CENSINET®

Podcast Transcript

Risk Never Sleeps
Episode 39
Jason Alexander

Ed Gaudet: Welcome to the Risk Never Sleeps Podcast, in which we learn about the people on the front lines protecting and delivering patient care. And I am Ed Gaudet the host. Today, I am pleased to be joined by Jason Alexander, the CISO at VCU Health. Jason, welcome.

Jason Alexander: Thank you very much. A pleasure to be here, and I'm glad to be on the podcast.

Ed Gaudet: Yeah, and I'm really blown away with your Grumpy CISO that, your new blog that you, I think you launched like in September, right? Just or maybe it was August.

Jason Alexander: Yeah, I'm on episode three. And so I, it's, it came out of one of the things that I'm passionate about, and one of the things that I think we have to do as CISOs and not just in healthcare, but all over is really, is education. And a lot of times, you'll see the CISO in the traditional roles and the risk management and the operations and the identity and access management space. And I think realistically, the way that the organizations are changing in the world is changing, and the malicious actors are changing, it's becoming less about firewalls and hardware and the pieces of technology that you can put in place. Certainly, they're still important. I think it's moving towards, and now that the user is the most important component of what we do on a daily basis, and I started writing this from the CISO perspective because I get a lot of people that reach out to me on LinkedIn and other various ways, and they're like, I just need ten minutes of your time.

Jason Alexander (cont'd): And I, we, our product, will change the world for you. And I appreciate that, I understand those people are working hard, and they're really trying to improve things, but I started this basically from the CISOs' perspective. I really give people the, this is what it's like to be a CISO, and this is what we see, and this is what we think through. And I'm hoping that people will find it useful and they'll go through. And so, like I said, we don't have very many topics out there yet. I just started writing it. I'm trying to get one a week out, but with my busy schedule, sometimes it's difficult. But working through the user piece right now, I've got to try and hit a large swath of topics that the CISO sees, and hopefully, I can continue to get more education out there.

Ed Gaudet: Yeah, that's great. And note to listeners, if you don't follow Jason today on LinkedIn, follow him, take a look at the blog series, off to a great start, some really interesting topics: identity, obviously, password management, phishing, which is great, we talked a little bit about that before we turned the recording on here, and other topics too. So I think, I highly recommend it, take a look at it, and I'm sure you're going to learn a lot. And I love the notion of sharing insights and driving empowerment, which I think was core to why you did this, which I think is really important.

Jason Alexander: Yeah, it's really important that the user understand kind of both sides of the coin. And one of the comments I made is that, especially in the healthcare space, everybody believes in the mission of healthcare. We wouldn't be in healthcare if we weren't, and if we didn't, and no user sits down on the beginning of their day and say, today's the day I'm going to give away my password to a phishing attack and destroy the entire hospital with ransomware. It doesn't happen. The, with the advent of AI and large language models, it's getting, the phishing attacks are getting super complicated and very good, even so much so that I got one the other day, I was like, wait a second, that's a phishing exercise, and that's the best English I've ever seen in a message.

Ed Gaudet: Yeah, no, they're absolutely getting better. And I have to stop off and look at them and think too, today, security starts at the home and starts in the home, and it's more important to ensure that we've got the right level of hygiene and the right level of insight and behavior, because if we're doing those things in work, obviously, it's bad. If we're doing those things in the office, it's obviously bad. But nowadays, those boundaries are blurred, right? The home is the work office. And any thoughts on that and how you take that message?

Jason Alexander: Yeah, absolutely. COVID changed the world, and we're not going. I know, you can open up LinkedIn or any other news site, and you can see there's ten articles on either side of whether people will ever go back or not go back. But for example, I'm 100% remote worker. I have a home office. I work out of my home office every day. My entire security team is remote. We are as productive, and this is not subjective, this is based on hard, real metrics. We are more productive remote than we were in the office, and I think that comes from the flexibility that we give our workers, the trust that we put in our workers. It really empowers them to do the things that they might need to do, but the work still gets done. And so using our own team is the starting point as we deploy controls and we deploy other things in pieces, we're always looking at how can we control the data, how can we control and protect the devices and the people? But how do we leverage these new tools and technologies to allow users to get work done wherever they're at? When we looked at, when we all dove into COVID in March and April of 2020, a lot of us put stuff together very quickly, put in massive upgrades to our remote access systems, our VPN systems, our remote technologies, our MDM devices, or all of that stuff. We certainly had all those things in play, but we were not prepared, like a lot of organizations, to send all of our non-clinical workforce out of the hospital. Obviously, our clinical workforce, they never got to go home, but all of our 7000 to 8000 non-clinical staff went basically remote, and we were staffed for a couple of thousand remote workers a day. We quickly put technologies in, we quickly built things. That's the world that we're going to live in going forward. The work happens everywhere now, and organizations need to be prepared to let work happen wherever it's going to happen, because even those workers that are being asked to come back to an office, they're still working at home. It's just not between 8 and 5.

Ed Gaudet: Yeah, yeah, no, that's a great point. So let's dive into your current role in your organization. Tell us about that.

Jason Alexander: Yeah, so I've been with VCU Health for about nine years now as the CISO the entire time, really came into a program that was, it existed, it was in effect, but really, over those nine years, we've done a fairly significant upgrade and retooling of the entire program. Now, I oversee all of the risk governance section, our security operations team, also our identity and access management, and then all of our cyber forensics and eDiscovery.

Jason Alexander (cont'd): So we support regulatory compliance, legal, HR, and then generally protect the organization from anything that goes bump in the night. So VCU Health is a regional health system in central and southern Virginia, and so we play the role of the large hospital system there with all of the advanced and specialized care.

Ed Gaudet: Got it, got it. And how did you get into healthcare? You got an interesting background.

Jason Alexander: Yeah, so that's a pretty funny story, actually. Actually, when I came out of college, my, in college, my intent was to work on satellites, space vehicles, and other stuff, and my formal bachelor's training is in electrical engineering with a specialization in communications. I actually came out and worked for an avionics and defense contractor out of school, and I was doing research and development on next-generation military communication networks. I've got some patents in self-organizing networks, and then actually was part of a larger multi-company team that worked on some of the first internet in the sky systems. You get on JetBlue now, and you hook your laptop up, and you get satellite TV and internet, that was some of the stuff that we were working on in the late 90s. But then 9/11 happened, and it wasn't such a great time to work for an avionics company. Everybody stopped flying, and since I had been working on my master's in information assurance at that point, mostly because I was going to be submitting defense contracts to DARPA and somehow fell into a healthcare leadership role in information security. So this was 2003, right after HIPAA had been passed, and my first healthcare job was with the University of Iowa Hospitals and Clinics, and actually went to that organization because the first finding that they had gotten from one of their outside consultants was hire a security officer. And so that was me. And so, from there, we we built everything because the hospital had all publicly routable IP addresses. Their opinion was, hey, we installed antivirus. We're good. So yeah, it was a, HIPAA was a big change for a lot of healthcare. So that's how I got into healthcare and kind of been there ever since.

Ed Gaudet: Yeah, I noticed you were at CarMax for a while too. What did you learn there that you were able to apply into healthcare, if anything?

Jason Alexander: What I what's interesting about CarMax is their model is significantly different than healthcare. Obviously, they're there to sell used cars. One of the things that actually, interestingly enough, shocked me about CarMax is I remember one time we were in an outage call, and the level of seriousness and just bluster around getting a certain system back up. I was tired that day, and I made the mistake of saying, you guys are taking this more seriously than when we would have outages at the last hospital I worked at; this is only used cars, and you would have thought that I had said something awful about someone's child, and so I learned very quickly that retail is not quite the same as healthcare. Obviously, in healthcare, there's a lot of backups and redundancies and checks and everything. Generally, patients don't leave the hospital when the network goes down. When you couldn't sell a car that, I learned very quickly, that was a much bigger deal. And so it was a very interesting experience, and I actually really enjoyed it. It was because it was a much faster pace than healthcare, a lot newer technology. In the end, I was recruited back to healthcare and came back to what I needed.

Ed Gaudet: Yeah, and it's that connection with the business that I think is probably, that's the story.

Jason Alexander: I never said that again.

Ed Gaudet: Yeah, you learn quickly. Yeah. So as you look at 12 to 24 months out, what are your top three priorities?

Jason Alexander: I think in the next 12, 24 months, it's really, for us, it's really, we, budgets are still tight from COVID, hospitals are still struggling. healthcare is still, we're, we'll never go back to what was normal before COVID, but especially now, there's a new wave of COVID infections happening. Everybody's looking to see is this going to impact us, some of our, some of the waves, like Omicron and others. So right now, for us, one of the things that we're looking at is really optimization. What can we do with what we've got that we're not doing? Have we gotten all of the benefit out of all the systems that we have in place? And so it's less about new systems for us right now. But really, we've also gone through a fairly significant shift in the last three years at VCU. We've replaced probably about 80% of our software.

Jason Alexander (cont'd): We went through a major ERP and electronic medical record project, we built a couple of new hospital buildings 15, 16 stories tall, we bought a regional care hospital, and a lot of change has happened in the last three years for VCU Health. And after all of that new system implementation and new software, a lot of what we're doing right now is really not necessarily stabilization, but enhancement and making sure that we're effectively doing the best that we can with everything that we've got.

Ed Gaudet: Yeah, no, that makes sense. A couple years post-pandemic, really hard for a lot of people. How do you think we're doing as an industry?

Jason Alexander: So I think, at least from my seat, things seem to be getting better. We've come out of the public health emergency, we've declared the pandemic phase of COVID being over, and COVID will be with us forever, and it's going to be like the flu. So I don't think it's ever going to go away. I think it's going to change the way hospitals operate and the way that we think about things. I think it showed us how quickly our world can change, and I think a lot of planning will be done around what happens the next time. What, if there is a next time, when everybody says they'll probably be something, it could be 50 years, it could be a hundred years, but it'll happen again, how do we plan and prepare for something like that? And I think as we learn what the new normal is, we learn how we're going to operate with, the labor costs have gone up because so many care providers decided that during COVID, they just, that wasn't what they wanted to do anymore. I cannot say enough for the people that were on the front lines during COVID, yeah, lots of good friends in the hospital that I know just had probably some of the worst years of their lives just trying to treat everybody and get everybody through this and to watch what happened, and it burned a lot of people out. It changed the way we think about a lot of things. I think everybody now is focused back on what our primary mission is, which is to help the greater good, and we're moving forward. And so I think things will change and get better as we go a couple more years through this, and we really start to understand, okay, this is what the new normal looks like, now we can plan for it.

Ed Gaudet: Yeah, that's a great point. I think it's also changed our perspective as it relates to cyber security in so much as we spent probably the previous decade thinking about identification and protection, and now it's more about becoming much more resilient. It's not a matter of if, it's a matter of when and when it happens, how quickly do we recover from the incident.

Jason Alexander: Yeah, that's definitely, again, so you look at, we look at the attacks that happened in the last couple of weeks. Again, I think this goes back to my beginning point, that training has become so critical because we're learning through the statements of the attackers that they gained access through social engineering. I actually have two days after I wrote my article that came out, and I just giggled a little bit. Not at MGM's pain, I would never do that to somebody else, but just, that's the world we live in now. It's not going to be a failure of your firewalls. It's not going to be a failure of your access controls. The biggest threat to any cyber organization right now is the user. And again, it's not through malicious action, it's not through intent, it's just through, it's hard, and the malicious actors are persistent, and they're dedicated, and they're good at what they do.

Ed Gaudet: Yeah, I think what makes it much harder these days, anyway, is that our users aren't just those people that we employ. It's the connectedness we have with our ecosystem. The boundaries have been blurred or removed entirely, and we have to consider the user on the other end that, our vendors, the user at the vendor, or the supplier or provider of goods and services that may be clicking on that phishing attack and opening up that breach for us. I think that's also getting harder.

Jason Alexander: My risk team is as big as my incident response team, and I have people that literally are dedicated into looking into these vendors and talking to them and working through their controls with them to make sure that they're doing the same kind of things that we're doing, to make sure that we're at least trying to all stay on the same level of risk tolerance.

Ed Gaudet: Yeah. What are you most proud of over the last couple of years, personally or professionally?

Jason Alexander: So I think one of the achievements, like I said, we rolled out a brand new ERP and a brand new EHR, and we went with workday and we went with Epic. Not all that uncommon in a healthcare system, right? And one of the things that my team did, in amongst both of those, and we went live with them six months apart. So we went live with Workday in June, and we went live with Epic in December of 2021, and I didn't really like 2021, and while we did that, while the organization did that, so my team obviously didn't run those projects, but we also implemented a brand new identity and access management system, and we went from a completely manual set of processes and procedures to one that is almost completely role-based access and basically was able to take the data that we were getting from our new workday system and automatically provision every user in our Epic system, based on what their job role was and what they were doing. And so we had some bumps in the night, but in the end, it was a fairly significant effort to get all of those pieces in play and built out. And then I'm pretty proud of that. The team did really well through all that.

Ed Gaudet: The nice thing, too, is now you have that round trip potential whereas people are leaving the organization as well, you can remove their access a lot easier than you might have been able to.

Jason Alexander: Yeah, real-time access removal is excellent. We don't have to get a list of people every Friday now from our HR organization to terminate. When they terminate them in Workday, they're just gone. They're gone. It is a significant improvement in security control.

Ed Gaudet: Outside of healthcare and IT and cyber. What are you most passionate about? What would you be doing if you weren't doing this?

Jason Alexander: If I wasn't a CISO, I'd probably be working in a boatyard scraping barnacles off a boat or something.

Ed Gaudet: Oh, tell me more.

Jason Alexander: Little, little Jimmy Buffett in me.

Ed Gaudet: Oh, yeah. Me too.

Jason Alexander: Growing up in Iowa, you wouldn't think it, but one of the things I spent a lot of my time doing is sailing.

Ed Gaudet: Yeah, me too.

Jason Alexander: So it's one of the reasons now I live out here closer to the Chesapeake Bay, but, yeah.

Ed Gaudet: Do you have a boat, I assume, or?

Jason Alexander: I do, I have a 43-foot sailboat.

Ed Gaudet: Nice. What do you have?

Jason Alexander: I've got a Juno 33 deck salon, so.

Ed Gaudet: Nice.

Jason Alexander: I go out and sail it all by myself all the time, and so it's quite enjoyable. So it would probably either be that, or one of the other things I do in my spare time is I actually work for a no-kill cat shelter, and so do a lot of what they call TNR, trap, neuter, and release of feral cats to try and control the population and generally try to help stray cats and others that happen to be in our area. So if I wasn't being a CISO all the time, it'd probably be one of those two.

Ed Gaudet: Yeah, very cool. I had the good fortune to sail aboard a Sparkman Stephens 43-foot.

Jason Alexander: That sounds like fun.

Ed Gaudet: It was a lot of fun. Yeah, I went to Bahamas. You've taken it to the Bahamas or?

Jason Alexander: I have not taken mine to the Bahamas, but I've done classes where I've sailed out of Miami, to the Bahamas, and then all the way through the the Caribbean islands, out to the Lesser Antilles. And so I did a big oceangoing class, NASA class, where they I sailed out of Miami and took the boat out there. And so it was, we were out for about, yeah, it was like 13 days or something. We bounced from a couple of nights, we were just completely out in the dark. And it's, I don't know, it's an interesting experience when you're out there in the water, in the dark and you're on a little 45-foot sailboat and there's nothing around, and you just hear the waves and the water and the rest of your crew down below snoring.

Ed Gaudet: Nothing like it, and someone's got to stay awake. So if you could go back in time, what would you tell your 20-year-old self?

Jason Alexander: So my mom would suggest that I've had a plan for life since the second I was born. I knew probably from a very early age, that it was going to be something to do with computers. I think my dad, who worked in technology for a very long time, plopped me in front of a computer for the first time, I think, when I was probably about 4 or 5, and it was the good old TI 99 4A, for those that can go way back in history in computing. And they plopped me down in front of this thing, and he said, these are going to be important someday, learn how to use this, and gave me a bunch of magazines and books and stuff to read. And I just started fiddling with it and playing games and writing code in Logo, and this was back in the day of the Apple Two, in the classrooms and everything, and so spent a lot of time playing with it and then just continue down that road. So one time I got out of college, I had this plan that it was going to be technology, it was going to be communications. It was going to be, I don't know if information security ever crossed my mind that early in life because I don't feel like in the 80s that we really knew what information security was. That concept of, nobody would be bad on the internet, this is all a bunch of scientists. We're all here to collaborate and communicate. Nobody would ever do anything. And then they got their world rocked when the first spam email came out. And I think the plan to do technology, the plan to move forward with some of these pieces, was always in place. I'm not sure I, my 20-year-old self, knew the plan was a good idea. I'd probably go back and say it works, stick with it. Don't doubt yourself, just keep going. Because like I said, I had come out of technology, went, right, like I went right into research and development.

Jason Alexander (cont'd): The company I started with, the guys in the research and development department, one of the guys invented the fax machine. There was a team of guys that worked on GPS that had invented the algorithm the GPS uses to calculate our position. There were guys that had worked on the space shuttle program. I came out of college, and I was like, I'm a college graduate, I know everything. And then I sat down with this group. I look around, I'm like, I don't know nothing. And it was shocking, it was like, wait, he invented the fax machine, and he invented the algorithm, and he worked on the space shuttle. Yeah, yeah, yeah, I got nothing.

Ed Gaudet: Last question. This is the Risk Never Sleeps Podcast, I have to ask you. What's the riskiest thing you've ever done, Jason?

Jason Alexander: A hot air balloon in Cambodia run by a group of Chinese that didn't understand the words, No smoking on the propane tanks.

Ed Gaudet: Okay, that's a new one. Listeners, that's a new one.

Jason Alexander: Yes. We're in Cambodia on a vacation, my wife and I, and we're going to take this hot air balloon right at sunset over some of the monuments that we're seeing in Cambodia. And we, the tour company were with takes us to the hot air balloon ride and everybody that's showing us around, everybody is speaking Cambodian. We don't understand any of the language. We're the typical American tourist at that point. And so we get to the location, and there's all these, they are setting up the hot air balloons, they're, they've all got some sort of Chinese writing on the side of the sleeves. They're all with some company that are running the balloons, and they've got the fans running. They've got all these big propane tanks around for the burners and everything. They're heating up the air inside the balloons, and there's three guys with cigarettes hanging from their mouths while they're running around these propane tanks. I think my wife and I questioned our sanity just a little bit before we got on those balloons, but it was one of the most amazing things we've ever done. I guess if you're going to do it, you just go for it.

Ed Gaudet: That's terrific, and that is a new one, so I love that. Before we end, any last advice to cyber professionals maybe just starting out in their journey?

Jason Alexander: Like I said, I think there's two things I'm really passionate about in the cyberspace, and things that I think that we need to do better is cyber leaders, and obviously the first is education. The more education you can do, the better. For people just starting out in this space, consume as much of that education as you can, learn as much as you can, and then be willing to share that information. I think the other thing that we as security leaders and security organizations don't do, and one of the things that I've been trying to change most of my career is we don't talk to each other enough. Sure, we get on LinkedIn, and we share stuff, and we have groups that were part of, and we join Infragard, and we share little bits of information here and there, but we as the good guys, we don't we're not sharing information the way we should be. The bad guys, they share everything. This company has this problem, this company has that problem, use this technique, this works really well against this software. You go out on the dark web, and you go into some of these forums, and it's amazing the amount of information they're sharing about specific details and hacks and the way that they're doing stuff. There are very detailed tutorials on how to compromise this, how to break into that. And here we are like, yeah, watch out for because one of the challenges that we have is we all have shareholder value, we all have organizational reputation, we all have these things, and when we get into these situations where something bad has happened, and we're going to know more and more of these bad things happen now because of the new SEC rules that are forcing companies to basically, at least publicly traded companies, to address any sort of material impact to their shareholders in filings when they have these cyber attacks. But we'll never find out the details inside of what happened to MGM and how we could all do better. We can all look at the news reporting. We can take what we can from it, but we'll never be like, hey, don't do this if, we saw this right before our 100 hypervisors got encrypted by the bad guy. If you see this, do something right away.

Ed Gaudet: Yeah.

Jason Alexander: Those are the kind of details that we don't share. And I just don't know, I'm always leery to say the government should fix it because the government doesn't always fix things. But I think there's got to be, and I'm happy to see the CISA is really stepping up from where they've been the last few years.

Jason Alexander (cont'd): But I think there's really got to be something where you can go to the FBI or the CIA or something and say, in a detailed fashion, this is what happened, and everybody needs to be communicated with, to watch out for these things, and it's got to be sooner than three months after the fact. We'll get some random message from the CSIA or Infragard or the FBI and 4 or 5 months with some random IOCs or something that were used in the MGM attack, and they're, the bad guys are already on to the next thing. And so those are the things if you can improve communication and you can improve user education, those are the two things that I think will do the best for most new people in the industry.

Ed Gaudet: Thank you, Jason. That's terrific. Great way to end the program. We've been speaking with Jason Alexander, the CISO at VCU Health. Thank you for your time. This is Ed Gaudet from the Risk Never Sleeps Podcast. 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