Podcast Transcript

Risk Never Sleeps
Episode 79
Nick Sturgeon

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 Nick Sturgeon, the Vice president and Chief Information Security Officer for the Community Health Network in Indiana. Welcome, man.

Nick Sturgeon: Thank you for having me on.

Ed Gaudet: Yeah. Welcome, sir. Welcome. I've been waiting for us to talk, so it's a pleasure to speak with you and learn more about your background. And I did take a look at it on LinkedIn. Thank you for your service. You're an Indiana State Police sergeant, I believe, right?

Nick Sturgeon: Yeah, I left as a first sergeant. Yeah.

Ed Gaudet: So thank you for that. That must probably have a lot of stories there. But we won't go into those. So let's start off with, tell us about your current role and your organization.

Nick Sturgeon: Yeah. So I said I'm the CSO at Community Health Network. We're about six-hospital healthcare system, and mainly central Indiana. So Marion County, Indianapolis, and some of the couple areas outside of Marion County.

Nick Sturgeon (cont'd): But, you know, I said mainly central Indiana and workforce, about 17,000-18,000 people that are providing care on the front lines, as well as administrative and IT staff and all that good stuff. Decent sized healthcare system.

Ed Gaudet: It's a big system. How did you get into health care and IT?

Nick Sturgeon: Yes. Yeah. I first started when I was a director of security operations at Pondurance, and our main focus was healthcare clients. And then from there, I went to Ernst and Young and had a healthcare client or two that we did some cyber program assessments for. And then after traveling got a little bit too much, there's a position that opened up at IU health for a director in the Information Security department. Applied for it, got in. I was at IU health for about four and a half years, left as an executive director. Late last year, the CISO position at Community Health opened up, and I was ready to take on that next step, that next challenge, and so ended up applying for it and obviously got the role. But getting into health care wasn't necessarily something that I was like, Oh, this is something that I was targeting per se, just happened as happenstance. But really the mission for me is protecting patients. And really it is about patient, not just the data, but protecting them, their lives, and making sure they're receiving the care and health results that they're looking for when they come into our system, for whatever it may be.

Ed Gaudet: It's consistent. Obviously, we're protecting citizens, and now you're going to protecting citizens, which are patients, which every citizen is mostly.

Nick Sturgeon: Yeah. The mission, you're right on point there, the mission that drove me, and really, in law enforcement, you call it getting bitten by the bug. And it really is that drive to protect and serve. In healthcare, been in multiple different industries since leaving law enforcement. But the purpose behind health care is as close as I've found to law enforcement of protecting and serving. So that really aligns with who I am and that need and drive to serve.

Ed Gaudet: That shared mission is unique and something that keeps a lot of us coming back for more, even when things get really rough, like the last couple of weeks. I'm sure you've been busy.

Nick Sturgeon: Yeah. Change Health, not to necessarily call them out, but I think it's just one of a continuing example of the criticality and really even the gaps within cyber in the health care system. And really, to me, that was a unique attack. It was directed at a provider. It went after one of the ancillary services that serves health care organizations. And man, it was as damaging as it would have been to an HDO directly or health care delivery organization. Sorry, government, former government, recovering government, official and the acronyms. Yeah, thankfully we weren't as impacted as some others, but I think just to how it affected every health care organization, it definitely eye-opening and continuing of eye-opening of how important cybersecurity is for not just, again, the delivery organizations, but all of the ancillary vendors, partners that connect into health care.

Ed Gaudet: Yeah, the blast radius. I don't think we've ever seen a blast radius like this one. I was on with John Riggi from the American Hospital Association yesterday. We were talking about some of the stats around it. 74% of hospitals indicated direct patient impact from it, and over 94% indicated they had a financial impact to it, and I think 60% were losing $1 million or more a day. It's just incredible.

Nick Sturgeon: Yeah. I had heard stories, healthcare systems, smaller ones potentially, going out of business because they could not get revenue in to pay their employees to buy, you know, whether it's, you know, the supplies that are needed, prescriptions. And it was hugely impactful. And I think for me, being in healthcare and just the attention we need to do and understanding the risk and that impact at such a new level of detail just highlighted a lot of things that really, as a technical guy, we focus on the technologies and patching and the vulnerabilities, but really emphasizes the need for having that deeper understanding of the business relationships and risk with our vendors and suppliers.

Ed Gaudet: Exactly. Having that ability to step back and look at every vendor and the relationship it has with their vendors and products and services, and draw that equivalent of an SBOM. But for vendors, a ..., right? This notion of where are my vendors and which ones have this unbelievable reach into my organization, across business processes, across all of my most critical, if you will, business processes?

Ed Gaudet (cont'd): And I think also, I heard the other day, too, from a resiliency perspective, from a continuity perspective, this brings up the need for alternative solutions, right? So for us to look at those and then map alternative solutions so that we can recover faster.

Nick Sturgeon: Yeah, yeah. And I, with the organizations like The Size of Change or United or some of these really critical pieces within the industry itself, you alluded and then mentioned changed about 74% of the market share of that particular, you know, service that they provide. It just highlights the supply chain weaknesses in that. And I think that's, whether you're in health care or other industries, I think that there's definitely some important takeaways to businesses and cyber professionals across the different industries.

Ed Gaudet: That's a really great point. As you think about other areas of risk, certainly, that have been introduced or being introduced into the system, we've got to talk about AI. What are you doing around AI, and how are you trying to proactively help the organization adopt it, but do it in a purposeful and a meaningful and a secure way?

Nick Sturgeon: Yeah. This is it's a technology that you cannot shy away from. You can't put your head in the sand; it's not going to go away. And you look at what Microsoft and Google and all these big and down to small technology companies, you know, bringing in AI in some shape or fashion. You've got to get a handle on it. That's something that we're doing internally. We're not shying away from it. We're looking at where it can be best served to help within the IT organization, within the clinical spaces. I think there's definitely a lot more due diligence that has to be done. When you look at introducing AI into the clinical spaces, and what are the use cases for that and not picking on your necessarily, what's the word I'm looking for, advocating for this particular technology, but nuance for us is to help with dictation and take some of the administrative burdens of the doctor or clinician, the patient interaction away from the doctor so they can focus on understanding more of what the patient is saying and coming up with better clinical outcomes and remedies, and allow the technology to do the voice recording and transcription. I think those are some really cool use cases for it. Obviously, if you go back to the early days, like Dragon and even currently Siri, if you're using the iOS and there's, it's not 100%. So I think you can't completely 100% rely on the technology.

Nick Sturgeon (cont'd): You still have to have that human interaction and vetting of what's being done, but at least it can start taking away some of the administrative overhead, if you want to call it that, and allow the clinicians to really focus on the patients and give more of that better bedside manner, if you will. And yeah, so there's use cases like that, I think in the clinical space, are really where we're focusing on. There's a lot of concerns of allowing the AI to, you know, highlight maybe what the prognosis may be. I think there's still some really cool future use cases there personally. Again, not a clinician, but I think until the technology gets to where it's more, that validation and verification gets to 100%, there's still going to be some hesitation about some of the use cases within the clinical space. But we're looking at it. I think for us it's what are those use cases putting a lot of good governance around when we use AI within the clinical space or within in IT or within HR or finance or things like that, to make sure that we're using it properly? There's a lot of privacy concerns with it as well. Where is the data going? And then the security around that: Who's got access to it? And making sure that the models don't get biased in the wrong way. So there's a lot to figure out. And I think, yeah, there's so many more, you know, smarter people than I are working on it and trying to figure that out. But I think it's definitely, in my opinion, something that we should be looking at. I think there's some competitive advantages to using it. And I think those who adopt it or not adopt it, I think, you know, you'll see some competitive differences depending on which direction you go.

Ed Gaudet: It's a great point, and there seems to be this level of urgency among our customers and other CISOs I talked to where they're setting up these governance committees that run across the business on the clinical side, all the way through to the technical side. Have you set up one of those as well?

Nick Sturgeon: Yeah, we've got an AI governance group that's looking at this, and it's a cross-functional team from legal to IT to HR to the clinical folks. So yeah, it's, and we, I think almost all don't have a choice because you look at Microsoft and with Copilot and how they're pushing it. And you, same with some of the other vendors they're, you know, incorporating that within their technologies. So we have to get a handle on it. And I think that would be something I would say to my other CISOs and other technologists, like, it's not going anywhere.

Nick Sturgeon (cont'd): It's not going to do any good by burying your head in the sand. You should figure this out for your organization because it isn't going anywhere. It's just going to get more entrenched.

Ed Gaudet: That's a great point. Oftentimes, we think about those new things coming into the organization. But what about all those other vendors and products that are updating their applications or their technologies with AI capabilities? How are we reassessing those? We definitely need to think differently about this. All right. Great. As you think about some of your other priorities over the next 24 months, what else are you looking at? What are the top three?

Nick Sturgeon: Yeah, I think one of the coming in, I'm just a little bit into three months into the role. So I'm still, and my approach coming in was very much a consultant. Put my old DY hat on and really say, Okay, I'm just going to sit and listen. I, you know, knew the that my predecessor and he and the team had set up a very good cyber organization. So I knew I wasn't coming into a situation where I was going to have to do a lot of overhaul. It was really much, okay, figure out where we can that real strategy and tactical approach instead of that kind of the whole cell changes because the team doing a lot well. So I didn't want to disrupt that. Don't fix what's not broke. Again, put that consultant hat on and really just sit, learn, observe. And with that, some of the things around identity management I think are a priority for me, figuring out our access controls and where more, and even from an insider threat perspective, a, there's a lot of focus on the threats from external. But even when those external threats are become internal threats, what can they get access to and looking at permissions? And are they set based on least privilege and appropriate for what is needed to be done? Working on that, I also medical device security is something that I've personally been focused on for the last, you know, 3 or 4 years, and looking at how we can improve that overall state medical in general is so susceptible to cyber attacks and the vulnerabilities, and a lot of these aren't getting patched or as quickly. And so how can we, you know, put in better protections there? But then it's just building that strategy for the next 3 to 5 years based on AI and some other emerging technologies.

Ed Gaudet: So a lot to keep you up at night for sure.

Nick Sturgeon: Yeah, a little bit.

Ed Gaudet: Think about the things you do outside of the job. What would you be doing if you weren't doing this job? What are you most passionate?

Nick Sturgeon: My family is first and foremost the reason I do everything. When I'm not working, it's spending time with the family. One daughter is already out of the house and married and started her own family. I've got two other daughters that are, you know, still in the house, and we're everything's about making sure that we set them up for success. And my youngest daughter, I think we spend the most time on because she's travel softball. So one word when I'm not at home or typically doing something softbally, practice or a tournament. And on top of that, I'm going back to grad school, getting my PhD at Purdue. So what spare time I have is either that, plus I got into the political game last year. I ran for local office, town council position, end up winning my election. So what ever time that I have outside of family and work is doing the town council thing.

Ed Gaudet: That's great. I saw that on LinkedIn. Congratulations. I have three daughters as well. I think you said you had three, right?

Nick Sturgeon: Yeah. Three.

Ed Gaudet: Yeah. My middle one's getting married next week, so.

Nick Sturgeon: Oh, nice. Yeah.

Ed Gaudet: Any advice you can give me.

Nick Sturgeon: Yeah. Just. Yeah. Say, Yes, dear. Whatever you want.

Ed Gaudet: Doing all that. I'm doing all that. Yeah.

Nick Sturgeon: Yeah. My oldest has been married for about a year and a half now. I was just an amazing time. And her husband is an IT guy, so he and I have a lot to chat about and a lot in common there. But she was just supported her every way that I could and just make it as special for them as possible.

Ed Gaudet: Thank you. Yeah. No, we're, that's what we're focused on. So that's good. If you could go back in time, what would you tell your 20-year-old self?

Nick Sturgeon: Oh, just keep focused. You know, early on, going back to 20, my early 20s just trying to figure out what I wanted to do. And I don't know if I would change much because I think those experiences helped me become who I am today. But it would just be, when things are rough, just keep your head down and get through it. There's lessons to be learned in those times. So as much as you may want things to be different, I think the trajectory that I went on was great. A lot of good, a lot of bad. But every one of those experiences helped build me to who I am today.

Ed Gaudet: Well, that's a great answer. I think that's a unique answer, too. I like that a lot. I have to ask you this question, this is the Risk Never Sleeps Podcast: what's the riskiest thing you've ever done, Nick?

Nick Sturgeon: So I mentioned I was an Indiana State trooper for about eight years. And law enforcement, by its nature, is very risky. So I can pull a number of experiences, like just from the number of pursuits that I was on, going into buildings, not knowing what was happening, the number of traffic stops that could have gone really bad. And I was driving really fast around 465, which is the interstate that circles Indianapolis. I think a lot of stuff there was very risky just because it was the nature of the job.

Ed Gaudet: Yeah. You're on a desert island. You can take five movies or five record albums. What would they be?

Nick Sturgeon: So this one's tough. I'm a big movie guy, and big sci-fi. Same thing with music. And this one was really tough because I look at the Star Wars movies, mainly the original trilogy, look at Lord of the Rings and The Matrix trilogy and Dune, the original Dune, and even now, the two new Dune movies. There's just a lot to pick from, but I would probably pick the original trilogy of Star Wars. Then I would pick probably Matrix, the original Matrix, and then The Return of the King from the last movie within from Lord of the rings.

Ed Gaudet: Epic, epic. Yeah, for sure. That's great. How about a DM manual? Would you bring a DM manual with you? Look at that. I assume you played when you were a kid.

Nick Sturgeon: Yes.

Ed Gaudet: Me too.

Nick Sturgeon: Yeah. The game, and get into the video game side becomes even more.

Ed Gaudet: I love ... as a kid growing up. Remember that one defender and?

Nick Sturgeon: Oh yeah. Yeah, the original NES Mario Brothers ... Yeah. So many.

Ed Gaudet: ... 2600. I mean.

Nick Sturgeon: Yeah, the Halo games, the first Halo.

Ed Gaudet: Fantastic.

Nick Sturgeon: That would be the toughest choice: figure out what I want to bring with me.

Ed Gaudet: Hardest lesson in your career?

Nick Sturgeon: Shoot, that's a really good one. There's been some tough lessons that I've learned. Yeah, one of the early ones, and this may sound bad, is sometimes work's not the best place to find friends. I know that sounds, because it's competitive.

Ed Gaudet: I tell my daughters that all the time.

Nick Sturgeon: So are you health in or in the employee engagement questions? Do you have the best friend at work? And everybody always struggled and answered that question on the low end. And I struggle with it, is because my first and foremost priority isn't to make friends. And I know that sounds bad. It's to do my job. And especially in leadership roles, you have to make decisions that aren't necessarily going to make you friends, and it's not going to make you popular. So I always struggle with that. And I've got friends from work. And it's not saying that I don't make friends, but it is very, when you're in a leadership position and you're making decisions if you're worried about how really, how it's going to make people feel, and it could put you in a bad position and really it's tough. It is a really tough lesson to learn. And sometimes you have to put friendships aside. And it's not that you're trying to do people wrong, per se, but there's certain decisions that you make that are not going to be popular. But that's the right thing to do. And to me, it is about doing what is right. And sometimes you've got to put those personal feelings aside and it's not to be careless and it's not to to negate how it's going to make people feel if you've got to make an unpopular decision. But it's the right thing to do, that's what you have to do.

Ed Gaudet: Perfect. That's terrific advice, and thank you for sharing that. I know that was probably hard to share, but that's such a great, such great insight and great advice for folks that are listening. So let's go to the last question. I saw you were an adjunct professor at one point. Do you still do that, or?

Nick Sturgeon: So the PhD program has put a lot of those things aside, and I'm still in part of their requirements for my degree is to teach. And I've, I have taught through that I love teaching. I think I come from a family of educators. So it's just part of that other thing to give back. So it's I think what I part of and I get asked a lot, what do you want to do with this? What's that's going to help your career? And I know really I'm doing it as my retirement gig.

Nick Sturgeon (cont'd): I want to, when I, you know, give up doing the technical stuff, the industry stuff, I want to find a community college and on, you know, close to the coast and I want to teach cyber somewhere in a community college. And so really the PhD gives me the best option.

Ed Gaudet: You'll love this question then. So what advice would you give out to, give to cyber people just coming out of school looking at a cyber profession or looking at coming here or both?

Nick Sturgeon: Yeah, I mean, I actually, I was just put in contact with an individual a couple of weeks ago. He's wanting to change industries and he's looking at cybersecurity as a potential way. And I'm like, First of all, you don't have to be technical. I grew up as a tech kid. Apple Two was my first computer, and I've been working on computers ever since. But you don't have to get into this industry if you don't have those technicals. There's many different paths and things to do that don't require to have that technical background. So don't let that stop you from getting into it. But once you get into it, figure out what drives you and what your passions, whether it's risk or it's digital forensics, it's sales, it's management, there's; just try to find something that you're passionate about and go that route. But then don't be afraid to pivot. Like one of the things I think I've been successful at is finding opportunities and pivoting to different areas to get different experiences. It's a great industry. There's a lot of opportunity. Again, I think when we talk about, I think as an industry, this, the talent shortage, it always drove me a little bit crazy. As you know, the talent is there in different areas. We just have to train and provide some basic skills, training. The talent is there. I think there's a lot of talented people that bring different soft skills to this industry that I think are sorely needed, but the talent is there. We just have to do better at training and providing opportunities for people to get in and not set these high expectations. And, or as one of the things that I experienced early on was, if you don't have the certain pedigree, you're not a true cybersecurity person. That's all bull hockey. That always, that, I think, that's part of the reason I think we've seen this lack of interest or a lack of pipeline, if you will, is because folks have put this artificial barrier onto what it means to be a cyber professional.

Ed Gaudet: We've seen more and more customers leveraging the process around risk management as a way to bring people in that have little to no skill, give them an unbelievable breadth of the organization of, you know, from the business process, from the impact of technology on those processes, and then putting them in the role for a year or two and moving them into other areas of cyber once they get that background because a really nice way to come into the organization. So I love that. I love that, Nick.

Nick Sturgeon: Yeah. And I think some, there are some things that obviously you have to have the technical aptitude for, but that isn't everything within cyber. One of the things, you know, I've noticed there are some really talented technical folks that I honestly wouldn't put in front of a board of directors. And it's not that just the communication skills aren't there. They want to get too far. And it just, and even from a charisma standpoint, just they're great at writing code, they're great at troubleshooting, but you necessarily wouldn't put them in front of an executive leadership team. So I think you need, there's a whole breadth of different types of personalities and backgrounds that you need that doesn't necessarily require that an technical aptitude to get into this industry.

Ed Gaudet: Yeah. That's great. Thank you, Nick, for your time. This is Ed Gaudet from the Risk Never Sleeps Podcast. If you're on the front lines delivering a patient care and protecting patient safety, 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