Podcast Transcript

Risk Never Sleeps
Episode 81
Alex Kot

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 Alex Kot, AVP of cybersecurity at, and I hope I pronounce this correctly, I was going to ask you, Aveanna.

Alex Kot: Aveanna. Yep.

Ed Gaudet: Oh, Aveanna. Aveanna Healthcare.

Alex Kot: Don't worry, you're not the only person to get that wrong. So it's common.

Ed Gaudet: And you're in Atlanta, I believe, right?

Alex Kot: That's correct. Yeah.

Ed Gaudet: Yeah yeah yeah. We've been playing the Braves recently. There's, I don't know if you're a baseball fan, but the Sox have been playing the Braves the last couple of days.

Alex Kot: Yeah. Our corporate headquarters is right across the street from the stadium, so ... that coming through.

Ed Gaudet: Excellent. Well, I'm honored to have you on the show. You sent, and we talked about some questions and some hot topics that we're going to get to today, which I'm excited about. But before we do, give our listeners a little sense about your role and your current organization.

Alex Kot: Well, first off, I appreciate you having me. I listened a few other podcasts, and I was very impressed with the topics and discussions. And so my current role, I'm a AVP of cybersecurity. Long story is I basically, five years ago Greenfield the cybersecurity program. So started from a director to AVP and basically kind of the company's ISO at the organization. So I went through a lot of interesting hurdles to get to where we are now, where I feel very comfortable state of our cybersecurity program.

Ed Gaudet: Excellent, excellent. How did you get into healthcare IT and cyber?

Alex Kot: So I've been in IT for pretty much my whole career path. I mean, I'm, I've been always a nerd. When I was in high school, I, you know, I was doing console hacking stuff like that. So it's just always been hobbies of mine. Started as help desk from, you know, started from the bottom at help desk to sysadmin, system engineering, security architect to, you know, where I'm at currently as the security officer at the company. So it's one of those things where it's just been a kind of a long going career path. I definitely worked in other career, which I'll mention in a probably in a few seconds, different industries such as payment card industry, retail, credit unions. Oh, wow. Okay. A little bit of previously in healthcare too. But this is definitely my biggest role when it comes to healthcare.

Ed Gaudet: What did you do in retail? Who did you work for in retail?

Alex Kot: So I worked for Macy's also. They're ITs headquartered in Atlanta; helped out with the purple team exercise that they have there and the Insider Threat Program.

Ed Gaudet: Excellent. Healthcare very different than retail in terms of a shared mission. What does that mean to you?

Alex Kot: It's very different. So and actually, I worked probably the most in the payment card industry in the realm of cybersecurity. And HIPAA and high tech doesn't really provide black and white, like these are the tools you need. So in the payment card industry, it's like you need a SIM, you need a laugh, you need IDs. It spells it all out there. So getting budget and approvals a little bit different process.

Ed Gaudet: Yeah. In terms of working in healthcare, how do you find that shared mission and the ability to, maybe articulate what you do to folks that may not be familiar with tech. Has that made a difference for you personally?

Alex Kot: It has. There's definitely a different level of obviously clinical support. So there's a lot more care for that. The healthcare industry compared to like fintech, obviously a lot more people are going to be technical in the fintech roles. And the end result, I mean, as long as you're able to basically take big concepts and explain them properly, most people understand. And even in healthcare, rolling out technology really wasn't that much of an issue. As long as you get the right support from the right leadership and kind of explain it properly and all the stages through that, the whole process, that building a cybersecurity program is my first rodeo. I've done it in the payment card industry. So that whole process of knowing what's going to happen and explaining that to people definitely helps a whole lot.

Ed Gaudet: Yeah, you've obviously you've seen a lot of change over the last couple of years in healthcare as it relates. And speaking of change, let's talk about the recent Change Healthcare incident. You had mentioned some claims coming from the PCI side, and I'd love to get unpacked that and get more information from you about that.

Alex Kot: Yeah, it's something that I think is a really good analogy that most people don't really think about. It's mostly the complexity of healthcare and the approval process. Obviously, you know, there's multiple parts of Change Healthcare that got hit. Their biggest thing was fix the pharmaceutical side. But a lot of it comes down to clearinghouses and claims management. Prior to this, you know, I had an already good relationship with our chief revenue officer who's over the claims management.

Alex Kot (cont'd): And, you know, when this happened, I was dumbfounded of all the stuff that I really wasn't aware of and getting into the weeds of it, but essentially, to explain on the payment card industry, because everyone has a credit card, no one knows really the back end as much. But it's a very simple. You have a merchant service that basically issues the card, and also sometimes merchant services are also the ones that do the point of sale terminals. So you swipe that card, it sends it to a transaction processor, like first data is a huge one, and they go through a back-end data. And then that process says that, Hey, you got the credits or not? And then it also first data or the whatever the transaction processor works with your bank who basically, you know, ... issue those funds through. So it's not really that complex. In the same exact scenario, you have your hospital system, sometimes you have claims management portal software you go through that basically aggregates because you're going through, we have like almost 300 payer portals we go through in our organization. And a lot of that's consolidated through some applications, but a lot of it's still manually through directly to the parasites. And then the clearinghouse will be which will be essentially Change Healthcare. Then that goes into the actual patients, you know, information. They have all that and they process that and then they get move the money back over when they submit the claims to our bank. So not very different if you think about it. There's a, you know, somebody that takes in that transaction process, which will be your clearinghouse. But in the circumstance of, let's say first data goes down. And a lot of organizations, they don't really rely on just one transaction processor. They could balance it. They could even if they want to code it, you could actually have up to a certain number of credit cards. We'll go to one transaction processor, another go to a separate one. So you could even have like almost a year built into it. And the scenario of a clearinghouse where a Change Healthcare goes down, in order to take that patient to another clearinghouse, there's a remittance process which has to get approved, and sometimes that takes up to 45 days. So imagine either losing your credit card, you have to wait 45 days, or the place you go to every day for lunch. Their transactions processor is broke and you can't use your credit card for 45 days. So loss that would be like, That's a deal breaker. I'm not using credit cards anymore. We're going back. But in the healthcare industry, that's kind of the norm because there's a whole approval process. And a lot of it is because, you know, you go through Medicaid. So even though Change Healthcare is doing that, they're going through Medicaid and through the payer site on that. So it's very complex.

Alex Kot (cont'd): And that's one thing that when we get through the scenario is like finding out all the entities that actually go through Change Healthcare because they're hidden behind either some payer portal that we didn't know that they use them as a partner. Sometimes they're exclusive. We go through a transaction processor. It's rare that you can't find them supporting a bank that you want. It's all, it's ... They were out the account over there. If they don't have it, they could spin it up in a few days.

Ed Gaudet: That's a great point. There's an opportunity to re-architect that system in a way that would provide that resiliency, if you will, the ability to continually transact, regardless of whether or not change or some other entity went down, similar to the PCI-DSS example that you just gave. That's a really great idea. Do you think people are thinking about it that way?

Alex Kot: It's slowly thinking about it. It's going to take a lot to change that process, but because of how large impact this was, it's interesting because I talked to a lot of the people in claims. You know, they always said that they didn't really know how big the picture Change Healthcare/United Healthcare Group was. And I said, Well, now we know; it's 1 in 3 transactions. So like it went from like we didn't really know how big of a problem it was to wow, this is a huge problem. All due to that. A lot of the, you know, our claims management software, they're working very closely with us and they're looking at how to balance things properly and look at kind of a VR side of things, which I'm not sure if they were even thinking about it at that time. And it's definitely opened up a lot of eyes, but switching a patient to another portal or that whole process, that's something that I think we need, eventually, I think government will have to step in and lobby to find a better way to address that.

Ed Gaudet: Yeah. There's a great quote by Mike Tyson. Everyone's got a plan until you walk into the ring, get punched in the face. So I think we're learning a lot. And you know, that's one of the consistent comments I heard from people that they had no idea the breadth and depth that the tendrils that Change had into their organization and business processes. So lesson learned. We got to do something as an industry to make sure it doesn't happen again.

Ed Gaudet (cont'd): You know, there's a lot of work outside of healthcare on, you know, making, moving accountability of cyber at the board level. I know the SEC is working towards that as well. Any thoughts on that in terms of that? Because obviously, you've had experience outside of healthcare. I love your perspective on that.

Alex Kot: It's a great thing. I feel like a divide in the security industry. A lot of people, like, especially the new SEC law and the CISO from SolarWinds, can prosecuted. A lot of people think it's kind of bad because it puts too much pressure. You know, it will make people want to not have CISO roles in the future. I find it different. I think that if you do it properly, which, you know, I'll probably talk about the cybersecurity steering committee and how you kind of disseminate that level of risk and responsibility so that you're not the fall guy. That does happen. But also when it comes to the SolarWinds person getting targeted, it's actually, I'm a firm believer it has nothing to do with cybersecurity the way he's targeted. They do the same exact thing in the past two previous CFOs. And their main goal is that if you personally prosecute somebody, there's two options. Hopefully SolarWinds is smart enough to pay a good personal lawyer for him for that. They don't dig up. But they can get more information out of by going to the person directly. And if their information is different from what the company is providing, because it takes a lot longer, because they got a full legal team and a whole process to go through, if they can get information directly through him, then they could actually take that and go directly, basically break down the doors of SolarWinds at will once they prove them wrong. I think it's more of a, it's just the process they have of doing that. But I think in general, it's good to have that oversight because cybersecurity is not going away. It's becoming more and more problematic. It's good to have that visibility and provide kind of that growth and non negligence, especially as a publicly traded company.

Ed Gaudet: Yeah, it's a great point. And it really raises the stakes for governance. And having, as you mentioned, a cybersecurity steering committee. And I think more and more organizations are moving to that. Your thoughts on the power of a committee versus a single function or group?

Alex Kot: So there's two caveats why we built that. And it's interesting because like a lot of people discuss like getting buy-in and power and like.

Alex Kot (cont'd): At that time, I was a director, so I wasn't a VP, so a non fiduciary. I didn't have a signature financial authority. So I got, I partnered with our chief compliance officer as a director and explained to him why this is important, and we put it together. And since then about, you know, almost like five years ago, we've been having monthly meetings. And so it's a twofold. So it's not only just to basically right education in the company. I mean, when we rolled out multifactor, we knew that there's going to be hurdles. Nobody rolls out multifactor without, you know, any hiccup. But because.

Ed Gaudet: Revolt, revolt of the organization.

Alex Kot: Yeah. Well, actually really wasn't that bad. We did a really good job of communication and basically just hands on, like we rolled up the sleeves. We were bunkered down in rooms trying to roll it out. This was like, you know, at the beginning when I built out the program five years ago.

Ed Gaudet: Yeah. And the technology has matured. It's come a long way. So it's a lot easier to, the modalities are, you know, much more friendly, if you will.

Alex Kot: Yeah, yeah. No, we use ... and the push prompt and education around; that was easy. It's still adding additional step to everyone's life. So no matter what happens, it's always going to be a loss in some situation. But as long as people understand it while you're doing it, you're not being intrusive, you're there to, willing to help out, it was super easy. So the steering committee, you know, you provide education around things that change the organization. We also provide growth patterns. We use Jira tracker projects. I'm a firm believer of your standard metrics of like how much our IPS block, our email gateway block this amount of emails or stupid numbers. They don't provide any value. But showing that how much, you know, applications you adopted through multifactor integrations with your SIM, how many more log sources you're pulling growth from that, and just providing that every month provides that non-negligence factor. But it shows that your program is not stagnant. By doing that also, if something bad happens and they want to go attack you, you have discoverable presentations, notes that shows that you are putting effort into the program. You're not negligence, and things happen and people understand. But at that point, you know, there's a whole committee of people.

Alex Kot (cont'd): So it's either you get rid of all the VPs of the company and go under instantly, or realize that you're doing the right thing and you're moving it without being in a silo. And that's I think the hugest power to that steering committee is that there is no one fault. But also at the same time is that the whole company is fully aware, so that everyone appreciates where you're going.

Ed Gaudet: No, that's a great point. And I'm seeing a huge driver for this as being AI. Obviously people are building governance committees around AI and how they think about dealing with risk and assessing risk of AI at a cross-functional level. And how are you dealing with AI currently?

Alex Kot: I'm thinking a, kind of a more simplistic approach. I'm not really, you know, trying to say against it or block it all or, but we already put together kind of a classification handling policy. So the company as a whole has all the documentation information of what's internal, confidential, restricted, internal use only. So we know what's sensitive or not on top of our HIPAA guidelines. I view it as whatever AI is, and we, I actually did a presentation of explaining AI and all the terminology; they got in the weeds too. But not to that, the leadership connect where, you know, took a more high-level approach. But I explained to them, like how that works and why it's important and you know, it is a self-learning machine. You go a ChatGPT, you type in a prompt. It's not like a Google search where it's just taking that prompt and going and fetching data. It's a relearning off your prompt. So basically the main thing is that if it's any public information, then that's fine. But anything outside of that, you know, confidential, internal, user-restricted, you should never, ever place an AI, even in a prompt. And then we treat it just like any other third-party software. So that's kind of the goal that we're sticking to just to make it less complicated, getting in the weeds of all these one-offs and what-ifs. You have co-pilot license, which is super expensive, which I don't think most companies will be able to afford. It creates a level of complexity, and I rather just keep it simple for most people for the time being until more information comes out there, better ways to handle it.

Ed Gaudet: So mostly as an enabler and an individual enabler for productivity purposes or other purposes.

Alex Kot: As long as people are fully aware of what public information and what is sensitive, and as long as you're doing that, I don't think it's really much impacting.

Ed Gaudet: It's a great approach. And then do you feel like you'll be applying it internally for any of your business processes in the near future?

Alex Kot: I mean, we do have security tools that have natural language processing or an email gateway. We have a chatbot we use for a lot of support, FAQs, and password reset. So we do adopt AI. Now into the sense of like what Meta or X or Google is doing; not even close. But I don't think most companies will probably even get there in the next ten years in what they're trying to do.

Ed Gaudet: Yeah. So let's kind of shift and talk about the people process tools. And specifically how do you think about. When you talk about building out your program, did you take an internal approach to it, or is it more of a hybrid where you're pairing internal people with an MSP capability, or how do you think about that?

Alex Kot: We did have an MSP for a little bit, and that's one of the lessons learned that I had. And it really depends. I mean, there's nothing wrong with an MSP. Some organizations don't have the internal talent. They need somebody else to help provide that. But if you're a company of our size, we're publicly traded, we're basically 2 billion of revenue, and we have the ability to basically in-house if we can. So we took that approach when building out your tools, if you've never done it before, my recommendation is just to basically kind of get an idea of what it really takes as a quote-unquote ransomware group or adversary, like a, you know, nation state sponsor. You could hire companies. There's plenty of them out there. We use Trustsec initially, and they basically did an adversary simulation. A lot of people call it different things, but it's basically an unskilled pen test. When the ransomware groups come in, they're not going to be like, Oh, well, that's their second network. We can't touch it so might as well treat it. As long as you know, the pentesting ferm you use is competent, it rarely come across issues nowadays. So having that provides of what your biggest weaknesses are. If you're green fielding, you know, I always start with like your email gateway multifactor; there's free stuff you can do that are huge wins like system hardening. Microsoft has a lot of good templates on that.

Alex Kot (cont'd): And that actually, interesting because, our equity partner, we're talking about this stuff. And when they went through the adversary simulation, they realized that out of all the stuff that they could buy, the best one that they recommended was free system hardening guidelines. And if you're a pen tester, you kind of know this like you know, SMB signing why that's important, how you could get hashes on the network through LNR responses. So there's technical aspects of there. When you're in that red team side of like, Oh, this is easy wins. But you never really think about it as, you know, higher level management. You know, I had the fortunate side of being every component of an IT and cybersecurity program at one point. So having that knowledge is like, oh yeah, definitely, let's spend more time initially on this because that's like, that's actually gonna piss off the red teamers. And if you piss off the red teamers, you're doing an amazing job.

Ed Gaudet: Yeah, exactly. So, you know, as you think about your program and you're in home health care marketplace, what's different about what you're doing, say, to a normal or to a health hospital? I wouldn't say normal because everyone went to a hospital.

Alex Kot: So it's interesting. If you classify it or organization, some people will want to classify it as a staffing company, which I find is kind of a disservice because there's obviously clinical support. We have to provide training and making sure that the notes are there. We do pretty much a lot of the stuff that any hospital does, but the big difference is that we don't have facilities that have like x-ray machines or MRIs, and that's a big issue with a lot of hospitals, those are vendor-managed devices. And yeah. It's been getting a lot better from what I've been told in the last few years. But those are still like.

Ed Gaudet: Problematic.

Alex Kot: Problematic. And it's always interesting because like when you think of a dialysis machine, you're like, Okay, why is it hard to get the vendor to support updates and all this stuff? And then you realize it's the same organization, the FDA, who tells what is the definition of what cheese is and the molecular structure that never changes also has to tell you, like, what is the, is ... a good wireless protocol or not, like the same organization has to decide that. So I can see the hurdles. And since Covid, they've been actually increasing and improving a lot over time on that.

Ed Gaudet: Yeah, that agencies have been evolving as well and things are definitely going in the right direction there. But you're still a covered entity or.

Alex Kot: Yeah, we still have the liability for our caregivers. We have to provide training, the clinical notes, all that. We have our custom EMRs that we have for all them. It's actually, and in the other side is that we're a little more complex because probably in five years we acquired 30 companies. So we were very heavy in merger and acquisition and we actually had to step in with an acquisition team, and I kind of worked through a better process in which definitely saved us because a lot of companies I see when they do acquisitions, there's a lot of steps in that process they do it wrong. And acquisition teams, their job is to get it bundled up and be one and done.

Ed Gaudet: Integration is always the hardest.

Alex Kot: You're never going to come back to it, so you're stuck with that. So we work with them closely and making sure that process is done properly. And you know, I've seen organizations do two-way trust where their domain is like full of all these companies. I'm like, That's a nightmare. That's about to happen.

Ed Gaudet: Yeah, multiple email systems like just standardize on. And so as you extend your presence, are you going into different states as well, or are you staying in Georgia or?

Alex Kot: For the most part, for some acquisitions in the past, we went out there for, but a lot of the stuff can be done remotely. It's not as complex. I would say pretty much the majority of my, since Covid, it's been, I go in the office almost like probably about four times a month now. A lot different now. So perspective and changes of, you know, what's needed. It's a little different.

Ed Gaudet: Yeah. Yeah, yeah, certainly it's changed over the last couple of years. So you know, as you think out over the next 12, 24 months, what are your top three priorities?

Alex Kot: We recently took over identity management. We automated a lot of that. We actually have it to the point where it's mostly coded and scripted.

Alex Kot (cont'd): So it goes from like the process of we pull data directly from our HRS system and auto term, auto provision. When they're terminated, we actually put an out-of-office notification on their email saying that, you know, they no longer work at the organization. We isolate their laptop. We have a lot of process involved, which I haven't seen a lot of organizations do out there. So we've just got kind of done with the majority of that process. And we're switching over to the asset management component, making sure that whoever has laptops, we actually tie it together with our security tools and monitor, you know, who is actually the right user, are they following the proper process, which another thing, both de-provisioning process that we created and that asset management process we're creating, I haven't seen a lot of organizations really integrate.

Ed Gaudet: Yeah, I know it tends to bite people, you know, terminating employees and their access. For whatever reason, seems to be the long pole for a lot of people until it gets them in trouble and then they recognize it. So it's good that you're getting, you know, your forward thinking there.

Alex Kot: It's not an easy process because our biggest problem, which I'm sure all organizations deal with it, is the naming consolidation. So you have different naming standards in different systems. So as long as you know that, you know, we use workday, which is our HRS system, that's our source of truth moving forward. We then reconcile all that data going back to that whatever system it is and then use that moving forward. So that helped us out a lot.

Ed Gaudet: Yeah. No, that makes sense. What keeps you up at night?

Alex Kot: So ironically, it's more, so recently we took over our infrastructure team. We moved level three, which is all of our sysadmins, networking, and other components under myself for a security-first approach. Our cybersecurity program is very mature. We've caught a lot of cool stuff in the past, but our infrastructure team, since they report to me, I would say they keep me up a little more at night because operationals never is always an issue.

Ed Gaudet: Yeah. 24 seven.

Alex Kot: Yeah. So I would say that keeps me up more at night than actually my security program at the moment, which is rare because most people always freak out about security program. But.

Ed Gaudet: Yeah, well, it sounds like it's new in terms of, you know, your purview. So I'm sure that'll settle down. Over the last couple of years, we went through a pandemic, obviously tough on a lot of folks. What are you most personally or professionally proud of?

Alex Kot: During the pandemic, we did an amazing job converting the last few people over to laptops. And I don't know if it was luck or forward thinking. A lot of our applications that were either SaaS-based or externally exposed in our data center. So a lot of people did software from that model of they had to be connected to the data center for a lot of the, you know, web proxy and stuff like that. When we went from work at home for most of our corporate, none of that really changed. And a lot of the tools we have, you know, our EDR that communicates through the internet, we pull Sysmon and Windows events through ..., which goes through our elastic, and that's all externally exposed to. So we were able to basically pivot and have the same exact information if they were on the VPN or if they weren't on the VPN. That definitely helped us a lot.

Ed Gaudet: Excellent, excellent. Outside of your day job, outside of cyber and healthcare IT, what are you most passionate about? What would you be doing if you weren't doing this job?

Alex Kot: I've always been a big gamer.

Ed Gaudet: Ah, I knew it! I was going to ask you that initially. So what's your go-to game?

Alex Kot: First-person shooters, I play a lot. So, Apex, call of Duty. I used to be huge into a game called Titanfall. I did actually some competitive on that, but I'm older now, so people that are ten years younger than me, like some of my coworkers, we game and they're ten years younger than me. And like, their reflexes are like insanely fast compared to mine. I'm like, Was I ever that fast, or am I just getting old now? Well, it's hard.

Ed Gaudet: Yeah. Did you play D&D ever or?

Alex Kot: Oh, yeah.

Ed Gaudet: Yeah, yeah, I was a big D&D player. I wish I still played. I know people that still play the game. I don't know if you do or.

Alex Kot: I have some friends that do. It's called d20, where they go on and they remotely meet up with people to play D&D.

Ed Gaudet: Oh, cool. Oh, interesting.

Alex Kot: It's definitely evolved.

Ed Gaudet: Yeah, I'm sure it has. So if you could go back in time, what would you tell your 20-year-old self?

Alex Kot: Definitely stick to the career path. But I would say one thing I learned in life is you got to put yourself out there. I created a lot of cool tools in the past and as hobbies, but nobody really knows who you are unless you put yourself out there. So that's one huge thing I learned is that you just go out to conferences. You know, when I was younger, public speaking was not my forte. So it's definitely something I learned over time. But if I was able to force myself at a younger age to do that, you know, I'd be miles ahead of where I'm at currently.

Ed Gaudet: Yeah. No, I agree with you. I froze up early in my career, public speaking, and it really just forced me to figure it out. Like what happened? Why did I freeze? And it came down to really a simple lesson, which is you have to practice; no matter how well you know the material, you have to practice. And that's what made Steve Jobs such a great presenter. He literally would practice insanely for any presentation, and he made it look simple. He made it look natural.

Alex Kot: But you can tell he's super analytical because when you pause, there's a deep moment of thought, which people like, you know, me and you, I'm sure we're both kind of like a little introvert analytical.

Alex Kot (cont'd): So it takes us a lot harder to do that public speaking part, but analyze a complex system, it's easier for us, though. You can see Steve Jobs was like that. You understand those complex systems but also had that guilt.

Ed Gaudet: Yeah, a lot of people don't know this. You probably know this. But he worked at Atari in one of his first jobs. A really interesting guy. All right. I have to ask you this question, Risk Never Sleeps Podcast. What's the riskiest thing you've ever done, Alex?

Alex Kot: So I wasn't, like, huge into the console hacking scene. So it was definitely some like gray areas at that time. And let's be honest, if you're a kid of the 90s, everyone either had a friend that knew how to use Napster or somebody that used Napster. So it's definitely more of a faux pas now. And I think it's awesome because like streaming services, like I don't mind that stuff. Like I'll pay for all that stuff because of how easy and convenient was. Back then that wasn't the case. But it was definitely an interesting scene kind of the developers, the custom homebrew applications, the emulators. And this is like the original Xbox, you know, going in from, at the end of my high school, like in 2003, 2004, and all the software modding. But it really got me into like understanding security a lot because like, there was like to do a softmod, you have to do a phone exploit. So you're doing a buffer overflow attack on a game to render your own custom dashboard. From there you overwrite files. It was something that I did because like, I got this Xbox and I could go to my friend's graduation party and they're all playing like old school ... on an Xbox. And it's cool ... Like people from the pool were coming out to play games. But ironically, it got me kind of that mindset of understanding cyber security.

Ed Gaudet: Yeah, that's a great example. Music or movies. If you were on a desert island, what would be the top five albums or movies that you would bring with you?

Alex Kot: Ooh, that's a good question. I'll probably go with movies, and like more complex movies that I could watch and relearn. I kind of think of like movies that I think that I could probably rewatch a bunch, like something like Donnie Darko. Like, I think I watched that a few times.

Ed Gaudet: That's a great movie.

Alex Kot: And like, there's still something you learn each time because how complex it is. It's a great movie. I wouldn't say it's the best movie out there by any means. But it's definitely something I think I would benefit of rewatching.

Ed Gaudet: Any other one? That's a good one. That's really.

Alex Kot: There's a lot of good movies out there that I could probably ramble off. I always love watching Shawshank Redemption.

Ed Gaudet: Yeah, that one comes up all the time. Yeah. This is the first time Donnie Darko's come up, though, so I appreciate that.

Alex Kot: I think it's something that I could probably watch, like I only watched a few times in the past, and I loved it each time, but I think if I keep rewatching it, I would learn something new.

Ed Gaudet: You see something different. Exactly. Yeah. All right. Hardest lesson in your career?

Alex Kot: You know, I would say, which also got me into cybersecurity. I did a lot of IT consultant for various companies. There's a home remodeling company in Ohio, and he's a super awesome guy, the owner of the company. So I built them a custom file share, redid all of their applications for their accounting software. So I was just kind of like their one-man IT person that came in, you know, like 10 to 20 hours a week. The file share actually converted over to Linux SMB. But the biggest mistake I made was, I, you know, I needed a support remotely. So I had an SSH publicly exposed, which is not a bad thing, but the password I had for root was a funky way of spelling the word password, so it wasn't really that complex. And again, this is like 2006, maybe very early on in my IT career path. And I was out there one day and they were saying they're, the network share was having issues. And I got on there and I realized that somebody installed a botnet on there. And this was interesting because like, botnets were still kind of a new concept. And luckily I used a custom distro called Gentoo. So it was, the packages were different, so they tried to install other packages, ironically broke it more versus actually did anything damage to it. So I was still able to get in there, pull the files and rebuild it.

Alex Kot (cont'd): So it wasn't like the end of the world, but at least gave me the warning that a botnet was installed because they did something different, the package didn't install properly. And going through the actual command line of what they were using and installing was interesting. It was like some IRC channel added in France. It ran some weird commands and it almost felt like there was like a kid on there trying to type in certain things. So like when you go through incident response and forensics, like you always plan to like go through those processes and question like, Why did they do this? Why did they do that? You know, it was very fast, but it was rebuilt that server, didn't sleep that night. And next morning, their file sharers was working, and he was super appreciative of it.

Ed Gaudet: Yeah. Excellent. Last question. What advice do you have for folks that are breaking into cyber or health care as they start thinking about pursuing a career?

Alex Kot: First recommendation, look up your local B-sides. There's always B-sides in most major cities out there, so you could always get an interest of your local talent. 100% conferences make things easier to get in the field. There's a lot of certifications out there that are good for offensive security. I feel like defensive security needs something better. It's actually something I put together as a purple team village. There's two conferences I go to: Space Hack Con in Orlando and Red Hack Con in Louisville, Kentucky. So if you go there, I'll, you know, I'll have that purple team village, but it teaches a lot of the incident response, blue team side of things that you could actually take back to an actual corporate environment. So I feel like that education definitely needs to be there. You know, there's certs out there like sans, but they're really expensive. They're good. But you know, I wish there was more things out there that somebody, you know, more entry level could take something and then literally get that knowledge and apply it directly back to the corporate environment. And on the defensive side, I haven't really seen a whole lot of that.

Ed Gaudet: Yeah, that's great.

Alex Kot: Like conferences is huge.

Ed Gaudet: Conferences. Yeah. You got to get out there and you got to talk to people and you got to see what's new and stay obviously up to date, because every day risk never sleeps. Every day something new is coming out. Right? Well, Alex, I appreciate your time. Thanks for being on the show. This is Ed Gaudet from the Risk Never Sleeps Podcast. And if you're on the front lines protecting patient safety and delivering patient care, remember to stay vigilant, because Risk Never Sleeps.

CENSINET®

Censinet RiskOps™ Demo Request

Do you want to revolutionize the way your healthcare organization manages third-party and enterprise risk while also saving time, money, and increasing data security? It's time for RiskOps.

SCHEDULE DEMO

www.Censinet.com