Podcast Transcript

Risk Never Sleeps
Episode 33
Christopher Lau

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 I am pleased today to be joined by Chris Lau, Director of Operational Technology, Security and Risk at Advocate Health. Welcome, Chris.

Christopher Lau: Good to be here.

Ed Gaudet: How are you today?

Christopher Lau: I'm fantastic.

Ed Gaudet: Excellent.

Christopher Lau: How are you?

Ed Gaudet: Great, great. So you've got a really interesting background. You were a financial analyst before moving into healthcare. Take our listeners through your journey into healthcare.

Christopher Lau: Sure. So, as you said, I have a really diverse background. I'm not a technologist by trade. I started my career after college in banking and financial services, so business operations, then moving into finance. Then, I pivoted from that as it got old asset management and finance into project management. From there, information governance and then transitioned, really, that was the start of my journey into cybersecurity was data and information governance and then operational risk. So I came into cybersecurity from the business side via risk, so I'm not going to code my way out of a wet paper bag. It's a different perspective that I bring because I'm looking at things from the business perspective, so it's a different lens, I guess.

Ed Gaudet: Yeah, it probably makes you more of a partner to the business as well, because you understand what their concerns are and how to speak the language.

Christopher Lau: For sure, it's something where if you can speak the language and align what you're doing to the strategic priorities of the organization, that makes a huge difference. I mean, just in building this program for operational technology security, it was a program that Advocate or before our merger advocate Aurora did not have. Making a proposal, if you will, to do this at the really late stages of a pandemic, you would argue is not good timing, but it really was because the case that we made was solid, and we used data that was meaningful to the organization that wasn't grounded in fear or techno-speak. It was just a state of, here's the risks that we face, and here's what it could cost us, and here's how we could mitigate that.

Ed Gaudet: And take us through some of the details of your program as much as you can share, obviously, with the listeners.

Christopher Lau: Sure. We're still, we're under construction. I recently spoke recently this past May, I spoke at the Sans ICS Security Summit. You might recognize the diagram behind me about building a program. And what we did to start with was just to get our feet set and to understand what today looks like. So we called it about establishing a baseline as we were, I guess, proposing the program.

Christopher Lau (cont'd): We were building the infrastructure. So we worked with risk teams at CSA and other places too, we built a, now it's a 32-page playbook, but we worked with them to help validate our scoring, to help validate our process, to help validate just the methodology and the steps that we wanted to take. We worked with them for about six months, and then, as we got funding and approval, we started launching our infrastructure. So I have a small team, but what we really focused was deconstructing the current state and understanding what we're doing, what our vendor relationships look like, and where we had gaps, and when we saw gaps. What were some of the areas of low-hanging fruit? So we started with medical devices and looked at that and then spent the last ten months working on industrial control systems. So both assessments took, between the two, last year, medical devices took about nine months, and industrial control systems took about ten months. It's not easy to do because we're going out to sites, we're seeing what the gear looks like, what it does, we're talking with vendors, we're talking with the people who actually touch it and use it and support it. And that makes a huge difference because it takes you from what you think to what is real. That's where we are. And we are implementing a tool that gives us, it's a passive scanning tool that gives us our inventory, it gives us risk exposure, it gives us metrics that we're starting to report, even to look at asset utilization on the medical device side.

Ed Gaudet: Okay. Is it like an order or a simple?

Christopher Lau: Metagate

Ed Gaudet: Metagate. Oh, great, excellent. And what are some of the similarities that you see between MedTech and the more of the industrial control side? Was there points of leverage there that you could pull from?

Christopher Lau: Yes and no. I think there's far, a far more diverse level of expertise between clinicians, IT, and vendors on the medical device side, I think. While it may be a black box to some extent, how the vendor manages it, which is easily remedied, there's a lot of similarities, and people often are on the same page with industrial control systems. It can be completely a black box to most people. An IT mindset does not translate well to OT simply because availability is king, right? We're taught in cybersecurity, the CIA triad, right?

Christopher Lau (cont'd): With operational technology, it's inverted. Availability is the primary. So learning that these devices, the average useful life of an industrial control system is seven times that of an IT system, right? that maybe they're only patched once a year. Some of them might only be patched once every five years because of the uptime requirement or other threats that could be masked in there, for example, crypto mining. I know I sound crazy, but when you're talking about systems that have high energy output and are always online, it's somewhat easy to mask that. So that was the big difference. I think vendor support, system knowledge integration with IT, it felt more robust on the medical device side than the ICS side.

Ed Gaudet: In your organization, where do you report into? Where does OT sit? Is it on that side or?

Christopher Lau: I report to the CISO.

Ed Gaudet: You do? Okay.

Christopher Lau: Yeah, and then a dotted line into clinical engineering to their VP.

Ed Gaudet: Got it, got it. So it sounds like the med devices then are on the biotech side, biomed.

Christopher Lau: Yeah, they support them. We're providing the insight as far as vulnerabilities to remediate protection strategies prioritization, and we're looking at asset utilization. One of my goals that I've stated, and this is my finance mind at work, is cybersecurity far too often is thought of just as a cost center, and I want to change that frame of reference. And I've communicated as one of my open goals, is to become cost-neutral by 2026. And how I do that is a blend of cost savings and cost avoidance. And the biggest hole in the tent to do that is asset utilization, because you can basically kill three birds with one stone, and that you can avoid lengthy or costly support contracts. If it's underutilized, it may or may not be supported presenting a risk to your environment, and then you're also losing out on from a cash perspective. You're paying for parts, for maintenance, for other types of support that you don't necessarily need.

Christopher Lau (cont'd): So if you start eliminating those, you eliminate the financial burden, and you eliminate the resource constraints because those same resources can now be redeployed in more valuable areas, and then you also eliminate the risk.

Ed Gaudet: Coming out of with the financial background, how did you get into healthcare? How did you, actually?

Christopher Lau: Totally by accident, literally totally by accident. After I left GE, I did consulting for a while, and because of my background, the legacy Aurora leadership team had brought me in originally as a consultant to look at building information governance program and PCI and what it would take to better manage that data. And then the merger with Advocate happened, and I was about done, and then they looked at what it would take to keep me on. And so I started off with information governance and policy, and then that morphed into vulnerability management on the IT side. And then, during the pandemic is when that really started the genesis early, I should say mid-2020 started the genesis of we need to build an operational technology program. It was a quick pivot, but a very illogical pivot into healthcare from finance.

Ed Gaudet: Yeah. It's really, I always find those paths very interesting in terms of how people end up in healthcare in particular. And how did you find it different from finance?

Christopher Lau: Much different pace. The regulatory side is similar, right, that it's a different group, but you're bound by the same principles. The pace is different. You also have a lot more people that have a lot more time and grade, if you will, that they've been here for a long time, and it's more reactionary, I think where somebody goes to a trade show, maybe a physician wants a certain laptop, they want a certain application, and depending on who the physician is, it might be rushed more than maybe it should. That doesn't mean that it doesn't happen in banking and financial services. Everybody knows that people have pet projects, but I think just the pace was a lot different.

Ed Gaudet: Can you talk to the shared mission? I know everyone that comes into healthcare for the first time notices this community and the shared mission that you find only in healthcare, it seems.

Christopher Lau: I think that's, the biggest positive difference was, in financial services and banking you very much feel like everybody's out for themselves. And if you ever watch the movie The Big Short or read the book and you lived through the financial crisis, there is a lot of that. Where in healthcare, I think people genuinely want to do the right thing and take care of patients, because at one time or another, I would argue we all see ourselves there, or we all see our spouse or our kids or our parents. And I think it's that shared experience that makes us want to more do the right thing. We may have speed bumps, we may make some silly decisions along the right way, but the end game, the end goal is genuine.

Ed Gaudet: You talked about some of your priorities. What are some of your other top priorities over the next 24 months?

Christopher Lau: Every year, we do strategic planning. My team and I break it out because I have vulnerability management on an enterprise level, and then I have the OT security team, and then I'm also building up a legacy IT risk team, which is dealing with all the things. So I work just a little bit of background when I say banking and financial services. I was 16 years in GE capital, and so mergers and acquisitions was called Tuesday for us, and it just was. And so looking at all of that stuff that's left behind that people don't, you know, you move through, and you integrate as much as you can, and then that stuff that rolls off, it doesn't always go anywhere, and that presents a risk. So that's my new project. I like to have a lot of things going on, apparently. But for vulnerability management, transitioning to more risk-based vulnerability management. So old school, and this is part of my bigger thesis, if you will. We're at a crossroads, I think, in cybersecurity. And I admit I'm a newbie. I've only been in it for about a day.

Ed Gaudet: What gives you perspective, too?

Christopher Lau: I think so, and I think we're at a crossroads where we have the old school versus the new school and the old school mindset of prevention and detection and patching every vulnerability is good, but firewalls and endpoint protection aren't going to save us anymore, right? Our adversaries are very quick to adapt. They share information far better than the good guys do.

Christopher Lau (cont'd): I mean, we break out the party hats for some of these. You mentioned some of the joint groups at higher levels, we break out the party hats when we send a letter to Congress. That's a nothing burger that does nothing. But when was the last time that a health system that did suffer a cyber attack, or even a non-health system that did an after-action review, or where someone could reach out from another health system and say, hey, what were the indicators of compromise that you noticed? What were the anomalies? And share that information and learn from it and get better? We don't do that. Vendors are quick to sell us products. But they're not helping us improve our security posture thereafter, our wallet. And so I think that's the crossroads. And if we keep spending how we're spending when I had a note, cybersecurity spending is up 121% from just the pandemic year, but cyber attacks are up 314%, so we can't spend our way out of this. So this is a long-winded answer to your question that I'm trying to change the culture and build a culture on my team where, and it feeds into risk-based vulnerability management that we need to think more about not prevention, but response, exactly, response and minimizing impact. So what does that look like for us?

Ed Gaudet: No, you're absolutely spot on because it's not a matter of if, it's a matter of when. And so, better off spending your resources, which are limited,

Christopher Lau: Right.

Ed Gaudet: On being able to recover, respond, and recover as quickly as possible so you can get your operations back online.

Christopher Lau: Exactly.

Ed Gaudet: Because without that, you're dead, right?

Christopher Lau: Exactly. And it starts with knowing what you have, where it is. And I would add a third, how it's used, right? What it's connected to? What are, what's the actual purpose versus what people are using it for? Prioritizing, we can remediate all the CVS's ten vulnerabilities all day long, so we can lock the windows.

Christopher Lau (cont'd): But if we have default credentials all over the place, we just left the garage door open, we didn't help ourselves, but we made it easier for the attackers. And it's just a different, it's a different mindset. What I've said to my team is we often fancy thinking of cybersecurity as a game of chess. We're trying to outwit our opponent, and I would submit that it's actually more like poker because we're making imperfect decisions with missing information, where in chess you pretty much know all of the information. And the other aspect of it is taking that imperfect information, but using history and past performance as a data point, but not as a guarantee. If I asked you, have you ever crossed the street on a red light? Have you?

Ed Gaudet: Of course. Yeah.

Christopher Lau: Of course. All of us did. Did you get hit?

Ed Gaudet: No.

Christopher Lau: Did you get a ticket?

Ed Gaudet: No.

Christopher Lau: So does that mean you should cross against the light every single time? No. Exactly. So that's the point of where we're going is, let's put some thought into this, as I tell my guys and girls, that you have analysts in your title for a reason. Let's look at this and let's figure out where the biggest bang for our buck, where our focus is. So risk-based vulnerability management, definitely, asset inventory and profiling on the OT side, what do we have? Where is it, and what does it do? And then lastly, starting ICS risk assessment. So now that we've completed our baselines, we know the good, the bad, and the ugly. Now, we want to start deconstructing our biggest footprint by vendor exposure and/or those systems that could have the greatest impact on our mission.

Ed Gaudet: What percentage of your assets are OT-related versus without?

Christopher Lau: Without, off the top of my head, I mean, it's maybe 40%.

Ed Gaudet: Okay, I was going to say around 30, but in any concentration in any particular area or?

Christopher Lau: Ooh, infusion pumps, man, that, everybody seems to like those. I don't know if they have a favorite on the clinical side or they just buy them by the gross, but that seems to be the one. And it's harder to pinpoint utilization on where the bigger stuff is easier. When we're measuring utilization right now on MRIs, CTs, X-rays, and ultrasounds, that's the biggest bang for the buck. But all those infusion pumps, they add up.

Ed Gaudet: It's hard to hide the.

Christopher Lau: It's hard to hide a CT; they're bolted to the ground.

Ed Gaudet: How do you think we're doing as an industry post-pandemic? Alluded to it a little bit, but.

Christopher Lau: So, I have a unique perspective in that I was in banking and financial services after the financial crisis. And if you remember, in 2010, banking really had a moment where people didn't trust banks, that people, they did the bare minimum with banks. And I think, just my opinion, in 2023, healthcare is having that same moment post-pandemic, I think we didn't have thought leaders and experts weighing in enough. We let it, let is an arbitrary term, I guess. It got too politicized, and you took a public health emergency and had it become a political talking point and has eroded a lot of things. Now can that be repaired? Of course, it can. It just takes time, and I think, like anything else, time and service, and I believe that cybersecurity plays a huge role in that. Because if you can show that you have a control of your environment, we used to say, keep yourself off the front page of the Wall Street Journal, if we can, as not just an organization but as an industry, reduce the amount of presence we have on the front page, right? Or the headline of the news, even if it's wrong, you will never see that story retracted. You will never see it amended. And if it is, it's going to be on page 12. Everybody assumes the worst first.

Christopher Lau (cont'd): And so cyber plays a huge role in that. If we can help work with our leadership and our board to not only invest in the right things, but build scalable, simple, sustainable processes while having a focus on engaging, what I would argue is the largest attack surface, which is humans, customizing, training, having things that are relatable to people, but also going out and doing lunch and learns, doing webinars, explaining cybersecurity is more than phishing. Cybersecurity is everybody's responsibility, and some of it is just a little common sense, but it's common sense that people don't necessarily have to know. Because if I'm a nurse on the third shift in the ED, I'm worried about saving a patient's life. I'm not worried about a phish, right? So to have them have the same training as someone in IT? Maybe not. The second point I'd make on that is just, I think everyone in IT should have a basic understanding of cybersecurity. They don't have to be experts. They don't have to know how all the pieces fit together, but when you're onboarding new assets or you're onboarding new applications, kind of important to know that if it has critical vulnerabilities, something that we may not want to push into the environment, let's stop the bleeding. We have enough trouble, and this isn't just healthcare, this is everybody in managing vulnerabilities and getting things patched consistently within a 30-day period, let's say, or a 40-day period to bring new stuff into the environment that already has vulnerabilities. That's just a question of why. And I would argue it's an education aspect that we don't leverage enough as an industry.

Ed Gaudet: And where do you find that information?

Christopher Lau: I think some of it is just having regular dialogue with these application teams or asset teams. And as you're talking about vulnerabilities like you would any given month, they start to see how there's a correlation between what they're putting on the network and our threat level. Look, there's many times in cybersecurity, and I'm sure people listening to this that have been in it for a while will agree. You're making the choice between stinks and stinks less. There is no winning option here, it's the lesser of two evils, right? It's do I protect this or do I protect that? And we do the best with the limited information that we have, but we can get better information by involving more people in the decision, and maybe decisions that bad word, but involving more people in the process and not just in our silo, only yell at people when they click the test phish.

Ed Gaudet: I think by taking that risk approach too, it's a better foundation. It grounds people in, again, the perspective of the business versus the technology, which I think is always a better approach, quite frankly.

Christopher Lau: It is, and when you start to engage people in the business, not only then do you have you start to even get a talent pool that you could draw on that maybe as you have open positions you may not have considered previously.

Ed Gaudet: That's right.

Christopher Lau: But now, if your cyber team is 100 people and your organization is 1000 people, and you train them appropriately, you just 10x-ed your cybersecurity team. And I know that sounds naive, but they're not going to deal with technical aspects. But if you can get people to start thinking that looks suspicious, I'm not going to touch it. You start to protect yourself better when people know, hey, maybe I should use a password manager instead of a post-it note on my keyboard. That still happens. Maybe I should lock up my laptop or take it home. Maybe I should just lock it, period.

Ed Gaudet: Right.

Christopher Lau: Those kinds of things.

Ed Gaudet: Or Chris never sends me a text like this.

Christopher Lau: Exactly. And that's all low-hanging fruit. And that's something you can build a nice report card on to go back to the board and say, here's what we're measuring. Here's where we were when we talk metrics, even just in vulnerability, my predecessor measured total vulnerabilities. That's a worthless metric because it can go up or down. Why did it go up or down month over month? Don't know, it just did. Where we're measuring SLA, how are we in terms of what is required? We're measuring patch efficiency out of our critical and highs. What percentage are we hitting and tracking that month over month? Where do we see default credentials?

Christopher Lau (cont'd): Where do we see unsupported operating systems or what's coming around the corner as unsupported operating systems? Because that's then where you can focus your effort and your limited resources to, okay, we know server 2016 is going into support in a couple of years. Let's start talking about that now, I think, what is it? 2012 comes end of life this year, memory serves. So you start marshaling resources in a more focused manner instead of playing whack-a-mole, and you're using data to support your decision.

Ed Gaudet: Technology end of life with an oxymoron, that is, does anything actually end of life?

Christopher Lau: No, as long as, I had a friend that worked in support, and he always said as long with enough money and enough time, you can do anything. So as long as they can get parts and you still have a wallet, they'll support it.

Ed Gaudet: Exactly. One thing, what keeps you up at night?

Christopher Lau: Children. No.

Ed Gaudet: That's a good answer, actually.

Christopher Lau: I think, what I don't know, and what I, this is just a development need on my side is, I try to go in with a bulldozer, and I have, while I have my priorities, and I limit them purposely to three. I see all the things that I want to tackle, and I start to think about how I can do that. And I wouldn't say it's a specific threat that keeps me up, because I would argue there's no one threat that is greater than the other, but it's the unknown.

Ed Gaudet: Yeah.

Christopher Lau: And to some extent, it's that known unknown that we know we have stuff out there, we know what it does, but we don't know anything about it.

Ed Gaudet: Yeah, and we don't really understand the blast impact that something could have, right? That's the most concerning thing like, block for Jay was sort of a like we.

Christopher Lau: Yeah.

Ed Gaudet: A graze. No one...

Christopher Lau: It was.

Ed Gaudet: And it was hurt.

Christopher Lau: It was a shot across the bow.

Ed Gaudet: It was.

Christopher Lau: But now you take an industrial control system and if someone takes it down or it's not upgraded in, it doesn't even have to be a cyber attack. It could just crash.

Ed Gaudet: Right.

Christopher Lau: Right? Now you're talking about that facility being shut down. And if that facility is shut down, now you're talking about patient impact, you're talking about reputational damage and risk and financial impact. If you take a facility again, I'm just using round even numbers, right? If you use if you take a facility that earns, has $1 million a day, and it takes 45 days to get that back online, you just lost $45 million publicly. Not to mention, the reputational damage.

Ed Gaudet: Which is what happened in San Diego. What happened in Vermont, right?

Christopher Lau: Yeah.

Ed Gaudet: We read about these incidents. And your point you made about staying off of the front cover of Wall Street Journal. I was thinking about if you did have an event and you could actually say you recovered it in less than a day, maybe that's actually a good thing to be.

Christopher Lau: That would be a good thing. That would be a good thing. And I think we could make better strides if we worked as a community and as a team to analyze events, to analyze data, leverage best practices, and work together. The bad guys have no problem doing it.

Ed Gaudet: They're doing it. They figured it out. They've got this notion of microservices.

Christopher Lau: Yep, but the good guys, we don't want to talk to each other.

Ed Gaudet: It's a lot more difficult. We're making progress. I mean there's definitely progress being, but you're right. It's too slow. Like we need to go faster because they're on to the next thing they're thinking about the next thing.

Christopher Lau: Right. It's every vendor that tells me, oh, this is AI, we have AI, and my first response is always, so do the bad guys. So now how does this protect me better?

Ed Gaudet: I would be concerned about someone telling you the AI too, where's the AI being hosted? The thing that people don't realize is like, you don't have your own personal model, that you're hosting yourself. You're leveraging a public hosting facility, which is exactly a security risk. It's a problem, right? Until we figure out how to solve for that problem, general use of AI, at security level is going to be challenging.

Christopher Lau: And I fully admit I have my tinfoil hat on, with respect to AI, maybe I watch the Terminator too many times, I don't know.

Ed Gaudet: Oh, some really great use cases there that are available. Our biggest challenge is we look at it internally is the security model of it. It's great that you leverage it, but at what risk?

Christopher Lau: Exactly.

Ed Gaudet: Will customers actually buy off on that and sign off on that? So that's.

Christopher Lau: And it's one of those things I think just because you can, should you.

Ed Gaudet: Exactly. Yeah, yeah. So it'll get fixed, it's rapidly changing. I mean, the progress AI has made over just the last six months, it's just, it's incredible.

Christopher Lau: It has. My consternation is the same groups that have given us the condition that we now deal with a lot of not just technology flaws, but things that honestly, I'm looking at you, social media, that haven't made the world better, those are the same companies that are working on AI, and I think that's where I get a little bit nervous that, are they going to do the right thing with this and make it a powerful tool, or are they going to make it for profit? Time will tell.

Ed Gaudet: They're going to make it for profit, there's no question.

Christopher Lau: Absolutely.

Ed Gaudet: That was an easy question.

Christopher Lau: I'm a silly optimist in that I'd like to believe that if you benefited, the whole on a large scale, you'd make more profit than if you benefited a few in the short term. But I'm naive.

Ed Gaudet: There's a lot of scary things going on, and it all starts with the phone.

Christopher Lau: It also. Anybody with a teenager, I'll tell you everything bad starts with the phone.

Ed Gaudet: That is the root of all evil right now is the phone. And I mean half of the things people don't understand.

Ed Gaudet (cont'd): I had a really freaky thing happen. I was just on vacation, and I was walking by this boat, this particular boat, it's a very unique boat style, whatever. And I didn't talk about it with anybody. I just happened to stop and stare at it, and look at it, and admire it, and check it out. And I was, you know, within four hours, I got an ad served to me for that boat. Now, I didn't talk to anybody about it. I didn't even mention the name. I was just in front of a boat of that make and model. And it was, now you could say that was a coincidence. And you've looked at other boats, and so maybe they just happened to be, I don't believe in coincidence. And it was so weird that they had my location, they knew that boat was there, and they were able to actually take those two bits of data and leverage that. So it's not just the, it's just not the audio that they're mining, location, they're mining the combination of data points within location. It's quite scary.

Christopher Lau: Yeah, it's everything. I mean, it's even when you look at data security, I would argue almost need to start by assuming your data is already out there.

Ed Gaudet: Right. Exactly. Yeah.

Christopher Lau: Now, how do you contain the blast radius? Because they're not going to come back multiple times for data. They're going to come back for more damage. So how do you build a moat around your critical infrastructure?

Ed Gaudet: And prioritize availability, like you said earlier. That is confidentiality used to be 20 years ago, right? And a bigger impact, right? It's like, when I started up Censinet, it was like we were starting to see the beginning of the impact of ransomware back in 2016, and thought to myself, nobody died when data was stolen.

Christopher Lau: Right.

Ed Gaudet: This is going to be a much bigger impact to health systems because they're going to shut down, divert care, cause real issues, and that's effectively what's happened happening with ransomware. And so I do think it's that availability that should be the focus on everyone's strategic plan to maintain that availability, and sure, we don't go down.

Christopher Lau: Well, and building a strategic plan to that point of assuming, start with the scenario that you had a ransomware attack and now work backwards.

Ed Gaudet: Right.

Christopher Lau: What? Think like an attacker. What would you go after first, right? Okay. They're going to encrypt backups first. So make sure you have offline up-to-date backups. Make sure you have a clean network. I understand that's not cheap to set up, but if you start with, and that's, earlier, I talked about that intersection of old school and new school. I was recently in at Pearl Harbor, and they, if you've been they have a film and not too dissimilar to what you see in school, right? High school history class, right? But at that time in 1941, from a military perspective, they were also at a crossroads. You had the commanding officers of the Pacific Fleet that were World War One veterans, and they believed in ground forces and big battleships, and they were worried about espionage, and they didn't trust radar. It was still newer, to be fair, and discounted junior officers that said aircraft carriers and aircraft are the that's the future, right? And Pearl Harbor was a tragedy, but some things where you think, just unforced errors. They parked the planes tip-to-tip on the airfield, making it easy for the Japanese to bomb it. And I couldn't help but draw some of the parallel to cybersecurity, right? That we continue to try to do that the old ways without thinking, wow, what if that does happen? We're relying on defense as opposed to scenario planning and giving some credence to what could.

Ed Gaudet: That's right, yeah. That's a really great observation. We are, I can't believe we're already running out of time. This has been so fascinating. I have a couple more questions, if you have some more time.

Christopher Lau: I absolutely do.

Ed Gaudet: Excellent. Outside of what you're doing today, what are you most passionate about?

Christopher Lau: I think just learning new things. I've always liked to learn. But outside of just cybersecurity and nerdy stuff, I love trail running. I love getting out in the woods, and it's my therapy. It's, you decompress, there's no phone around, and you just, it's a way to, it's meditation. It's just, you out there, especially, I go early mornings, and it's really nice.

Ed Gaudet: You run alone, or you have a dog that goes with you or?

Christopher Lau: I, no, I run alone. Occasionally, I've seen more than my fair share of deer that they look at me like, what's this strange thing doing out? I did have one, one time where I came around a corner and ran literally almost into a coyote. So you could say I ran with a dog that day. Otherwise, just by myself, just to kind of collect my thoughts and and recharge.

Ed Gaudet: Now, do you go outside of where you live, or do you do you travel?

Christopher Lau: I do. I do some races, and I'll go, I'll travel a little bit. Next year is a big race, a trail race in Utah. I'm excited about that.

Ed Gaudet: Where is that?

Christopher Lau: It's in Salt Lake. It's in Salt Lake. It's one of the trail series is called UTMB, Ultra-trail du Mont-Blanc. And it started as just in Chamonix, France. That would go around and up Mont Blanc, but now they have a global series and one of the big races is in Utah in July. So I have a couple races between now and then, but that's the big one on the real.

Ed Gaudet: Salt Lake that's going to be warm.

Christopher Lau: Climbing a mountain, though. Climbing a mountain.

Ed Gaudet: That's true.

Christopher Lau: It'll be more power hiking than running, I suspect.

Ed Gaudet: That's very cool. If you could go back in time, what would you tell your 20-year-old self?

Christopher Lau: A great question. I think, work hard, and look for opportunity. There's things that, don't accept things as they are just because they've always been that way. Look for how they could be done better.

Ed Gaudet: I love that. Stay curious.

Christopher Lau: Stay curious.

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

Christopher Lau: But I can name the dumbest thing.

Ed Gaudet: Which could be the riskiest.

Christopher Lau: It could be. It probably is. I was playing golf with some friends. This is probably over a decade ago, and we were playing on a course. My buddy had gotten a tee time and it was a tough course to get on, and a thunderstorm came up and we, despite them blowing the horn, we did not go in. We did stop playing for a period, but we finished our round. Let me put it that way because we were on 16, so we were going to finish.

Ed Gaudet: How many people get struck by lightning on the golf course?

Christopher Lau: Yes, and I'm thankful every single day that I can't...

Ed Gaudet: Hopefully, you were 20.

Christopher Lau: I was in my 20s, so yes.

Ed Gaudet: So maybe you could tell your 20-year-old self don't do that.

Christopher Lau: Don't do that. That was not smart. You could've not gone home that night.

Ed Gaudet: That's terrific. Thank you so much for sharing your experience and your background with our listeners. Any last-minute comments or thoughts you'd like to leave people?

Christopher Lau: I think two things. One, that I just said, stay curious and challenge. Even if you built the process, look at it new with fresh eyes and ask, if I were to redesign this, would I do it the same way? And the second thing is, be comfortable with imperfect information. Treat it like you're playing poker, not chess, and learn to adapt, using past experience as a data point, but also leveraging the business and the strategic goals of the organization and where you want to go with your program as other data points, not just relying solely on technology.

Ed Gaudet: That's great advice and a great way to end. This is Ed Gaudet from the Risk Never Sleeps Podcast. If you're on the front lines 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