Podcast Transcript

Risk Never Sleeps
Episode 100
Tim Swope

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 Tim Swope, the interim CISO at the University of Chicago. And welcome! This is the 100th episode of the Risk Never Sleeps Podcast. You are the 100th participant.

Tim Swope: This looks like I might win a prize for that.

Ed Gaudet: I think someone knocks on your door and gives you a cake or something. I'm hoping anyway, they show up soon. I'm just kidding. All right, so let's start off with, tell our listeners about your current role and your organization.

Tim Swope: Yeah, the current role I have is now as an interim CISO. So what that is, often I go into an organization when they either a CISO is left. There's been some issues that they need to have remediated, a lot of them center around risk. So I go in and I assess the risk, their cyber posture, and put together plans, capital corrective action plans, and sometimes training. I look at people, process, and the tools they have in order to make sure that when I leave, and my goal is that I do have to leave, I usually stay for anywhere from 5 to 6 months.

Tim Swope (cont'd): And when the next CISO comes in, and usually, I work with them for a month or two for transition, but then they have a clean slate. I walk in and the flag is hanging upside down, and when they leave, the fort is corrected. So that's a little what I do for a living.

Ed Gaudet: Excellent. So that must give you the opportunity to see a lot of things, right?

Tim Swope: It does. It does. And I also take, I take a real objective eye because objectivity means you based on evidence. But one of the things I told people is, and everybody listening to the podcast might not be as old as I am, but they, our parents told us not to look at the TV because all you saw was dots. The thing is, when you stand back. What do you see? The whole picture. So that's what I do. Standing back from the organization allows me a little bit of ability to see the picture that others don't.

Ed Gaudet: That's great. Tell our listeners how you got into healthcare and how you got into IT.

Tim Swope: One of the things is I actually have a degree in economics and math. And right now, I probably couldn't get a job at Starbucks with that. And I studied Fortran in college at Indiana University. So yeah, I think things have changed immensely over the years. I've actually have 28 years in life sciences. I started off as a data science scientist. I worked with companies like Thomson Reuters Health, which is now Truven, Reed Elsevier. And I was often, I did a lot of business intelligence work for pharmaceutical companies, which in the 90s and the 2000s. One thing that was interesting that happened from a pharmaceutical standpoint, of course, they had GXP requirements almost, and they were very heavily regulated, just like health hospitals and such. We, and I'm going to date myself again, they called it information assurance, right? And so they didn't have the term cybersecurity; none of us did at that time. As things were moving ahead and you looked at from a data science standpoint, now they do it for patient analytics. They had different levels of aggregation. Those became security levels for what details you could see on a, you would say, now I say now in healthcare patient. But back then, they were doing clinical trials.

Tim Swope (cont'd): So they are under the same requirement. So, I leverage that to assist healthcare organizations from a cyber standpoint. I got started with many. I worked with over five large health systems in New York City health and hospitals, Northwell, Catholic Health, Stony Brook, to name a few. And there was a program about, it was probably around 2014, it was called District Delivery System Reinvestment Incentive Program, federally funded program, to see how hospitals could work together for Medicaid population, reduce emergency room visits. What that required was that you had a standard cybersecurity requirement from the Department of Health, and that was my entree into really working from this capacity with health systems.

Ed Gaudet: Wow, excellent. And so you mentioned data science early on in your career. Lots changed in that area. How are you thinking about and how are you helping University of Chicago and others as they think about introducing artificial intelligence, Gen AI, and other capabilities in their organization?

Tim Swope: Our organization is very interesting too because we have university health. We also have Texas University of Health, Harvard. So, one thing is we're all connected with the university, and the university loves AI. Plus they don't have as many requirements with their healthcare. We're very we have risks around using generative AI and learning models that are outside the organization, because then you have patient health issues and issues. One of the things I do say is we will adopt it sooner or later. In fact, IBM has they've used AI, we call it assisted intelligence. When you look at cancer cells, they'll take a picture of it. They've got 476 million plus pictures of it, and they're able to see if you need a second opinion. So we've been doing assisted. They've augmented intelligence. One of the things that I'll be honest, which I use from a cyber standpoint and risk standpoint, is actionable intelligence. When everybody's looking at the greatest tools, the tools actually give us this information. And that information will say, and as we're talking about risk, this might be a risky endeavor. And sometimes, we use quantitative analysis. Everybody does one of these. That's a one. Maybe that's a two. And everybody understands all the things the likelihood, the the impact of the organization. You have to have something behind those. That's the first thing. The other thing, too, is how do they factor of your control effectiveness. In other words, a very high risk. But I have very good controls becomes a lower risk.

Tim Swope (cont'd): I'm in healthcare. I'm going to triage the highest ones first. And so that quantitative analysis allows us to look at it in a different way. Now, that's actionable intelligence, so then I can make operational decisions.

Ed Gaudet: I love that. And you can manage the residual risk in a way that allows you to focus on those things that matter. That might be more risky that you haven't been.

Tim Swope: And we really never ... It's incumbent upon the work that we do. We have risk everywhere in healthcare. In fact, I try to break it down to things. We have enterprise risk, large organizational risk. We have some ad hoc risks. And these come up all the time. People sending patient information potentially through their Hotmail, or they can put a thumb drive. You don't belong to us. Those would be ad hoc risks. And then you have vendor risk, all those three. When you look at a Venn diagram of them, they center upon a risk posture. However, you can pull them apart and analyze them separately, and that shows where your real risks are coming from an organization. So again, those are actionable intelligence. I always hate to pivot from the AI. I'll be honest, in my world right now, Skynet is not fully aware, right? We're getting there. We're going to learn how to use it. But again, it will most likely be from a standpoint, we have more alerts that are coming in every day. So, you use tools that give you certain types of event alerts. We correlating those alerts is a very tedious business, and that's where that AI will come in. Is it going to there's some decisions we actually have to make ourselves? A lot of people can say, I can identify anomalous behavior in months in your organization. It never worked in our hospitals. Not only that is, they're all different from there. You really have to have that human intervention, and then the AI really is augmented intelligence for us right now.

Ed Gaudet: I love that. And you've got to be able to connect with the business to communicate the differences and help them make the decision about taking on risk in that technology.

Tim Swope: Yeah, we just have a new CIO. I worked with our older CIO in a couple of different places, and he understands my way of working. But if I had my way, we might be on dumb terminals right now. I'm just saying. But we can't do that. In other words, you could secure things if you can lock everything down. You can't operate as a hospital entity right now.

Tim Swope (cont'd): We have things like the Cures Act, not the CARES act, the Cures Act, which actually is giving patients more information freely, opening things to them. A huge risk is digital transformation. People have to understand it's the first time for many people that they've actually had to get data outside of their four walls. There's a risk. Now, what we have to do is have control effectiveness to mitigate it, because that risk will always be there, and then we actually monitor it. And one of the things we can't forget is monitoring that risk and monitoring the activity. That's a key thing that we have to do. Is it easy? It was a Kennedy said. We go to the moon, not because it's easy. We go to the moon because it's hard. I tell people that my business is the patient safety, security, privacy business. It's not the convenience business. There are risks. And sometimes, we have to accept some of those risks but monitor them because you actually have to make patient care effective, efficient, and sometimes easier on the doctors to perform it more quickly.

Ed Gaudet: Yeah, that's a great, great point.

Tim Swope: One of the things I always say, I work closely with our privacy officer, Karen Havercroft. In fact, I think she was on one of these. She was?

Ed Gaudet: Yes, we love Karen.

Tim Swope: She's a blessing for me because she actually knew as an interim, you really have to rely on the people in the organization. I'm not going to find out everything myself. But the other thing is, I am not always going to be in agreement with the CIO. This is going to make operations move minus to make them safe, and Karen's is to lock us down if I failed in any of those attacks. When you work together like that, I think you can manage risk. And I think that's the biggest thing we have to do is how do we manage it?

Ed Gaudet: That's great advice. As you think about that, what advice would you have to listeners that are trying to build relationships with those clinicians and other business leaders?

Tim Swope: One of the things, too, is we have a research area and we have to be very visible to them. I tell everybody during COVID, we were like physically dispersed. We were like socially distancing, too. We have to be we could be physically distanced from folks, and a lot of people work remote, but we have to be socially connected. In other words, I don't email them. I call them up. I meet the main users or the main people that I need to secure down. And it's interesting when sometimes you get research folks, and they really need to put that thumb drive and carry that everywhere they go. And sometimes you have to ask them, how important is that? Research your lifetime research. What is the value of you losing that or retaining it? And that's where I say that's where I come in. I partner with them on that.

Ed Gaudet: Yeah, that's excellent. What are your top three priorities that you're currently managing at the university?

Tim Swope: Oh, one of the things that everybody is looking at is that identity access management really, from a privileged access management standpoint, it's usually a huge risk for everybody. There's it's there's tools. There's the plethora of things to to use. However, you have to understand what you're doing. In other words, you have the ability for hackers now to come in and do a credential harvest credential. How are you going to stop that? You need to understand, first of all, what would happen in the event of a privilege escalation and how you can see that. So those are the things we monitor. We identify and then put processes and rules in place to literally stop things from happening. One of the key things that people don't do. And I always tell people when I come in as an interim, it's like a one-term president. I don't have to worry about being reelected. That's right. And so there's a lot of things I could do.

Ed Gaudet: So there's power in that.

Tim Swope: There is. Actually, there is power in it. So, I do things that ask for forgiveness later. But people have to you have to be willing to block things that are not. They don't look right. You can investigate them later, re-enable people, but you better be prepared to block instantly. That stops the bleeding. It stops the risk until you can remediate it or investigate it.

Tim Swope (cont'd): So that's some of the other things we're doing is obviously, you have endpoint protection. But if you look at have you had an incident? We have events. It's like anybody that has healthcare, other industries where you get over 10,000 events that we block them. You have to identify what you block. You have to keep watching them. Understanding anomalous behavior, tracking that one of the key things is really understanding the tools that you have to block it. Reassessing your rules all the time, and then, and having the staff be able to respond to them quickly. I ran track at Indiana University. And our coach, Sam Bell, used to say, he said, I'm going to train you like others won't, so you'll react how others can't. And we have to do that with our staff too. We, it's still human beings running the tools. So those are some of our large priorities. And then again, some of the ancillary things. It's there's always you have outside threats. You have to understand that a patient record is very valuable, and you have to track insider threats. Also, sometimes people are doing things they're not supposed to do that could cause problems. Sometimes it might be nefarious behavior, but innocent behavior, like I'm taking my home thumb drive and going to put it in. I just happen to have a freeware version of Adobe that has a backdoor ransomware on it. And these things happen; we block those now and again. Also, there's phishing. You can, to be honest with you, you'll get down to about if you can get under 10%, you're good. You're going to have your frequent flyers, which we always have. They'll click on anything. You send them, you retrain them, and it still doesn't work. So then you watch them. The other thing too, is those usually are the first vector for an account takeover, and you have to have those controls in place to identify. Those are the things we look at till they're fully remediated, we monitor. And at that time, once they're fully remediated, we're going to monitor something else. I'm going to the next patient, in a sense.

Ed Gaudet: With those frequent flyers, some organizations will tie punitive recourse. Have you thought about that, or have you done that in the past, or what do you...?

Tim Swope: Well, yeah, the top cardiologist that brings in the money that pays my check is usually not good to have punitive damages on those. I like to counsel them. I contact them and counsel them.

Ed Gaudet: Yes, I love that. Always pragmatic. You always have pragmatic approach to things. If you weren't in this role, what would you be doing outside of healthcare and IT? What's your passion?

Tim Swope: See the boat right here?

Ed Gaudet: I did, I did.

Tim Swope: My wife and I actually have bought a home up in ... Maine, and it's in New Harbor, Maine. I hope this doesn't bring a lot of people there because it's a beautiful small town. ... Lighthouse one, is the third oldest lighthouse in the United States, I think, is at the point. And I work on a house that was built in 1780.

Ed Gaudet: Nice. Now, where, is it up by Boothbay or its harbor?

Tim Swope: Boothbay Harbor. It's Boothbay Harbor. In fact, it's off the road to Damariscotta. Like I said, I'll stop there. I don't want people coming.

Ed Gaudet: Yeah.

Tim Swope: It's a beautiful place to visit.

Ed Gaudet: Boothbay is beautiful.

Tim Swope: Yeah, the weather's beautiful. So what I do up there is I work on an old house that is, and you'd be surprised they built these things really good ..., Ed. Yeah.

Ed Gaudet: No, they'll last

Tim Swope: The walls behind.

Ed Gaudet: Forever.

Tim Swope: Are logs. And then they put clapboards on them. They were the original log cabin. And then they, rather than plaster, it is lime crushed up shells mixed with clay, and so it's like concrete. So this will last forever. And we're the only third generation, third group family that's owned it.

Ed Gaudet: Really? Wow. That's incredible. I won't be seeing an Airbnb, will I?

Tim Swope: No.

Ed Gaudet: Okay...

Tim Swope: ... Stay here, and I'm not sure. You know, I like to know who slept in the be, so.

Ed Gaudet: There you go. There you go. If you could go back in time, what would you tell your 20-year-old self?

Tim Swope: Well, I did give some advice to my son one time. I had two older sons, the 27-year-old, a 24-year-old, I have a four-year-old daughter. But before the one was getting married, somebody asked me, what advice would you give him? I said, if you've got a car payment and a house payment and you can only pay one, you'd pay your car payment. He said, why? I said, because you can live in your car, but you can't drive your house to work, so you mitigate those risks of needing to get somewhere.

Ed Gaudet: I like that. Okay, so that's what you tell your 20-year-old self. What's the riskiest thing you've ever done?

Tim Swope: I'll tell you, my wife is the, used to be the conservator of the ancient art collection at the MET. She had no idea what I did for a living, so I brought her to a risk conference. And one of the things I will say, and it's very interesting, she speaks fluent Cantonese.

Tim Swope (cont'd): And when I was discussing this with her on the plane, she says, in Cantonese, risk, and this is very good for people, you could use this in any presentation, she said, risk in Cantonese is loosely translated to crisis, but it's two symbols: danger and opportunity.

Ed Gaudet: Right.

Tim Swope: So I'm like writing another slide on the plane. Anyways, it's, it ended up being. But if you think about it, if you identify the danger first, proactive risk management, right? It's the only time you have the opportunity to remediate it. Anyway, I brought her there, not knowing that she was. I needed a good opening. And my second slide was a picture of our wedding, and I said a little bit more about me. I got married last month. She's sitting right back there as her face turned red and she looked quite angry. And I said, in full disclosure, this is my second marriage, so I'll let you know if this risk management stuff works out in a personal standpoint, and that was the riskiest thing I think I ever did.

Ed Gaudet: I love that, and I love the Cantonese, the opportunity and danger. Because if you don't take risks, obviously you miss out a lot of opportunities, so yeah.

Tim Swope: And life is risk.

Ed Gaudet: Life is risk.

Tim Swope: Everything we do is risk. It's just how you identify it. There's a lot of people in our business that, they wait for an auditor to tell them the risk findings, right? I'll be honest with you. They're going to be the same ones that they find everywhere else, so they're not uncovering anything really special. You can only find those risks when you work there. You work with somebody; you interact with people. Again, I'll be honest with you. I've done a presentation with my old privacy officer, Leslie Giglio. I'm sorry. She's probably, so maybe she'll hear this, but her and I also got along very well. And I did a group, a co -resentation, and I asked CISOs how many of them work closely or even know your privacy officer. Very few of them raise their hand.

Ed Gaudet: Yes.

Tim Swope: The thing is, the risk comes to privacy after the fact, right? But they see it from a different lens than we do, the risk from other people, from a different view. So you really have to understand who's in your organization. I'm one of like the Holiday Inn thing. I'm not a doctor. I play one on TV. I'm not a clinician, but I do work with them closely because they know the inherent risks and other things they do, too.

Ed Gaudet: That's right.

Tim Swope: And the risks that are involved, if I make things more ... to them, make it harder to get into something.

Ed Gaudet: Yeah, and you're the benefactor of that in so much as you're a patient. We're all patients, right? So, we all understand the give and take as it relates to risk in healthcare.

Tim Swope: So those are some of the things we have to really, you have to look for the risks. And now, I'll be honest with you, I do bounce around to different hospitals. Like I said, mainly, there's a couple of reasons why people out there look for a CISO. Someone retired, maybe they let them go, or unfortunately, they just didn't have one, or someone was doing a dual role, which is very hard to do these days.

Ed Gaudet: Yes.

Tim Swope: That dual role. So what I get to see is a lot of different scenarios. Unfortunately, I'm seeing the same risk over and over. So I'm trying to evangelize, and maybe through podcasts like this, there's things that we should do as a group. Some hospital systems, some people at other areas of healthcare life science think that this is secret sauce for them. It's the same for all of us. And if we do this all together as a consortium, we're going to know how these risks get remediated.

Tim Swope (cont'd): And I think that's what I'm trying to do in my second act here of my life play. My second act is to get this out and say, you guys aren't unlike everybody else, and this is what's been successful, and let me help you walk.

Ed Gaudet: And how are you representing that? In a book or are you writing a book?

Tim Swope: I've written some articles. I teach a privacy and security lecture every now and then through Columbia University. So, but a lot of what I do is actually go into the health systems themselves.

Ed Gaudet: A couple last questions. Hardest lesson in your career?

Tim Swope: Hardest lesson in my career, I don't think there's, the hardest it was one best learned is the fact that in order to stay in this game as long as I have, you have to always be relevant. That's a huge lesson because you don't understand it until you fell behind, and then you realize that, I keep telling everybody, tomorrow is when you start learning what you should learn today, and it's constant. One of the things I do tell when I do the people part of what I say, I will help even through automation, maybe cut down the hours and the time that you work, and in that next free time, you best start studying for the next attack.

Ed Gaudet: Exactly.

Tim Swope: Yeah.

Ed Gaudet: Yeah. Work that top of license, for sure. Movies or music? If you're on a desert island, you could bring five. What would they be? Or three?

Tim Swope: Oh, wow. Movies. Definitely, The Natural. I'm a big Robert Redford fan, because The Sting is pretty good.

Ed Gaudet: Yeah.

Tim Swope: Movies. I'd probably actually, music, maybe hope that Eric Clapton was sitting there with me, and ... so, yes. And then one more, I'm gonna have to say this. The movie of my wedding. My wife is gonna watch this, so.

Ed Gaudet: She's been mentioned twice, so I hope she does watch it. So you brought up The Natural. Are you a Mets or a Yankees fan?

Tim Swope: I used to live in Boston. I'm the only guy that's, yes.

Ed Gaudet: You're a Red Sox fan!

Tim Swope: Yes. In fact, a good friend of mine.

Ed Gaudet: Awesome.

Tim Swope: Martin is a very big Yankees fan. Another one is minus a Mets fan, and I sit right between him and let him argue.

Ed Gaudet: I grew up in, I grew up in Connecticut, which is the halfway point between the Bronx and Fenway, and so I'm a Red Sox fan.

Tim Swope: I lives in the greater New York City area.

Ed Gaudet: You did? Yeah.

Tim Swope: And so, even though I'm up in Maine now, but so, yeah, I go to both.

Ed Gaudet: Oh, very nice. Yeah, yeah.

Tim Swope: I say I go to whoever gives me the free tickets.

Ed Gaudet: There you go. Maybe we'll have to catch a Red Sox game That would be fun.

Tim Swope: It is one of the last old-school ballparks.

Ed Gaudet: Yes, it's special. There's no question. Hopefully it stays that way. Yeah, go ahead.

Tim Swope: Oh, I was going to say, nothing like seeing someone hit one off the Green Monster.

Ed Gaudet: Yeah. Yeah, and they look like they're clawing their way back to a wild card.

Tim Swope: I lived in Watertown after college.

Ed Gaudet: Oh, you did? Oh!

Tim Swope: It was a lot different than it is today. Trust me.

Ed Gaudet: Did you go to the New York diner? Do you remember the New York diner?

Tim Swope: Yes. Yeah. Yeah. Now, those same apartments are like $5,000 a month or something, and it still looks the same.

Ed Gaudet: Yeah. Yeah. Where did you go to school? Did you go to school in Boston or?

Tim Swope: I went to Indiana University.

Ed Gaudet: Oh, Indiana.

Tim Swope: I went to work there after after. And I was from Portland, Maine.

Ed Gaudet: Got it, got it.

Tim Swope: Portland, Maine is like a mini Boston.

Ed Gaudet: It is. It is. Yeah, very similar. Last question. What advice would you give to kids coming out of school that would like to pursue a profession in cyber, IT, healthcare, etc.?

Tim Swope: Well, one of the things is there are some schools that have cyberschooling, right? But we all know that CISSP, you take it, you pass it, and to get it you have to have some referenceable background. Look for some internships. But also, if you're going to go into the cyber world, you can't really do it unless you understand the infrastructure architecture networking side. So those are the pieces that we try to secure. If you go that route and then you can move into the cyber world, you actually know what we're protecting, you understand a little bit about it, and you can get that reference for requirements that you need to finish those to get those certifications. It's almost for people that come out of school and they're going to be a consultant, but you got to know something in order to consult about something.

Ed Gaudet: Right.

Tim Swope: So, in order to be able to secure things, you have to know something about that.

Ed Gaudet: Right.

Tim Swope: That would be the best advice I would give to somebody coming out. It's almost that becomes your internship or your almost like your pre-work requisite for cybersecurity.

Ed Gaudet: I love it, I love it. Tim, thanks very much for your time.

Tim Swope: Thank you very much.

Ed Gaudet: This is Ed Gaudet from the Risk Never Sleeps Podcast. And if you're on the front lines protecting patient safety and delivering patient care, remember to stay vigilant because Risk Never Sleeps.

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