

Podcast Transcript

Risk Never Sleeps

Episode 27

Skip Sorrels

Ed Gaudet: Welcome to the Risk Never Sleeps Podcast, in which we learn more about the people that are on the front lines providing and protecting patient care. I'm Ed Gaudet, the host, and today, I am pleased to be joined by Skip Sorrels, Director of Cybersecurity at Ascension Technologies in Austin, Texas. Great, well, let's get started. Skip, tell us about your background and your health system.

Skip Sorrels: Sure, happy to. Thanks for having me. Background, I'm a little bit older than most, so in a bachelor's degree in nursing, critical care trauma nurse for about eight years. Last thing I did was flying around on jets with a transplant team recovering organs for transplants, that was in the Dallas marketplace. While I wasn't doing that, I was having fun with the nonprofit IT department that I worked for, Southwest Transplant Alliance, doing network administration in my off time. That turned into a job because I've been on call, and the dot-com craze was happening, and I've been a geek and a nerd at heart since the days of Atari, so I'm like, Heck yeah.

Ed Gaudet: Another Atari fan. I love it.

Skip Sorrels: That's it. That turned into a request for my resume from Dell, and I ended up in Dell in 1998, supporting as a technical sales rep, their white server box product line, and my career developed from there into many, many different avenues, biggest part of which my first stint at Dell was with the DOD doing solutions, architecting solutions, and providing guidance for Navy-Marine Corps Intranet and several other big projects and programs that were kicked off in the early 2000s. All that to say, I had a blast. Family happened, I was traveling too much, I took a break, I went out and did some things on my own: Internet marketing, strategic direction for Internet marketing, pay-per-click advertising, you name it, I did it. And eventually, I ended up back at Dell in 2011, working with several people I knew from years past on the Ascension account, and we were providing services to Ascension. So 2011 is where I got back into healthcare on the IT side of things. 2011 is also the point in time where I met the security team at Ascension, who was feverishly working to encrypt things like hard drives and start the process of cyber, you know, 12 years ago. And that relationship, after many years, afforded me an opportunity to this team. So I stepped into this role as director, and five years ago, one of the main things that I was asked to do was develop a program around med device security and those things IOMT, Internet of Medical Things. We didn't have a program. It's pretty early on. So kind of where I've been, what I've done and how I got there, and lots more to talk about in the last five years as well.

Ed Gaudet: Awesome, yeah. And I think I saw on your LinkedIn, did you just graduate with a master's?

Skip Sorrels: I did.

Ed Gaudet: Congratulations.

Skip Sorrels: I appreciate that. Super exciting. I missed my goal by two weeks. My goal was to finish in 12 months, and did it in 12 months and two weeks, so I'll take it.

Ed Gaudet: Awesome. Awesome. And also, you're an ethical hacker, too. You got your start doing that as well.

Skip Sorrels: That was the last course I had to have and certify into to pass the Master's. So, yes, my forensics exam is up next.

Ed Gaudet: Awesome. So as you think about your organization, what are some of the priorities that you're looking at over the next year?

Skip Sorrels: Personally, continued maturation of our med device security program. We are operational, and we are doing things related to patch management, vulnerability management, asset management, the fundamentals of the CIS top controls one, two, and three, and my next charter from leadership is to do the same for operational technologies. So I'm already starting the process down that roadmap, and our fiscal year is a July to June timeframe. So that's my big initiative that's new on the horizon, the run and maintain aspect of what me and my teams do is singularly focused on risk reduction. What can we do today and tomorrow to reduce risk, versus identifying it and saying, okay, we know about it, but what are we doing about it? I think that's the common challenge that we run into. We know about a lot of it, the question is where are we doing about it?

Ed Gaudet: Exactly, yeah. It's obviously an area that's near and dear to my heart and my company's heart. I love your thoughts on AI and how you're thinking about AI as it creeps into your health system.

Skip Sorrels: Man, Mark and I had an interesting conversation around this yesterday. AI is an interesting evolution of technology. Takes me back to the first Terminator movie, Skynet. Makes you really start to think about what technology is doing and how much control it really already has in our global space, and we just don't think about it, it's kind of taken for granted. So from where we sit, the bells and whistles went off really fast with leadership and our board, and executive people in our organization seeing this buzz in the Wall Street Journal and all of these other media outlets asking us the question, what does this mean? What do we do about it? Should we be worried? Yes, yes, and yes. We're well aware of it. Yes, we have concerns. Do we see its value? Yes, but typically, the trust but verify words follow very quickly after. So we quickly had to develop a policy for acceptable use of AI in our environment.

Skip Sorrels (cont'd): It's based on the honor system. So people have to do the right thing based on what they've read on a piece of paper, but ultimately, it's intended to discourage behavior that they might not realize is unwarranted. So please don't put PHI into an AI tool. Please don't use your corporate email to log into or sign up for. Your typical things that you say about, Hey, don't use your corporate email to sign up for sports betting websites. I mean, the common sense things get past people. Think about what you're doing and what it really means. Do you understand the power of AI? It's a learning technology, so whatever you feed it, it consumes, and it becomes part of that organism, and you don't get it back. So those are the words of caution that put into the policy, the education that we're doing, but we've also made some efforts around technical controls. How can we prevent people from making an unwarranted mistake in accessing something that they shouldn't unknowingly? So we're working through that, too. That's a little bit ... but trickier. It's not just a simple firewall setting so, but that's how we think about it, and that's how we address it. We recognize its power, we welcome it, we just approaching it with ... caution.

Ed Gaudet: Yeah, cautiously optimistic, of course. Assuming that is one thing that keeps you up at night, what are some of the other things that might keep you up at night?

Skip Sorrels: Ah, third-party vendor risk. To be quite honest, I think it's probably the largest risk to healthcare in general. It's because we don't control it outright. We don't necessarily have the visibility. So again, it becomes, in some cases, a black box type of environment, and you just don't know. You can do all you can do inside contract language, but again, it's only as good as the words on the paper. We're back to a methodology of trusted behavior and practices, and so, as I look across the landscape and every week the journal newsletter comes out and it lists all the stinkin' breaches, I would say a large portion of them, over 50%, are related to a vendor or some entity outside of their control or direct control no different than ours, and that's really troublesome to me because it's hard to get our arms around that. Technical controls don't limit people behavior outside of your organization. When I think about the third parties and their ability to reach into our organization gives me the more concern. And so med device is a, healthcare is a space where vendors remote into entities or enterprises and use various methods to do that, and some of them get past us.

Skip Sorrels (cont'd): We have a very regimented review process in order to allow those types of things, but we're big, we've got people that need to move, we're talking patients, and things get biased at times. So we're continually trying to look and say, what do we miss? How do we go get it?

Ed Gaudet: No, it's right, and the frequency of changes on the vendor side, the third-party side, also has the opportunity to change scope of risk over time. How do you think about that when you think about the certificates, SOC 2 certificates, and other certificates that could be used as a proxy for security? What are your thoughts there?

Skip Sorrels: We lean on SOC 2 type two heavily with regard to hosted data or data processed data. It's a contractual requirement. We'll allow a high trust in lieu of a SOC 2 type two, our preference is SOC 2 type two. Where I'm challenged by that is the likes of the bigs in the med device manufacturing space. They don't have SOC 2 type twos, albeit they may be processing or even hosting our data. We know they're accessing it, and I'm trying to get, I'm educating myself and coming, drawing some conclusions around, is it possible to adopt the ISOs and the ICSs, knowing those are global standards organizations, and to what limit of scope should they be used? Because those are typically device-centric. I've not seen where they expand in scope to encapsulate the ecosystem things outside of the device. So the verdict is still out on that, but I do believe there's an opportunity there to further or better understand what an organization is doing at a device level. But the big scope enterprise view of what are you doing with regard to hosting data, data, and transmission, those things become more challenging. As you all know, the price tag on a SOC 2 type two is prohibited for some companies.

Ed Gaudet: Yeah, yeah, and also there's a time dimension to the actual assessment. Does that force you sometimes to do, do you continually still require the questionnaire, or do you accept the SOC 2 in lieu of a questionnaire, or do you do both?

Skip Sorrels: We've taken a pretty hard line on the requirement of SOC 2. Where one is not available and there's no intention, that becomes a finding, a risk finding, with great concern and ultimately has to be elevated to the business level at an executive level for either acceptance or denial.

Ed Gaudet: Got it.

Skip Sorrels: We don't have much leeway on that one. That one's, because it is related to our data in third-party teams. We're pretty stringent on that one.

Ed Gaudet: That's great. And what about fourth-party data? Are you able to get a handle on that, or any tips and techniques you can share with listeners?

Skip Sorrels: That one's tough. Two years ago, when we started really heavily pressing for the SOC 2 type two, a vendor had to have it, their hosting organization had to have it, ... if they were with one of the inner cloud service providers. Those are pretty readily available now, that was less of a problem. But then when you start asking the question of contractually, who else do you sub to? Who else participates in your business? What other software companies? And you start going fourth, fifth, and sixth levels deep, it starts to get pretty untenable. I don't have any good advice for that except to say due diligence. We've made a decision that the company that we're signing into contract that has met the provisions, those provisions extend to their fourth and fifth levels, and that is a legal expectation in the language. But we've refrained from digging deeper and requiring more documentation because the value of that effort just hasn't proven to be worth the time.

Ed Gaudet: Now, that's prudent. So what are you most proud of over the last year, personally and professionally? It's been a rough couple of years for folks with the pandemic, obviously, and recovering from that. And it looks like you've made some progress personally on the education side, so I'm sure you're proud of that. But any other things that come to mind?

Skip Sorrels: I'm a proud new grandfather.

Ed Gaudet: Hey, all right.

Skip Sorrels:

Ed Gaudet: That's great. So tell me more. Tell me more.



Skip Sorrels: Sure. My latest granddaughter was born about five months ago, and I've got five grandkids.

Ed Gaudet: Oh, geez.

Skip Sorrels: ... to a new toddler.

Ed Gaudet: Yeah.

Skip Sorrels: So we have a fun time around here. School wise, the master's degree had been something I said I was going to do from the time I went off to college. I was the first one in my family to get my bachelor's, and I said, I'm going to get my master's, and I let things get in my way. And finally, I came back and said, I never said I wasn't ever going to do this, so I'm going to do this now, and I just was very intentional. And with, you know, the new educational platforms, going to college back in the 80s was completely different than going to college these days, and being able to do it at my own pace was not only financially helpful, but it also allowed me to be flexible. You know, work late at night sometimes, cramming, writing papers, taking, whatever needed to happen, and it allowed me to keep my full-time job and not have competing priorities. So it never felt like one took the place of the other. I just had to manage it, budget my time.

Ed Gaudet: Yeah. There's really no excuse anymore, is there? It's a matter of time and setting priorities and then keeping to them.

Skip Sorrels: Absolutely. I think on a technological front, my biggest sense of accomplishment is we set out to deploy a deep packet inspection technology. We originally slated it for taking 24 months. We managed to be done in 11 months, data flows from 100 different sensors. Ascension is an amalgamation of many mergers and acquisitions, suffice it to say, 150,000 employees total and a little over 2600 locations. My deployments focused on our largest footprints, and I now have visibility that we've never had any other form of technology in one view, and it has expanded not only our thinking, our concerns, and also has allowed us in many different ways to help the business.

Skip Sorrels (cont'd): When I first began to research this five years ago and identified it, I said to management, We're the tip of the spear. This thing is going to be a business intelligence goldmine when we begin to really unfold the data and look at all of the different applications that we can provide our stakeholders around their activities, apps rationalization, standardization, EMR rationalization, standardization. You start to get into some conversations around, how much is it going to cost me to go from one to the other? Because I have to understand all of the devices that talk to one another. Are they all still compatible in this new environment? And I'm able to produce that type of data now and literally show a topographic view of a device talking to all these different devices and what it means to your organization. So it's been a very exciting opportunity for me and our company. And the timing of all of the 405 (d) and HHS and all these things that are coming out from left and right, careful what you ask for. I've been flying under the radar with my team for quite some time, and now we are in the spotlight, and I'm getting a lot of questions about our capabilities, what we've done, what our successes and failures are, and more importantly, what are you doing next?

Ed Gaudet: Yeah, yeah, the bar continues to raise, and we have to stay vigilant, there's no question. So outside of healthcare and cyber and IT, what's your passion? What would you be doing if you weren't doing this?

Skip Sorrels: I'd like to sit in the woods.

Ed Gaudet: I'll bet it's great. Me too.

Skip Sorrels: I grew up with a fishing pole and a BB gun in my hand, I grew up on a farm.

Ed Gaudet: You too. That's great. That's fantastic.

Skip Sorrels: In the last ten years, I made some relationships that have afforded me some, a very large piece of ranch land south of here that I'm able to go and be at anytime I want. And get to see the cattle that are there, but more importantly, the wildlife, and I actually have places where my phone doesn't work.

Ed Gaudet: So that's terrific. That's the best.

Skip Sorrels: It's peaceful.

Ed Gaudet: Yeah, I have a little corner in my basement where I go where my phone can't work, so. If you could go back in time, what would you tell your 20-year-old self?

Skip Sorrels: Never doubt what you can accomplish. Do not let fear get in the way. And so for me, I'm always my own worst enemy in terms of what I expect of myself and what I allow myself to be distracted from. And so if I look back, a couple things come to mind, Why didn't I buy real estate? You know, there's that song out there now says, Buy Dirt, right? Absolutely. I still tell my kids and young people around me, that's one thing I wish I had stuck with. I had a desire to do that and didn't do it. And now it's like, well, wish I had. But the other part was, if you set your mind to something, and what I really, kind of looking back at is, I always wanted to travel and see the world that I knew I could do that as a nurse and I didn't do that. But when I got into IT, I found myself traveling all of the time, and so I got what I wanted, it was a bit delayed. And looking back, there's several things where I said, I'm going to do this and I eventually did it, but the reason I didn't do it then was I let a little bit of a fear or the unknown step in the way, or paralysis by analysis, and so I'm a firm believer in progress over perfection now. I'm absolutely a believer in, you got two ears and one mouth for a very specific reason.

Ed Gaudet: So true. And it's a good point. And often I hear that from many of my other guests where they kind of revisit their their 20s. I love that question. But it brings up the next question, which is, and I'd be remiss if I didn't ask this because this is the Risk Never Sleeps Podcast, what is the riskiest thing you've ever done, Skip?

Skip Sorrels: I can think of a few things. I guess having been a ranch hand, blocking out horses for rodeo was probably one of the scariest, dumbest things I might have done ...

Ed Gaudet: ... unique answer, a unique answer to the podcast.



Skip Sorrels: There's just so many things. You know, the other part about being a youngster is there are times when you're truly fearless and you should be afraid, driving a little too fast or you name it. Doing stupid stuff is a fraternity pledge, you know, I mean, you don't even think about it, and then you look back and you go, Dear Lord, thank you. I should be dead.

Ed Gaudet: There by the Grace of God.

Skip Sorrels: To be honest, yeah, because otherwise, he was watching over me, because I certainly wasn't watching over myself.

Ed Gaudet: I subscribe to that. Okay, well, that's a good, bucking is a good answer, and not many people have said that, so I think you're the only one. So that's, we'll add that one to the list. All right, my last question. You're on a plane. It's heading down, unfortunately. You're going to land on a desert island and you have the ability to bring five albums with you. What would they be? Five music albums, and no greatest hits, Skip. So let's stay within the constraints of this question.

Skip Sorrels: Thunderstruck.

Ed Gaudet: Ooh, thunderstruck. That came up the other day, actually. That's a, wow.

Skip Sorrels: Let's see. I gotta go Van Halen, Jump.

Ed Gaudet: Good one. Nice.

Skip Sorrels: We gotta have some George Strait. So I would probably say Troubadour.

Ed Gaudet: Good.

Skip Sorrels: I gotta have Garth Brooks, The Dance.

Ed Gaudet: Okay, good, two country albums. Good.



Skip Sorrels: And.

Ed Gaudet: One more. This is a good list, by the way. I'm going to be in your desert island.

Skip Sorrels: Trying to think what else. Probably some Billy Idol or Loverboy. Just some.

Ed Gaudet: Okay, that's a curveball. I wasn't, I didn't see that one coming.

Skip Sorrels: I.

Ed Gaudet: Eyes Without a Face and Working for the Weekend. All right.

Skip Sorrels: Absolutely. I love music, I love all music. It elicits motion, you know, and kind of like to be upbeat.

Ed Gaudet: So does Thunderstruck, though, that's a good way to end. Any last-minute thoughts or tips for our listeners?

Skip Sorrels: I think from a security perspective, I'm often asked, you know, what's the one thing that anyone should do? And my response is, get started. I mean, even if it's a pad and pen and you're creating an inventory, I've learned painfully that the most fundamental activity of security is knowing what you have in order to know what you've got to do. And I see people wanting a silver bullet or seeking a technology, and the reality is just having a simple asset management plan goes so far in the overall scope of cyber that you just can't overlook it. And where I have and where my team has, it's slowed us down. And so we all remind one another, keep it simple, keep it to the basics. We're blocking and tackling. And it's not glamorous, it's hard work, so get started.

Ed Gaudet: Thank you, Skip. I appreciate you joining us today. And this is the Risk Never Sleeps Podcast. I'm Ed Gaudet. And if you're on the front lines protecting patient safety, remember to stay vigilant because risk never sleeps.



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