Podcast Transcript

Risk Never Sleeps
Episode 31
Chris Plummer

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 this morning I'm pleased to be joined by Chris Plummer, senior cybersecurity architect at Dartmouth Health in Manchester, New Hampshire. A little rusty for Monday morning, Chris; my apologies.

Chris Plummer: That's okay. That's okay. We ease into it. And by Friday, it's Friday is another Monday, actually.

Ed Gaudet: That's right.

Chris Plummer: So we've learned that there's no more Friday. It's just five Mondays in a row. And then we start over. So.

Ed Gaudet: We have learned about that. Yeah. And I love your, I love those movie posters in the background.

Chris Plummer: Yeah, those are, cool story there. Right in the beginning of the pandemic that year, we were supposed to go to Comic Con in Boston, and we had all of the big names lined up. We were going to, I was going to meet Chris Hemsworth. I was going to meet Chris Evans.

Chris Plummer (cont'd): I was going to meet him, actually. I was going to be in a photo with him together. So we bought these posters to have him sign, and that whole thing fell apart as everything fell apart.

Ed Gaudet: I was launching my company that year, and I guess you get a red badge of courage as an entrepreneur during the pandemic or something like that, they tell me. But it's all.

Chris Plummer: Well, you're still here, too, it says a lot. So.

Ed Gaudet: That's right. That's right. I didn't expect to start that way, but I am captivated by those posters. I'm a big movie buff as well, so maybe we'll have time to jump into that and talk about Thor I see on your shirt.

Chris Plummer: Awesome. Hope so.

Ed Gaudet: Yeah. Awesome. So tell our listeners about your background and about your health system.

Chris Plummer: Well, my background, if we use the whole time, I think we were just talking about Wild Wild Ride, but.

Ed Gaudet: Abbreviated version.

Chris Plummer: Yeah, I came into healthcare like on my sixth year as a senior cybersecurity person in a hospital, and the bulk of my infosec experience is a little over ten years working infosec for US Navy as a civilian contractor. Most of that time was with IBM, which was afforded me some huge resources to help assist really important mission of the US Navy submarine maintenance program and really learned a lot about certification and accreditation and was like the person on this contract; we were building this submarine maintenance software, really what it was and but was like the technology person so was the system administrator was doing CNA.

Chris Plummer (cont'd): And the thing about CNA is it's arduous, and you have to see, you have to learn how to run everything, patch everything, demonstrate that your systems are secure and can process certain types of information. So.

Ed Gaudet: You're the one if it goes down; they come to you.

Chris Plummer: Yeah, but think it an easier time, though, compared to today, where like the cloud was not a thing back then. So grateful for that. I'm like our work was very hard because we forced everyone to have a complete physically separate network to do the really important stuff. It was very hard to climb over the bridge and get into the crown jewels, and today we don't work like that today we wish we did. But yeah, I've always had roles where I've been like the one-person show, and I think those are increasingly less and less popular. But this is borne out of the dotcom revolution. Like the late 90s came right out of school and was like the technologist for a company who wanted to be the Spanish Amazon.com. And that was really interesting.

Ed Gaudet: Learn a lot in those experiences, though, don't you?

Chris Plummer: Yeah, you do. I learned a lot back then that even then, I knew what I didn't know, and I knew that if I didn't know something like firewall was a good example, like you had to you need managed services. You need to outsource this competency. And so that was a good lesson going forward, not to try to take on the world and pretend you, especially when today you can't pretend to know something about cybersecurity and stay afloat for very long.

Ed Gaudet: That's right.

Chris Plummer: You're going to be torched. So.

Ed Gaudet: How did you get into healthcare?

Chris Plummer: I left the Navy after about 10 or 11 years. That sounds. It sounds better when I say that. It sounds better when I say I left the Navy instead of the contract turned over for the third or fourth time, and they were like, okay, we're done with Chris.

Ed Gaudet: Always better to do it on your terms.

Chris Plummer: Yeah, but truthfully, I'd burned out of that experience probably three full times where burned out. Like, you don't even want to get out of bed. You're just like, I can't do this. I cannot wake up. And so finally, I don't know, a year that was 2012 or so. I went to work for a completely different industry. I had a friend at the Timberland Corporation, the Timberland Boot Company. Just massive. Yeah, massive fashion brand. And for the next two jobs, I just was like a security embedded person, like working in project management and worked there and worked for Phillips Exeter Academy, huge private high school here in New Hampshire, for a couple of years and got more cyber involved at Exeter. I was on cybersecurity team there. But like a lot of places, cyber security is by committee. It wasn't there wasn't a department there and I really wanted that for Exeter and they weren't really ready for it. And so I started branching out and taking a look. I was just this probably, I don't know, 2016, 17. Hard to keep track, but there were a lot of like big cyber stories brewing. Wannacry was like making big news. And I found this ad for a cybersecurity senior analyst for a hospital right here in Manchester, where I live. And okay, I think I, I think I can do that. And so I went in and I interviewed and I remember I was in this huge room, and the CIO said, like, where do you get your threat intelligence? And I'm like, no hesitation. I said I get it from Twitter. And I thought, you know what? That is exactly the truth. That is where I've learned everything for the past at that point in the past, like three years, about cybersecurity. And I said, if I get this job, I'm like, I'm not going to, I'm going to be completely transparent. And I got it. And that was, I think, working in hospitals is this cool intersection for me. I think. Anyway, I think I'm a pretty philanthropic, sort of community-oriented person, and I'm just. I'll look at my posters, right? I'm like, I think I'm an Avenger? I think I'm like a superhero. And so.

Ed Gaudet: That's what I love most about healthcare, that shared mission that you have that you can't get in any other industry.

Chris Plummer: The thing, Ed, though, is healthcare is powered by superheroes, like how many are there to go around, right? We can't just we can't hire those people. We can't. We have to cultivate them. If we're lucky, they walk through the door, but that's not the norm. So this is, I think, in another, if we're talking in another 5 or 10 years, maybe, I don't know if that's optimistic. Healthcare does not move that fast. But I want to say like the state of at least staffing for cyber teams in healthcare will be materially different, say ten years. But I don't know, I think five years ago, we weren't even really talking about cybersecurity teams and hospitals. Still, I was the only cyber FTE at my hospital back then. Now that hospital probably has, I don't know, maybe 2 or 3. I'm not sure the awareness is building in leadership. So I think even if leadership teams know they don't have what they need today, they know where they need to go. It's just a resource issue like today. I've read this story today. I guess it's the state of New Hampshire has some funding to, this is for school districts, but they have some funding to do some cybersecurity awareness outreach for school districts here in New Hampshire, which is something. But we're down to we're still back to the people problem, especially school districts are so, just absolutely overtaxed and don't know don't want to say it's still preaching to the choir. I think people who are in place in most organizations know cyber is a thing, and it just comes down to humans. How many how do we get those people in place? So I want to be optimistic, but I think we do need to materially look at, I think healthcare as a whole needs to reinvent itself when it comes to and maybe consider attracting people on some intangibles. We have a few wrecks out there right now that we're hiring for. So I've gone out and taken a look at what's on the street, what's attracting other people. And sure, pay. Pay is a big thing. Of course, we're, nonprofit healthcare is not going to... Yeah, but we know that though. But we can't just sit here forever and lament that we have to. We've got to look at what we can materially do about that. That's forging a new culture that's empowering people to be who they want to be and give them a path to go where they want to go and educate them and give them some personal flexibility. I don't know what else we can offer.

Ed Gaudet: That's a really good point. You know.

Chris Plummer: So I think. Yeah.

Ed Gaudet: When you think about that, the people issue obviously is a big one not going away. What are some of your other priorities over the next 12, 12 months, either tactical or strategic?

Chris Plummer: Phishing is.

Ed Gaudet: Oh, I thought.

Chris Plummer: I don't think we're actually going to go fishing in real life. I read this was a perception point; I think a month or two ago had a report that phishing was up 40% this year.

Ed Gaudet: Really?

Chris Plummer: And I said, wow, that's a that's a number. Like I'm a scientist. I want to know where that number comes from.

Ed Gaudet: That's huge.

Chris Plummer: I have a way to prove that out, like loosely on my side. I can go through some metrics and I don't know about 40%. That's really subjective number, but it's up. It's like it's up. When I took a look at the without getting into it, but I think I have way, I took a look at how we're doing at the beginning of August this year compared to last year. Yeah, it's up and but the other half of that article was that it's AI Right. AI is in every story is the Dot-Com Gold Rush really this year, it's in everything. It's like the new IoT. It's like web-enabled everything. AI enable everything. Here we are. And so, what can AI be doing for phishing right now? Is it improving the quality of the phishing emails themselves? I don't know. I've personally analyzed thousands of phishing emails in my career, and the ones that I'm seeing today are they're not like materially different than they were last year. There are more of them. Okay, so is AI then contributing to the phishing kits themselves? Is it somehow making it easier to distribute phishing? I don't know, it's hard to say. Is it writing better?

Chris Plummer (cont'd): Is it writing code to create phishing? I've wrestled with ChatGPT and writing code, and I've had plenty of days where I should have just spent the day reading a book about code because I've done that day was argue with ChatGPT about why something is completely made up and not working right. And yeah, I don't know.

Ed Gaudet: So phishing is a big area.

Chris Plummer: I don't know. Yeah.

Ed Gaudet: Any other areas you think?

Chris Plummer: You'll find this pandering? But third-party risk is unbelievable. That is the story.

Ed Gaudet: Yeah. I know, I agree.

Chris Plummer: That's always been the story. But it is so in focus this year.

Ed Gaudet: Why do you think that is?

Chris Plummer: Hospitals are getting better. Undeniably we are all of us, even those orgs that only have the one-person show who's trying to stitch it all together like hospitals are like materially getting better. They're getting there. They're at least getting a better front door. They know where their windows are closing them. But hospitals are they're comprised of hundreds of third parties. And so they're just it's just a matter of time until one of those weak links is, is exploited. And then and you get under the covers and then you learn about the state of affairs at these places. They don't even have a cybersecurity program.

Ed Gaudet: No. And what we find is people always underestimate the number of third parties they actually have that are material to their business, and it doesn't have to be a technical third party. It could be a non-technical third party, and if they get hit with some type of event and take and are taken down, that could have an equally critical impact to the health system.

Chris Plummer: Yeah. Remote access is remote access, right? It doesn't matter what operational function they serve. And that's been that frustration is why I mean, you're a part of Health Sector Coordinating Council as I am. And that's that sort of fire. That's what got me into that space where I could vent constructively about problems like healthcare suppliers that have no security program or just it's so highly variable where some orgs are really mature and accountable when it comes to cybersecurity and others are just still they just they don't understand the risks that they are projecting onto healthcare until they get bit.

Ed Gaudet: Even the events ones, look at move it, look at the move it event that just happened.

Chris Plummer: Yeah, really with anything that's so pervasive, though, that's just I don't know what we can do about that, really. It's analogous to Log Forging, which is a little tiresome to making that connection but.

Ed Gaudet: We got to do better. Speaking of doing better this year, in June 2023, you found a critical bug in Gmail.

Chris Plummer: That's world-famous for a month. It was pretty world-famous.

Ed Gaudet: Take our listeners through that, for those that may have not heard about it.

Chris Plummer: Oh man, that was it was just one night. One night in June. I got a phishing email. Everyone gets phishing email, but this one had this new digital seal on it that I'd never seen before. And this is a thing that Google does. And other mail. Other big mail clients do this, too, where if the message meets certain requirements without dragging the audience through the whole technical details, if the message meets has a certain provenance like Google will say, this is legit. And I looked at this thing. I was on the way out the door at karate that night. I couldn't spend a ton of time with it, but I was like, this is off the wall. I've never seen anything like this. And so I got back to it, and the more I looked into it, I'm like, this is this looks I could report, I could click the report spam button on this, but this was this looked severe enough and this was impersonating UPS.

Chris Plummer (cont'd): And it looked to me like anyone who knew how to take advantage of this could send any kind of payload, any kind of call to action to a user, and they could assert themselves as UPS. I know how victims. I could see how there could someone could be extremely susceptible to this. And so I reported through Google's bug reporting program, which I've never done before. It's just not something I personally really have time for. So Google rejected the bug. They rejected the bug outright. They said this is working as designed. And I was like inflamed. I could not believe I was so mad. So I did what I do when I'm really mad, which is to go to Twitter and I rant. And so I rant. It was probably like 9:30 at night or something, and I put it to bed and I woke up and it was just like 100,000 views and it was going nuclear and crazy. Then I felt validated. I felt validated; I'm like, okay, I'm not crazy because it's like Chris versus Google. What do I know? Like, I'm a kid who grew up in a trailer park, and I'm telling Google that there's a problem with their stuff, and it affects all of their users. And so Google ended up changing its mind, which was crazy, and had the leverage of this tweet that I put out, which had all of these people pig piling onto it, defending me. And then two days later, I woke up and I was on Forbes. And then that night, I was on TV, I was in a newspaper, I was on New Hampshire Public Radio. I was like every tech pub on the planet. I was an Apple News. I couldn't, like the one place I couldn't get into my local paper where I grew up here in New Hampshire. We tried, I say we, because my wife was, like, had a lot to do with media outreach. Like we tried so hard to get into this little paper and they just wouldn't hear it. But we were everywhere else. It was nuts. But that was the moral out of that is to just, self-confidence. It's hard to have when you have a big company telling you, and Google is full of some of the brightest minds on the planet, and you're like, maybe I'm misreading this because I've never felt like my background is, and I'm not from a whole other thing, but I just am don't come from a very confident background. Let's say that, yeah, that was quite a ride, and made some awesome friends through that process and just learned, really, the fallibility of email in the end is really no better. We are; email is no better today than it was like a decade or even two decades ago. It's still just the softest spot. And that's why it's, that's why we talk about it.

Ed Gaudet: Yeah, yeah. Well, we were proud to know you on the HSCC, I know we all talked. We're among royalty here. He discovered this incredible. Yeah, that was cool. So outside of healthcare around IT and cyber, what would you be doing? What are you most passionate about?

Chris Plummer: I'm a karate student with my daughter. We're both both got our black belts last year. We've been doing this for about seven years. Thanks.

Ed Gaudet: That's great.

Chris Plummer: Thanks. Work on our second-degree black belts right now. That is just. I know she's 11. She spent half her life doing that. But for me, it's that has been so transformative. It just made me just a different person. I can handle this line of work in a way that I could not before I started that.

Ed Gaudet: It's more than physical. It's mental, spiritual. It's there's so many dimensions to that art, which is great.

Chris Plummer: Yeah. I think that's why really I'm really attached to it. And I think it, I used to be a bicycle racer before that, I used to race.

Ed Gaudet: I saw you were a mechanic, actually, I loved, I love that.

Chris Plummer: That's my first job ever. Yeah. Building bikes.

Ed Gaudet: I built bikes when I was a kid, too.

Chris Plummer: Oh, really?

Ed Gaudet: Probably different than you did. You were sawing bars to make banana bikes and these long chopper bikes. And with the banana seats.

Chris Plummer: That's great.

Ed Gaudet: Yeah, in the 70s. Yeah, yeah.

Chris Plummer: No, I paid my dues at this little bike shop in the upper Valley in New Hampshire one summer, and then and then went on to. I've raced a bike up Mount Washington like 13 times. That's. I don't do that as much anymore. Karate has taken my life over, which I've allowed it to. I've wanted to, but so have a lot of I have a lot of self-discipline from that, and I know what it's like to suffer, that's for sure. That's what helps get through this. When you spend ten hours in a seat every day doing this job, you have to have gone to the, you have to have gone to the pain cave before and have been there plenty of times.

Ed Gaudet: Pain means you're alive. Life is pain and suffering is pain. And there's a Buddhist adage that says, embrace your dread. You learn so much from that, and try to live that as much as I can, but.

Chris Plummer: I can't wait till, I can't wait to talk to you again down the road. And we'll have far more positive spin on state of affairs. And I know we are miring ourselves down right now. It's unfortunate, but it is.

Ed Gaudet: These are different times, right? These are different times. And speaking of that, what would you do if you could go back in time? What would you tell your 20-year-old self?

Chris Plummer: Whoa. Back then, right around that time was I was exiting this dotcom I was working for. And so a lot of companies were dying off, but there were still a lot of opportunity out there, for there were a lot of consulting shops that were trying to draw in talent. And so I had offers from a couple of these places, these big places like Compaq Consulting and some local places like CMGI and Steel Point here in Boston. And I was afraid of those. I was afraid to take those things, and I took really safe work like I worked in my apartment doing some contract work and play video games all day. And I just, I wish I had. And some of those companies I just mentioned are like they evaporated not long after, but I wish I had taken the leap and gone out on a limb and maybe spent some time working for some of those companies because I probably would have grown a lot more than I did just working in my apartment. Let's say. I wish I'd taken different risks. I wish I'd walked into my karate studio back then, too. I'd have a lot more under my belt. I'd have a different belt, too,

Ed Gaudet: Literally. But that's great. I'd be remiss if I didn't ask this question because this is the Risk Never Sleeps Podcast. What is the riskiest thing, Chris, you've ever done?

Chris Plummer: Well, riskiest thing I've ever done.

Ed Gaudet: Yeah. No, I love this question because when interesting answers.

Chris Plummer: When I first got to the freshman in college at the University of New Hampshire, I was like unleashed at UNH. I had grown up with, like, my first computer ever was a Commodore Plus Four that I got from,

Ed Gaudet: Oh, plus four.

Chris Plummer: It was a plus-four. So I was like seven. And because they ran out of 64, because we had this program in my school where if you, it's called cancer computers, where if you recycled £500 of aluminum cans, it would give you a computer. They ran out of commerce, ran a 64. So I got a plus four. And so I learned to code and I got familiar with computers. And of course, we're right in the age of Atari there, which I'm like, can't believe I'm on this podcast. Can't believe I'm in a podcast that Howard.

Ed Gaudet: So I interviewed Howard. It was fantastic. Did you listen to it? It was fantastic. This is he's coming back again, by the way. He's on again. Yeah. He's so interesting. Such a fascinating.

Chris Plummer: I'm halfway through his book and it's.

Ed Gaudet: So good.

Chris Plummer: It is. And by the time I get to you and I have a computer network now, this is like multiple computers that talk to each other and had a Unix account, but my I had a 1200 baud modem and a terminal emulator. I did not have graphics. That's not a thing. All I could do is read.

Chris Plummer (cont'd): And I found Usenet and I found all 2600, and I just read and read about things that good ways to get in trouble and with computers. So I started downloading a lot of risky things, and I had no sense of where these things came from or who wrote them, or what did they really do. And, like, I had big trouble. I got in big trouble. I almost got expelled from UNH.

Ed Gaudet: Oh wow. And I had a similar experience, by the way, but it was involving a sink and a wall and the removal of said sink.

Chris Plummer: Oh wow.

Ed Gaudet: Yeah, I know it's stupid, but yours is a cooler story.

Chris Plummer: I just. Yeah, I just had no. And I was like, I was issuing commands in Unix that I did not. I was using Sendmail and Wall and these other things and no sense of consequence. I had no awareness of what I was really doing or if I was now, today if I had a user doing that, they'd be out the door.

Ed Gaudet: Yeah.

Chris Plummer: But yeah, it was back then. Yeah. I took my future in my own hands. And maybe in addition to maybe the safety of the people in the system and but I had some good people around me who really helped me get through that period of time and was able to stay in school and somehow finished. That was really tough. The agreement was I'd stay in school, but I wasn't allowed to touch it. This is very Kevin Mitnick story, by the way. But I'm not allowed to touch a computer. And. But I was taking a lot of computer science classes, so that's how they thought this was going to be very burdensome for me. And so I had to get, like a shell account from some other company. And I had friends in the inside of UNH were submitting my homework for me and professors who were okay with that. And. Yeah, that was a risky time. That's the riskiest thing I've ever done.

Ed Gaudet: Excellent. We're almost at our half-hour here. Any last parting thoughts to the listeners before we wrap it up? This has been. Thank you for your time by the way.

Chris Plummer: Oh. You're welcome. I've had so much fun.

Ed Gaudet: Glad to have you back on, we'll talk movies next.

Chris Plummer: Well, where do we start? We start.

Ed Gaudet: We probably need an hour or two.

Chris Plummer: So Marvel.

Ed Gaudet: We'll need an hour next time.

Chris Plummer: Yeah, I would just say we cannot give up on our goal of trying to bring good technologists into hospitals. I think we have so much, I think hospitals have so much to offer. I think we, as hospitals, have to better recognize what our intangibles are and market them. And I think there's I really think there's a story there. I think there are, I would call them civic-minded individuals who want to do this kind of work for the common good. This is, there's hospitals are incredibly signal-rich environments. There's so much to learn and see and do. And in a place like this, and that's what.

Ed Gaudet: And it's rewarding as hell come join us if you're out there.

Chris Plummer: No question about it.

Ed Gaudet: You're looking for a challenge and you're looking to protect patient safety. And this is Ed Gaudet. We're wrapping up the Risk Never Sleeps podcast. And for you on the front lines 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