk about the strongest link in an organization. I hate this comment. I hate this label of weakest link for people because I think people are the strongest link. We just need exercise. We need to exercise that link to be strong. So what about the people and what about, how do we get people from doing things that cause more risk to an organization, like clicking on the link when they shouldn't click on the link?

Aaron Weismann: Yeah. So I think I like that you're putting it as the strongest link. I talk about our frontline staff as our strongest detection engine that we have. They are going to see impacts that the clinical environment before we will even see it with our tooling because they're able to do the associations of, Oh my gosh, this process has failed. It shouldn't fail. This is a technology issue. Let's call the help desk. But balance that against the fact that I think it's 85% or 90% of all ransomware attacks start with a phishing email. Right? So it's very successful to socially engineer your frontline staff and ultimately your organization suffers as a result.

Aaron Weismann (cont'd): I don't think you can train enough both for phishing email, for downtime processes, for how you handle business operations. I think that's one of the most critical non-financial investments, any security office, and I think it's critical to invest in people. I think we're at a point where social engineering attacks are the most successful point of entry. They're one of the three primary points of entry that everybody talks about and not covering that is borderline negligent in my opinion.

Ed Gaudet: Yeah, I agree, and I wonder if we should maybe shift our minds to how we think about it and move from training, which tends to be more educational. Right? It tends to be, people tend to process learning differently, right? Versus exercise, which is fairly consistent across, maybe the weights might be a little different, but the exercise is still pretty similar. Right? And I wonder if that notion of exercise and strengthening the link could help us in the long term. Because we were thinking about this today, we were talking about analogies. But how do we get people to build muscle around that detection and subsequent reaction to an attack. And I harkened back to when we were kids, and invariably you'd have the wise guy point to your shirt like you'd spilled something on your shirt, and then you get the fist of the face. So I was like, oh my God, that's it, that's the phishing reaction I have now. Whenever I get an email that I just stop and I'm like, Oh, I'm doing that same thing I would do if like someone pointed out.

Aaron Weismann: Well, I think it's important. That's a very visceral feeling, building the muscle memory around being able to do things and building the confidence around doing the when we drill things, when we do tabletops, the thing I like reinforcing with all the participants is you are all very smart people, right? You wouldn't be here working for our organization if you weren't. You wouldn't be nurses. You wouldn't be doctors. What we need to do is build your confidence in this area where you're not comfortable, and the area they're not comfortable is technology unavailability. So how do we get to a point where they have that comfort? And to your point, it becomes muscle memory, right? They just say, Okay, this is down, I moved to this, or I'm not able to do one thing, I must do another thing, right? And getting folks to that point and getting them to understand that, yes, there's a way to continue patient care operations without technology. And not only do we have the processes and documentation, but you can do it, biggest message we could possibly give to our staff.

Ed Gaudet: Yeah, to tabletop is the spinning classes, if you will, whereas training tends to be that passive. I turn on the training, I click a box, I answer a question, and I feel like I've accomplished something, when in fact maybe I really haven't. So I wonder if more people will be investing in tabletop exercises. And look, they have the word exercise in them. So it works.

Aaron Weismann: It does.

Ed Gaudet: All right. Cool. So yeah, I was really interested to talk to you about the gamification idea, because I think more and more people will be doing that. And it's inspired some additional thinking that I like to pursue. I think one of the things since we last spoke is the announcement of the HHS cybersecurity performance goals and the subsequent rulemaking process that's happening now. How are you thinking about that as part of your process?

Aaron Weismann: It's a compliance metric that we are going to have to meet. If I'm reading the tea leaves correctly, it's going to be mandatory for health systems across the board. I'm confident we meet all the objectives, but I want to make sure that we're actually evaluating that. And should we fall short in a space, I want to be able to meet that. I'm cautiously optimistic about the focus being placed in the space because I think it's pretty rational. I think the areas of focus are great. The flip side, I was an attorney for Massachusetts Medicaid during the deployment of the health insurance exchanges across the country, the EHR incentive payment program, etc. and those had rough starts, right? So I think this is probably going to have a similar rough start. And the more HHS can do to communicate about it, to develop an understanding of why they're doing it is going to be absolutely critical that that communication, it hasn't happened previously, and it really caught people off guard when there's an abrupt shift. And I think this is one of those places where there is going to be that abrupt shift, and the more preparation people can have, the better.

Ed Gaudet: Yeah. And that equity and inclusion is going to be very important too, because if we can't solve it at the rural level and at the critical access level doesn't really matter long term, right? We're still going to have that vector of attack that we'll have to deal with as an industry.

Aaron Weismann: Oh, 100%. And rural healthcare has a ton of challenges. Now, if you just keep heaping things on rural healthcare without providing assistance, it's untenable. You will lose rural healthcare.

Ed Gaudet: This is what's happening. People are going in business and, or they're merging with other organizations. The other thing that obviously is a lot of steam over the last couple of months is I obviously, how are you working within your organization to either evaluate it or adopt it? Have you built committees, any cross-functional committees, etc.? So I've heard a couple of different approaches to that. I'd love your thoughts.

Aaron Weismann: Yeah. We have a cross-functional committee including technology, clinical ops, legal, internal audit, compliance, privacy, etc.. Right? Everybody we want to include on here are the business use cases for AI. Here's how we're responsibly using patient data and here's how we're securing it. I think it's a good approach. We originally took a let's wait-and-see approach, which I also liked. I thought that was good. The use cases started trickling in and we had the conversations and that sort of guided where we'd go with the steering committee. I know a lot of organizations jumped right to let's create rules around it, let's create the steering committees. Let's go. And I think that's a great model, too. There's no judgment in the space. It's all new. And I think a lot of folks are applying preexisting ideas to how they're going to handle it. As long as you're handling it, I think you're in a good spot, right? If you're just ignoring it head in the sand. That's problematic long term.

Ed Gaudet: Yeah, because your users are ignoring it. Your leaders aren't ignoring it, they're actually using it. And do you feel like this will have an impact on your 2 or 3-year strategic objectives, your plans as you look out?

Aaron Weismann: No. When I think about they're all SaaS applications and we already have SaaS security. So the complexity is the model training and using data for model training. To the extent HIPAA already applies to that data, I don't know that there's anything that like, I don't want to treat it as a net new, we don't know how to handle AI because we know how to handle patient data. We know how to handle SaaS applications. We should be applying that to AI.

Aaron Weismann (cont'd): I think as that becomes more and more complex and more and more sophisticated over time, and as we start talking about generative AI as opposed to like large language models and truly generative AI, that is going to become a little more difficult to handle, because then assumptions are going to be made based on some level of intelligence that exists there, as opposed to just rote recall based on oh, reliability scores.

Ed Gaudet: Yeah. Okay. Yeah, yeah. And the ONC is also looking at creating some type of label for transparency. Have you been looked into that at all or?

Aaron Weismann: No. I think we're going to be consumers of AI largely. We're not really going to, there are a couple of use cases for developing internal AI engines, but by and large we're consuming SaaS applications. So my idea would be that it's incumbent on our vendors to tell us that and to let us know when they're leveraging AI. And by and large, they've been very open about that. And frankly, at this point, it's a marketing proposition. So nobody gets a foot in the door without AI or machine learning or what have you, right, regardless of what the thing is. I think everybody's being very open and transparent about it, where they're not necessarily being open and transparent is what's happening with the data on the back end, and how is that being either de-identified or isolated, etc., etc..

Ed Gaudet: How about existing vendors too? I often hear that folks are worried about existing third parties and product where they're updating or providing a patch, and that's introducing AI into the system where, you know, an SRE may have been completed a year ago. Have you thought about that as you roll out your process or as you think about AI long-term?

Aaron Weismann: Yeah, and we're having conversations with our vendors around that, but that does not hide the fact that they are developing AI infrastructure for how note-taking is handled, how some patient communications are handled, etc. I think they're all net benefits. And we've had to have conversations with Epic about, okay, what is the security around this? What are you doing to protect our patient data? How is this net new adding functionality that we're going to have to be concerned about. And we do security risk assessments on an annual basis. So we're going to capture a lot of all of that new stuff in the next annual review.

Aaron Weismann (cont'd): And that doesn't happen just all at once. It happens throughout the year. Right? So we're capturing vendors as we go through that, but we're also having really targeted conversations with vendors as they introduce AI into their platforms. What's the potential security impact? What's the potential patient data impact? How is this going to impact usability? Et cetera. Et cetera. And that's not just a security conversation that's across the board, which is why I think that committee approach that we are taking is ultimately where it's where we need to go. I'd say others need to go, but I don't know what other personnel architectures look like, if you will.

Ed Gaudet: Okay. Interesting. Yeah, that's that's a good, maybe that's what I'll talk about at my next customer advisory board meeting to get more of a broader view on that. And I'll let you know what I hear.

Aaron Weismann: Thank you. Yeah, that'd be fantastic.

Ed Gaudet: Yeah. Cool. Any other new things you're seeing that you think listeners would be interested in either from a process, resource perspective and or tooling perspective, whether it's commercial or free even?

Aaron Weismann: Yeah, I'm trying to think specifically most of what we're evaluating, again, AI. We're also looking into ways to harden our environment. So we're doing the tabletops. We're doing downtime drills. We're trying to figure out how we keep our environment working during a downtime. We're also looking at infrastructure to prevent downtime. So network microsegmentation is like the big buzzword now. And we're implementing that actively now. I think a lot of other organizations probably need to be looking at tooling around that, especially in health care, because my IoT and medical IoT environment dwarfed my, what I'd call traditional production environment of like PCs, servers, printers, etc. by tenfold, right? And I can't touch any of those devices because they're all FDA-certified. And if I touch them, I ruin the FDA certification and therefore can't use it with patients. So looking at ways to figure out how to collapse the network around those devices, in the event that we need to and figure out how to safeguard those devices more importantly, and keep them up and running is critical.

Ed Gaudet: Yeah. Do you run that as part of your program or is that part of biomed or?

Aaron Weismann: It's shared responsibility. So the actual infrastructure is being run by my program. But biomed, our networking team, our operations team, our clinical operations team are all in on the decision-making for policy development. Because if we do that in isolation, you're absolutely going to break something. That's right. I'm totally calm. The more input we get into it, it's an area where the more input the better.

Ed Gaudet: Excellent, excellent. All right. Any last-minute advice to people, folks that are graduating, coming out of school looking to break into health and or cyber or IT?

Aaron Weismann: You couldn't have picked a better time. And it's a fantastic industry to be in. I love every day coming to work, working in health care, cyber security, and IT. I think one of the challenges we have is we tend to compete with a lot of other organizations because security is fungible. We're doing the same security that a software development shop that a finance company is doing, etc.. I think the great thing about health care is you see the tangible impacts of your work on a daily basis. Your patients are safe. They're coming in and leaving the door. You're able to see the rev cycle impacts and you're able to continue that community promotion and promotion of health care across the board. I really enjoy that. I think it's a fantastic reason to be in health care, especially in the cyber security space, and would encourage more people to do.

Ed Gaudet: Excellent, excellent. Well thank you, Aaron. This is Ed Gaudet from the Risk Never Sleeps Podcast. And if you're on the front lines protecting patient safety and delivering patient 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