Podcast Transcript

Risk Never Sleeps
Episode 69
Eric Bowerman

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 Eric Bowerman, a health industry CISO with a lot of experience. Eric, welcome to the program.

Eric Bowerman: Thank you, Ed. I appreciate you having me on the show. Yeah.

Ed Gaudet: No worries. So tell us a little bit about your background. You got a really interesting set of experiences, not only just in healthcare, but also on the vendor and solution provider side. So I'd love to hear more about that.

Eric Bowerman: Sure. So, I started off interestingly in the mailroom before I got into tech, but that's how I got into tech. There was a company called Grid Systems back in the day. We'll just leave it at that. And they made ruggedized laptops, and I got in with the tech support guys there and just worked through various acquisitions. We kept getting bought and sold a bunch of times, so that was a pretty interesting time. But a friend of mine got a job at Checkpoint Software and invited me to come over. They had a bunch of jobs they were hiring for, so I did, and I started working on the firewalls, working on DNS, DHCP really got into it, read DNS and bind cover to cover probably twice, which is really nerdy, but it was really good. It was well-written book. I stayed there for a few years, went to a couple of other gigs, and ended up at McAfee for about 12 years.

Eric Bowerman (cont'd): Started in proserv there, which was just a continuation from some of my other jobs that I'd been working and really enjoyed Proserv, but it really wears on you with travel. I decided it was probably time for me to see if I could seek other opportunities within the company. Office of the CISO had a senior manager opening, so I went there, went through the whole Intel acquisition, Intel security, just Intel, and then the the divestiture of that. And the whole time we're doing PCI, we're doing I was working on an estate hunter 171 before it was a real thing. I was out at the Dib and working with my legal team to see what kind of feedback we could provide to them on that, and we were able to get some of the changes done. Not obviously, just me; it was the whole div, right? So, I'm not going to take any credit for that other than agreeing with most of the big guys. Ended up at NTT Data for a couple of years, working with clients directly on that services side and just trying to make sure that they were secure, and then ended up at my last healthcare. It was a home healthcare hospice, and I really enjoyed the opportunity to work with them. I can't, you know, I've told them a bunch of times, I can't do what you do. So I'm going to help see if I can protect you in order to let you do your job. Right. Because all they really want to do is make sure the patients are taken care of and not have technology in the way. So even with the cyber guy, we can't be the opposite of no. Just like you've always heard, we try to enable and just get out of the way. The more that we can do that, the better off those the clinicians are with that.

Ed Gaudet: Yeah, that makes a lot of sense. And so, how did all that experience prepare you for the protection patient care experience that you had?

Eric Bowerman: Yeah, that's actually a good question. Since I really hadn't had any experience other than vendors working at vendors and services, moving into this position was different in a bunch of ways. One was I had a budget I had to deal with, which was a brand new concept for me because working at McAfee, everything's free or Cost of Goods, which was really stupid cheap at that point for us. But coming here, you had to rub two pennies together and make that decision on what we really have to have. Let's talk to the vendors really get those partnerships working, a lot of it to leveraging those services experiences that I did have at NTT. I knew how to work with those clients. You get that feeling of, okay, where should I be going with this? Is it there's a lot of friction that we have to remove, or we just really need to focus on security? We will worry about the friction later.

Eric Bowerman: So moving into this, you just spend that first few months really getting to know the business, getting to know the personnel that are involved. And I really saw that there were, you know, way too many accounts that that they had to have. Looking at that, I said, ah, let me get an identity and access management solution. Let's just start with that. I don't have any visibility. It was really greenfield when I got there. Building up that program was really the priority was the visibility. Let me look at stuff. Let's not make any major changes. Now here's some tools that we need to start looking at.

Ed Gaudet: What do you choose for that?

Eric Bowerman: For the visibility, we went with Rapid7. There was me and one other person that was doing security full time, and it was 8000 accounts. So there were that was a bad ratio, to be perfectly honest. So everything I'd had to look at was where is my force multiplier on these? And going with them and using their managed detection response service was really the right answer for us so that they could take care of all the chaff and the low-hanging fruit. And then we get the phone calls, and we knew it worked because we ended up testing breach attack simulation software and forgot to remove their agents, and it lit up to sound like a Christmas tree, apparently. So they were calling me just nonstop. And I'm like, why do these people keep calling? But yeah, it was a good test. But everybody laughed about it like we are now said, good point. We're removing that from that laptop, so we won't have you guys freaking out every time. But we got that type of visibility. We did end up with Von Scanner, so I could see what that looked like and then moved into better endpoint protection progressing forward. What's that minimum viable that I always hear about? I don't know until I can have that visibility.

Ed Gaudet: How about on the access side? Do you do anything that accelerated or anything like so on the side that enabled a more smoother transition into systems or?

Eric Bowerman: Yeah, that's great, because that was really what I found when I started talking to the field and the clinicians was I've got 50 passwords. I'm either going to make them all the same, which is not good, or I've got it taped to a sticky note on the back of a tablet. So that's not good.

Ed Gaudet: Yeah.

Eric Bowerman: So yeah, it's six of one-half dozen of another. I said, okay, what if I could make it one username and password? Maybe it's a little longer, but it's not horrifying. And they said that would be great because I could probably remember 1 or 2. So I said great. So we went, and we started implementing the Microsoft SSO and MFA solution initially and determined that at the time, anyway, it was just a little lacking with some of the capabilities that we wanted. So we did end up going with Okta on that, and that has been a great partnership. I'll be honest: the customer service rep that we had or the customer service manager, rather sorry that we had, was just fantastic. He was on the ball. Johnny on the spot. We have a problem. We call him. He takes care of it. He's the fixer if you will. As far as dealing with Okta, he was in front of the two issues that they had and was very forthcoming, arranged meetings with executives, which I thought was amazing. I didn't even ask for it. So anyway, not to tout them too much, but they were really good partners with it. And we went from initially everybody hating the solution. Oh my gosh, this is yet another thing that I've got to remember. I don't remember how to do this to maybe six, eight months later going I don't like Okta because it doesn't have all of my apps. I don't have all my accounts in there. How fast are you guys going to do this? Can you make this go faster? Where's the velocity? So, it was a good conversation to have. It's much better than I hate it. Can you get rid of it? It's I don't like it because it doesn't have everything in it. So, let's see what we can do to move forward with that. And we were moving as fast as we could, so had really good team. Eventually, there it was. After we got Okta, it was we were able to expand the team a little bit further as well. But and I can't say enough about them, it's who you hire, right? I can't do everything. I didn't have to. Once you get the right folks involved.

Ed Gaudet: Yeah, it truly is about the team and the people.

Eric Bowerman: Absolutely.

Ed Gaudet: What were some of the things that kept you up at night during that time?

Eric Bowerman: I think part of it was just the, and it wasn't even so much our side, but the business email compromises. We did have a lot of our partners that did not have MFA set up on their emails and or office or even Google accounts. Mostly, I think, office, but we would get phishing emails a lot from them, and it was really just crude phishing. So we ended up the segue that we had the security email gateway rather that we had just was not cutting it. It was not seeing those advanced attacks. So we ended up having to go with a different tool for that, and just an amazing product there. I think we picked some good horses in the race for these octopus-grade abnormal securities, who we went with on the but email security and just an amazing product. I think there's several others in the market, but that's the one we liked due to the partnership. And that was I think that's one of the key deals you have to look at with your vendors is even your vase, for that matter? Are you going to be around, or did you show up at renewal time?

Ed Gaudet: Yeah.

Eric Bowerman: And the ones that show up at renewal, there's plenty of commodity products out there that you can go change and get a better partnership with it. Are they coming to me saying, hey, here's the latest and greatest widget, or hey, here's a problem that we're seeing the QR code phishing? For instance, one of my VAR brought that to me. I'd never even heard of it up until that point. So they were bleeding edge and getting that information to me. But yeah.

Ed Gaudet: Now, I'm always surprised at the vendors that kind of just show up and worry about renewal at renewal time. So, when you think about the last couple of years you had, how do you think the industry is doing post-pandemic?

Eric Bowerman: As far as healthcare specifically? I think they're starting to wake up a little bit more. Honestly, and again, without trying to sound too prideful, I think I built a pretty good program, and without trying to make it sound like I don't have to run faster than the bear, I just have to run faster than you kind of thing. We were probably a harder target to hit than some of the other organizations. A lot of it. Also, though, I don't fault the cyber folks or the IT folks, mainly because they aren't given the support or the funding for it.

Eric Bowerman (cont'd): A lot of these, especially the mom and pop type places, they're just. Trying to keep it all together and keep the bills paid, so they don't really have that consideration of the PHI like we have. And, of course, it doesn't hurt to have some sort of significant event to help push that along and try to get you the money flowing. I didn't necessarily see that, but it didn't hurt. Never leave a crisis to go to waste.

Ed Gaudet: That's right. Yeah. Outside of healthcare and outside of it today, what are you most passionate about? What would you be doing if you weren't doing this job?

Eric Bowerman: That's funny. I've been thinking about that for years. Trust me, you get to that I'm burned out part, and I start looking at chef school looks pretty good. I like playing with the knives and I like doing the cutting. I like making stuff. I think cooking is a good passion I have, and as an extension of that, I have this bad habit of trying to go to the lowest that I can go. So I don't want to just go buy the stuff. I have to grow it now, growing my own peppers and my own tomatoes and things like that out in the garden. That's where we're going to go, and then start using that to do the cooking.

Ed Gaudet: Are you doing that now?

Eric Bowerman: We're planning a bigger garden in the backyard right now. So my wife is finally on board with that, and we've got some unused space. Basically, it's time to start using that for something fun. So we're gonna do a raised garden and then stick some tomatoes and things like that in there. She doesn't like that. I like my peppers. I'm focusing on one variety at this point rather than 2 or 3.

Ed Gaudet: I remember doing that with my dad, building those raised garden beds, and very therapeutic.

Eric Bowerman: It is. The hardest part is just mixing the dirt and sticking it in.

Ed Gaudet: So yeah, making sure you got the right mix of vegetables too because sometimes that can go bad and then trying to keep everything else out. What if you could go back in time? What would you tell your 20-year-old self?

Eric Bowerman: I think there's two things I would tell my 20-year-old self. One is don't be lazy and get and do some exercise once in a while because that has not helped me in my adult time. I've started doing it recently because my wife has been pestering me for years that I need to get off my butt and get out of the chair, and I'm finally started doing that. But it's a lot harder right now.

Ed Gaudet: Is her name Diane?

Eric Bowerman: Since the pandemic, this is what I do. I sit in the chair, and eight hours later, I get out of the chair for longer or longer takes. But it's mostly just sitting here in the upstairs and my variety of monitors. But I think the second thing I would tell my younger self rather is stay on top of everything and keep the education going there. There really is, if anyone wants to admit it or not. There's a glass ceiling out there, and you really have to get some of that stuff out of the way. And the sooner you do it, the better you are or better off you are anyway.

Ed Gaudet: Amen. Now, where are you from? Where do you live?

Eric Bowerman: I live in Rockwall, Texas. So up, uh, near Dallas Fort Worth or right on the edge of Dallas rather.

Ed Gaudet: Native, born and raised or.

Eric Bowerman: Yeah, I had a short stint at my parents, moved me to Denver, which was a lot of fun, actually. I enjoyed skiing a lot, so we had season passes up there to Winter Park, which was is the best. I'm just saying. Yeah, but moved back down here in the early 90s at 1.8. GPA really didn't help me very much. So they weren't willing to pay that kind of tuition money for me. I had to find myself, had to figure it all out, and cyber really gave me that opportunity. I think it helps me focus, stay focused on something. And I know a lot of people work. Probably a mixed bag, right?

Eric Bowerman (cont'd): Some people like incident response, some people don't. I don't like doing it all the time, but when it happens, I don't shy away from it. I feel like I can get in, make some decisions, start trying to figure things out quickly, and then escalate as we need to get those communications and such going. And probably just there's so many different things in cybersecurity. A couple of the folks that I did hire in, I said, get in. We'll just immerse you in it. Then we'll try to start figuring out which niche you want to be in, right? Do you like the GRC side? Do you like the security awareness side? Do you want to be more button-pushing incident response? What do you like? I like all of it. I will shy away from the GRC side whenever I get a chance, but it's always enjoyable, I think.

Ed Gaudet: It's interesting. Yeah, and just a thought came to mind as you bring it up. It's unlike any other industry, insomuch as or any other job, because there's so many opportunities to map your personality type with different roles within cyber. So, to your point, GRC tends to be more dealing with the business and dealing with risk conversations and a little more esoteric than, say, the cyber side, which is more hands-on, more visceral, if you will, when you're being attacked like you said, you need to.

Eric Bowerman: Yeah, it is, and it's costing education all the way around. I was just listening to something here, uh, just before we got on, as a matter of fact, about artificial intelligence, which you can't throw a rock and not hit something with artificial intelligence.

Ed Gaudet: I'm glad you brought that up because we hadn't brought it up until then.

Eric Bowerman: Sorry, somebody had to do it. There's a lot of regulation going on that is coming down the pipe. And this already has their framework out or their guidance out. And then the EU apparently has some stuff that's going to have some significant impact for those that are dealing with if they're going to have some sort of AI that deals with their business in the EU, then they're going. I have a lot of regulation going on with that that they're going to have to start trying to figure out. And, of course, that the SEC guidelines and all the other the fun things that have happened, privacy. There's another, is it cyber? Is it not? It blends into cyber and compliance, which also bleeds into all that.

Ed Gaudet: But there's a really good paper that just was published by the Health Sector Coordinating Council. That and I did some work on it with the task group, but it basically unpacks the whole notion of privacy versus security and a very logical and thoughtful way. If you're interested in reading anything on that, take a look at that should be available on the Health Sector Coordinating Council website. But you're right with the AI it took that whole landscape and ecosystem of cybersecurity and risk management and accelerated our understanding of the impact and the risks and the threats and the vulnerabilities and everything about regarding AI in a very short period of time. We're still learning. We learn every day something new about AI. But the fact that organizations. I'm just giving one example today: I was in Acrobat, and I was downloading a couple of PDFs, and I was looking at them in Acrobat, and there's a banner that comes down across the PDFs that said, basically, that AI is available in beta. Click this button to restart the application accept it. And then there's another button that says Learn More, but there's no X to X out of this thing. So they want me to take an AI beta capability in a program that's pretty ubiquitous, which is I just think is crazy. And for CISOs like yourselves that are on the front lines and having to deal with now this every single day as companies are updating their software, it's not just, oh, we have this AI system now that we want to implement. Let's take a look at it. These things are coming in. They're insidious. They're coming in multiple different ways into the organization.

Eric Bowerman: Yeah. And my general counsel and my contract lawyers would have a problem with that, I'm sure because then you have an end user that's agreeing to something for the company.

Ed Gaudet: Exactly.

Eric Bowerman: That you don't know what the license is on it. So is the reason that they're doing that because they want more training data for their model. Is that a good thing or a bad thing? That seems silly to me, but.

Ed Gaudet: And it's Pdf, it's a general document reader. So you're pulling in all types of documents into this thing that now has AI-enabled because you just can't turn it off now. It keeps coming up, and you're finally like, all right, enough, enough. I'll accept it; I'll restart it or whatever. Exactly. Don't get it. Yeah. Anyways, it's only going to get worse before it gets better, but it is an interesting time for sure to be in.

Eric Bowerman: Yeah. I think the biggest challenge that we've seen was just in the phishing attacks and them getting so much better; they escalated quickly. I'll put it that way. It was going from yeah, I can see what that one is to it's indistinguishable unless you really have to look at every other factor, which most end users are not going to do. And I can guarantee my nurses' work. They just don't have the time. Again, I'm not blaming them for anything on it. It's that's not their focus. I didn't want the nurses to be cybersecurity experts. That's my job. Right? So we needed to make the tools, or at least the processes where it would get it out of their way so that they didn't have to worry about clicking on something. They could click away and not have to worry about going to a malicious site. It has. We did see quite a few AI-generated phishing attacks that came at us. Abnormal alerted us to those and said, hey, you guys are being targeted. This is not the first one we've seen on this. So they already had some of their own models, their counter models built up their counterintelligence stuff. They were able to block all of those things for us, which was great. But I also know that there's going to be a lot on the hey, can you help me develop this code? I really wanted to do this particular type of thing, and you can just be a little nefarious about it without actually telling it. Hey, go write me a malware, right?

Ed Gaudet: Yeah. And that's the analog of what's coming, which is being able to do this where we're hosting a Zoom meeting, and I'm telling you to go do something, but it's not me. It's actually not me. Although it looks like me, it sounds like me.

Eric Bowerman: There was a story. What was it three weeks ago? I think there was that guy in Hong Kong. Supposedly, he got on a Zoom call with 3 or 4 other people, and they all told him transfer the 25 million, and he did it.

Ed Gaudet: So exactly.

Eric Bowerman: It's wonder about that. Was it really six people on the Zoom meeting, and they were all fake? Or was it him just transferring 25 million because he wanted it? I guess that'll fall out eventually here. But yeah, I see the deepfakes being a problem as well, especially with the CFOs and such.

Ed Gaudet: So I'd be remiss if I didn't ask you this question. This is the Risk Never Sleeps Podcast. Eric, what's the riskiest thing you've ever done?

Eric Bowerman: It's funny. Maybe that's why I fit into cyber so well and risk management, because I've been doing risk management my whole life. I think I was trying to think about that, and I guess it has to just be skiing when I was a kid because I do still have the scars from that, and I get new ones about every ten years when they have to go redo my knee. So.

Ed Gaudet: Oh geez. Yeah.

Eric Bowerman: Yeah, that's probably the riskiest thing. I've never jumped out of a plane. I've never done anything too traumatic. No paragliding. How about that? I did paragliding.

Ed Gaudet: Paragliding?

Eric Bowerman: Yes. And I could feel myself sliding out of the little ropes.

Ed Gaudet: Oh, no.

Eric Bowerman: I was having a blast. She was having a blast. And I'm just hanging with the death grip on the ropes. So yeah, that was terrifying to me. That's pretty scary. Absolutely. Yeah. And normally I don't have a problem with heights, but I guess that would probably be the best one. Yeah.

Ed Gaudet: All right. So, music or movies for the next question.

Eric Bowerman: Movies have music in it. So I would have to go with that, I think.

Ed Gaudet: Movies okay.

Eric Bowerman: Yeah.

Ed Gaudet: If you're on a desert island, you can only take five movies with you. What would they be?

Eric Bowerman: So that one's interesting. I'd have to show you my poster collection behind me, but I've Star Wars. Any of the original ones okay? Or the original trilogy? We could just call all three of those because I think I still have those memorized.

Ed Gaudet: You got two left.

Eric Bowerman: Yeah. I always liked The Abyss. That was probably one of my favorites, and probably Blade Runner.

Ed Gaudet: Blade runner is great. The first one of the remake. The original one. Yeah. The originals.

Eric Bowerman: The nondirector's cut. You have to have that one because it has the, the the goofy voiceovers. But Harrison's goofy voiceovers are the best. And you can't find that anywhere now. It's it never existed. They did their own cancel culture on it. But yeah, that's sad.

Ed Gaudet: Those are good. So it sounds like you and I were playing the same game when we were 10 or 11 years old. You were playing D&D with your dad?

Eric Bowerman: I did a little bit of that. Yeah, and funny enough, I started doing it more. I got with my team in person last year once, and I bought that black Dawson britches.

Ed Gaudet: Oh yeah?

Eric Bowerman: From Black Hills Security and we bought my idea was to play it once. That way, we could get a tabletop in. We enjoyed it so much we bid three, uh, in a row, and we were just having a blast with it. So it's almost like being a dungeon master, though, so those skills are still useful. I'll put it that way.

Ed Gaudet: That's so cool. Last question. So, for folks that are coming into the profession either in cyber and or healthcare, what advice would you have?

Eric Bowerman: I think, especially if you're coming into cyber and healthcare, is look over all of the HIPAA regulations the HIPAA security rule anyway, and make sure that you have a plan for how to address it. So, make sure you have the policies in place. It's very holistic, honestly, and it's generic enough so that it gives you some leeway. Just don't go giving yourself enough rope to hang yourself with it. But make sure that all the policies that you have to have in place. What controls do I have? Are you doing encryption where you should be? Things like that. People just getting into cyber; I would say just dive into it. Having some sort of IT background would probably help. But if you're just coming out of college, hopefully, you've picked up some of that and then just do a bunch of different pieces to it as well. We talked about a while ago, I think getting into GRC, do I like this? No. Move it into Pentesting. No, I don't like that either. Hey, blue team, that's fun. That's where it's at. I love doing Blue Team and or innocent spots. Okay, that's where you need to be, then.

Ed Gaudet: Yeah, and I love that. And the nice thing about starting in GRC is you get connection with the business and why it matters right up front. So when you're doing these other, and you're in these other areas, you at least can go back to that connection to, okay, why are we doing this? What's the importance and what's exactly to the business?

Eric Bowerman: And there's another piece to that too, even from the blue team or in my position, getting out and talking to the end users, how are you actually using the technology? They may be doing something completely different than what you envision, but being able to see what they're doing and say, hey, I think I can make this easier for you, or I can make it more secure or better, or whatever little bitty tablet, you need a bigger tablet because I see you. You're struggling with it when it goes readers. Yeah, but that type of stuff.

Ed Gaudet: Where you're putting Phi in there, which is okay, but now we need a bar and we need additional controls.

Eric Bowerman: Yeah. Just because it's built into the tablet doesn't mean you can use it for sending Phi to somebody.

Ed Gaudet: Yeah, exactly.

Eric Bowerman: Exactly. Yeah.

Ed Gaudet: All right. That's great. We've been talking to Eric Bowerman. This is Ed Gaudet from the Risk Never Sleeps Podcast. And remember, if you're on the front lines protecting patient safety or delivering patient care, 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