Podcast Transcript

Risk Never Sleeps
Episode 41
Keith Price

Ed Gaudet: Welcome to the Risk Never Sleeps Podcast, in which we learn about the people that are on the front lines, protecting data and protecting patient safety. I'm Ed Gaudet, the host of our program, and I'm pleased today to be joined by Keith Price, Head of Information Security for the Envisioned Pharma Group. Is that still correct, Keith?

Keith Price: That's still correct.

Ed Gaudet: Yeah. Excellent, excellent. So tell us about your current role, your organization, what you do in security, and IT.

Keith Price: Yeah. Thanks, Ed, and thanks for having me on your podcast. It's a real honor and a pleasure. I enjoy doing these, and it's about sharing what I do, but also, I think, highlighting some of the areas that I am most passionate about, they're not traditionally tied to cybersecurity. But I've been working in cybersecurity for 22 years now, 32 years in tech more broadly. I started young as a 14-year-old in school programming on our Commodore 64, and then the last two years, I've been working with Envision Pharma group as our head of infosec. They're a farmer technology company dealing with sort of the 38 top pharmaceutical companies. And I came in after they had a ransomware attack two years ago and helped them recover from that. And then, they asked me to stay on and build the entire infosec program from scratch. I like to use the CIS-18 and the CIS RAM frameworks.

Keith Price (cont'd): And here at EPG, we have come a long way to include building out an infosec team, mostly from existing employees from within, not just the IT team, but also from other groups, software development, facilities and operations, you know, touch the ISO certifications. And we've developed those skill sets in-house.

Ed Gaudet: How did you do that? That's interesting, actually.

Keith Price: Well, it was primarily driven through, You can't hire Keith. So I said, Okay, well then, I'm going to be tricky and find the folks that are interested in security. I've been introduced to a couple that had already sort of gone and developed their own skill sets outside of working hours into sort of security certifications and so forth. So, an example, a network engineer who saw networks sort of disappearing into the cloud, and he didn't want to work at a data center. So he says, you know what? I'm going to go into Azure security. But application security guy who did some of the very good sans certifications, and then someone who worked in our facilities and operations, who ran all the ISO audits, and we basically helped develop her a little bit. She didn't really need a whole lot, so it was more a case. Now we're trying to get all these folks laterally moved over during the hiring freeze, which works a lot better than going external because you have someone who's within the organization, in some cases ten, 15 years, and you know, the folks that we steal them from, they're not entirely upset because they've said it helped recruiting by saying, look, here Envision. You have opportunities to move around and maybe cyber. And they provide real-world examples to those candidates, which here perks up their ears a little bit.

Ed Gaudet: No, that's terrific. In fact, you probably also extend the culture of security to other parts of the business, which you wouldn't have done otherwise.

Keith Price: Correct.

Ed Gaudet: Can you talk a little bit about that?

Keith Price: Yeah. Well, I'm a people over process over technology kind of guy. So, I always start with the people and the return on investment, on building a security culture and awareness within your organization is pretty much the greatest out of all cyber tools in the toolbox. So, as an example, I implemented what we call cyber coffee, which is every month or two. And there's a five-minute LMS that the folks can take if they want. It's around relevant and timely security awareness topics.

Ed Gaudet: Interesting.

Keith Price: You know, that people might see in the news or they hear about, and it's kind of scary. And so we have these cyber coffee events where I show up, and we have a couple dotted throughout the day for our time zones, you know, and globally. And it gives me an opportunity to give a quick five-minute primer and then 25, 30 minutes of interaction with the employees. And I always tell them, you know, this is not restricted to asking questions just about the business hours. You know, if you have questions about your teenagers and TikTok, your elderly parents or grandparents and how best they can secure, you know, their online banking and things like that, we expand to all those. And we found in the last year since we've been doing those, they're very popular. You get a lot of positive feedback. People like the fact that we are trying to help them understand their role, but also introducing some of the technology pieces that say, our Azure or our E5 uplift that will improve the user experience by doing security kind of in the background, you know, so not enforcing MFA every day if they're on a trusted devices example. So, these wins with the user base tend to make us a little more popular. We get more invites to their business unit team building events. You know, we get invited to those as guest speakers. We get invited to take part in projects at the ground level, which we all know traditionally it's, hey, security, this is launching tomorrow. Just have a look at the risk and security functions. Now, we get invited early on because people see we're not here to stop the progress. We're here to help drive maybe through a quality initiative implementing security through quality and safety.

Ed Gaudet: Yeah, I'd imagine the word gets out in more people want to join. And this notion of security starts at the home. Everyone has security issues or challenges, whether they know it or not.

Keith Price: That's right.

Ed Gaudet: Because everyone's running technology at the home. So I bet you there's some connection there that's driving participation.

Keith Price: Oh, for sure. I had one question. They said, you know, my father has a notebook that he likes to put all his passwords in. And I said, well, that's great. You know, was he using log? Oh, he has passwords are crazy long. They don't make any sense. But I'm worried that he's written them down. And I said, well if somebody breaks into your dad's house to find this notebook, we got bigger problems. And they said, oh, we're not worried about that. He has quite the gun collection. So I said, well, you know, the notebook is better writing a funny character password on a notebook than reusing a simple password every time. Right.

Ed Gaudet: So, putting in a sticky or something.

Keith Price: Exactly, exactly. So those things, you know, they're traditional, you know, sort of outdated thought processes around good security practices because we didn't think of all the use cases around it.

Ed Gaudet: Yeah. Well, that's a great example of taking a risk management approach first to solving a problem. Oh, I love that. You've had a very diverse background. I was checking out your LinkedIn page and DoD, Deloitte, Sentara Healthcare, Air Force; thank you for your service. Of course. Yeah. So, take us through the path to get to where you are today.

Keith Price: Yeah, sure. Well, three days as an 18-year-old, I enlisted in the Air Force back in 1991. So Desert Storm, first Gulf War was happening. I had already enlisted the previous summer, so I was on a delayed enlistment program, so I knew I was going in anyways, but joined the Air Force got stationed over here in England for my first duty station. I started out as a munition specialist, so I was building for A-10 warthogs. I was building missile systems, testing missiles, laser-guided bombs, 30-millimeter ammunition.

Ed Gaudet: Oh, yeah.

Keith Price: That's an A-10 bullet.

Ed Gaudet: Yeah.

Keith Price: That's, you know, one of those going through you.

Ed Gaudet: That'll rock your world, folks.

Keith Price: Yeah. So, I started out as that. But then one day, a few months in, my shop chief comes in and says, hey, is anybody here good with computers? Oh yeah, I'm okay. Well, we just bought this new mainframe in the Air Force to keep track of everything, and we need people to operate it. And so they sent me to Ramstein, Germany, and I went and became a mainframe. It was an IBM Z something. I can't remember the numbering, but it was green screen, terminal dot matrix printer. And that was it. I started I was still a munitions AFSWC, but was doing it from then on because the IT people in the Air Force didn't like coming out to the munitions area three, four miles away. So they said, Keith, we'll give you admin rights, you just do it. So that's great. Became a network engineer and a server admin and a customer support and crypto, and you name it. And then, after ten years of that, I moved over into security. Back then, it was called Compusec and working in architecture. So helping design the Wan Lans and also then the higher GRC architecture for policy and process, so did 20 years retired went back to the States with the family. And then we decided, you know, I've lived here for almost the whole 20 years in Europe. We decided after two years, I worked for Sentara at the hospital Building HIPAA privacy program. My wife said, oh man, we really missed the UK. So, I took a job with the Army as a GS over in Stuttgart, Germany.

Ed Gaudet: Oh, nice.

Keith Price: I was doing network operations. So back in the IT world with a small information assurance cadre, and after two years of that, demoted myself because a job came up here in England. So I said, oh, I'm going to demote myself so I can move back over there to the UK and move back into security operations with the J2 folks. So J2 is the Intel part of the military, and we had US, Africa Command, European Command, and the NATO fusion centers, which is all military intelligence. And so our part was to add the cyber intelligence into that bigger picture. That was three years, and that was a lot of fun. And then from there, I was looking to go back to the States, work in DC, but company in the Emirates reached out, called Dark Matter, and they wanted me to come over and help build their consulting practice over there for a year. Did that. That was a lot of fun. Deloitte then reached out, can you come over back to Europe and help build? It was called North-South Europe, Middle East, that it was their internal Deloitte cybersecurity. So I started doing that. And then COVID hit, and everything changed, and they found out, I think I messed up a little bit. I said, oh, I used to work in the military. I used to work with epidemics on supply chain. And they were, oh, you're doing that now for Deloitte. But that experience served the company well. Unfortunately, as things were starting to wrap up, my project my program kind of faded away. There was less interest now in what they wanted to do, which was to synergize everything and all the various Deloitte practices. And Europe said, no, we kind of want to stay our own bosses for a little while longer with cyber. So white worked for Littlefish for a very short period, building again a very young cybersecurity consulting practice, and then moved over into my own limited company. That's what I've been doing for the last two years with Envision as the head of infosec. And I've got something new coming up in about a month or two. Back to a permanent role. It's very exciting role. I don't want to announce it yet.

Ed Gaudet: But you're staying in England or.

Keith Price: Yeah, yeah, it's back in civil service here, working for the Brits this time. So we'll see how well a yank can do, you know, working for the British government. But very excited with that new role.

Ed Gaudet: That's great. Congratulations. So, what keeps you up at night?

Keith Price: Oh wow. Thinking about my kids.

Ed Gaudet: Yeah, yeah. You have a big family.

Keith Price: The daughters were easy. The daughters they stayed out of trouble. At least I didn't hear about it. So if there's a risk and you don't see here. Yeah. No monkey see, monkey do, then there's no risk. You know, head in the sand. But no, all joking aside, my daughters are very good. Now, my three sons are coming up starting to become teenagers. And that's what keeps you up at night. But from the cyber world, ransomware is still top of the list for me. We put together some very good, robust tabletop exercises. We practice, we practice. It's about building muscle memory. It's about knowing who is the incident commander when things hit the fan and who is supposed to be communicated, and who's communicating outward to our clients, who's communicating to the media. And we practice this. And it's very important, obviously, to include the whole business. We started out with just IT. There was a little bit of PTSD because they had suffered a real ransomware attack, but the more we did it, the more it became just second nature. And so we're now looking to build upon that and start going to other areas of business continuity that aren't just ransomware, but other things like data exfiltration. And how do we handle if it's gone, what do we do? So those are the kind of things that keep me up at night, really, but more so, I would say the availability piece, if we lose our clients, lose access to a platform, what could that mean to the business? What could that mean to our reputation? Security and risk is really about protecting the reputation of the business. And so making sure that we test those backups and recovery processes, as well as not just not doing the cyber piece of work.

Ed Gaudet: That's a great point. I think if we learned anything over the last five years, it's that eventually you will have an incident. And so it's not so much protecting against it. It's more of how you recover, how quickly you can respond and recover to that incident. Do you have the right business continuity and disaster recovery plans in place? Have you practiced them, as you mentioned often, early and often? Anything else you'd like to provide listeners in terms of advice around managing ransomware attacks? And you seem to spend a lot of time focused practicing, at least on that, which is good.

Keith Price: Well, you know.

Ed Gaudet: Learnings that came out of that.

Keith Price: Yeah, the rules are changing. The rules have changed. You know, back then, it was we have your stuff, and we have an encryption key, and you pay us to unencrypt your stuff. And now most organizations have solid backup recovery, solid offsite or disconnected backups, encrypted backups, one drive for each individual. So that's another option for the individual. But the ransomware is now are, in some cases, just even releasing because less people are paying the ransom. So they'll release the data publicly. And so it's about being open. And just like with any attack in the security community, and obviously, there's some things you can't share. But whenever security leaders see an attack and then the first thing that's released is it was a sophisticated attack. We all chuckled a little bit because we're like, was it really? Or are we about to blame the intern the next day? So it's about being honest with society because, again, that builds trust in your brand, right? And as a community, we root for each other until we find that you're behaving unethically and then we're not so much as a backup. You know, we're not encouraging as such. And there's been some instances in our career in the last year or two where senior security leaders have not been ethical, and they almost paid the price in terms of things like prison and stuff like that. But you got to be open on it, and you got to document everything there. Sees those out there and CSOs out there and chief risk officers that the business pins them with the risk. You're the risk owner. Well, it shouldn't be the case. It should be unless it's in your domain.

Ed Gaudet: Yeah.

Keith Price: And I really feel for those folks because just the mental health anguish that they must be going through, knowing that they own something that they may not have full control or budget or resource to mitigate or compensate against.

Ed Gaudet: Yeah. And in fact. They can't say no often. Right? So we just had a webinar with the head of GRC over at Intermountain yesterday, and he pointed out that the risk teams don't own. They can't say no. All they can do is communicate the risk and the insight through the analysis of the data. It's up to the business to make the decision. It's up to the organization to understand the risk associated with their tolerance level or their appetite for risk.

Keith Price: Exactly.

Ed Gaudet: So that's a great point.

Keith Price: Yeah. In the military, I was spoiled. You know, the military had that big no-red stamp, and no, no, no. And it's not realistic. But obviously, in the military, we have much more stringent security controls. So, it was easier to get away with. Yeah. And when I came into the real world and learned. Yes. But yeah, I've done the risk assessment on this thing that you want to do for the business. Here's your 3 or 4 courses of action and what they mean on that spectrum of risk. And there have been a few times where they said we can put a couple compensating controls in realistically, but the vast majority of the risk is going to be accepted. However, we have now a project in scope to address it over the next year. So and that was my job was to continuously monitor that risk and update any changes because sometimes a vulnerability can go from a CBS score of 3 or 4 overnight. It's an eight, nine, ten. And so you have to keep your eye on the ball with those and have a plan ready. Good hygiene is sort of the basic foundation. Patching systems is always where you should start. And again, comes from a place of quality, too, because a lot of those patches aren't even related to security. It's about improving the performance of the system, which has a big knock-on effect towards availability for your users.

Ed Gaudet: That's right, that's right. You're obviously passionate about security and IT. What else are you passionate about outside of that?

Keith Price: Oh wow. Mental health for me. So, if you look at my LinkedIn, typically about horrible hiring practices, it's about mental health of our community. And it's also about mentoring and developing military veterans to come into the career field of cyber risk and also work with some bootcamps and student groups, mentoring them as well, and basically giving them the reality. You know, someone told you that you're going to be leaving the military and earning $85 - 90,000 a year. That's not really true. Maybe. And, you know, we have to look at this from the 35,000-foot view and what the reality might be. So I help bring that to folks. And again, mental health for me. You know, I suffered PTSD from my time in the Air Force. You know, I'm in the Air Force, and normally, we're 50, 60 miles behind the enemy lines. And here I am in Bagram in Afghanistan, and I'm sitting in an old Russian tower doing my thing, and I got bullets flying past my head, and I'm like, whoa, I didn't sign up for this. I'm in the Air Force. Damn it, you shouldn't be shooting at me. But that's right. You know, that's the reality. That's the reality of Afghanistan. So mental health for me again, depression, dealing with overstressed, overworked people, especially in the mid to high tiers. A lot of the folks in cyber they take jobs, and they're wearing four hats. I think they don't realize just how tricky that situation might be. So for me, that's big. And then also dealing with diversity, neurodiversity in our field and also helping, you know, in these tough financial times, looking at offering people like stay-at-home moms the ability to work part-time for an organization from home any time of the day so they can help contribute to the financial security of their family. So those are the things that outside cyber that I'm really passionate about.

Ed Gaudet: That's excellent. It's been a rough couple of years for folks. What are you most proud of?

Keith Price: What am I most proud of? Of the industry or of myself? Could be.

Ed Gaudet: Personally and professionally?

Keith Price: Okay, let me think about this one. This is kind of tough one because, well, I guess for me personally, I would say with Envision the last two years, I'm most proud of what we've accomplished in the. So we had a cyber attack, we did a claim on our cyber insurance, and then a year later, we were insured again and for 30% off premiums.

Ed Gaudet: Oh, that's terrific.

Keith Price: Wow. So I'm proud of the team for achieving lowering the risk score to be able to pull that off. I'm proud of, you know, the things that we've done to make lives easier. You know, you think about security questionnaires, and oh my goodness, you get these from the sales team on a Friday. And it's foreign questions, and they need it. And so we've built out a better-automated system where the sales folks can take the first pass. And then we do the sanity check. And it's taken it from days down to an hour, you know. So, I'm very proud of those types of programs in our community and our profession. I would say I'm most proud of the support that we've offered each other over COVID. When I was with Deloitte, we were in the thick of it, and we were thinking of ways we already had sort of a remote work at Deloitte, so we were a bit ahead of many of our competitors and many others. But what we did was we did information sharing with our vendors and with our B2B, and then that went outwards, and it was ways to work remotely, collaboratively, securely. So I would say from a community perspective and from a enabling and protecting society during a global pandemic. I would say cyber it was a bit of an unsung hero in that we did it under the radar, and we only ever hear about cyber when things go wrong. These things went right. Nobody really made a big deal about them, but we know that we helped with the broader community and making that successful. It wasn't just us. It was a team effort, for sure. But I'm proud of cyber and our risk folks who really had to react and respond so quickly to that pandemic.

Ed Gaudet: Yeah, there was a lot of that, obviously, and the people on the front lines really kept it together, held it together, and it could have been a lot worse. So we, of course, salute them every single day. If you go back in time, what would you tell your 20-year-old self?

Keith Price: I would say choose sports cars instead of kids for your midlife crisis. So we'll start there, seven kids.

Ed Gaudet: My wife's gonna kill me for laughing.

Keith Price: Seven kids? No, it's been great. Would have to say make sure you work on your mental and your physical health more in life as you get older. You know, that's something.

Ed Gaudet: We took it for granted, didn't we?

Keith Price: Yeah. You know, we live sedentary lifestyles, careers in this job where I've got to now, I've got a standing desk, and I've got a treadmill under that desk, and I'm working on that. And funnily enough, improving my physical is already had a marked impact and improving mental health. It's well-known fact. So, I would encourage younger people today who are dealing with like the fallout from COVID to reach out for help with their own mental health challenges. So we had a lot of folks go through university remotely. They didn't have the same experience that others did with building out that community and having the university experience. We had folks that worked the front lines, people that had to go into work during the pandemic and put their own lives at risk. And that has a huge mental burden. And again, going back to the mental health, I would say to myself, just take better care of yourself. Sometimes it's okay. You know, I was a non-commissioned officer, and I always put my people ahead of my own needs. You know, I was just taught that by my father. I was taught that by my NCOs, that were good. But good NCOs and good leaders also make some time for themselves to make sure that they are fit and capable to lead.

Ed Gaudet: You have to and did fail sometimes in doing that.

Keith Price: So that's probably what I'd say to my 25-year-old staff sergeant self.

Ed Gaudet: No. That's great advice. So I'd be remiss if I didn't ask you this question because this is the Risk Never Sleeps Podcast. What is the riskiest thing you've ever done?

Keith Price: Oh, okay. So I kind of prepared for this one because I wanted to make sure that I didn't drop anything that was top secret or anything like that. So, when I was in the Air Force was deployed to Afghanistan within a year of 9/11.

Ed Gaudet: Wow.

Keith Price: And one of the jobs we had was to clear out old explosives caches from the Russians invasion. And we also found around 2000 sticks of aircraft layers. There are about a pound each of flare material that needed disposal. So we drove all these munitions and all the crates and crates of C4 and a few £500 warheads that we found for good measure, and we drove them up this old riverbed into this valley, and we set everything up we had there. So it wasn't just US munitions and technology. We had proper people there. Needless to say, the time fuze didn't set off the explosives. So I drove the guy the two kilometers back up the riverbed to reset the fuses. When this was scary as hell because I kept thinking it could still go off. You know, as we were driving up or as we got right up to it. And if it goes off, we're done. You know, we're vaporized. So, needless to say, all went according to plan the second time, and it was a glorious fireball that went up into the falling snow at the time. So that's easily the riskiest thing I've ever done. Won't ever do that again. And I don't know how bomb disposal people do that kind of thing for a career.

Ed Gaudet: Yeah, that's a crazy job, isn't it? Always when they put on those suits, and they go in there to defuse the munitions or bombs or. I mean, that's just insane, but that'll get the adrenaline pumping.

Keith Price: Oh yeah. Oh, for sure.

Ed Gaudet: All right. Well, this has been terrific. Any last advice to cyber professionals just starting out or pursuing a path towards the profession?

Keith Price: Yeah, I think starting out, there's many different paths. You know, there's university, there's boot camps, there's doing it yourself. There's military. I would say I was privileged because I entered the field without knowing it. You know, the military just tells you where to go and what to do. Pick it up, put it down. But I would say, don't try and burn yourself out trying to climb that ladder of success, you know, don't sacrifice, again, your mental health. Don't sacrifice relationships. Things that will happen. Cyber and risk careers are much faster and promotions than other careers as it is. So it's going to happen. Just don't rush it. Because when hate to see as people who become like CSOs or CSOs or CROs too soon.

Keith Price (cont'd): Yeah, and we had the same thing in the military where people were very, very good at passing the test to get promotion, and they get promoted very quickly. But then, when they were in that position of leadership and people were looking to them, they didn't know what to do because they hadn't had the life experience.

Ed Gaudet: Right, right.

Keith Price: And then I think the last thing that I would say is if you're doing degrees, I went to college in 37, 38 in the 40s, used my GI Bill and stuff. In cyber, I did a cybersecurity master's degree. What I would tell people now, when I know now, is do an MBA because if you're looking to become an executive, the business degree, or maybe even a psychology degree or a sociology degree, and that master's level will actually do you more service. If you're looking to become an executive because you're then able to speak the language, those executives see you as a comrade in arms, you know? So if you're looking to do that second degree, think about something other than cyber unless you're going to stay technical. And then that cyber master's degree may help you out on the technical track.

Ed Gaudet: Great advice, Keith. Thanks so much for joining us today. And.

Keith Price: Of course, Ed. Thanks.

Ed Gaudet: Yeah, this has been terrific. Listeners are going to get a lot from this podcast. So we really appreciate your time. And for those of you on the front lines protecting patient safety and patient care, remember to stay vigilant because risk never sleeps. This is Ed Gaudet from the Risk Never Sleeps Podcast. Thank you.

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