Podcast Transcript

Risk Never Sleeps
Episode 22
Paul Connelly

Ed Gaudet: Welcome to the Risk Never Sleeps Podcast, in which we discuss the people that are protecting patient care. I'm Ed Gaudet, the host of our program, and today I am pleased to be joined by Paul Connelly, former CISO of HCA, and held a number of jobs in the government with the White House and NSA, we're going to talk some more about that as well. Paul, welcome to the program.

Paul Connelly: Thank you. Good to be here, Ed.

Ed Gaudet: Yeah, good to have you. So let's start off, how did you get into healthcare?

Paul Connelly: It was kind of fortunate. As you mentioned, I worked in the beginning of my career in the federal government, and then I went into consulting, and my team won a big project at this company in Nashville called HCA. And what I discovered was that, I mean, I loved being in cybersecurity information security to begin with, but the addition of doing it for a healthcare provider to me is just such a noble cause that I instantly fell in love with this company and being part of it. And at the end of our big project, we made a bunch of recommendations, and one of them was, you really need to have a chief information security officer. And they said, okay, what about you? Took me like all of three seconds to say, I would love to do that. So that was back in 2002. I got to be there more than 20 years.

Ed Gaudet: Wow, that's terrific. And now you're retired. How is that going?

Paul Connelly: I don't know yet.

Ed Gaudet: Too soon?

Paul Connelly: Yeah, I retired in April. In some ways, I feel like I'm just as busy. I've got a lot of stuff going on. And, you know, the good thing is getting to spend a lot more time with family and do things that I want to do, but it's been great so far.

Ed Gaudet: And you're on a couple of boards still, I see.

Paul Connelly: Yep, and hoping to continue down that path. I really kind of went into retirement with three goals, and one was to keep building the workforce in cybersecurity. One of my proudest accomplishments is 33 members of my team have become CISOs, so want to continue mentoring and helping people develop. And I've taken a role with Belmont University here in Nashville to help them come up with cybersecurity education programs, so that's been a really interesting thing. And second goal was, stay involved in healthcare. So I'm a technical advisor to the board of the Organ Procurement and Transplantation Network, which is basically the US system for organ donations and transplantations, which has been fascinating. And then the third thing was I wanted to continue to develop myself. I'm not ready to call it the end of my career, so I'm hoping that serving on some public boards and especially companies that are in critical infrastructure industries, in some discussions with companies and hoping that will be the next step.

Ed Gaudet: And other than family in those pursuits, any other hobbies or things that you're interested in or passionate about?

Paul Connelly: You know, that is the big one. And I'm from a big family, I've got five brothers and sisters who are all my best friends, and we live all over the country, so we've been doing a lot just to get together. And then I've got my wife and two children, and that's been kind of the core.

Paul Connelly (cont'd): My wife and I are learning to play golf, so I'm doing a few regular retirement things too. As you're aware, I mean, being a CISO is just such a relentless role that I've got stacks of books that I've been wanting to read for years that I've just never taken the time to read. So just a lot of things like that that I'm hoping I'll get the chance to do now.

Ed Gaudet: Any interesting book you've opened and started lately or?

Paul Connelly: I recently read a really good book about the US Secret Service. That was interesting to me, having been there and worked really closely with those folks over the years. I've just started a book about the wonders of the human cell and how cells make up everything, and working my way through it, but I'm getting there. Maybe one day I'll even write one. Who knows?

Ed Gaudet: Oh, boy, you heard it here first. Our listeners are excited. All right, well, maybe we can have you back on once that's in print, it'd be terrific. So you've seen a lot, obviously, over your career. How has cyber evolved since you were with the NSA and with the White House to more recently at HCA?

Paul Connelly: It's crazy, as you know. I mean, when I started in this field back in 1984, cyber wasn't even a word, the Internet didn't exist. When I first went to the White House, there was no Internet, by the time I left, there was, so it's been a really fascinating transition. And going from where you're pushing and trying to convince people like, hey, pay attention, this is important or this is going to be important to today where everybody recognizes that this is critical, this is a board-level issue at big companies, all almost every company really, but that evolution to where it is so critical to business and being part of it has been fascinating. And our roles as the professionals providing the defenses have really changed as well. I mean, in the early years, I was really just sort of heads down part of the IT group behind the workstation most time. And in recent years, especially in my role when I was at HCA, it felt like a third of my job was to be an evangelist and just convince our workforce, get them on board, make everybody feel like this is part of their job. Talking with our board of directors, meeting with our senior leadership, meeting with partners, it's really incredible how the role has changed, and the demands on the leadership have changed as well.

Ed Gaudet: Yeah, it's a full-contact sport, for sure.

Paul Connelly: That's a great way to put it.

Ed Gaudet: What was HCA doing that was maybe different or more advanced, or things that you could share with other organizations today, as you think back on your career and things that you put in place that really made a difference?

Paul Connelly: Well, it's interesting. I had been, after I left federal service, I spent six years at PriceWaterhouseCoopers as a consultant, and that was at a time when companies were just sort of getting started or deciding what they wanted to do in this field. And in a lot of cases, I could tell companies were just sort of checking the box, okay, we did our pen test, we checked the box, and we'll wait till next year. But the thing that I'd always really appreciated in my time at HCA was from the very beginning, they recognized how important this was and that patient care was at stake if we didn't do the right thing. So that's the biggest thing. I feel like they have always really cared. I always got time with the very top leadership, with our board of directors on a regular basis, and at, just the buy-in. As you know, there's just a different kind of mindset, I think, in healthcare, I mean, everybody's about taking care of people, and once they realize that this is part of how you have to take care of people, you've got to protect our systems and our data, It really became rewarding to be part of it. So just a couple quick things we did that were a little bit different also. About ten years ago, I made the case that I should not be in IT, and our CEO and CIO were on board, and they moved me out and made us a business unit, more of a peer to IT, which I think had a big effect on how well we were able to engage with the rest of the business leaders. And then another thing we did, this is about five years ago, we brought privacy together under the same umbrella, and then we brought physical security under the same umbrella as well. So I went from being a CISO to CSO, and I know a lot of people, this is like a religious debate, and a lot of people don't agree with it, but I am convinced that having physical security, privacy, and information security all together on one team is the best way to approach it.

Ed Gaudet: I would agree with you on that. I'm interested in the organizational learnings when you separate it from IT. What were some of the things that you could do once you made that change that you couldn't do previously?

Paul Connelly: I think the biggest change was that it was no longer viewed as an IT issue and that some of the decisions budget, big investments, and so forth, instead of being made at the CIO level, they were being made at the CEO level. So it's sort of that visibility, two-way visibility. Not only was I see more things across the company, but more people across the company were seeing me as opposed to me kind of being a level down. And the other big thing was our CIO was hugely supportive, and I think that's what really made it work. There was no antagonistic feelings or anything like that about it, and they continued to be our number one partner, but they recognized that this was giving us some additional advantages, so that's why I think it worked well.

Ed Gaudet: And how was that relationship with the business owners? What were they doing differently that maybe you couldn't get them to do when you were in IT?

Paul Connelly: I think just being a step-down and part of the IT, they kind of felt like they should be working through the CIO. And when I was brought out of the organization, it was kind of like, okay, I'm another person who's at the table that you need to work with. So it's not that there was a barrier, but it just made a more direct connection.

Ed Gaudet: It's more of a peer relationship.

Paul Connelly: Yeah, that's a good way to say it.

Ed Gaudet: Yeah, that makes sense. And then my understanding from the outside looking in, HCA does a lot of its own organic development for tool. What were some of the things that you had to build yourself that you just couldn't find publicly?

Paul Connelly: We're a big organization. I mean, HCA is a Fortune 100 company, so I have had the good fortune of having lots of resources and being surrounded by incredible people. So we build out our own, we call it our cyber defense center, but basically a SOC and all kinds of tools that augment our SEM or tying into threat intelligence. We partnered with Miter, we're very active in the Health-ISAC, so there's a lot of things that we go out, and we buy publicly available tools, but because we're kind of a unique size and shape organization, we do a lot of modification and development as well.

Ed Gaudet: Got it. What advice do you have for new CISOs or aspiring CISOs?

Paul Connelly: I think maybe the first thing is, you know, buckle your seat belt, it's an incredible role. I mean, you have 29 years out of my career where I was in that role has been fantastic. It is high pressure, it's relentless, as you know, it's, you just never know when your phone is going to buzz in the middle of the night, and something's going on. But I think the biggest advice I would give is, make sure you're focusing on the softer side of the skills. Most CISOs have tremendous technical expertise. I don't put myself in that category, by the way, but most do. But what really, I think, makes you successful is when you can develop those partnerships and other business leaders view you as a peer, as you said a few minutes ago. When you've got those communication skills, when people know that you're a trusted partner, when you're somebody who has a track record of delivering on what you say you're going to do and recognizing the mission, I think all those kinds of things are equally important to any technical skills that you have. And, you know, the last thing I would just say is, outwork everybody. I've never been the smartest guy in the room at any meeting, but I'm always the first one there and the last one to leave. So I just kind of felt like I've outworked everybody.

Ed Gaudet: I subscribe to that, Paul. I was just saying that today to somebody, you know, you might be smarter than me, but you're never going to outwork me. That's so true. And so, as you think through lessons that you've learned over your life, what are some of the hardest lessons you've learned?

Paul Connelly: Well, what I said a moment ago about, it's about the mission. And it's funny, when I was at the NSA, security was everything. They're a great organization, I loved being part of that. And then I got detailed to the White House to build the first program there and I thought, okay, we're going to do this, we're going to do this, going to do this, and I can't tell you at the beginning how many meetings I was like, well, we can't do that for security reasons. And the answer was, oh, yes, we can do it, we're the White House, we have a mission that we've got to fill, you figure out how to make security work. And I think that really applies in healthcare as well. I mean, we don't want to get in the way of our doctors and nurses and other clinicians doing what they are so good at. So you have to understand the mission, get out there and see how things work and then figure out, okay, how do we make security fit in there so that we can do this in a safe way?

Ed Gaudet: That's right, yeah.

Paul Connelly: So that probably seems obvious to everybody, but it was sort of a revelation that I learned the hard way.

Ed Gaudet: I don't think it's obvious at all. I think people gravitate towards the enforcement aspect of security when actually you've got to think more about the enablement. What can I enable that I can't do if we were to lock everything down? Because that obviously is not going to work for the company.

Paul Connelly: Yeah, you are so right. I never wanted to be the policeman. It was always the partner of how do we figure out how to meet your goal but do it in a secure way.

Ed Gaudet: Yeah, exactly. So you mentioned earlier about board participation and how more and more organizations are really starting to elevate cybersecurity as a board role. What are some of your experiences? Have you done that yet or are you leveraging your cybersecurity experience on some of the boards that you're on today? And do you feel like more and more organizations are going to have that as a standard committee, like have an audit committee, would you have a cybersecurity committee at some point it?

Paul Connelly: Wouldn't surprise me, it has become such a huge issue. I mean, you see poll after poll of business leaders ranking their risk, and everybody has cybersecurity as one of their top 2 or 3 risks, and it's not going away either, so I'm hopeful that that will happen. The scenario that you describe where, you know, the SEC obviously has draft guidelines, I was hoping they were going to come out back in April and they pushed it back till October. But I do think what's going to happen is forcing companies to list what cybersecurity they have and what processes they use to oversee what management does is going to drive boards to have people who understand it, and especially the companies that are really in the high-risk category. If they have an event and it turns out they really have nobody on their board who's been there and done that, then to me the board is not fulfilling their duty, you know, their fiduciary duty to their stakeholders, so I'm hoping that's the way it will evolve. And I've seen some articles that say that most CISOs are not ready for board service, and I understand you want to have well-rounded people, boards can't afford to have just a one-trick pony that has one narrow area of focus, but I do think the way the CISO role has evolved, more and more people are board ready. And if you think about it, boards have people who have been CEOs and CFOs and head of M&A, and head of marketing. It should be the same way, you want to have people who have been there and done it. I'm hoping that's the way it will evolve, so we'll see.

Ed Gaudet: We have compensation committees. We have finance committees. We have audit committees. We should absolutely have a cybersecurity committee.

Paul Connelly: Yeah, and maybe it's cyber and technology together, but that, the typical audit committee has so many things on their agenda and this is such a big risk that is just sort of been added on to the bottom. Is that really a good way to do it? I do think there will be that evolution, like you said, of the committee structure as well.

Ed Gaudet: I'm hopeful it's going to happen. I certainly, I think the SEC is starting to drive it that way, so we'll see. Obviously, the time you spent at the White House and the current administration is making some really significant, bold moves towards pushing cybersecurity agenda. Any advice you'd have for the current administration or folks at the White House as they're thinking through their overall agendas for cybersecurity as it relates in healthcare, specifically?

Paul Connelly: I really applaud what they're doing. Not only are they pushing companies, but they're pushing the government to be more connected and share intelligence and help us with best practices, which I think will really help. So I guess the biggest thing is, keep going, don't be daunted by the criticisms. It's tough anytime you're trying to create new regulation, new requirements. I understand all that, but I do think that there are industries that have to start with regulations, or else if you wait too long, it's just not going to happen. And this is such a current severe threat today, we just can't wait for industries to naturally evolve. You have to push it.

Ed Gaudet: You do, absolutely. So it sounds like you would support a meeting, the equivalent of a meaningful protection. We had one for meaningful use, we probably need one for meaningful protection at this point.

Paul Connelly: Yeah, I agree.

Ed Gaudet: Well, I'm sure we'll see more coming out of the administration over the next few months in that area. I know there's some work underway to push towards more of a common set of standards for healthcare organizations. And I'd love to get your take on the rural communities and what the rural communities could be doing, given the fact that they're financially constrained. A lot of them are going out of business, closing their doors because they just can't support the business any longer. Any thoughts on what we could do as a country or even as an industry to provide better, you know, a better set of services as it relates to cybersecurity, to the rural communities?

Paul Connelly: Yeah, it's a great topic. It's a really tough thing, and as I mentioned earlier, I always felt like I had the advantage of this huge Fortune 100 company resources. In our model, you know, with 187 hospitals, we could basically put standards in place and share information and do a lot of things that these smaller, especially rural facilities, just don't have that capability. So I think that's where the government can really play a large role, and industry groups like the H-ISAC and other groups sharing of information partnerships. I feel like there's no competitors when it comes to cybersecurity.

Paul Connelly (cont'd): If we find out something malicious is attacking us, we want to call the Vanderbilt right across the street and let them know, we want to let CHS, we want to let everybody know, or reach out to the H-ISAC. So the more the industry does that, I think the more, especially the smaller systems, can benefit from it.

Ed Gaudet: Yeah, that's great. One last question. I'd be remiss if I didn't ask you this since this is the Risk Never Sleeps Podcast, what is the riskiest thing Paul Connelly has ever done?

Paul Connelly: No, no. Maybe I've had a boring life.

Ed Gaudet: I kind of don't believe that.

Paul Connelly: ... CISO at the White House and the HCA have been pretty dangerous roles. But I was trying to think back, I have two brothers, very close in age, we grew up in Fort Lauderdale, and we did some crazy stuff. Probably the one thing that jumps out to me that I would absolutely never do again was one time we went snorkeling to catch lobsters at nighttime using these sealed lights that could go underwater and were down at the reef off Fort Lauderdale. And if you see a lobster and you shine a light on it, it sort of paralyzes them, and you can just reach in and grab them. So that part of it worked well, except everything around you is black, and, you know, there are sharks and other scary things out there. I just remember I got out of the water, I said, I am never going to do that again. That was like the creepiest thing ever.

Ed Gaudet: Oh, that's great. That's awesome. Any last comments or thoughts for our listeners you'd like to share?

Paul Connelly: You know, thanks for doing this. At healthcare, especially, we have to act as one community and share what we can with each other and help make everybody better. I feel like if we can just raise the bar for everybody and try to get healthcare out of the center of the target list for these threat actors, everybody is going to benefit. And whether that's driven by the federal government or people like you or just actively taking the role, I just really appreciate all the help.

Ed Gaudet: That's great. Thank you. It's a great way to end. And this is Ed Gaudet from the Risk Never Sleeps Podcast. And for those of you on the front line protecting patient safety, remember, 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