Podcast Transcript

# Risk Never Sleeps
# Episode 35
# Joe Sullivan

**Ed Gaudet:** Welcome to the Risk Never Sleeps Podcast, in which we learn about the people that are on the front lines, delivering and protecting patient care. I'm Ed Gaudet, the host of our program, and today, I am joined by a special guest, Joe Sullivan. Basically, you're the CEO of Ukraine Friends, is that correct?

**Joe Sullivan:** Yeah, thanks for having me on the show.

**Ed Gaudet:** Yeah.

**Joe Sullivan:** So, yeah, I'm the CEO of Ukraine Friends, which is a nonprofit. And I also have a background in cybersecurity, and I've spent my whole adult life working in cybersecurity.

**Ed Gaudet:** Tell us about your organization. Tell us a little bit about your role there.

**Joe Sullivan:** Sure. When the, a little bit before the full-scale invasion of Russia happened in early 2022, I was working at Cloudflare, which is a leading internet security company, and I've been there for about three years at the time, helping the company grow, and we got contacted by the United States government, and they asked us to help the Ukrainian government and kind of businesses in Ukraine get ready for an invasion.

**Joe Sullivan (cont'd):** That was back at the time when the United States government was telling everybody who would listen that the, that Russia was going to invade Ukraine, and nobody seemed to believe that, including the people in Ukraine. But I spent a bunch of time at Cloudflare, and in that role, getting our cyber defenses in place for Ukraine. And sure enough, the invasion happened, and we had to be at Cloudflare essentially on the front lines. We had a lot of companies and government agencies and everything in between behind Cloudflare on the Ukraine side, but we also were operating in Russia and so had a lot of websites and things like that in Russia protected by our servers, even when we chose to stop making money from the Russian side. And so really got exposure to that war and the tragedy of it really quickly. So fast forward to last fall, I left Cloudflare after four years there and kind of going through a personal saga on the side, dealing with what I sometimes call the hangover from my time at Uber, where I had to go through a bunch. And I left Cloudflare and I contacted a friend, actually a recruiter, who had placed me both at Cloudflare and at Uber and said, I really would like to do some volunteer work related to Ukraine on the cybersecurity side, I was thinking. He contacted me in January and said, I found the perfect role for you, CEO of a nonprofit doing humanitarian work in Ukraine. And I said, wait, I wanted a ten-hour-a-week volunteer thing, not the CEO role, and he said, well, talk to the board. And I talked to them, and they were really passionate about what they were doing in Ukraine, and they had a real energy and decided to take it on. Before you knew it, I was in Ukraine learning firsthand about the humanitarian challenges, and here I am still doing it as we get to the second half of the year, and I'm committed to doing it at least through the end of the war.

**Ed Gaudet:** And are you getting, are you traveling over there at all now, or?

**Joe Sullivan:** I am, yeah, my most recent trip, I was there at the end of June into July. I actually spent the 4th of July in Kyiv, which was definitely a weird experience, but also the time there, every time I go, it's a strange going into a war zone. People won't make plans to meet with you when you contact them from the United States and say, hey, I'll be in Ukraine next week. They say, yeah, sure you will. But then, when you actually get there, you end up having a million meetings and connecting to people, and there's just a lot going on, and at the end of every visit, I feel like I wish I'd had more time there. This last trip, I was doing a lot of work related to a new initiative we started this year, we call it Digital Wings.

**Joe Sullivan (cont'd):** We get companies in the United States to donate their recycled laptop computers, and we bring them over, and we give them to children in Ukraine. I had three daughters have to go to school through the pandemic here in the United States, and it was an awful experience for us, even though we live in a good community, and I'm very blessed to be able to make sure that they have good laptop computers and everything they need to do remote schooling. It was still, it was hard, and the kids who had to go through that in our country will that'll be a shaping experience for their whole life. But imagine the kids in Ukraine who went through the pandemic the same way our kids did, only to be told, now you're staying in remote learning because we're in a war. And by the way, the school just got blown up, and your teachers are 500 miles away because they're refugees, and we got to try and piece together, and do life in the middle of this war. On top of that, it was an economy even before the war started, where the average family made about the equivalent of $2,000 a year. So it's not like they have, they don't have the option to go online and order a laptop computer and have it delivered to their house, even if they had the money. It's a tough situation, and the first time I brought a laptop computer over and gave it to a 13-year-old girl who was living with her mom in temporary housing because their house got destroyed, they started crying, and I almost started crying myself because they were just so happy that there were people out there, people in the United States who cared enough to reach out and make that moment happen, and now she gets to do her remote schooling on an actual laptop computer instead of borrowing her mom's phone.

**Ed Gaudet:** And that was, I assume, the inspiration to Digital Wings program.

**Joe Sullivan:** Exactly. We were, we started out this laptop initiative kind of slowly to figure out what it work. Would a used computer from a company in the US be valuable and meaningful over there? It turns out we're a country of abundance. When our employees leave our companies after two years, the company looks at that laptop and doesn't give it to the new employee coming in, they just kind of putting it in a stack in the corner, and getting, lots of companies have come forward and said, hey, we've got 50 of those laptops. We've got 20, like small companies have donated 10 laptops, big companies have donated hundreds. And we take those over, we refurbish them a little bit, we make sure they handle the trip, and then we give them out to kids, and they're making a difference.

**Ed Gaudet:** And how can people get involved if they want to get involved, Joe?

**Joe Sullivan:** Sure. Anyone can reach out to me directly. I'm on LinkedIn, highly visible there, and we have a website also, UkraineFriends.org, and through that, appearances like this, I've met a lot of people who said, hey, I'm going to go check what's going on inside my company. What are we doing with our old laptops? And I've even had some people say they've gotten some laptops from their company, but they've told their kid, why don't you go find five laptops with your friends? And honestly, we even need chargers. A lot of companies donate laptops to us, but the employees always keep the chargers. They give back the laptop because that's company property, but they forget to turn in the charger. They don't forget, but everybody needs our chargers. We collect chargers from communities, and we send them over.

**Ed Gaudet:** Thank you for that. For your service there. I mean, that's incredible. And again, encourage listeners to go to Joe directly on LinkedIn or to the Ukraine Friends website and get involved if you can. What are your other priorities over the next couple of years with the foundation?

**Joe Sullivan:** With Ukraine Friends we're, I like to think of us as kind of a start-up in terms of, we look at the situation and we adapt based on what the market needs. So in the same way, you know, I grew up in my career here in Silicon Valley, working at companies that were growing. And one of the things that I always saw was a mark of success for an organization was that they didn't get set in their ways, they were nimble, they listened to their customers. And so that's why I personally go to Ukraine as I want to see, okay, how do we navigate corruption to get these laptops through borders into the country safely and into the hands of the kids? Do these laptops make a difference? Is there something different we should be spending our time on? I mean, we know with the different seasons come different challenges. We've focused on kind of with this season right now, being the start of school, we really wanted to help out. We found a few different schools in the country where we've donated laptops to the schools and the teachers, but we've prioritized getting them to the kids who are in remote learning going direct to them. But we're also thinking about mental health and the challenges there. We recently put together this big sticker.

**Joe Sullivan (cont'd):** We worked with a bunch of different groups that have thought about mental health challenges during a war, or during remote schooling, or the combination of both. And so we actually have a full page sticker that covers the top of a laptop that we give out, and it has important contact information. Like here in the United States, we have something called lifelines, which is a hotline number, anyone can call for free, and you'll get a trained therapist if you call that number, if you're thinking about suicide. And I used to work a lot more on suicide prevention here in the United States. I was on the National Action Alliance for Suicide Prevention, which was a public-private partnership, and we focused on trying to educate people about when someone's contemplating suicide intervention is so critical. Even just having that person having a chance to talk to someone, if in that moment they're deterred from the suicide, they may never come back to that level of desperation again. And so having visible reminders that there's someone that can talk to matters. It turns out another nonprofit had worked really hard to set up the equivalent of lifeline in Ukraine, but their biggest challenge was nobody knew they existed. So we put their contact info and the hotline right on the sticker that's sitting on every laptop that we give out. Because what's the one thing you never lose? That you're always looking at your laptop, it's nearby. So we turned that real estate on the top of each laptop into kind of health information. There's a little breathing exercise for teenagers on how to reduce stress and anxiety. There's all that contact information, and we kind of adapt the sticker to the different audiences that we give out the laptops to, okay.

**Ed Gaudet:** Wow. What a what a smart idea. What a great use of the, how many laptops have you given out so far?

**Joe Sullivan:** So we've, we're in the hundreds of thousands of dollars worth of laptops, probably getting close to a million. We regularly ship over bulk laptops and kind of 100 to 200 at a time, depending on the donations from companies. I've learned a lot about shipping ... because laptops are hazardous. They have those lithium-ion batteries and things like that. So you can't just you can't just put them in a padded envelope and mail them. You've got to think through and make sure you're complying with hazardous materials, shipping standards, and stuff like that. But we've worked through that. We have some good logistics partners who volunteer and donate their time to teach us how to do that, and make sure that we ship things safely.

**Ed Gaudet:** What a great program. Any thoughts about extending it outside of the Ukraine?

**Joe Sullivan:** Yeah, it's interesting. When you start in a new role, part of what you typically do is you talk to anybody you think you can learn from. And for me, my career, my last three titles were Chief Security Officer, Chief Security Officer for Cloudflare for years, Chief Security Officer at Uber for two and a half, Chief Security Officer at Facebook for six plus, and going and being a CEO and being CEO of a nonprofit were just totally new growing experiences for me, and so I've talked to a lot of nonprofit leaders, and I've learned from every one of them. And you're right, the need we're addressing in Ukraine is a challenge everywhere. And funny thing, our nonprofit, when the founders started it, they incorporated the 501C3, so we're an official nonprofit under the name Worldwide Friends but operating as Ukraine Friends. And so, as a result, we do have internally that bigger mission. Now, at the moment, I'm 100% volunteer, and I'm based in the United States. We have one employee in the United States who's full time, and she is a refugee from Ukraine who arrived shortly after the war started all on her own independently because she was fortunate to have a visa to come to the United States for a model U.N. event that she got issued the week before the war. And she's our only employee in the United States that's a dedicated full-time employee, and then the rest of our employees are in Poland, in Ukraine. But we are really focused on what's happening there. But we have expanded our remit a little bit, we've given some laptops to Ukrainian students who fled the country and are in other countries. So like, logistically, we're just working on getting some to a family in Croatia, for example. And then, when we see other humanitarian situations, we look and see how we can help. For example, with the earthquakes in Turkey and things like that, can some of our logistical experience around medical equipment or any of the supplies we have in the region, easily deployable there? But it's been much more kind of like little one-off things and not what I would call a program to this point.

**Ed Gaudet:** Yeah. Well, the experience you highlighted earlier about being able to ship into certain areas and know how to use a core competence that building up.

**Joe Sullivan:** Yeah, for sure. Absolutely.

**Ed Gaudet:** I imagine there, are there any implications for security perspective as you educate and train the recipients, or how does that work?

**Joe Sullivan:** Yeah. So a couple of interesting kind of anecdotes to share on that. I was working with one college here in the United States. A couple of professors were thinking about doing a course, and this was last spring. They were thinking about doing a course focused on the Ukraine war, and they wanted to look at it both from a computer science and psychology perspective. And so the two professors from the same university thinking about it from two completely different sides. And so they were contemplating bringing their college class either to Ukraine or near Ukraine. And so someone put them in touch with me just to talk about the logistics of something like that. And I explained to them that you really don't want to bring people into a war zone. When I go, I go very carefully with an express purpose, and I don't want to create more risk for my family, or honestly, for the Ukrainian government or the US government to have to deal with. So I'm, I try and be very laser-focused, get in, get out, do what needs to be done, and I don't want to bring people there unless they have a real intentional purpose, could be really meaningful. And so I started talking to these professors, and they're actually going to bring their class to Poland near the border, because there's a lot of support happening for the Ukrainian community just inside Poland, and Poland, I don't think has gotten enough credit for how many refugees they've absorbed into their country from their neighbor and how much they've done. And as I was talking with them, one of the things that came up was the idea of having an American college student partner almost be a pen pal, if you will, with someone in Ukraine who is at a similar stage. We, I set up the first of those, that's happening right now. So it's a cybersecurity major student in the United States who we've partnered with a team in Ukraine who wanted to get into a career in cybersecurity. So we're doing that as a pilot right now, and we hope to expand that even more. So that's one example of how we're thinking about cybersecurity. A second thing, that when I first arrived in Ukraine, I started meeting with government officials, and they would all look at me, and they'd say, okay, Joe, we've looked at your background. You've been in cybersecurity for 20-plus years. We could use some help, and you helped us already on cybersecurity. What are you doing here? And I'd say, oh, I'm here for humanitarian stuff. Kids, laptops, medical equipment, stuff like that. And they'd say, sure you are. Come help us on cybersecurity stuff. The war, from a US perspective, it feels like the war in Ukraine is a little bit politicized here, or maybe it's becoming more and more politicized.

**Joe Sullivan (cont'd):** We're seeing, to put it in its most simple terms, it feels the Biden administration is very pro-supporting Ukraine, and some of the Republican candidates for president have expressed concern. And I think there's merits to both sides of, and their perspectives on this, there are, it's a complicated situation. And so, we as a nonprofit, we focus on the humanitarian side. I think one thing that's amazing is how we as Americans, we care about people who are in bad situations, whether it was their own making or otherwise. It's a natural disaster or any other situation where a country has run its economy into the ground, the United States is always number one in reaching out to help other countries in times of need, and I see that in Ukraine. The volunteers, when I go to Ukraine, the volunteers that I meet, nine out of ten are from the United States. The people who are there to help, the people who care and want to make sure that the people there are okay, come from America. All of our donors are in the United States. They come from across the political spectrum. And so they don't expect us to take us a strong view on the war, but they expect us to take care of people who are in a humanitarian crisis. We try and navigate that and not be actively involved in kind of wartime activities, if you will. There are lots of other organizations doing that, but even because of my background, I have gotten a lot of exposure to kind of the cyber side of what's going on there. I've been asked repeatedly to put on training programs for people there, inside and outside government, and so I have led some training programs over Zoom on specific areas of security. Because it's funny, if you think about Ukraine, it is a country full of very, it's a very technically savvy country. There have been a lot of companies in the United States that have had teams there.

**Ed Gaudet:** And still do work. I used to work with a bunch of firms over there, Softserve, and others for outsourcing in the past.

**Joe Sullivan:** Exactly. And so there are a number of Ukrainian software products that you don't even realize are Ukrainian that we use here in the United States. And there are lots of US companies that have continued to employ Ukrainian software security engineers, software engineers, technical people of all types, IT outsourcing, you name it, and so that, it is a very technical country. But the interesting thing is that they operated very differently. I think the businesses there, in particular from an infrastructure standpoint, were not kind of set up the way we were setting up our company as the last ten years.

**Joe Sullivan (cont'd):** The things that we're good at here now, after years of being bad at them and then learning how to get better. For example, like think if you're on a security team in the United States, one of the things you worry about is cloud security. How is our cloud configured? Who has access? What's stored there? Do we have the right backups to handle a ransomware attack? For whatever reason, Ukrainian businesses, they weren't setting up shop in AWS, and they didn't have to think about incident response in a cloud context, or how to make sure to have multiple layers of defense against ransomware. Because I hate to say it, but it was Eastern Europe that was leading the attacks on the West, and there may or may not have been some Ukrainians involved in some of those attacks on the West. So they were good at the offense, but not so good at the defense, and I think in the West, we're quite good at the defense because we've been under it. There's not an entity in the United States that hasn't essentially been under cyber attack almost consistently 24 hours a day for the last 20 years. We take for granted how good we are at defense. We beat ourselves up in this country when we fail, but we're actually pretty darn good. And so it's been interesting and educational for me to see that country and their businesses and economy have to deal with stuff that we've been dealing with for 20 years.

**Ed Gaudet:** Let's switch topics, and I have a question, just came up. Actually, I was talking to someone today, and I was thinking about our conversation. I want to be respectful of how I ask the question, so just bear with me. But I think that if I think about one of the things that you have done for the industry. You've made the CISO role a lot more aware of the responsibility of that role. So I wonder, are there, is there advice you can give folks out there? Because there's a lot of people that are, look at that and actually think about it in the negative implications of ..., and so and I think in a time certainly in our industry, in healthcare, but also just in industry in general, the demand for cyber professionals has never been greater. And so the last thing we want to do is obviously scare people away from joining the profession. It is a great profession. Any advice you give for folks that are in the role today or on their path to becoming a cyber?

**Joe Sullivan:** It's funny, I, you know, I went through a lot for the last six years dealing with what I call the Uber hangover, and I learned a lot from it. And I was very fortunate, in May, when I went in for sentencing, and the judge in my case, he had really taken the time to understand the profession and the challenges of it and the reality.

**Joe Sullivan (cont'd):** One of the realities of this role of security executive, security leader, CISO, CSO, we haven't even agreed on the title yet, is that, it is, we can all agree on a few things. One, it's evolving quickly and becoming more and more important. Two, it's really hard to do because you don't get, nobody notices when you succeed, and everybody notices when you fail. Number three, there's no clear set of expectations for how to get to the top and what good looks like at the top. And I guess there are a lot of other things too, but just taking those things and breaking them down. When I think about the evolution of the profession, when I first got the title back, and I guess it was probably 2010, most companies didn't have someone with the title. They had someone with the responsibility, but they were buried down inside the organization. And, you know, I was fortunate, and kind of inside tech companies it was obvious that there needed to be someone more senior who was navigating and building out and making sure it was resource. And I was not the first, but there was a very big event that I think really helped, it was shortly after I became the CSO at Facebook, it was when Google went through that major attack and compromised from China that everyone calls the Aurora attack. That really opened eyes in Silicon Valley and drove budgets and tech and prioritization of security. And it helped me, it helped my peers, and we've seen growth in the profession. Some professions and some categories or industries like healthcare and financial services, I think leap to the forefront because of, honestly, I think because of good regulation or at least attentive regulators being proactive with rulemaking. One of the things that I think about, and I've mentioned it a few times recently to people, I read this article in Bloomberg by, in this newsletter last year, by this guy named Matt Levine, and he wrote about regulation, and he said, there's two types of regulation. There's regulation by rulemaking, and there's regulation by enforcement. Rule, regulation by rulemaking is when the regulators come along, and they set a bunch of standards, and they basically they tell us, where's the yellow line that you shouldn't cross on the street and where's the white line? Okay. You've got to stay in between these two lines and do these things, and you'll have a safe ride. Some industries have had regulators provide those lines, and it makes the security leader's job much easier when you have those lines, because there's, you can say, we're doing the minimum things required. So you have certain industries that kind of live in that regulated world, and then the rest are kind of like regulation through enforcement, and that's where mostly the tech industry has been. And in tech, everybody likes to bemoan, oh, the government's coming after us again for right now.

**Joe Sullivan (cont'd):** This week, the big news is, of course, the Department of Justice versus Google antitrust case started, I think, yesterday. And everybody says, well, it's us and Big Tech. We're, the government's mad at us and coming after us, and there are all these lawsuits and contention. But why are we in that place? Because for the last 20 years, tech has been saying to government, you don't need to regulate us. We'll figure it out on their own. Trust us, we got it covered. And you know what? For a long time, I had to be the person inside the company who said that for the company. But as I've kind of stepped back and thought about it from the perspective of a security leader, I would much rather work in an environment where there's a clear yellow line and a clear white line, and I know, and I can demand that the company, do the minimum to get to those places. And I think security leaders are often at odds with our own company on the concept of regulation. We would like to have clear lines. The company, especially in tech, doesn't want that regulation because they view regulation as a cost on innovation. And like everything, there's two sides. We don't want to stifle innovation. Innovation has been incredible for our economy and kept the United States ahead of the world in terms of, I think, our financial situation. Our, the tech companies that have grown up in the last 25 years are the biggest companies in the world, not just selling to the United States, but selling to the world and bringing the profits back to the United States to all of us who work at those companies. So there's the good in that innovation, but we, when it comes to cybersecurity, we need more frameworks. We also need more expectations, like these new SEC instructions. From our standpoint, that's only a good thing, right?

**Ed Gaudet:** Yeah, I agree.

**Joe Sullivan:** We can nitpick over the nuances of each requirement, but forcing companies to stand up and talk about their commitment to security is fundamentally a good thing. The thing we need is more transparency about everything that's going on around security, because the bad guys share all the information, and the good guys don't get to. Every company that gets compromised, they'll do the minimum to disclose they had a data breach, but they won't disclose the details of how it happened so that other companies can learn. It's frustrating. So we're, we still have a long way to go. And I'm optimistic about the future because I think, like you said, it's a noble profession of people who, we go into this to help people, to make our companies better, and to ensure that our companies are doing the right thing by our customers.

**Ed Gaudet:** Yeah, it's so critical nowadays to the health of an organization. The work that the SEC is doing, I think, is the right way. I do think that until we get a cyber, a specific cyber at the board level, until we make the board accountable, which it should be, quite frankly, then I think once we do that as an industry, then things will start to change. And what better industry than tech, that has the funding, that actually has the resources, and imagine them driving now in, in this area because they have to, because they got to figure out how to how to minimize the cost of regulation. Tech will do that, healthcare won't. Healthcare is a thin line, thin margins, right? Very thin margins, revolutionary impact, and on cyber, whereas tech will figure it out if they're forced to figure it out.

**Joe Sullivan:** The one other thing I think we need to do, and we need to figure out, as people who care about security and are in the profession of security, is getting ourselves a bigger voice and making ourselves the leaders we should be. And what I mean by that is, we grew up in the profession when the ceiling was lower for us as individuals, and we need to get comfortable with the idea that we're going to push through that ceiling. And I got to be honest, a lot of security leaders that I talk with are afraid to do that, especially those for first time in a security leadership role. They're, you get in that role, and you're like, oh, crap, I have a lot of responsibility. I'm personally going to make sure that our organization doesn't get hacked. And so you go into heads down, I got to focus on my team, I've got to focus on identifying all the risks. I've got to get technical controls in place. I've got to get the right policies in place. I've got to get the right people, the right policies, the right technology. And so you're just focused on your team and doing the bare minimum, but we actually have to be leaders inside our company. We have to understand how the business works. You actually can't manage risk if you don't understand the, what the business is trying to do. You need to know where the business is going to run tomorrow and be there with them, not wait until they get there and then try and Band-Aid security on. It doesn't work.

**Ed Gaudet:** Great point. Risk is a business decision. It's not a technology.

**Joe Sullivan:** Exactly. And if you're not in the room when the business decision is being made to launch a new product or go into a new market to do something different, if you find out about it a week later, you're a week behind. If you find out about it, a month later, you're a month behind, and you're never going to catch up.

**Joe Sullivan (cont'd):** We have to be the people who are going to be vocal inside our company about the importance of security. We have to be the ones who are going to engage with our board members and offer to help them look at them and don't be intimidated by them, look at them and think of them as people that you want to work with.

**Ed Gaudet:** That's right. Protection is much more than playing defense. In order to play offense, you've got to be proactive with the business, understand the needs of the business, and create that relationship so the business understands the importance of cyber and vice versa, cyber understands the importance of business. And we've got a ways to go, but I think we're making some really good strides. If you could go back in time, what would you tell your 20-year-old self?

**Joe Sullivan:** Well, probably the biggest lesson I learned from my case was there's one investment that always pays off, and that's in people. The silver lining, on my case, was during my worst period, the jury came back with a guilty verdict last October, and I had to get through the period between last October and this May, not knowing and not having control over my own future, not knowing where I was going to be right now. The US government, the Department of Justice, was arguing and argued in court at my sentencing that I should go to prison for over a year. And like said, the silver lining was the people that I'd gotten to know through my life, they showed up like I could never have believed would happen. I started almost within two weeks of the verdict, receiving emails with letters attached from people I hadn't talked to in years, saying, Joe, I know that you're gone to your sentencing. I wrote a letter to the judge. By the time I got to the sentencing, I'd received well over 200 letters like that. My lawyers thought we would annoy the judge if we gave them that many letters. We gave the judge, I think, 186 of the letters. We called out some of the ones that were less personal or less detailed, but the letters, I got to read them over those months, and they would come in, and they would be, hey, Joe, you probably don't remember this, but eight years ago my son was in high school and interested in cybersecurity, and you said, sure, let him come in and have lunch with me and show him around the company. Or I fought for somebody else's project inside a company that prioritized security in a way that, or I did a bunch of work on my companies on diversity and inclusion, or just like all those little things that you do, they came back in a way that just made my heart grow.

**Ed Gaudet:** Yeah. No, I just got a chill. It's almost, I hate to say this, but it's almost like worth it. And to deal with that outpouring of love and respect and oh, Jesus.

**Joe Sullivan:** Yeah. I joked with people that it felt like I got to be president of my own Irish wake, you know, that.

**Ed Gaudet:** I was thinking that too. I was thinking that.

**Joe Sullivan:** Because usually, and everybody should get the benefit of this during their life to be able to. And so that, to me, you're right, it was a gift that I'm so grateful for that, because I was lower than I ever was in my life and not able to make plans and not knowing what was ahead, and to have these people want to help. And it's funny, when you go through stuff like that, there are people you think are going to be there for you and they just, they disappear. And there are other people who you, you know, you just had a couple of interactions with them, and all of a sudden now I see those people differently because they saw me in my time of need and they dropped everything. There's a guy who I had worked with probably a decade ago, and we'd run into each other once every year or so at a conference or something, and we'd say hello. And all of a sudden last October, he would text me every few weeks and say, do we get a beer? And, you know, he'd say, oh, I'm going to meet so-and-so who used to work with us, meet us, and stuff like that just started happening. And now that I'm past the crisis, he doesn't text me anymore, but he was there for me when I needed him. And I never want to forget those people in that side of it. Because, like I said, the lesson I learned is that every, when you do things for people, you might forget them, but they remember them. Yeah, it's so true.

**Ed Gaudet:** We're almost out of time. I do have one last question. It's the Risk Never Sleeps Podcast, so I've got to ask you, what's the riskiest thing you've ever done, Joe?

**Joe Sullivan**: I've had a lot of time to reflect on my career and that, I just, over and over I've jumped into the deep. You know, people, some people run towards burning buildings and some people run away from them.

**Joe Sullivan (cont'd):** I never thought of myself as a person who run towards building burning buildings, but I went into those security leadership roles knowing that I was walking into train wrecks. You know, these companies that had grown incredibly fast, had high valuations that had never invested in security. Like when I walked in the door at Uber, that was a pretty dumb thing to do. When I joined Uber in the spring of 2015, the company had just announced a massive data breach they were dealing with. The negative publicity of the insiders had been looking up riders' trips, and it was very publicized, and there had been a really tragic sexual assault in India that was global news, and I walked into that. And, you know, my family would say it was really stupid to go to Ukraine twice this year. So I haven't stopped kind of going towards those things. But the reason you do it is because if you're successful, then you make a difference. It feels really good and it feels really rewarding, yeah.

**Ed Gaudet:** I imagine the next time you're in need of help, God forbid, but there's going to be like 100 times the number of letters given the work you've been doing in the Ukraine. So it's amazing, and we thank you for your service. And again, for listeners that want to get involved, DM Joe directly on LinkedIn or go to the website Ukraine Friends. Really great interview. Any last comments you want to or advice you want to?

**Joe Sullivan:** I don't know, I would just say thank you for doing this. Like we said, the profession, the world of security is growing. It's evolving quickly, and the more we talk to each other about the things that we failed at and the risks that we're facing, the stronger we all will be together, and the people who come after us will learn and not have to experience the mistakes that we made. So thank you for doing everything you're doing.

**Ed Gaudet:** And thank you, Joe. And this is Ed Gaudet from the Risk Never Sleeps Podcast. If you're on the front lines protecting patient safety and care, remember to stay vigilant because risk never sleeps.

CENSINET®

# Censinet RiskOps™ Demo Request

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

**SCHEDULE DEMO**

www.Censinet.com