Podcast Transcript

Risk Never Sleeps
Episode 34
Matt Modica

Ed Gaudet: Welcome to the Risk Never Sleeps Podcast, in which we discuss and explore the individuals that are protecting patient safety and delivering patient care. Today, I am pleased to be joined by Matt Modica, CISO at BJC HealthCare. So, Matt, welcome to the program. Excited for you to join us today. Our listeners are excited. You got a really interesting background. So we're going to dive into that in a little bit. And then I think we got some funds in store for later on too to explore, if we've got some time here to do when you're not protecting patient safety and patient data at BJC. So tell us about your current role in your organization.

Matt Modica: And as you mentioned, I'm the CISO for BJC Healthcare, it's Midwest, a regional healthcare system, provider system in Midwest Saint Louis metro region primarily, but Missouri, Illinois kind of go mid-state, middle of the state in Missouri to the middle of the state in Illinois, if you think about that from a region, perspective. Size and scale on the perspective, so we have 14 hospitals, we have over 200 clinics and acute care facilities, we have 32,000 employees, and when you take into account all of the, all of the external physicians and folks that need access to our systems, we're usually about 50,000 users that we're dealing with on a day to day basis. Bed count for in-patient beds, so we're sitting here at about 3500 beds across these 14 hospitals. So yeah, large provider system. I've been with BJC now for just over six years and have been steadily building and sustaining the program.

Ed Gaudet: Excellent, excellent. And how did you get into healthcare and IT?

Matt Modica: I'll start a little bit with my origin story, right? So I really wanted to be a graphic designer or an architect. Like, I wanted to do one of those two.

Ed Gaudet: It's very cool.

Matt Modica: And how I got here was very meandered into this career. Long story short, basically went to college for that, graduated from college, was at my wedding reception and my, and I didn't have a job yet. And my wife's cousin says, You know what, he worked for Edward Jones at the time, and he said, and he was recruiter for them for technology, IT, and he said, I know you want to get into graphic design. There's this really cool IT job I think you'd be great at. And long story short, was able to get that job. My thought process was I was going to move into Marketing or Communications as soon as I could after I got in, but I got into it and it was essentially a business analyst role in IT. And I moved into Project Management, did Project Management work for many years, and then got into security kind of focus toward my, toward the end of my stint there at Edward Jones for, for about ten years, I guess. Got into leading a security team of project managers and architects, right? So it was all about selection of technology, implementing technology, implementing change, that kind of stuff. And so it fit well with my project management love and skill that I've learned to love. And then also that's really when I started getting into security. It's pretty cool. And then, you know, for a little bit. So worked there and then went to Express Scripts for about eight, nine years, worked in a variety of security roles there, started with certification and accreditation for federal clients and vendor, vendor management, client security, identity and access management, really dug into risk management and some of the more proactive technology stuff that we do in security in that role. And then I moved to Equifax and I worked for Equifax for about four years, and with them really came in as their BISO, Business Information Security Officer for, for the Saint Louis Market and Saint Louis Company, based company that they had. And eventually we grew my responsibilities there to where I was responsible for all of the business globally before I left, reporting directly to the CSO and. And then, was able to get this job back in my hometown and focused in area I wanted to wanted to focus on. So yeah. Kind of meandered about. Again, how do I, how do I get from graphic design to security and then ultimately to a CISO position? That's, that's kind of a wild story, but it's been a fun ride so far.

Ed Gaudet: And how has some of that experience in that background, especially in information risk management, helped prepare you for the BJC role?

Matt Modica: So it all built upon itself. I mean, so it was one of, as I was talking with my wife about it, and actually, earlier today, I was just like, How did I get from there to here? And I think luck was some, but I think skill is another piece of it where I just constantly, I'm constantly learning, right? I'm constantly pushing myself to learn and understand more things. So as I think about it, it's really those core skills from a business analyst and project management perspective. On the business analyst front, knowing your business, knowing your audience, understanding how you make money or why you do it, or why you're providing the service you're providing, right? And having that tie to the mission and objective of your organization. That was key from a business analyst.

Ed Gaudet: So important.

Matt Modica: Yeah. And then the project management component. Okay, get stuff done on time, on budget, on schedule, in the right amount of energy and all that stuff put into it. And then from a security perspective, again, just the love of learning and constantly pushing myself. So I've never been the super technology expert. I definitely dabble, I definitely understand kind of, kind of perform the sniff test that I need to, but my real strengths have been really, how do I organize? How do I motivate, how do I, how do I deliver on what the organizations need that I support ultimately? So it's I think that and a lot of leadership training, a lot of people that put their faith in to do the right thing, and then, and ultimately trust me to to try to do a job, right?

Ed Gaudet: Really great background of core building blocks obviously, that puts you in a great position at BJC. Talk about the difference in the shared mission that you have in healthcare that maybe you hadn't seen in other organizations.

Matt Modica: Yeah, that's great. So we, what really drew me to BJC is the fact that the Senior Executives really walk the talk. It's a mission-based organization. It's a nonprofit organization. So it's not all about revenue and money, although that's important because we need that to provide the services we do.

Matt Modica (cont'd): But it's really, truly how do we help the communities in which we serve? How do we get people the best outcomes that they can get, from a healthcare perspective? How do we educate the community? How do we help with social disparities? How do, really just how do we serve ultimately? And that is huge from my background and my beliefs, right? Is my, my kind of core, three core values as I look for any organization for me is faith, family and fun, right? And so, I need to have something that I'm going to have fun at. I need to have something where I'm going to have good family-work-life balance. I do believe in God and I believe in faith. And so those things, when they all match, is great. What makes it even better, from a healthcare perspective, what's exciting about that is you have organizations like BJC that allow you to be your full self, warts and all, and they recognize that and that's okay, and they embrace it. So the diversity component in making sure that we're, again, we're just allowing people to reach their full potential and do what they do best in the way they can do it best.

Ed Gaudet: I love that. Like, being authentic is so important these days. And and being able to bring your first, the first right version of yourself versus that second rate version of somebody else to work and I love that. What are your top three priorities or strategic initiatives over the next year or two?

Matt Modica: So I would say I'm going to kind of go, maybe go back to a boring statement of zero trust, right? It's identity data and, and really identity and data and endpoint would be the three components, right? And probably we're doing really good. Identity, we are continuing to work on that, right? How do we make sure we understand all of the users that are supposed to be in the environment, why they're supposed to be there, or what role they're in, what job function they play? And continuing to push that principle of least privilege. So we've done a lot of work in the last five, six years around automating access management, around getting things more efficient, making making sure that we're doing things for our employee population. Our focus now is the non-employee population, right? And how do we make sure, we know for sure who the third party is that needs access and what they're doing on our system when they're doing, when they're in there in the, and they're doing that. So that's a, really everything around that identity understanding, what they're doing, the behavioral components, monitoring components, those kinds of things.

Matt Modica (cont'd): Data loss prevention would be another one, right? And focusing on where are all the data repositories and making sure that we have the crown jewels understood and the best we can. Not that we don't know what those are today, but validating it, making sure minimizing the amount of exports and things that, the amount of really the data that has to transfer back and forth. Healthcare, at least in my experience, there's a lot of older practices. We still use fax machines a lot. And it's not just us. It's all of the industry. And so it's just thinking about solutions of, How can we get to maybe a different and more secure approach for that? How do we support that with some of the technologies and some of the things that we have in place? And with the data warehouse stuff that we're doing and a lot of the stuff we're doing from, just from a data management perspective. We have a very good data, data and analytics team that has been stood up and is working on the things. How do you, how do we leverage those investments in a secure way? You have security by design ultimately along the way there. Yeah, that's really the third thing to talk about endpointbut I think we have that pretty well covered for Zero Trust. The biggest thing that I'm focused on right now is risk management. In making sure that the organization that we, that I am reporting the right information to the management team at the organization to say, Here's the quantified level of security risk that we have, right? Here is what we could do to buy down the risk, right? Here are the potential impacts and drawbacks of doing that. And ultimately presenting it as a business decision and working through that with my peers across the organization to help them understand that story and what we can do. Because I go back to, again, the last five years, it's been building the program, strengthening the program, getting the basics and the fundamentals. And so we have all of the things that we have, need to have in place there. Now, it's a matter of we're never going to be able to fix 100% of everything. What are those most important things that we need to fix and should fix? And do we agree? Is that on that as a management team?

Ed Gaudet: Yeah, that alignment is so critical. Absolutely. Congratulations on the FBI CISO Academy. That's terrific. Tell us more about what that means to you and what your experience was going through that.

Matt Modica: I've always been a strong supporter of our law enforcement from local and federal. They are truly heroes, right?

Matt Modica (cont'd): And I think participating in this, for those listeners that don't know what it is, the FBI CISO Academy or CISO Academy is, it's a select group of CISOs that are selected, and they have to be nominated and recommended by their local field office, their local FBI field office. And so it's a really, all about public private relationship, you know, how do we build and strengthen that and support each other in the shared mission of protecting our country, protecting our services, protecting our critical infrastructure across the United States? And how do we bring consequences to those that are that are trying, have too much fun with our organization, with the country? And so yeah, it was a really great program. It's a, it's about a week in length and I will compliment the FBI Cyber Division on what they have done. They've put together an incredible program where, you know, for the week where, we were cleared certain clearances so we could get some additional briefings that aren't necessarily public, which was very insightful to help us understand just how much effort and energy goes into the things that they're doing to ultimately protect us and ultimately help bring people to justice at the end of the day. And so, it was very insightful from that perspective, very helpful to build those relationships even stronger, to have agents that have been behind, as example, the crackpot takedown and some of those other things to speak directly to us and talk about, Hey, here's how long it really took us to get there. Here are the things that we did to, to ultimately get behind the scenes and get behind who is behind all of this. And then here's what we did to take down in this day of action that occurred. And you can read some of the information about that takedown out there on the, on the public news. So there's. Yeah, it was just, it was incredible. It was great. And building the contacts and building the connections to fellow CISOs and to, again to the FBI and other agencies. So they actually brought in their equivalent from Canada, their Canada cyber folks come and join this session. They had Department of Justice contacts. They had CISA contacts, NSA folks come and present. So it was really the whole of government kind of coming together to say, Here's how we're trying to fight against that.

Ed Gaudet: You probably got to see some, with the clearance, you probably got to see some real details around the whether or not there was a compromise and any indication of compromise on a more broader scale. Is that accurate or?

Matt Modica: Yeah, we received several briefings right on just the state of critical infrastructure, right? So if you think about power or you think about utility, you think about, or just general utilities, you think about any other critical infrastructure, healthcare, they did help articulate, Hey, here's reality, here's what we think, here's what we think we're dealing with, and here's where you need to be focused. Very good to have that bidirectional communication. A lot of times people will say, Gosh, my experience with the FBI is, it's a one-way street. And I can understand that but you have to be understanding that there are some things that are national security that they just can't share. And they're working every day with their law enforcement partners and other partners across the government to make that faster and to get that actionable information back. But a lot of times we have laws and we have privacy for a reason in this country. So they're working through all those things in the right way, but they're ultimately trying to get things in our hands faster.

Ed Gaudet: I definitely see that. The last couple of years have been tough with the pandemic. How do you think we're doing as an industry based on conversations with peers or what you're seeing in general?

Matt Modica: Yeah, I can say probably two aspects, right? If I think about it from a pure cyber perspective, right, the threat landscape, for the most part, overnight dramatically increased, right? Especially in healthcare, it wasn't typically a lot of folks with remote work from home, working in altering locations, right? And overnight that changed. So we, at BJC's case, we had about 4500 people literally in one week, we're told, Okay, you're working from home and here. Oh, by the way, here's new tools Microsoft 365 that you're going to use to do that. And here's the guidelines and the guardrails that you should use when you're working with documents and all that kind of stuff. So that was a shock when we went through that. And I think we've got to a more normal. So we've figured out how do we do those things securely? How do we enable the workforce to do what they need to when they're in a location? And where are those situations where we say, You know what, we're just not going to allow remote work because it's just too dangerous or too risky for whatever reason. So we've kind of, kind of that teeter-totter of efficiency versus security. We've kind of, we've been tottering for a while on that. I think it's not as dramatic of a shift, but many more is kind of this, it's always that back and forth, right? So we're just kind of leaning here in there on our risk posture and what we're doing around it.

Ed Gaudet: Yeah, certainly it keeps it interesting with the ebbs and flows, given any given Sunday, any given week, right? Any given, any given day. What are you most proud of this last couple of years, personally and professionally again, given the pandemic and given everything we've had to do?

Matt Modica: The most proud of, I guess what I'm most proud of is really the team I have been able to, or that we have been able to create. Behind every good program there's people that make it real and partners that make it real. I think we've done good job over the last, again, five years, really focusing on what are those fundamentals we have to have in place? What are those key capabilities? Who are the right resources that can help us get there? And who are the right partners that are going to help us get there? Because we're not going to do it ourselves. And so we have to figure out what is that right balance. And we're not perfect. Nobody's perfect, I don't think. But I think we've, I've got a solid team. When people ask me what keeps me up at night, I say, Not a whole lot. I mean, maybe the ability to recover, maybe the ability to the unknown unknowns, right? But I'm confident that my team is going to be able to see something. We're going to be able to react to something. We're going to be able to respond and contain. Those are huge. Rather than the key, the key things that I really focused on to build the program around. And we're pretty good at the proactive. So from what everybody tells me on our endpoint security, on some of the data security things that we're doing, I think we're keeping up with the Joneses and maybe do a little bit better.

Ed Gaudet: Resilience is so key. And you're right, as long as, there's things out there that we can't control, so why let it bother your sleep, right?

Matt Modica: As long as you can respond, recover appropriately.

Ed Gaudet: That's a great way to think about it. If you could go back in time, what would you tell your 20-year-old self?

Matt Modica: I would say, and the short answer is patience. I've never been a very patient person, and I had this boss at one time in my career telling me, You just need more big time. And I hated that answer. I hated that answer. But he's so right, looking back on it.

Matt Modica (cont'd): Because I think when you first start, or even if you've had a career for a while, you think, Okay, I'm pretty solid. And it's the old book of what got you here is going to get you there, right? You have to constantly change. You have to constantly learn. And that big time, you just need time to get experience. You just need time to make mistakes. You need time to have successes. I think that's the biggest thing that I would give to my younger self, just say, Listen to that, listen to that boss, because he actually knows what he's talking.

Ed Gaudet: Enjoy the journey. Enjoy the ride. So good. Outside of healthcare, IT, Cyber, what's your passion? What do you, what's passionate about if you're not doing the job? So I think this is where we get to have a little fun, maybe in unblur screen.

Matt Modica: I guess so. I guess so. So I'll turn my blur off and we can just.

Ed Gaudet: Oh, look at that.

Matt Modica: So there you go. There's my passion right now. I am a droid builder as a hobby and, and what that is obviously you've got R2D2 here, you have, right there is our 5J2 too, which is a very little known Imperial droid. Totally geek out. So I've always been Disney fan, always been Star Wars fan, and things like that. And the pandemic hit and I said, Gosh, I love graphic design, I love electronics, I like doing things with my hands. And my son brought home a 3D printer.

Ed Gaudet: Oh, there we go.

Matt Modica: And he's and I was like, this is pretty cool. So I ended up printing R2's dome. And both of those are, by the way, are fully 3D printed and I printed R2's dome on my son's printer. And then I invested more in other printers and did some other things. But yeah, it's been so fun and so rewarding because not only is it a hobby and something that I really enjoy doing, but it ultimately gives back. And that's kind of, that's what I'm about. I'm about service and the service-minded aspect of things with the copyright rules and all the things that we need to do in Disney and Lucasfilm here. We can't do anything for profit with these. And there's a global group that actually does this. Does this work?

Matt Modica (cont'd): I want to say, I last count of about 20,000 members. Everything we do is charity. Everything we do is for public. As an example, on May the 4th, this past May, we went to Children's Hospital here in Saint Louis and visited with over 100 patients in their rooms. And, you know, just brought joy to them and just had fun. We opened up an accessible playground not too long ago, and spent some time with the kids in the accessible playground. And and of course, we do comic-cons and things like that and just hang out and do some of those fun things. We had a radio station that wanted to have us out and just talk with them and things like that. So it's just, again, it's things for fun. It really energizes me. And it's, it's really.

Ed Gaudet: That's remote active. You said you, you can, we have a remote control. You can, those things move, and.

Matt Modica: They're not on right now but basically all the lights, everything screen accurate, dome moves, panels move, arms come out and it's fully remote-control.

Ed Gaudet: Video of Princess Leia?

Matt Modica: What's that?

Ed Gaudet: A video of Princess Leia?

Matt Modica: Not the video, but I have the audio of it.

Ed Gaudet: Oh, do you have the audio? Of course.

Matt Modica: There are some people in the group that have started, little projectors and, you know.

Ed Gaudet: That's so cool.

Matt Modica: Yeah, that's the exciting thing. And then when I'm not doing that, I'm usually doing something with my wife and kids and that kind of thing. So it's, it's just nice. Love her.

Ed Gaudet: Thank you for sharing that with the listeners. That's incredible. I would be remiss if I didn't ask you this question. This is the Risk Never Sleeps Podcast. What is the riskiest thing that you've ever done?

Matt Modica: I was trying to think about this. And I'm like, man, and this is, this is part of the conversation I was having with my wife earlier is, What do you think the riskiest thing I've ever done is? And because I struggle, because I'm a pretty risk-adverse. I like to plan things, that kind of thing. But I think the thing that I came up with was when we got married, I think I've mentioned it before, kind of my origin stuff. I had a degree, wanted to go into graphic design, was trying to stick it out and do that. Didn't have a job. We decided, we got married literally a month after we got out of college. My wife still had a semester to go in college, and on top of, my, my parents were in between houses. They were moving from the house I grew up into a new house, and they were in an apartment. Did not have room for me.

Ed Gaudet: Oh no.

Matt Modica: So I had to find a place to live, and I had to figure out how I was going to pay for things, and I got married and my wife still going to college. And so just that unknown right, of, Okay, we're just going to figure it out. And that was the conversation we had, was like, We're just going to figure this out and see what happens. And thank goodness things worked out. And I was able to get that job at Jones. And, you know, rest's history. So it's just. I've had.

Ed Gaudet: I've had a similar journey. I love that I slept on a friend's couch for a couple of months. Same thing. I had no place to go. I was getting married eventually and.

Matt Modica: No, luckily, my brother and family were all like, You can hang here. I was like, Yeah, but I'm going to get married and all this stuff, so.

Ed Gaudet: This has been terrific. Any last thoughts for our listeners? Anyone breaking into maybe cybersecurity as a profession or thinking about getting into healthcare?

Matt Modica: Not much more than we already said, but what I would say is the same thing I tell a lot of people that are looking at security and they're saying, Gosh, I just don't have the skills, or, I don't think I have the skills. And for me, do you have the passion? Do you have the desire and the excitement around this kind of field or this kind of thing, right, Security in general? And do you have the aptitude, right? Are you willing to learn or are you able to learn? Are you able to deal with change? Are you able to deal with what I call is, the gray, right? Because a lot of times I'll see a lot of folks in Security that are totally black or white, like it's either right or it's wrong. And all of our jobs, especially in risk management, is the gray. It's never going to be perfect. How do we fix it and make it as perfect as it can be? So it's those kinds of things that I think really can frustrate people if they're really in that mode of good versus evil, black versus white for something like that. So it's, Can you deal with the gray? Do you have the aptitude? Do you have the attitude and the passion? And if you do, great, I want to talk to you. And I'm sure my colleagues want to talk to you as well, because we're looking for people to help us.

Ed Gaudet: That's, that's great. That's a great way to end. Thank you, Matt, and thanks listeners. This is Ed Gaudet from the Risk Never Sleeps Podcast. 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