Podcast Transcript

Risk Never Sleeps
Episode 83
Rebecca Kennis

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 Rebecca Kennies, the Chief Information Security Officer at Arnot Health. Welcome. Let's start off by telling our listeners about your current role in your organization.

Rebecca Kennis: Thank you for having me. I appreciate the opportunity. So I am the CISO at Arnot Health. And Arnot Health is a, I want to say, small to medium-sized organization, health system in the Elmira, New York area. We are made up of three hospitals with a total bed count of right around 451, outpatient medical practices of various specialties. We have skilled nursing facilities and a graduate medical education program. My role at Arnot is really to try to protect the organization from cybersecurity risks and other information security risks through physical security as well as cybersecurity.

Ed Gaudet: And you've been busy, I'm sure, the last couple of weeks to say the least.

Rebecca Kennis: It's the only time, if you're referring to any of the change, healthcare, and all of that. We luckily were minimally impacted. Yeah, we're one of the few.

Ed Gaudet: Oh, that's great.

Rebecca Kennis: Yeah. We were not directly impacted. We did not. We don't have any contracts directly with Change Healthcare. Some of our third parties change a little bit downstream, but not a whole lot.

Ed Gaudet: Any learnings or anything you could share with listeners as to maybe why you weren't impacted? Was it much more?

Rebecca Kennis: Was, yeah, it was more not really luck, but just that we had a different vendor that we use.

Ed Gaudet: I see.

Rebecca Kennis: Yeah. So, unfortunately, I would like to take credit for that. But you know that one's not on me.

Ed Gaudet: Did the incident cause you to pause and maybe take a look at your current approach and maybe do anything differently than you've been doing?

Rebecca Kennis: Absolutely. Any time you see any kind of security incident like that, it always makes you pause, go, and look at your own practices and say, okay, is this something that we could be impacted by? And I won't say that we weren't at all impacted. You know, we still had to go through and verify that. We have contracts with them because they have a number of different services that they provide and the tools that they have. And we didn't have one contract with them, but it was not for anything that exchanged PHI or anything like that. But yeah, one thing that we did take away from this was really looking at our vendor management processes and our contract management. You want to make sure that it's easy to identify, do we have a contract with this vendor that is having this issue and be able to identify that quickly? Because if you do, then you want to make sure that you're going to cut off all ties to them so that nothing is going to impact your organization directly. And then what happens operationally beyond that as well? We did have an incident command center to make sure that there weren't any operational impacts and all of that, but that was relatively quickly determined that there were not any incidents for that.

Ed Gaudet: I imagine that must have brought in a lot of other functions: legal compliance, audit, contracting, and supply chain.

Rebecca Kennis: Yeah, absolutely. Absolutely. Yeah, the entire organization gets involved with that. You want to make sure that from a financial perspective, from a clinical perspective, from the technical perspective, and obviously from a compliance legal perspective as well.

Ed Gaudet: Have you been just changing topics here? Have you been following the HHS cybersecurity performance goals that were announced last year and that are going through the rule-making process now?

Rebecca Kennis: And yeah, keeping a close eye on that, and it's very similar, I would say, to what New York State is looking to do as well for our hospitals. There are a lot more regulations that are coming down the pipe, which some I think are good and some are probably challenging. I think a lot of it is in the way that it gets implemented. It's not necessarily bad to have a low bar, let me say what you should be doing. The challenge then becomes when you have, you know, small to mid-sized organizations; finances are always a challenge. I don't know of any health system or organization that is looking to spend money or has extra that they're looking to do it for. Hospitals really want to make sure that they're doing the right thing. Unfortunately, a lot of times, it comes down to what we do for clinical care versus what we are doing for IT and other types of things. So there are a lot of those decisions that need to be made, and it is not always the first thing that gets looked at because we want to make sure that you're able to treat the patients. Part of my job is to help leadership understand that you're not looking to implement it for the sake of IT, but we're looking to implement IT. Upgrades are required to maintain security and the infrastructure and maintain the availability of patients' charts and other things so that they can continue to treat their patients without having to give any second thought to any of their IT tools.

Ed Gaudet: Yeah. That's great. Really pulling in the business requirements and the business processes. And I noticed you had a background in clinical from some of the earlier jobs you had as an analyst.

Ed Gaudet (cont'd): And I was wondering, any insight you've learned over the years? And for those folks that are in security and trying to maybe establish that relationship with a physician or clinical leadership, any tips or techniques that you'd suggest?

Rebecca Kennis: Well, I worked in healthcare for 30-plus years. I'm not a clinician. I was never a clinician. But you learn to understand clinicians the more that you are around them. I worked very closely with one of the health systems that I worked with, with the physician specifically, and you really need to be able to meet them where they are. And you want to make sure that whenever you're implementing whatever security controls you're implementing, present the least friction for them as possible, because their end goal is they want to be able to treat their patients. They don't want to have to care about it. My concern is their concern is not. Immediately, whether the data is going to be breached or obviously they don't want that. Their immediate concern is I need to treat this patient. And in certain cases, it's literally life and death. You know, you want to make sure that you're not presenting obstacles in the way. So whenever there are things that they want to do or need to do. And your first instinct might be like, let's not do that. You don't want to just come right out and say, no, you can't do that. It needs to be a conversation. What is it that you want to do? Let's see if we can come up with a better solution than that one. That will work for both of us.

Ed Gaudet: Yeah. That's great. That's great. So, as you think about the next 12 to 24 months, what are some of the top priorities that you're currently managing?

Rebecca Kennis: You know, our top priorities right now are third-party management. We're looking to lock that down a little bit more, getting some better processes in place and ensuring that we are trying to take it. I guess beyond just giving the vendors an assessment to fill out because of course, they're all going to fill out. Yeah, we're doing great. Nobody would have ever imagined that the healthcare of this huge organization would have these issues. But the thing is that every organization has the potential to have issues if in the right circumstances. So that then leads us to the people. So we're looking to ensure that our training and awareness programs are strong. We've got monthly phishing campaigns that go out to our staff. We're doing monthly small fund short training for everybody, so they're trying to keep it to eight minutes or less.

Rebecca Kennies (cont'd): We don't want to make it anything that is a major, major project for them to have to do. But we also don't want to do it once a year. Most organizations do the training for them when they join the organization. The training is once a year with all the mandatories. And I guarantee nobody remembers anything after they finish it because they're checking that box. They need to finish it. You want to make sure that this is up front, like for most in their minds, of what you're trying to get across to them. And really what you're trying to get across to them is to be cautious when they're receiving emails, when they're getting phone calls, when they're seeing somebody come in to try to get into a security area, all of that stuff to make them stop, think, and pause. Because the bad guys work off of emotion, they're trying to pull on your emotions, trying to get you to react without thinking about it. So you want to give people the tools, give them that comfort level to know, all right, I'm just going to stop and think about this for a minute. Give them those signs that they're looking for. Is it urgent? Is it unexpected? Is there a link to click on or something to download in there, or are they asking for sensitive information that they really shouldn't be? To give you that situational awareness to look at and question for that? So that's another big component of what we're doing. And the third component is along the same lines with the vendors. All of that is one of the reasons that an organization gets vulnerable because there are constant vulnerabilities that are being discovered. Whenever you have an upgrade, there are more opportunities for there to be a bug in there and make a whole new one.

Ed Gaudet: Vulnerability.

Rebecca Kennis: Coming through. You need to ensure those vulnerabilities are being mitigated in a reasonable time frame. You want to make sure that, particularly anything critical, anything that's currently being taken advantage of out in the wild, those holes are being plugged as soon as you can. And there are challenges with that always because whenever you're upgrading or whatever you're doing, sometimes you have to take down a server, and you have particularly healthcare.

Ed Gaudet: You're right.

Rebecca Kennis: You get the the areas that are like, we can't have any downtime, right? It's like, okay, I understand that, but either we have a small downtime now, or we're going to have a huge downtime at some point in the future because either the system is going permanent.

Ed Gaudet: Permanent downtime.

Rebecca Kennis: Right? It's going to crash, or we're going to end up with, you know, we're not going to be able to take care of these vulnerabilities, and we're going to end up with some breach, ransomware, or something. Rather, that's what I have to say.

Ed Gaudet: Yeah, no, that's a great point you get to. And I love that notion of continual training, too. That's reinforced because you're right; that one-and-done or that annual training isn't enough these days. We have to create that culture of vigilance, if you will.

Rebecca Kennis: And that's exactly it. What I'm really trying to do is build up that culture of security, to make it more of the norm that the staff are going to be thinking about. And taking into consideration, is this really a good idea because you put controls in place? People can find ways to get around them. But you want to make it so that they have an understanding of why these controls are being put into place. We're not here just to make your job more challenging. We want to make things better and easier for you. You don't want to make it more challenging. So they need to understand that big why of why are we doing it. Once a person understands the why, the what can follow. But until then, they're not going to get it.

Ed Gaudet: Yeah. It always makes sense to start with the why. Where does AI fit into all of this? You hadn't mentioned that. And I'm just wondering how you are managing that.

Rebecca Kennis: Yeah. So AI is one of those things. It's it's the big buzzword now. There are definitely a lot of good use cases for AI. We are right now still evaluating what we want to do. And, of course, AI means different things. It has been around for years. It's just most end users didn't recognize it because we built it into it.

Ed Gaudet: It was deterministic; it was rule-based.

Rebecca Kennis: But now with the new ChatGPT and all of the other generative AI, that's where it's becoming much more available to just anybody. And we've had a lot of not a lot. We've had some requests to allow the use of some of the generative AI for documentation, charts, and that sort of thing. We started with the policy, and we created the policy. And one of the big things with the policy is that we need to make sure that first, we're going to not harm. First, we need to make sure that one is a good source of generative AI. Is it reliable? Is what it's going to produce going to be accurate? So you want to make sure first of all, especially if it's going to be something that's going to be impacting a patient's chart, that you're going to have accurate information going into it. And second thing, is it secure? You know you have to obviously worry about privacy. Where is this data going to be going to? Do we have an account with them? Can we have a business associate agreement with them? Can we do an evaluation of how they are treating this data? But it's starting with the clinical leadership and having them evaluate it and say, is this something that we want to do in this circumstance? So before IT, before security even looks at it, we're saying, okay, here's the CMO signed off on this. As the medical director, your area signed off on this. Are they approving this? And then once we get that approval, okay, we'll look at this. But what we do want to do is get to a point where we're going to have more of a standardized approach to it so that if they agree that they want to have a generative AI documentation tool, this is the version. This is what we're going to be using. We're not going to be doing that 1Z2Z, hey, I saw this because number its a lot of excess work. It's a lot of excess risk. And on the security standpoint as well as the output. So you want to ensure that all of that is valid and good.

Ed Gaudet: Many folks I talked to have created these governance structures and committees. Have you done that as well?

Rebecca Kennis: Specifically for AI? No, we're not at the point yet where we have an AI governance structure, but we have the policy that says it needs to first go through the clinical or business area. And then from there, we have a privacy committee, a compliance committee, and an ethics committee.

Ed Gaudet: The committee states that.

Rebecca Kennis: So, at this point, we don't have one overall AI committee, but it's going through a number of other hurdles.

Ed Gaudet: I like that. It seems more streamlined, quite frankly.

Rebecca Kennis: Yeah, I think so. Why make another committee?

Ed Gaudet: Right, exactly. I think it took everyone by surprise, and they didn't know how to deal with them. We had to create a committee and cross-functional. And that's certainly one way to do it. But your approach is very streamlined and treats it more like just another technology that's come into the full.

Rebecca Kennis: Exactly, exactly,

Ed Gaudet: I love that. What keeps you up at night? Obviously, it's a lot like anything in particular.

Rebecca Kennis: What doesn't keep me up at night? No, honestly, I sleep like a rock because I do have a great team. Yeah, but I don't sleep like a rock because I'm not worried about anything, but because I do a lot of worrying during the day. You know what? It's always the unknown. You can put in, put together your fortress. You can. I like to use the analogy of a castle with a moat and with an armed guard. The armed guards out there in their armored suits of armor, and all of that. You have all of your firewalls, you have all of your MFA, and you have all of the other technical tools that you're using, your sins and your sores and all of that. We can do all of that. Make sure that all of our vulnerabilities are good, but it literally takes one person to click having an off day that clicks on a link. That's where it's also it's so important to build that culture of security so that if somebody does click on it and then they realize that, oh my gosh, I probably should not have clicked on that, that they're not going to be afraid to let us know that they're not going to say, well, let's just pretend like that didn't happen and nobody will find out. We were constantly encouraging them. Let us know as soon as possible. We can try to mitigate any issues that happen.

Rebecca Kennies (cont'd): You're not going to get in trouble for making this mistake. I promise you won't. If we find out later that you did this and tried to hide it, No promises on that. But you want to make sure that there's that trust that. That they can trust us, that we're going to be acting in good faith for the organization, what's best for the organization, and not be punitive about it.

Ed Gaudet: Yeah, yeah. That's great. I don't think I asked you this question, but how did you get into healthcare?

Rebecca Kennis: How did I get into healthcare? I got into healthcare backward, let's say that. So my undergrad was in mechanical engineering. I graduated at a time when there were a lot of layoffs. I did not have a job right out of college. I got a job working on the lab system at our local health system, and it grew from there. I went in there thinking, this is a temporary job while I'm still looking for my real job. And opportunities presented themselves. And I came to love it. I came to love working with clinicians. I came to work and loved working with teams and just doing like the moon landing on the janitor, saying that I helped to put the man on the moon. I'm doing that as well. Implementing EMRs ensures that things are safe and secure. Here I am pretty closely, years later, and still there.

Ed Gaudet: Yeah. Now, that's a great story. And I think, probably that background coming out of me. We had that curiosity too. So that really enabled you to get into IT pretty seamlessly.

Rebecca Kennis: Yeah absolutely.

Ed Gaudet: That's great. Outside of healthcare and IT, what are you most passionate about? What would you be doing if you weren't doing this job?

Rebecca Kennis: Oh, my family. I'm very passionate about my family. I am also an avid Buffalo Bills fan. Yes, my husband and I went to the year that we went there. The year that Jim Kelly became a card-carrying member of the Bills Mafia then.

Ed Gaudet: That's great. My favorite poet was, I think taught there, Robert Creeley. Oh, does that name ring a bell? In the University of Buffalo, maybe.

Rebecca Kennis: Yeah.

Ed Gaudet: Yeah, cool. So, family, any hobbies, or anything that you do outside of this day?

Rebecca Kennis: Honestly, I love a good book when I want to turn my mind off from everything that's going on in real life and just fall into a good book and read. Honestly, this time of year, it's not quite there yet, and I'm itching for it, but I love to just float in my pool.

Ed Gaudet: Yeah. There you go. Me too, with a book, I'll bring my Kindle in there too. And my wife's like, don't drop the Kindle in the pool.

Rebecca Kennis: Even better.

Ed Gaudet: Yes, exactly. That's great. If you go back in time, what would you tell your 20-year-old self?

Rebecca Kennis: And I would tell my 20-year-old self to just roll with it. Everything's going to be okay. I've always been a little bit of a worrier. I guess that helps a little bit in my current role, but it sure doesn't hurt. Yeah, and always a bit of a perfectionist. So I think I would tell my 20-year-old self that, you know what? Everything's gonna be okay. You're going to do great things and just be patient.

Ed Gaudet: Excellent. I have to ask you this question, though, since it's the Risk Never Sleeps Podcast. What's the riskiest thing you've ever done?

Rebecca Kennis: It probably will not surprise you to know that I do not have a high tolerance for risk. I've never really been a very risky person.

Rebecca Kennies (cont'd): I think probably the biggest risks that I've taken were just the leaps of faith into new roles and sometimes going in and saying, am I really ready for this? Am I leaving this role in this organization? The things that I know moving into a new organization, a new position, and new responsibilities. We're just taking that leap of, yeah, I can handle this. So that's probably as risky as I'm going to get.

Ed Gaudet: That's pretty risky, though. You're constantly driving yourself to embrace your dread. Like, embracing the newness of something that you really don't know or understand. That's a huge risk. I love that answer. All right, I think I have some time. I'll ask you a couple more questions. So you're on a desert island. You could bring five albums, CDs or five movies with you. What would they be? That doesn't have to be five.

Rebecca Kennis: Yeah. Okay. So movies, I'm going to say just about any Adam Sandler movie. I can watch them.

Ed Gaudet: Didn't see that coming.

Rebecca Kennis: Yeah, that's like my husband and I are.

Ed Gaudet: That's great.

Rebecca Kennis: Adam Sandler fans have to love that. Just stupid humor. Some of them. There are a couple of them that I probably wouldn't, but most just about any other Adam Sandler movie. I can watch The Wedding Singer over and over.

Ed Gaudet: Great soundtrack, too. Wedding Singer.

Rebecca Kennis: Yes. And honestly, I was going to say that would be one of the movies that I would bring to as a wedding singer. Yeah, the 80s music.

Ed Gaudet: Yeah, I love it. Yeah, yeah.

Rebecca Kennis: Also Queen. I bring Queen music.

Ed Gaudet: Which deal is the album? the night at the opera or the one with Bohemian Rhapsody?

Rebecca Kennis: If I would have to choose one. I would probably have to choose one of their greatest hits because there are so many good ones. Which one? Is one of those double albums that I can get the most of them into?

Ed Gaudet: Love it. You're thinking about the island.

Rebecca Kennis: I would go with that. And then just to throw things up a little, I would probably bring, trying to think which one, I'd do some Broadway. Go to Broadway shows probably Come From Away. Is probably one of my favorite albums on that.

Ed Gaudet: No? Okay, check that one out.

Rebecca Kennis: I'm a little bit of everything.

Ed Gaudet: Nice I like it, I like it. Last question. What advice would you have for professionals who want to break into healthcare, IT, or cyber? What advice would you give them towards that profession?

Rebecca Kennis: So my advice is to just do it. If you're interested in cyber, take a class. Take a look online for some tutorials or something like that. And it doesn't have to be only on the technical side. So information security covers obviously the cyber realm, like with all of the technical pieces and tracking the codes, the ash, and all of that, it's also making sure that you have understood and recovered the requirements, the governance, the risk management, and the compliance. You have to know some of the language there. You have to be able to speak that language. You're interested. Just do it. Talk to somebody, take a class. Just do it. Don't feel like you can't. You can't do it because you haven't been immersed in servers networks and firewalls for all of your life. Honestly, my background is not on the technical side.

Rebecca Kennies (cont'd): My background is in the operations. On the application side. I came into information security from the background from there as well. And you learn as you go. And if you want to learn, just do it.

Ed Gaudet: I love that advice. We have a customer that uses their third-party risk management program to onboard newly graduated students into risk management, and that gives them this purview of all of the business aspects of cybersecurity, as well as the technical aspects. They basically will do a stint for a year, and then they get to pick where they go next. And a lot of folks are moving. Yeah. So I love this idea of getting, like you said, to go as an analyst. Go in as an assessor, learn, you can learn a lot from that perspective, and then decide where you want to go from there.

Rebecca Kennis: Oh, right. Exactly.

Ed Gaudet: Yeah. Love that. All right. Thank you. Rebecca, this is Ed Gaudet from the Risk Never Sleeps Podcast. And if you're on the front lines protecting patient safety and care delivery, 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