Podcast Transcript

Risk Never Sleeps
Episode 53
John Frushour

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'm pleased to be joined by John Frushour, Vice President and CISO at NewYork-Presbyterian. Welcome, John.

John Frushour: Thank you.

Ed Gaudet: So tell us about your current role in your organization.

John Frushour: Sure. Well, you have the title right, you have the traditional infosec CISO roles, vulnerability and risk and forensics and engineering and SOC and all. I mean, it's the standard kind of pedigree for any CISO of any large institution, I guess, not too much different here. I have a few more responsibilities around, like email and Azure, and cloud footprint stuff is probably gone too.

Ed Gaudet: And how about NewYork-Presbyterian? 4600 beds, I believe.

John Frushour: Yeah, yeah. Good research. So not as many hospitals probably as organizations of similar size. But for us, a hospital is not like three buildings. It's like 25. So our campuses are quite large, sometimes better known by our teaching hospital affiliations with Columbia University, Columbia doctors, and Weill Cornell, Weill Cornell Medicine.

John Frushour (cont'd): Most people just call Cornell. But several hospitals, around four of the five boroughs of Manhattan and kind of, I think a brand name in New York healthcare.

Ed Gaudet: Is that Ithaca, right, you get up to Cornell at all or?

John Frushour: Cornell University. So Cornell is like a mini-headed organization. So Cornell University, which we would call like the schoolhouse, is up in Ithaca, just like Columbia University schoolhouse is in Morningside. And, but we have affiliations with their medical education side. So we have affiliations with their clinical degree programs, a resident education, graduate medical education. And then, of course, their doctors largely work in our hospitals. So it's a great partnership.

Ed Gaudet: I did some research on your background as well. So thank you for your service. You were in the Marine Corps for a while.

John Frushour: Retired. Yeah, yeah.

Ed Gaudet: Tell us how that uniquely sets you up to be a CISO in healthcare.

John Frushour: Wow. Probably one to disparage my alma mater, but I don't know that was uniquely set me up to be a CISO. First, the military is a little bit different around that type of thing, but I did eventually, in my career, I became a communications officer, and that set me up to really explore my nerdery, and I kind of locked in on networks and networking and network design. My twilight tour, my last tour, I worked for a branch of the Acquisitions Command, a testing facility on California, where we would kind of test all manner of tactical networking and communications equipment, transmission systems, and landlines, and data center equipment, servers, and everything. And that set me up to kind of understand the the civilian side of it, the commercial side. I got a lot of certs with Cisco and with Palo Alto. Back then, Palo Alto was the, generally a new company. But, you know, with heavyweights like Cisco, got a security cert, got my ..., and kind of started to recognize that, oh, there's a world outside of a uniform, and it's a lot bigger.

John Frushour (cont'd): Yeah, eventually kind of drank the security Kool-Aid once I landed in the private sector and then just kind of matured from there, as I think a lot of security engineers saw that path, like networking, security, database security, service desk security, the kind of maturing the security, and so that was my path.

Ed Gaudet: Was that in 29 Palms, or where?

John Frushour: I was everywhere. So my, that that particular command's called McChesney Marine Corps Tactical Systems Support Activity. It's in Pendleton. If you ever drive in south on the ten you'll see those like two giant golf balls right on the beach, and that's the command right there. Those are actually big radar units that we test. And yeah, right there. But my job took me, like I was forward deployed a couple times servicing and supporting the, those communication systems that we put out very technical, complicated systems that that the Marines often don't have time. They're busy blowing stuff up and saving lives and forward deployed with them. What we call the stumps for 29 Palms was there several times for testing exercises, East Coast, West Coast, overseas, and non-tactical environments. All that job was, definitely took me to a lot of places.

Ed Gaudet: And how did you end up getting into healthcare? What was your first healthcare tour?

John Frushour: A little bit, because I had a, I worked for Motorola for a little bit, but during the split, and eventually landed in Nuance Communications, who makes pretty much every voice recognition technology you've ever heard of. And they had a healthcare division, and so a little bit of experience there, but really came to NewYork-Presbyterian, I think, was my first formal healthcare role. I think it was, security is not, it's not so specific that it changes drastically. There might be a little bit of a different focus depending on the vertical, but I don't think information security is so unique in that you can't port it between financial services, healthcare, retail, logistics, commerce, even government public safety.

Ed Gaudet: Yeah, no, that's a great point. And I did a little research, a little more research. I noticed, you set up the SOC at Nuance. What was that like?

John Frushour: I think you're probably talking about Motorola and at Nuance. I did, but I think it'd be a, better let me mutate your question a little bit, it'd be a better narrative to talk about the SOC Motorola, because of the kind of ... that it became for so much top talent out there. Motorola's focus was on those local institutions, those local fire departments, police stations, government facilities, and they were kind of like a managed service for all this stuff, providing radio, Wi-Fi, streaming media, all this kind of stuff. And the security operations center there was really unique. This is at a time when SIM was still with a promise, Sword didn't exist yet. Our network perimeter was mostly still at the network edge. That's where most of the threats landed that we cared about. And so I'm really proud of the security operations center at Motorola, kind of mutating and being forward-thinking enough to start looking inward and developing tools, one of them was called Radar, tools, and technologies that looked inward to these buildings, these facilities. There's okay, there's nothing on the firewall, but yet, all the doors to the evidence locker room magically went unlocked at midnight. I'm making this up, but I think it was really novel that they started that. At Nuance, yeah, we did a lot of the same things at Nuance. Nuance is a development company very focused on development and pushing code out to hundreds and millions of TVs, and phones, and little desktop devices, and things that are listening. SOC at Nuance is a lot different. You're mostly concerned about data center security. But yeah, that was just kind of a, I don't know, feather in my cap at Motorola. Some of the talent and the engineers that you've their names today as like heavyweights in incident response and threat intelligence at big name companies that are, and they're constantly on the speaking circuit. And I knew them as young engineers in the SOC at Motorola, so really proud of that.

Ed Gaudet: That's terrific. And did I read that you also took some of those learnings and applied them to NewYork-Presbyterian? Did you build your own SOC there as well?

John Frushour: Yeah, I mean, we started it at NewYork-Presbyterian. The security program was just single digits, a handful of people. Before I got there, I think it was literally three. And I started focusing on operations at NewYork-Presbyterian. My title in office was to be in charge of operations. And so we did, I think what is common for a large enterprise that's making investments' security, we turn to our partners and those MSSPs, the big names of the world that can provide that remote assistance and coach us.

John Frushour (cont'd): But we knew it wasn't a permanent thing, and we morphed a dependency on MSSP into organic FTEs. We hired a SOC manager, and I remember one of the first conversations I had with him was, welcome, start writing everything down. Every knowledge article, every KB, every, you know, incident response guide, playbook, just write it all down and start to get a taxonomy because you're going to do you're going to repeat this every day. There's going to be endpoint alarms, there's going to be perimeter alarms, there's going to be stupid humans, there's going to be all this stuff, and that's, the MSSP has a big playbook, a big generic playbook. We need an NYPD playbook. And so he did a fantastic job. I am so happy and proud of our SOC. They have evolved in ways I couldn't even imagine with their level of acumen around threat hunting, intelligence simulation, stimulation, their their automation capability. Just recently, they basically rebuilt a commercial product that we depend on, and it'll probably save us about $250,000 a year just because they're motivated and they're like, I can do this better. There's nothing better than motivated engineers that can appreciate documentation.

Ed Gaudet: That's right. Amen.

John Frushour: Definitely built it ourselves.

Ed Gaudet: That's great. Thanks for that foundation. As you think through the next 24 months or so, what are the things that are top of mind? What are your top 3 or 4 five priorities?

John Frushour: There's, I can kind of try to put that in the context of what are my priorities and what are my threats, like the softball answer is like, where are my risks? And then that's what Henry Cecil's supposed to say, right? Like, here are my risks, and here's how I'm going to address those risks. Here's the investments I need to make. That's not a bad strategy, I think. I think about priorities. I kind of move away from not necessarily risk, but one of the problems or the initiatives of the gaps in delivering a good service that I think are going to appear in 24 months. So, for instance, I think one of those top priorities is our passwordless initiatives. We recently moved to mandating 16-character passwords for our constituency, for our our employees. That's painful, painful. Now there's tricks that we can use around using song lyrics and using poems and making it better for the end user. But still, at the end of the day, you're whacking away 16 characters.

John Frushour (cont'd): That's not fun. That introduces password fatigue, which introduces, when users don't find it easy, they'll find another way, and that's a risk, that's a threat. It's not something, it's, I don't put that on the stack rank of risks, but I know that a happy user population is very important, and I want to make security transparent, I want to make it easy for them. So we've invested a lot in passwordless initiatives. And when I say passwordless, a lot of these, these vendors out there, they'll say it's passwordless, but you have to type your password in once, just that one time, and then it's passwordless. That's not passwordless. So our passwordless initiatives are truly passwordless. They are based on behavioral biometrics. We have tooling that records things like key gate, the amount of time between successive key punches on the keyboard or key depressed time, the amount of time your finger lags and pushing down a particular key or mouse dwell time or mouse movement or whatever. We have behavioral biometrics that record that kind of data that we are using to then offer passwordless solutions by basically proofing those users in real time, called continuous authentication. With that, we have certificates, we have Kerberos tokens, we have SAML tokens. We have a lot of session reuse and risk-based authentication mechanisms, but all combined together in a big conditional logic portfolio that is meant to be as transparent as possible and then offer our users a completely passwordless experience. A surgeon cannot step away from having his fingers in your guts to type into a keyboard or whatever; that's insane, but,

Ed Gaudet: Right.

John Frushour: It happens all the time.

Ed Gaudet: Yeah.

John Frushour: And we've got to get ahead of that and get rid of that. I think number two for us is really enhanced use of identity to improve business process and to strengthen the security of business processes. Identity and healthcare is very much, in my opinion, are, we're a top ten hospital in the country. I think we're pretty advanced in the areas of identity management and identity and access management.

John Frushour (cont'd): I think at this level, identity is not just a set of attributes that you use to query, but it's the inner lake of information around digital identity that can be used for everything from query to entitlements to provisioning to RBAC to filtering and controlling things in the cloud, in Azure, which we're a big Azure shop. So we take identity, and we consider it. There's a couple tools that are kind of at the center of that, but we take identity, and we view it really as a data lake, just in an organized way. It's not unstructured, but in an organized way into everyone's individual profiles so that we can say, okay, it looks like you're a nurse, and you work here, and you're in this ward or this department, and you have this much tenure, and you came from wherever, boom, slot them with all these entitlements, grant all these just applications, and we're learning from that data lake. We're learning that certain groups of people are power users. So let's give them more stuff. Or certain groups of people are not power users, and they rarely use product X. So take away product X, or they always seem to float around with these campuses. So let's make sure their badge can get them into those doors. So it's access control, of course, but I think it's also making these business processes better, granting more rights, giving more access, entitling more users, birthright entitlements so that we don't have an onslaught of light. And get this, I started last week, but sometimes it, I've heard problems at different hospitals around things like ordering scrubs. Not in NYP, but there's kind of a problem. The logistics of onboarding people and healthcare is complicated because it's every day it's it's very frequent. And things like getting scrubs, I don't want anyone to ever wait to get a uniform, a jacket, scrubs. If we can make that better with intelligent use of identity data, then that is a top priority for us. Top priority. Along with that comes better identity proofing. More accurate determination of entitlements. That's a security function. And so I think using identity to influence business processes has a byproduct of enhancing security and getting better at proofing for sure.

Ed Gaudet: How about number three?

John Frushour: Number three, it's probably somewhere around biomedical device security. You've seen the, we've seen the requirements for bombs. We've seen the government take a much more dedicated interest in biomedical device security, which is fantastic. We're an advocate where, we lobby for that, we are hugely invested in that. I also understand big Biomed and big MDM, their problem as well.

John Frushour (cont'd): One of the things I learned in the Marine Corps was that it takes anywhere from 7 to 11 years to push a ship out to build a ship, in some cases up to 14 years, like for a really large warship. By the time that ship hits the water and the Marines embark on that ship, and I, as a communications guy, I'm walking around looking to plug in all my little tools and whatever. I'm dealing with technology my kids are better at, or know, are more familiar with. Excuse me, I'm dealing with technology that my parents, excuse me, my kids are more familiar with because it's just old tech, right? It takes a lot. The bureaucracy, the funding, the building, it's a long fight. We see that with biomedical devices as well, certification process and the FDA 2 or 3 years on the, on a good day, that's not their fault. But those systems have to be designed in a certain way, is that when they do hit the patient's bedside, that we can be assured that they're secure without some overwhelmingly complicated path towards patching or additional technologies that represent compensating controls and really just increase the risk. There's I think there's definitely ways to do that, and it doesn't have to be as hard as it is today. It's a big area of vulnerability for us.

Ed Gaudet: How about AI? Where does AI fit in all this for you?

John Frushour: I'm like kind of a curmudgeon on it. I like a old man yelling at you to get off your, get off the grass. I have degrees in this field. I know what AI is, I know what a level one, a level two, I consume educational material about. I consider myself intelligent, to some degree, in AI. A professor, I don't teach it, I don't practice it every day, so as much as that's worth, I think I, I'm relatively intelligent on the topic, and I'm a little bit pragmatic, maybe a lot pragmatic over the reality of AI in what we do. I think a lot of conditional logic and a lot of complex conditional logic get branded as AI, which there's no doubt is a certain view. You could consider that a baseline form of intelligence, but a true learning model performs a type of mathematical regression against every decision or model's decisions in that way. I don't know that we've necessarily seen that yet. The large language models that are all the rage right now, and everybody's running around talking about Copilot and ChatGPT and how these things are going to do great. Yeah, yeah. Are they forms of artificial intelligence? Yeah. I don't think anyone's passed the Turing test. I think we still know that ChatGPT is ChatGPT. I saw an article recently how the, someone asked ChatGPT to do something, and it actually initiated a task rabbit, and asked another person to do that thing, and that and that person that responded to the task rabbit request said, is this an AI?

John Frushour (cont'd): Are you at ChatGPT AI talking to me? And the and the AI said, no, of course not. Why? No, I'm not a computer. Why would? And so the guy did it. Oh my God, he performed that task. Is, does that system pass the Turing test? He, it certainly did it for this guy. But I don't know that we're necessarily there yet where we can really call things. It's hard to say, and I.

Ed Gaudet: Not to mention the security implications too, right? I mean, the security implications, it's like we went back 30 years from a security perspective in terms of what people are doing with the data and what vendors are saying they're able to do. I think, I think with bulk, with large data sets, there's definitely a lot of stuff, a lot of open AI, a lot of AI out there. Microsoft, Google, and the Amazons, these heavyweights have mechanisms by which we can manipulate large data sets and make intelligent decisions. Are, is that AI? Yes. Is that working today? Yes. Is AI going to crack TLS 1.3 tomorrow, and we're all post-quantum resistant and quantum-friendly cryptography? Is AI going to make that available tomorrow? I don't know. I'm a little skeptical in its use, and it's almost, if you remember a few years ago 3D, there with, 3D was the rage. You got to see the movie in 3D, you got to get a 3D TV, you got to wear the glasses, and everybody was just gaga about 3D. But then when you actually practically sat there and put the glasses on or went to the movie theater, you're like, did I really pay an extra seven bucks for this?

John Frushour: Yeah, exactly. And that's kind of where I am now. Like when vendors pitch us on AI products, I'm like, all right, explain how you do it. Like, talk to me about your modeling to walk me through your math model and where's my data going.

Ed Gaudet: Where's my data going?

John Frushour: Where's my data going? How do you enrich my data? Is my data the only thing that, certainly, if I'm the only contributor, that's not a great model. How do you enrich it? There's massive security ramifications around data sharing, especially healthcare, where we're governed by HIPAA and HITRUST. And so lots of security questions around the data itself as well.

Ed Gaudet: Yeah. What keeps you up at night?

John Frushour: Right now, I think it's mostly around business email compromise and people falling for, you know, crafted campaigns. I'd be spoofing, people calling into our service desk, claiming to be an executive and having the ability to mimic their voice, using AI as an example, to take a presentation off YouTube and then working away from that base set of audio and then manipulating it and growing it in such a way as that, you can create a complete deepfake of of that particular person. You've seen it out there with, Arnold Schwarzenegger seems to be the most popular deepfake out there, but like people layering his voice on all these different things, that really scares me. It's very hard to combat. I think we have a pretty good approach, but it's hard to check. And of course, your weakest link is always going to be that human. And we have the best doctors, we have the best nurses in the nation, in my opinion. And to be the best, they need to focus on the clinical function of their job, not necessarily not falling for a spoofed email, and to them that's, that makes me nervous.

Ed Gaudet: That's a great point. Last couple years have been tough on a lot of people. What are you most personally or professionally proud of?

John Frushour: Industry standards and best practices. I hear this all the time. I hear vendors say, that's industry standard, John. ... This particular function is industry standard or best practice here is to put a next to be. Where's that book? Where can I put that on my Kindle? Can I buy that off Amazon? Where's the industry standards book? I would love to read that. This great bathroom reading right there. I would love to have that book. But the simple point is it doesn't freaking exist. And when you use terms like industry standard, the only thing you're talking about is that a bunch of people chose the same thing. A bunch of people drank Kool-Aid in, I think that's South Africa, that was ... people drank Kool-Aid in South Africa. I'm not doing that. So what is the industry standard? What is it? At NYP, NewYork-Presbyterian, I firmly believe that we set those industry standards, and I am immeasurably proud of my engineers, and my architects, and my managers, and my directors, and the staff that work here, because they do it every doggone day. And I wouldn't be so confident in saying that if I didn't attend a conference every year, or a panel discussion or a meeting with my peers, and somebody says, hey, what do you do for this? And I'd say, well, I at NYP, we do this, and we document a standard. We created a process for it, and it connects to be a beacon.

John Frushour (cont'd): And whatever the definition of that thing is, we've created our own remote access platform for vendors, eliminating or attempting to eliminate the proliferation of vendor-controlled, agent-based remote access. We created a platform to track narcotic diversion. We created a platform for our privacy team to look at privacy alarms across our then EHRs, now one EHR. We have, we have really set the standard, I think, in a lot of these different key areas of technology, of information security and setting those standards. And that it just is, I'm like the proud pa. Sometimes I blush or I drop the idea in there, but it's just one ingredient. It's a little bit of salt in a very complex pot pie. And the engineers put it together and produce things that other hospitals call us and say, hey, how did you do that? What are you doing here? What are you doing here? It tickles me pink. And it, and it's an area where I have to kind of actively reduce my arrogance and mute myself. Because I think we really do set industry standards, and we create best practices here, they're for NYP, they're the things that we do. They might not be applicable everywhere, but you better believe that a lot of them are. And I think we've got, in my opinion, the best infosec team in healthcare. There's my area.

Ed Gaudet: I love that answer. What, outside of what you're doing in healthcare and IT, what would you be doing if you weren't doing this job?

John Frushour: That's easy. In my spare time, I volunteer my time with organizations that build homes and structures for vets, individuals that, homes for heroes, those kinds of things where these individuals are either, because of some type of disability or service-connected status, we owe them everything. And working on those homes and being a foreman, or just being a plumber for a day, or being an electrician for a day is, I enjoy the hell out of it. My house is full of abandoned projects and ideas my wife would love to complain about and tell you. So I'm very handy, but I like to keep involved in there and providing those homes for vets.

Ed Gaudet: Thank you for that service to that. That is a, that's a hugely needed service. And we ask a lot of those folks, obviously, we have asked a lot of those folks over the years, and they deserve our time and our service. So thank you for that. If you could go back in time, what would you tell your 20-year-old self?

John Frushour: Join the Coast Guard? No, just kidding. But do apply for interservice transfer to the Coast Guard.

Ed Gaudet: That's great.

John Frushour: Let's see. That's a tough question. I think two things. One thing is, you're not always right. And that's hard to learn, especially being a part of what I consider to be the finest fighting force the world has ever seen. You're not always the best. You're not always right. There's a lot of people out there that are smarter than you, and keeping your mouth closed, there is strength in silence, and there is respect in silence. And although you you think you got to contribute and you think you got to open your mouth, there's a lot of power in just listening and recognizing that there's a lot of people smarter than you. That's probably the first thing I would say. The second thing I would say is, I don't know, it's the inverse of that coin, which is there's a lot of dumb people out there too. Don't always believe everything you hear at first sight, it's probably the inverse of that. But I think the best, if I could, I only got this later in life. I only received this information later in life, so if I could give it to myself. Prior to that, I was at Arlington one time with some friends, and there was a woman there. She was the aunt of an army soldier who had lost his life, and she was searching for his gravestone in section 60 there at Arlington. I was having some trouble. I was there with some friends, and so we were just enjoying a beer, and we had our little lawn chairs out, and we were just telling stories. So I walked up to her. I helped her, showed her how to look stuff up, and whatever. And so she came and sat down with us, and we had, and it was a nice chat. And we all, we talked about our friend in particular, that we were sitting around his grave and other individuals we knew, and she talked about her nephew and she was very prophetic, very intelligent woman. And I know, I've never known, I know her nephew's name, I don't know her name, but very intelligent, and kind of near the end of our conversation, she told us, she said, never suffer mediocrity. And that was something that it was very, it was profound. I thought that it's just, it's so simple. Never suffer mediocrity. All, it essentially is, strive for the best that you can find, that you can do, that you can appreciate. Strive for the best that you can find in others. Promote them. And it's a, it's something that if I could tell my younger self, because you get stuck on that a lot, right? You're like, man, that's good enough. I did my best.

Ed Gaudet: Also, surround yourself with those people that have.

John Frushour: Oh, absolutely.

Ed Gaudet: Yeah, I love that.

John Frushour: It applies in so many things. You can abuse it, right? You can abuse it and take it to a point where you've just become neurotic about it, and you don't realize that you don't need something. But, I think it's still a great little, I don't know, mantra to carry around.

Ed Gaudet: Excellent, excellent. I would be remiss if I didn't ask you this question because this is the Risk Never Sleeps Podcast. John, what is the riskiest thing you've ever done?

John Frushour: I mean, do I have to answer in terms of cyber, and like in my role you can.

Ed Gaudet: Answer any, there's, there are no guardrails on this program. No profanity other than that.

John Frushour: Yeah, that was hard for me.

Ed Gaudet: I know, me too. But we can edit it out so you can say it, and we'll edit it out.

John Frushour: You know. Well, so I'll just, I'll try to answer you two ways and be brief. The cyber, the riskiest cyber thing I think is just, it's almost like a weekly or monthly, maybe even a daily thing. It's the assumption of risk for devices that are trackable or vulnerable, but that there is a clinical need, and I can't avoid that. There's, we saw a case, I think it was last year in, was it Arkansas, about a child, an infant that passed away because of a ransomware compromised, I think, of a fetal heart rate monitor, I want to say.

Ed Gaudet: Yeah.

John Frushour: I might have the details wrong. Tragic, horrible story, but that kind of thing, putting those devices that we know are susceptible on our network happens every day in healthcare, going back to the FDA thing and, you know, the age of the devices and all that stuff. And you can't provide healthcare without some of these devices, you have to do it, and it's a tough pill to swallow. I don't know, cumulatively, it's probably the riskiest thing, but individually I don't know. So, you know, compensating controls. You lean on a strong network. You lean on access control, you lean on all these other tools that we have in our infosec toolkit, but it's tough. The second riskiest thing I ever did was I was stuck in Kandahar trying to get home. I was forward deployed and my boss had recalled me. I had a small team in Afghanistan, and my boss had called and said, hey, you need to get back here. We got these ten things to do. We're going to put a warrant officer that worked for me, and he's going to be in charge just for two weeks, because there's more important stuff back at home. The mission was pretty much over. It wasn't a big deal getting called back home. And the problem was, getting out of country is hard if you're a small unit, not part of some larger battalion or regimental-sized unit, and we were a very small unit, and I flew into Kandahar, and then I had to get a flight to, I think it was Camp Virginia in Kuwait, and I was stuck in Kandahar. Which Kandahar, if you're an Army soldier, is like Paradise. There's a TGI Fridays or the Nathan's hot dog stand, and there's, like, air conditioning and a PX, and you can buy t-shirts and coffee cups. If you're a marine, you're like, is this what heaven looks like? Is this Disneyland? Is this because we don't have all that crap? We're all stuck out in the middle of nowhere trying to make water and make fire and stay alive. And so I was a pilgrim in a foreign land going nuts because, do I assimilate? And do I become just another soldier and go and eat my chicken crispers at the Chili's and the Fridays and all this stuff? Or do I persist in my marine arrogance and obstinance and grumpy attitude and whatever? And I was caught, and I was stuck, and I just wanted to get out of there so freaking bad. I was miserable. So I stowed away on a, I think it was a C-5, big aircraft, holds up 300 soldiers, and I was an officer, so I was a little bit of loot. I kind of stayed over to the side while they all got in the aircraft or whatever, but there's still a very rigorous control mechanism. You got to show your ID, and somebody counts you, and they tap you on the head, and there's accountability for getting on the aircraft. It's very strict. Your army does an excellent job with it. But I was just kind of stowing away, and no one was saying anything to me. And I thought, screw it, I'm going to try to get on this aircraft and see if I can get back, because otherwise, it was like another four-day wait somehow for a C-130 or something, a marine C-130, and I'm like, I cannot stay here any longer.

John Frushour (cont'd): So I stowed away, and when they loaded, the aircraft were of course plus one. They couldn't figure out who it was. And they were screaming and whooping and holler and everything. They were like, everybody get off the aircraft. We got to ..., and I was trying to figure out how I was going to sneak out, or I was going to jump out of the side, like the side door, and get run my ass off and get away from them, and I was sweating it. And some colonel was up in the I remember there was the cockpit was you had to go up a ladder to get to the cockpit. So whatever airframe that is. And some colonel came down, and he was all steam, and he's like, I got, I'm on a deadline, you freaking soldiers. And he's barking fire at everybody, and I'm sweating it, and I'm looking around. And keep in mind, one of these things doesn't look like the other, right?

Ed Gaudet: Right, exactly.

John Frushour: They got all their army fatigues with their army gear, and I'm covered in dirt, and I look like I've been rolling around in the sand for six years.

Ed Gaudet: That's great.

John Frushour: And I'm like, I'm sweating like, pick on first. And so I'm freaking out. And then apparently some crew chief comes up and he's sure we got to go. I don't give a shit if you got two more camels and three more dogs and I don't care, you get off my tarmac, blah, blah, blah, I think I just cursed, sorry about that. So anyways, we take off, we land, but the heat is still on. Who is this stowaway, right? So they get off the aircraft, and a bunch of the senior enlisted army guys are telling me that I need to go stand in their formation and be counted, and I'm just like, yeah, it happened. So I grabbed my stuff and I just hoofed it as fast as and nonchalantly as I could to a marine tent where I knew I'd have friends. There's some staff NCOs in there that, and these are my guys, and I just, I hot-footed it over. And then they had a big, a big kerfuffle. There was a, they announced, we have a stowaway on the base. We have.

Ed Gaudet: God, no.

John Frushour: Someone got on the plane. We don't know who it is. And it was this whole big kerfuffle, but it was, it's an army base now. And so I just, I told the Marines, I was like, listen, I need to be on a flight out of Kuwait airport at eight hours. As long as you can hold my lie for eight hours, I don't care what happens after that, because then I'm back in the States and they can court-martial me later, and they're like, we got you, sir. We got you. Don't worry about it. Bold move, sir, bold move. I can't, I want to kill myself on day three, so yeah, I made it out of there. But it was, I probably could have just. I mean, I could have gotten into a lot of trouble for that.

Ed Gaudet: Yeah, absolutely. Yeah. That's terrific. Any last advice to cyber professionals that are just starting out or maybe a couple years into it and are looking to grow their career?

John Frushour: Of course, my biggest piece of advice is, stop holding on to a dream that you're going to be a cyber professional tomorrow. You're not. Get the certs, stay engaged, stay motivated, but I would encourage you to master some block and tackle discipline of IT. Become a master network engineer, assess a service desk analyst, an escalation support a project manager, a database engineer, systems admin. Make sure you understand the fundamentals because cybersecurity touches everything. We've got our fingers in every pie and every recipe. Any issue that comes across any attacker is going to touch ten different disciplines of IT. And we're, need to know not just the fundamentals of RBAC, but how RBAC applies in an on-prem Active Directory environment, and how permissions and heritage works with federated access, and how SAML authentication and TLS encryption. And these are fundamental things that need to be understood to react and be effective and be proactive in the cyber world. If you want to get into cybersecurity, you want to be as good as an engineer as you can be. Earn it through a block, and tackle discipline of IT, because that's where I hire from. That is where the best engineers come from, they mature into cyber, but get the certs, get the training, stay engaged, read, watch, learn. There's nothing wrong with focusing on cyber as well, but it's, you know, if you think that getting a four-year degree in cybersecurity from an accredited institution is going to land you a job on graduation day, at least in our business, that's hard.

Ed Gaudet: That's great, great advice. And thank you. We've been speaking with John Frushour from the NewYork-Presbyterian Health System. This is Ed Gaudet from the Risk Never Sleeps Podcast. And if you're on the front lines, delivering patient care or protecting patient safety, remember to stay vigilant because risk never sleeps.

CENSINET®

Censinet RiskOps™ Demo Request

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

SCHEDULE DEMO

www.Censinet.com