Podcast Transcript

Risk Never Sleeps
Episode 101
Adam Rosen

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 Adam Rosen, the Chief Information Security Officer at Roswell Park Comprehensive Cancer Center. Welcome, Adam. How are you today?

Adam Rosen: Thank you. I'm doing well.

Ed Gaudet: And I hear you're from Buffalo.

Adam Rosen: Yes.

Ed Gaudet: How's the weather?

Adam Rosen: Weather right now is good. A little cool. Don't ask me any questions about the bills, because I won't be able to say anything intelligent about it.

Ed Gaudet: How about the Sabres? You're a hockey fan?

Adam Rosen: No, pretty much the same position, ... I'll show up for games there from from time to time. Enjoy the stadium food, but that's about the extent of my sports participation.

Ed Gaudet: Okay, that sounds like me. So we'll probably get into what we did when we were kids.

Ed Gaudet (cont'd): Were you dad? Were you a Dungeons and Dragons player?

Adam Rosen: Yeah.

Ed Gaudet: Me too. Okay.

Adam Rosen: It's very much a go-sports ball.

Ed Gaudet: Yeah, exactly. All right. That was a little off the cuff, but we usually start with a little bit about you, your background, your current role, and your organization.

Adam Rosen: Sure. Currently, I am a Chief Information Security Officer at Roswell Park Comprehensive Cancer Center. We are an NCI-designated cancer center. And that means that aside from our patient care mission, as far as curing and treating cancer, we also have research areas and very heavy focus on cancer research and also on education. So those three define our mission as far as it relates to cancer. So we're very focused on that particular area of medicine. We were the first NCI-designated cancer center in the US, if my memory is serving me, and then as far as what got me here, before talking about too much about what I do. I've always been into computers. My father was a computer person, did sales, and I think the first computer we had in the house was a compucolor, which nobody ever has heard of. It seems like when I talk to people, but 3D, then we got an ... We moved up and then the very early IBM laptop, back when it was a big box with a small screen, and it got me into like basic programming and just fiddling and tinkering around. It was something I was always interested in. And so then, through high school and into college, the focus was computer science and engineering, and originally, it was going to be starting my own game studio. That was my original plan.

Ed Gaudet: That's cool.

Adam Rosen: And then went into grad school and started getting into security there, at least theoretically. I put to work as an independent study on a security project. that wasn't what I was expecting. It was really around user behavior analytics in the sun environment and analyzing and detecting unusual activity patterns.

Adam Rosen (cont'd): It was written, I think, in Java, which was not my language at that point that I was familiar with, especially with the GUI programming, and I spent two out of the three months of the semester tearing this apart, trying to understand how it worked because I couldn't figure it out. And it turned out all he did was UI stuff and it wasn't me. It was like I just figured I was missing something when I was tearing it apart. So, that was my first security project that didn't really pan out the way it did. But from after grad school, I went to the Naval Undersea Warfare Center island and did some ATM networking, but also did some work with on firewalls with an allied submarine program there, started getting more into security and monitoring in that role. And I was there for about three years and then we moved back to Buffalo. At that point, I started my own IT consulting company because I figured it's easy, just hang my shingle, and it was a lot harder than that. But I had a set of clients, and just naturally, my focus started becoming more on just the basic security of small business security, antivirus, backup recovery, disaster resiliency setup, early cloud backup to my own data center kind of environment, and then turned one of my clients that was a small healthcare provider became my they were becoming my larger clients, and they ended up just becoming my full-time job, and I had shut down the shop that I had started. And I was doing everything there, the only IT guy, so, soup to nuts, VMware design and resiliency, and sand configuration, but focusing more and more on the security side, I was just getting more interested in the HIPAA compliance, and it was just given the different projects. That's where I'm willing to spend my time. And so, after a certain amount of time there, I decided to seek out just a security-focused role. And I came here as a security engineer under the previous CISO, who was the first CISO here. That escalated quicker than anticipated. I was there for about six months, and she came and decided that I was going to be her succession plan for when she left 2 or 3 years down the road, and she wanted to start getting me up to speed and on some of those operations. She left eight months later, so a little faster than planned, and then just it was a leap, but one that was, I liked the challenge that took me into the role. And for a while, I was doing double duty. I was doing my old duties on it, but the new stuff with that has mostly settled down over the intervening years.

Ed Gaudet: Interesting, interesting.

Adam Rosen: So that's what brought me into this world. And it's been challenging. It's been interesting. It's joining a community that is in healthcare security, and it's been an experience where you have a lot of people to lean on and good people to commiserate with. When you're sharing your challenges that everybody shares, it's a role I've been enjoying most days.

Adam Rosen (cont'd): And then, as far as how what we're doing here, I don't think it's too much different than you see in most healthcare organizations, except it can be a little more challenging because we have the academic and we have the research, and we have the clinical all in that same environment. Serving different masters can provide some of its own challenges, balancing and enabling the researchers to be flexible and access the services they need while making sure that the PHI is secure, the environment is secure, because patient care is number one.

Ed Gaudet: And this is like an IRB research function. Interesting. And how were you working that into your overall security process? Because obviously I'm assuming you're exchanging data. Yeah, the parties that are involved in the research, how are you managing that process?

Adam Rosen: We interface with legal and privacy teams. We work to make sure that wherever we're giving our data, it's third-party vetting to make sure that they're following the appropriate controls and that we have the assurance that high level of assurance that our data is going to be kept secure, contracts are in place, ... liability, cyber insurance, but I've always taken the stance of, those are good things to have, they help mitigate the overall impact. But from a patient privacy perspective, regardless of how much you're going to be reimbursed for it, the records are just as brief if you haven't protected the privacy. We focus a lot on that due diligence and looking at the architecture for exchanges, a lot of which have been standardized at this point through various platforms, which kind of makes things a little bit easier. We don't have to keep reviewing everything as its own entity.

Ed Gaudet: And are you an Epic shop or?

Adam Rosen: No, we are not.

Ed Gaudet: Okay. And when you look out over the next 12, 24 months, what are some of the top priorities on your plate?

Adam Rosen: Number one has really been that I'm trying to change the way we communicate and involve the business. One of the, especially when I first started the job, I would talk about risk in very technical terms, about what's on our risk register, about not having a hole in our DLP or configuration that wasn't secure, but that just goes over the heads leadership and then supportively nod their heads and expect me to take care of it and do our best.

Adam Rosen (cont'd): What I've been focusing on in the past six months, and this is an evolving process, is really working with the business. So, first of all, risk is the intersection of impact and likelihood. So, my line of thinking has been my team is proficient in determining the likelihood of something happening, but we're not the best at determining the impact, right, and where it's scale, the scale is. So, instead of us doing a thumb in the air, where do we think it falls on that matrix? We've been bringing in the business very heavily. So, like privacy, compliance, and legal. You tell me what level of number of records is a medium impact, catastrophic impact, etc., so that we're all talking the same language when we come back with risk, and then we're following better governance because we're creating tolerances about where we need review when the risk level hits a certain threshold. And we're doing that with financial, you tell me what the dollar values are for each of these different criteria. Catastrophic essentially being something that jeopardizes our ability to operate, and we're doing it with intellectual property and reputation, which has been more challenging to follow. And also, with clinical impact, right from a senior executive level, looking at you, tell us if this particular system meets the criteria that an outage would be a catastrophic impact. Obviously, the EHR qualifies as that.

Ed Gaudet: Sure.

Adam Rosen: That lets us talk more about the risk on a, on an equal footing because we've gotten that buy-in and everybody is aware of what we mean when something is a medium risk or a medium-high risk, etc. The other part of what we're doing is that I've been really focusing on is really talking to senior leaders and executives about the high-level business risks instead of the technical risks, and we've revamped our risk register to take, I think we've got about 40 business risks like loss of clinical availability due to ransomware, breach of privacy due to ransomware, or external attack, or in general breach of privacy due to internal threat. Loss of the data center because of fire or flood, right? Environmental risks and everything. And then we're taking our risk register, and we're tying each of those technical findings to one or more of those business risks and then mapping that out on a risk matrix to the, what do we feel the risk of all of these business issues are that they care most about. And then we can talk about the technical things we're doing to address them. For example, loss of PHI to a third-party breach change healthcare or, you know, Blackbaud a few years ago.

Ed Gaudet: Yeah.

Adam Rosen: That's up in the high dark red because you look at a five-year period, which is how we look at it; it's pretty much guaranteed to happen. And the impact, as defined by the business of the loss of that number of records, is a high impact. When we talk about that being high up in the upper right corner, they understand that, and it's not an arbitrary decision on my part. And then we can say, okay, well can we need to reduce that if and and same thing with ransomware. And then what we're doing is then we're taking the various information security projects that we're working on now or proposing for the near future, and we map that. So you can actually see in the dashboards that we built this project touches these risks that are distributed hopefully usually in the high-risk areas, because those are the ones you need to address. Giving them that feedback and that hopefully clear understanding of what we're trying to do on an annual basis with our projects.

Ed Gaudet: Got it. And where does the adoption of AI fit within your priorities and your scope today?

Adam Rosen: It's something we're actively working. We're trying to create best practices around how to use it, and not just from a cyber perspective, but from a data quality perspective, a bias perspective. Copyright and the legal aspects of it. And how do we manage that? How do we make it effective and enabling for the business? As we've sampled certain AI technologies that are more consumer-focused? We're looking at it in clinical areas about how it can improve physician productivity and patient experience. But all of these work from the security side. We're creating our standard expectations around it. A lot of these things, especially when it's cloud-based or SaaS-based, so much of it is just the same due diligence you would usually do.

Ed Gaudet: Right.

Adam Rosen: But then it's what do you go above and beyond with when it's okay. How are you taking prompt data and integrating that into what can be returned, and making sure that access control is properly, is respected when you're returning data? And then, when we're talking about internal internally developed projects, what are our expectations there? And, ideally, I'd like to say to make sure that your model is not subject to to model poisoning attacks, but we're not quite at the point where we even know. What does that mean in an AI world that we can be providing them the guidance as to what you have to do to an AI model to make it resilient to that?

Ed Gaudet: Yeah, that learning curve. And how are you handling governance? Are you have you set up a governance process committee policy yet?

Adam Rosen: Yeah, almost. It's almost, we've had some other stuff in place and checkpoints and conversations, but we're working on getting that last piece of formality in, right? Yeah, a lot of folks are on that journey today.

Ed Gaudet: So, when you think about your current job and what you do, what would you be doing if you weren't doing this role? What are you most passionate?

Adam Rosen: I go back to that game programming that I, that was my original dream. I found out during one of my projects in grad school I am horrible at 3D modeling and animation. So I probably would have I would have hired out a chunk of it, but I missed some of the programming days from my earlier experiences. That was always very rewarding to face a puzzle and get to work it through to completion and see the finished product, which is harder in security because you've never done it. ... We do wrap particular projects, but when I look at the big picture of what I'm trying to accomplish, it's, there's the next thing and the next thing.

Ed Gaudet: Yeah, interesting. What games did you play? I assume you're a child of the 80s or.

Adam Rosen: Yes.

Ed Gaudet: Yeah, yeah. So, what were your favorite video games?

Adam Rosen: Going back to Nintendo, I think Zelda 2 was one of my favorites. Moving into like high school and early college, I worked at an internet cafe. So this was before everybody had computers. Games were not networked for internet connectivity yet. Shim in place for those. So my friends and I, we'd get together at night after the cafe closed and we'd go. We'd play Duke Nukem, Descent, and just kill some hours doing those while I'm running back and forth, getting people sodas and coffees and various snacks, and keeping the register going for my boss. So he was always willing to let it go for that.

Ed Gaudet: I love the game. I don't know if you remember Tempest.

Adam Rosen: Yep, yep.

Ed Gaudet: And Defender. Remember Defender?

Adam Rosen: Tempest was that one where you go around the circle.

Ed Gaudet: Yeah, yeah, yeah, yeah, yeah, yeah. They'd start they start from the bottom and come up, and yeah.

Adam Rosen: I think that was the first vector graphics.

Ed Gaudet: Yeah, that's right. Yeah, and Defender, the spaceship. And I would just go ...

Adam Rosen: I remember some. Yeah, I think I know which one you're talking about.

Ed Gaudet: And then the first one where it was animation, Dragon Slayer, I think it was called.

Adam Rosen: Oh yeah.

Ed Gaudet: Dragon Slayer. ... was my other, one of my other favorites in the Deadly Discs.

Adam Rosen: Oh, yeah.

Ed Gaudet: An arcade. Nice.

Adam Rosen: I wasn't good at it, but I like it.

Ed Gaudet: Nice. Yeah, we talked about D&D earlier. Were you multi-class?

Adam Rosen: No, I was always, I was typically the wizard.

Ed Gaudet: The wizard?

Adam Rosen: I spent way too much time on my prop spellbook that had for my one character that was going through the campaign, and I had all the pages, and I burnt the edges so it looked like I had been thrown in a fire. It was just nerd-tastic.

Ed Gaudet: Those are the good old days.

Ed Gaudet (cont’d): Yeah, so if you could go back in time, what would you tell your 20-year-old self?

Adam Rosen: I think the easy stuff is hard, and the hard stuff is hard, too. But so much is, from the technical perspective, and I faced this early on when I first started in this role, and we needed to do a much wider MFA deployment than we, that we had at the time. And from a technical perspective, it's you flip a switch, you put everybody in the right Active Directory group, and you're done. Or maybe you're nice about it, and you send people instructions on how to enroll.

Ed Gaudet: Yeah, until the uprising.

Adam Rosen: Yeah. So it's going into these things saying, yeah, technically it's easy, but it's culture change. Yeah, it's again, we're heavy research. And so the researchers are saying we don't deal with PHI. It's mouse data. Why do we have to? Yeah, but you're on, you're in our email system business compromise. You're on our network getting that buy-in throughout the organization was a bit of a culture change for some of the key players. Making sure that again, you just from that technical perspective, you're that from that engineering background I have. I just was so used to just being in control of it. You turn it on and make it work and you make it work as easy as possible, and it's smooth sailing from there. But when you're dealing with that large organization with people at different skill levels, you got to make sure that the supporting infrastructure is there, right? Like the service desk understands how they have to support and handle calls that are going to come in, and what's the rate of enrollment before you're overwhelming the system and the people that are supporting you? Yeah, it's just, it was that early mindset that it's just flip the switch and you're done.

Ed Gaudet: Mhm, yeah, it's great. Hardest lesson in your career.

Adam Rosen: Just like the fragility of the ecosystem. When you look at Change and look at CrowdStrike it's not coming from where you expect it. We're defending our borders and our perimeter and our applications. And you look at Kronos a few years ago, you're aware of the impact of third party and supply chain, but Kronos didn't affect the entire healthcare ecosystem the way Change Healthcare did and was focused on that one industry. And then CrowdStrike, the tool that you have to prevent outages, is the tool that created the outage. And you just start having to look at everything with a different lens and start weighing the risk of bringing on this new tool.

Adam Rosen (cont'd): We evaluated the other endpoint, two agents that we have on the system, from a security perspective, and could they do that? How are we rolling them out, and staging upgrades are we doing? The best way. And so we made some changes there. It's just how fragile the system, the entire environment can be.

Ed Gaudet: Yeah, that was amazing to see, the CrowdStrike debacle, because you would, one would expect, after so many years of rolling out client software and having the scars, that we would have still been faced with an outage of that scale of magnitude.

Adam Rosen: But when you're doing your evaluation for software, how many people are asking if it's operating at ring zero and then bringing in? They're not.

Ed Gaudet: Nobody is. No, they will now, but, yeah. Or what are your, how do you roll out upgrades, right? Big bang? Do you stagger them like, how are you?

Adam Rosen: We were n minus one, right, with the sensor. We were n minus one. So we figured we're covered because we're looking at that piece of it, not, same thing with when semantic or whatever your endpoint agent of choice was before. We never questioned the impact of that definition you could have.

Ed Gaudet: That's right. That's right. All right. I've got to ask this question. This is the Risk Never Sleeps Podcast. What's the riskiest thing you've ever done, Adam?

Adam Rosen: And the problem with that one is I'm so tame.

Ed Gaudet: I don't believe it. Everyone says that. And then I hear these stories, and I go, wait, that's pretty risky.

Adam Rosen: Okay, I don't know if this qualifies as risky. I'll tell it anyways. Getting drunk on stage during a play and then taking a bow and almost falling off stage.

Ed Gaudet: I think that's just stupid.

Adam Rosen: Behind it. He made me do it.

Ed Gaudet: Okay, who made you do it?

Adam Rosen: The stage crew.

Ed Gaudet: Oh, they did. Oh, were you part of the theater group or?

Adam Rosen: Yeah, I was part of a theater.

Ed Gaudet: Oh, awesome.

Adam Rosen: We were doing a series of one-act plays.

Ed Gaudet: Oh, cool.

Adam Rosen: One that I was in, it starts off with me and my father sitting at, like, a kitchen table, sharing a bottle of wine, talking about my relationship problems with my wife. And then halfway through, the lights go down on us, and it's dim. You can still. And we would pantomime talking. And then the scene moves over to my wife and my mother talking, her side having the same type of conversation. So the last night of the show, we go to drink our wine, and it's actual wine. They gave us a bottle of wine.

Ed Gaudet: Oh!

Adam Rosen: And so the lights come down. They're like, we're in the middle of the scene, and we realize, and we got to hide it. But as soon as the lights come down, I say to my partner on that, we're finishing this bottle. So we're just downing a glass after glass because we've only got a few minutes while the other half of the scene.

Ed Gaudet: Oh, no.

Adam Rosen: Downing this. And I thought it was fine. And we were the last of, I think we were the last one, so right after that, it was curtain calls, and that almost did not go well.

Ed Gaudet: Almost a little bit of a mosh pit stage dive. Nice. Nice.

Ed Gaudet (cont’d): That's pretty risky, I guess, not so much stupid. Well, yeah. I'm glad you told the story.

Adam Rosen: Best I got. I'm sorry.

Ed Gaudet: No. Never. No Whitewater rafting. You worked on a nuke sub, right? Didn't you work in a warfare?

Adam Rosen: Didn't get to go out. I went on a couple subs for configuration. I almost had to get flown out to one that was at sea and having technical issues.

Ed Gaudet: They must airlift you, right? Drop you down, yeah?

Adam Rosen: Yeah.

Ed Gaudet: That's pretty risky.

Adam Rosen: But I did, but in the end, I didn't have to do it. They fixed the problem, but it would have been interesting. But at the same time, like if they had to dive, I'm cut off for weeks.

Ed Gaudet: Yeah, you're in a sub. Pretty risky.

Adam Rosen: It didn't pan out, so I don't have any good stories.

Ed Gaudet: Well, that's pretty funny. That's good. All right. What, I asked this, I'll ask you this question. You probably are steeped in the finer parts of culture, music, and movies. What are your, let's see, desert island top five records or movies you'd bring with you?

Adam Rosen: Can I bring books?

Ed Gaudet: You can bring books. Sure, yeah.

Adam Rosen: All right. Ender's Game.

Ed Gaudet: Oh, okay. Now you're talking my language.

Adam Rosen: Zen and the Art of Motorcycle.

Ed Gaudet: Oh, Robert Pirsig. Beautiful. I'd bring The Matrix. Oh, how about Cryptonomicon?

Adam Rosen: That one, I don't know.

Ed Gaudet: Oh, that's, oh! Neal Stephenson, you have to read that.

Adam Rosen: Okay.

Ed Gaudet: That you're a cyber guy, and.

Adam Rosen: I know. Yeah, I know The Cuckoo's Nest. Cuckoo's Egg.

Ed Gaudet: Oh, no. This is fantastic. This is one of the. Yeah, it's a historical novel. So, if you like historical novels, they bring in these three time periods together, and it's all about cryptography.

Adam Rosen: All right.

Ed Gaudet: I mean, it's great. It's big, but it's a good book.

Adam Rosen: Okay.

Ed Gaudet: It'll keep you busy. Yeah, let me know what you think.

Adam Rosen: Okay.

Ed Gaudet: Awesome. So, no music?

Adam Rosen: Oh, I'm, Margaritaville, the Jimmy Buffett best of, but Ocean by John Butler. I don't know if you know that one.

Ed Gaudet: I don't.

Adam Rosen: That's my Zen. That's my amp-up music.

Ed Gaudet: Oh, okay. I'll check it out, John Butler.

Adam Rosen: Yeah, yeah.

Ed Gaudet: Nice.

Adam Rosen:... is the song.

Ed Gaudet: Okay, cool. Any advice, last question. Any advice to folks coming out of school? They want to break into cyber. They want to break into healthcare.

Adam Rosen: Dabble in a lot of things. Some of this is my bias, I think, coming from that general technologist perspective, right? Where I've done programming, I've done Active Directory administration, I've done networking to a certain level, VMware administration, including site recovery and replication. All of those have contributed in some way to the, my contribution to security. Even the stuff that I'm not good at anymore or haven't kept up with. Just understanding the jargon, understanding the ecosystem, understanding some of those big picture challenges that the infrastructure people are dealing with on a daily basis. That, I think, has value. I think having that broad understanding and not just I've done pen-testing and coming through, just having done those kinds of tasks, but not understanding how it's going to interact with Active Directory or the other aspects. I think that broad view is very valuable.

Ed Gaudet: Yeah, I love that.

Adam Rosen: Harder to get nowadays.

Ed Gaudet: Yeah, it is. Yeah, I love that, though. It's, be a multi-class technical infrastructure and cybersecurity.

Adam Rosen: Yeah. No, it definitely comes in handy. You didn't use to have people that graduated cybersecurity, did IT, and then you specialized. And I understand why we're moving away from that model because there's so much that's necessary. Even if you don't have that as part of your formal training, go to the lab play.

Ed Gaudet: Yeah, yeah, yeah, yeah. And that third dimension is, that you brought it up earlier is, understand the business and understand how to communicate to the business, yeah, which is great. All right. That's a great way to end, Adam. Thank you very much. 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.

Ed Gaudet: Thanks for listening to Risk Never Sleeps. For the show notes, resources, and more information in how to transform the protection of patient safety, visit us at Censinet.com. That's C E N S I N E T.com. I'm your host, Ed Gaudet, and until next time, stay vigilant because Risk Never Sleeps.

CENSINET®

Censinet RiskOps™ Demo Request

Do you want to revolutionize the way your healthcare organization manages third-party and enterprise risk while also saving time, money, and increasing data security? It's time for RiskOps.

SCHEDULE DEMO

www.Censinet.com