CENSINET®

Podcast Transcript

Risk Never Sleeps
Episode 4
Lucia Milică Stacy

Ed Gaudet: Thank you and welcome to another episode of Risk Never Sleeps Podcast. I'm Ed Gaudet, I'm your host, and today I am joined by my good friend Lucia Milică Stacy. Did I get that right?

Lucia Milică Stacy: Yes, you did. That's pretty good, actually.

Ed Gaudet: Perfect. You know, it'd be tough to say good friend and not be able to pronounce your name.

Lucia Milică Stacy: Exactly, 100% agree. Well, thanks for having me. Good to be here.

Ed Gaudet: Excellent, excellent. So maybe give our listeners just a little bit of background of your current role, your current job, which you've been up to over the last couple of years.

Lucia Milică Stacy: Oh, happy to, so I am currently the VP and Global Resident Chief Information Security Officer at Proofpoint, which is a leading cybersecurity and compliance company. In my current role, I have the privilege of leading a team of peers, a team of CISOs, and really focusing on bringing value-add advisory services to our CISO community to first and foremost, of course, our CISO customers, but just broadly the bigger cybersecurity community.

Ed Gaudet: Okay, great. And how did you get into cyber and how did you get into healthcare cyber?

Lucia Milică Stacy: So, sort of to set the stage a little bit, in my previous role, I served, and then it's the same with my entire team, we all served as chief information security officer, and that was the same for me, I was Chief Security Officer and Chief Privacy Officer. Now, I've had the privilege of building an extensive technical and business experience for various different roles running IT, governance strategy, and cyber risk and compliance and corporate and product security and privacy and IT Infrastructure, you name it. And through my journey, I happen to have both a legal and a technical background that I think is very unique to the industry or to the CISO role in particular. And through that, through that legal lens as well as security and running product, you name it. I've worked for a number of technology companies that provided services or technology services to the healthcare industry. So being a business associate through that over time I became the HIPAA compliance officer.

Ed Gaudet: Oh, lucky you!

Lucia Milică Stacy: ..., yeah, right? I spent quite a bit of time diving in into the HIPAA requirements, but also, how do I protect the data, right? So through there was telehealth or various different services over time. How do I hone in into protecting the health information? What are the requirements for business associate and making sure that I build in the right policies, procedures, training necessary as part of those programs, and educating the user community and employees for the particular organizations on how to adequately protect that data. So those sort of earlier maybe, gosh, I don't even know how many years ago that's been, it's been some time. That was sort of my entry point into healthcare. I think over time, as I've taken on this responsibility, a couple of different organizations, I got deeper and deeper into patient safety, care delivery, the challenges associated with it. We always hone it into third-party risk. And, of course, as a business associate, that's always a, the risk associated with the services that healthcare providers have to employ, etc., which really brought me to healthcare, and I continue to be very involved in the industry today.

Ed Gaudet: You are, and let's talk about the work you do outside of Proofpoint. So specifically in support of the 405(d), and there's some listeners, I'm sure that don't know what the 405(d) is. And so how would you describe the value of the health industry, cyber security practices, documentation, and a set of recognized security practices that are made available through the 405(d)?

Lucia Milică Stacy: So working as part of the 405(d), really volunteering in our spare time, as you and I have done for many, many years now, as we know the cyber threats to all of us, but very specific to healthcare organization are really core in terms of placing patient health, patient care, and delivery and patient safety at the core of everything we do, right? Threat actors are continuing to innovate, they're continuing to employ new tactics. And it's important for all of us, but more so for healthcare organizations to stay at the forefront of a lot of the tactics and techniques and the various different tools that threat actors are leveraging to disrupt care delivery and impact healthcare organization. But really, a lot of this has to do, of course, with the value of personal health information that's, I think, stays at the center of what threat actors are after, right? So I think it's imperative for all of the healthcare organizations to understand those, but also understand what are the top risks to that organization? How are they being attacked? How are they being targeted? What are the right adaptive controls that they have to implement to constantly try to stay ahead of what's happening in the ever-changing threat landscape, as you and I both know, right? So through the lens of 405(d), and for those of you that are not accustomed to 405(d) is really, under the umbrella of the Cybersecurity Act of 2015, there's a section named 405(d) where the US Department of Health and Human Services convened the CSA 405(d) task group to really enhance cybersecurity and align industry approaches by developing the set of voluntarily consensus-based, and/or industry-led guidance methodologies, best practices, recipe cookbook, you name it, and bring a lot of that knowledge to you so you can take those very, practicer guide, or what we love to call it recipe books, right, on terms of cyber risk and be able to implement them in your organization. So part of that effort, super excited, there'll be some cool new content coming up hopefully soon. Ed and I've been working on this for quite some time.

Ed Gaudet: We have been.

Lucia Milică Stacy: And in one of the co-leads under the bigger umbrella of the CSA 405(d) task group focusing on just a very small portion of those cybersecurity best practices.

Ed Gaudet: Great. Well, so obviously, your customers rely on you, your organization relies on you. The public-private partnership of the 405(d) relies on you. What keeps you up at night?

Lucia Milică Stacy: Well, I wouldn't say quite the full 405(d) relies on me because there are a number of folks, I'm sure. I would be remiss if I don't mention the amazing work that Erik Decker has done to lead us as well as Julie. So, so many people have been, not to mention yourself as well from the beginning, about so, so many people have been involved in this. I think we have what, over, not even exact, 150-200 cybersecurity and healthcare experts?

Ed Gaudet: Yeah, I think with the greater Health Sector Coordinating Council, it's probably closer to like 700, 800 now, so.

Lucia Milică Stacy: It takes a village, that's just a small, small portion of the total story. But for me, I think, look, our jobs never end, right? As a security leader, it's upon us to stay ahead of understanding the business risks organization and how cybersecurity threats are impacting their business risk broadly. More than that is making sure that your team is functioning in all cylinders, that you have the right resources, and it's not if, it's when one of us will be attacked is how are we acting when that happens? Do we have the right defense mechanism in place? Is our team resilient and able to respond when that happened, or is my team overworked and stressed out, and they're not able to think through the intricacy and nuances of any particular incident? But really, the bigger piece is what you don't know. We can't protect what we don't know, which is why so often Tom and I talk about this quite a bit is visibility is key, right? Understanding what you have is a huge step forward into formulating your approach to mitigating that risk broadly.

Lucia Milică Stacy (cont'd): While you don't know, it's what I think oftentimes gets us in trouble, which is why there so many challenges that in a broadly, in the industry that we have not been able to solve for. One that comes to mind right away, that we just mentioned is supply chain and understanding. Obviously, third-party supply is important, but further than that, going to fourth, fifth, six-party supplier and where that risk can come from, that you don't always have your visibility into those environments that I think are some of the bigger challenges.

Ed Gaudet: Yeah, I know, I agree. I often say transparency is the enemy of risk. If we have full transparency, we have a better shot at combating where the next risk is going to come, whether we understand it or not, we're much more agile as well as an organization can adapt, and that point about recovery is so spot on. It's like half of the job is preparing, and half of the job is being able to recover from an attack when it happens, so really spot on. It's been an interesting year, 2022, coming out of the pandemic. What are you most proud of over the past year, either personally, professionally, or both?

Lucia Milică Stacy: I would say professionally is really being able to, I've published a couple of reports. One of them was around Voice of the CISO. This was the second annual. We started doing that during the pandemic as a way to really understand what all of us are grappling with around the globe. So we're able to publish the second annual. But the bigger one, I think is the second report was a compendium to the first one is focusing on board of directors and their understanding of cybersecurity risk, as you and I talk about quite a bit, right, there continues to be a gap between boards and CISOs while, I think boards understand the cybersecurity is important, it matters, thing that meeting of the mind between board members and security leaders is not always there, and what we always knew anecdotally was very apparent in seeing that data. So taking a step was really, I think, the first step towards trying to bridge that board-CISO relationship and communication and kind of, same as cyber risk. It starts out with data and visibility and understanding what those challenges are. So I think being able to put that together and publish that and the latter part of last year was really phenomenal in terms of having, okay, we have a problem, how can we start addressing this and trying to close the gap? Well, I think we have long ways ahead, right? I think it's a beginning towards hopefully a stronger partnership in the future.

Ed Gaudet: Absolutely agree. All right, so let's turn to the person behind the protection of patient safety. Outside of your day job, outside of cyber, what are you most passionate about? What do you love to do?

Lucia Milică Stacy: Oh, gosh. So, you know, the security and law are my two passions, and I love them both. But when I don't do that, I love spending time with my family. My husband, who is also in technology and cyber security, he's my best friend. And I think we're fortunate to be raising a kind and brilliant son who's 11 going on 18, to say the least and.

Ed Gaudet: They all are these days.

Lucia Milică Stacy: Exactly, and we're surrounded by the unconditional love of two crazy, amazing dogs, they're in the middle of our life at all times. But when we're not just home spending time together, I think we all love playing tennis and golf in the summer and skiing for me, snowboarding for the boys in the winter. So I think between the various different sporting activity and business travel, oh, we all love travel as well. So whenever, when I'm traveling, it's for business or pleasure, but we prioritize at least two vacations a year, whether they're just small, three, four days, or extended vacation every year. I am one of those people that I, and I know it, right or wrong, I give 150% of myself, but I need ... the break. And when I don't take that break, I definitely will feel it. And I think last year I probably had a little shorter break than I would have liked, and I definitely felt that towards the latter part of the year. So I really want to focus. One of my personal goals for 2023 is to really try to focus on resilience, taking the downtime, right? I can't, I can't be an effective leader if I'm not true to myself and I'm not able to pause and restore and bring that balance every day to work, so.

Ed Gaudet: Yeah, 100%.

Lucia Milică Stacy: I'll tell you how I do it at the end of the year.

Ed Gaudet: It's so needed, especially I think, certainly for me, I'll be in Aruba next month. So I'm looking forward to that downtime. But I just need to sit and read a book and unplug, quite frankly, because like you, I give 150% and it's so tough to unplug. But once I do, I just want to do it for like ten days. Just give me ten days.

Lucia Milică Stacy: Yes, that's awesome.

Ed Gaudet: What would you tell your 20-year-old self? I know that's a tough one.

Lucia Milică Stacy: Yeah, I would say, believe in yourself and listening to your instinct, I think way too often we overthink everything. Have that little voice or this, I feel like I do. I have that gut feeling just telling me like, you need to do this, but then I start to overanalyze it or overthinking. And ultimately I feel like every time never failed. When I did not listen to my instinct, it proved that I made the wrong choice for something small. Regardless, definitely try to listen to what your instinct tells you.

Ed Gaudet: Excellent. Similarly, I always find when I go against my instinct, my gut, often wrong, but never in doubt. Because this is the Risk Never Sleeps Podcast, I have to ask this question. What is the riskiest thing you've ever done?

Lucia Milică Stacy: Well, so you ask, it's interesting because you ask the question about whether to tell your 20-year-old self. So I think I have a few that top the list, but which is interesting because I'm absolutely very risk averse in general. But I think probably the riskiest thing I've ever done, I moved halfway around the world in my early 20s, the beginning of my career. And interestingly enough, my first role, so I moved from, I'm originally from Romania as I moved from Bucharest, Romania, to the Bay Area, which was a big move when you're in your early 20s, and I worked for Wells Fargo Bank, doing Y2K compliance is my first official technical role. I know.

Ed Gaudet: 11 years old?

Lucia Milică Stacy: I just dated myself, I know, I just dated myself on that one, but I'll say that was by far the riskiest move now. Now, at the top of the list is also jumping out of a perfectly good airplane.

Ed Gaudet: Absolutely.

Lucia Milică Stacy: And going to get my dive certification, besides the fact that I had a water phobia at the time, so I was determined to overcome it, and somehow I made it. I got my dive certification and I can say, been there, done that, check the box, but I was petrified throughout the entire time.

Ed Gaudet: Did you swim with sharks?

Lucia Milică Stacy: I did, except they're just Nurse Sharks, so, but at the time I was a little bit nervous. I did swim with sharks.

Ed Gaudet: They're still sharks. That is fantastic. All right, well, that's really helpful. Any last comments or thoughts? This has been fantastic.

Lucia Milică Stacy: I would just say, if you ever have the chance to check out, for those of you security leaders in the industry, as I mentioned in the beginning, I'm fortunate to lead a team of phenomenal peers. And last year we launched what we called the CISOhub, which is a place where every month we bring resources, content for various different topics, they are top of mind for the broader sense of community. So if you have a chance and or have any particular areas of interest you want to hear more about, you're looking for resources, check out the CISOhub and you'll be surprised. There are quite a few amazing resources and interesting insights from the entire team, not just myself.

Ed Gaudet: What's the URL for that?

Lucia Milică Stacy: It is Proofpoint.com and I believe CISOhub, there you go. So it's Proofpoint.com/US/CISO-hub.

Ed Gaudet: Perfect, all right. Okay, well, thank you for your service protecting our health systems, our health infrastructure, and overall patient safety and care delivery. And thanks to everyone for listening, this is Ed Gaudet with the Risk Never Sleeps podcast. And for those of you on the front lines, protecting patients every day, remember to stay vigilant, and 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