



Podcast Transcript

Risk Never Sleeps

Episode 68

Greg Garcia

Ed Gaudet: Welcome to the Risk Never Sleeps podcast, in which we discuss the people that are protecting patient care. I'm Ed Gaudet, the host of our program, and I'm pleased to be joined today by Greg Garcia, executive director of the Health Sector Coordinating Council. Hey, Greg.

Greg Garcia: Hey, Ed. Good to talk to you.

Ed Gaudet: Yeah, how's it going?

Greg Garcia: Going well, it's going well. Excited to be here.

Ed Gaudet: Interesting couple of weeks for you, but we'll get to that in a second. I love your role. I love what you're doing, obviously, for the health sector. How did you get involved? How did you get started in this role?

Greg Garcia: I'll tell you, the fundamental skill sets that are needed for this role are something that I've honed over so many years, and I think what it comes down to is a combination of understanding coalition management and the intersection of public policy and business. In this case, in the context of security, national security, homeland security, and in my case, specifically, cybersecurity. But I've held roles very similar to this over the years.



Greg Garcia (cont'd): I was the executive director of the Financial Services Sector Coordinating Council sometime before this and helped stand up the Information Technology Sector Coordinating Council. You're seeing a pattern here, and a lot of that came together with my time at the Department of Homeland Security, where I oversaw the National Strategy for the Government Partnerships with all of the critical Infrastructure Sector Coordinating Council. So it certainly was a natural fit for me. And it started for healthcare more than five years ago when some leaders in the health sector were going to testify before the House of Representatives on healthcare cybersecurity. And it was the president of the Health Information Sharing and Analysis Center, or the Health ISAC, Dennis Anderson, who called me at my current role at the time in a policy consulting firm, saying, can you help us with this testimony just in terms of preparing and understanding the politics? And sure, let's do this. And in the preparation of that hearing, I learned a bit about what was going on in the health sector and some of the gaps in their mobilization, in their organization behind cybersecurity, not just at the operational level that the Health ISAC was excelling in, but in the longer term strategic and policy focus that was so sorely needed for the Health Sector Council. And it was at that point that Denise and the Health ISAC understood that the success of the Health ISAC was dependent in part on the success of the Sector Council, they are two sides of the same coin. So it was at that point that the Health ISAC funded this executive director position for me to run the Sector Council and really reorganize it and build it from what it was five years ago.

Ed Gaudet: You've always been in policy, I actually don't know the answer to this question, I know we know each other pretty well, but did you go to school for policy, or how did you get into this?

Greg Garcia: Oh, I had, no, I had a degree in management, but I was always interested in the intersection between public policy and business. I wasn't particularly interested in going into business and marketing or selling or finance, but I understood that business and government are inextricably linked. And so I really had, while going to school in California, had set my sights in Washington, DC, and started out in public policy as a consultant and moved on to industry association for the high-tech industry, and it progressed from there.



Greg Garcia (cont'd): So spent a good part of my career in the high-tech industry, some time in the United States Congress as a congressional staffer, spent some time in the Department of Homeland Security as a presidential appointee, and then back into the private sector. So I feel like I've got this well-rounded perspective about how policy is made and how business is managed and where the intersection is in a way of how to maximize your business under a regulatory environment and how to develop policy that really achieves its objectives without overburdening government, without overburdening business.

Ed Gaudet: Yeah, and this role, in particular, is really interesting because there's that almost that three-legged stool of public-private partnership that includes not only DHS 405(d), but also CISA. And I'd love you to talk about the relationship of those other agencies and other aspects of government that are part and parcel in the functioning, if you will, of a secure, critical infrastructure like healthcare.

Greg Garcia: This was really, I would say, an innovative experiment, and it's been a more than 20-year experiment now, that is based on, at least in terms of critical infrastructure protection and, even more specifically, cybersecurity. There are challenges we have as a country that market forces alone are not going to solve, and that government regulation and government policy alone is not going to solve. So we're going to need to be more resilient, more resourceful, more creative when it comes to government and business working together. That it isn't just business saying leave us alone or government just saying we're going to just regulate you and that'll take care of everything. And so it really started with a presidential executive order back in 1998, which has been updated a number of times since then, which simply recognizes these critical infrastructure sectors, 17 of them. Healthcare is in a category of financial services and telecommunications and electricity and water, and transportation, all of the things that the country depends upon, and this statement of government policy said just what I just said. We can't market forces nor regulation alone can solve this, we need to have a public-private partnership, and we need the federal agencies that are responsible for any given critical sector to serve as partners to their critical sectors in a way that is collaborative, cooperative, and innovative to see where together we, government and industry, can develop initiatives and programs and policies that will facilitate critical infrastructure protection rather than get in the way.



Greg Garcia (cont'd): And overseeing that whole national strategy is a role that I had under President Bush, the second Bush, which conferred upon DHS the responsibility for coordinating all of the critical industry sectors and their agencies in this national public-private partnership. With CISA being really the hub for national risk assessments and mitigations and working individually, which with each of the sector agencies about how best can we incentivize and guide the private sector toward improving the security and resiliency of their individual sectors. CISA providing the risk and mitigation expertise, the sector agencies providing the sector-specific knowledge. DHS cannot be the everything, they can't know everything about electricity and healthcare and telecommunications and water. They have to rely on the sector agencies to provide that level of specific expertise. And so together, it's a triangulation where CISA has the overall coordination. Each federal agency deals with their sector, and then you have the sectors themselves, the industry representatives, who are the owners and operators of those critical sectors, and it's ultimately their responsibility for doing most of the work.

Ed Gaudet: And there's a lot of work that gets done, obviously. Share with our listeners some of the work that the HSC brought into market and some of the impact that's had for these providers.

Greg Garcia: We learned at the start of our reorganization in 2018 that we really had a paucity of good cyber security guidance specifically for the healthcare sector in the language of the healthcare sector. Yes, there's a lot of cybersecurity framework, there's the cybersecurity framework, and there's ISO, and there's the Sans Institute. There's a lot of cybersecurity guidance. But how do we apply this specifically to the various complexities of the healthcare industry, whether you're a medical device manufacturer, a pharmaceutical company, a hospital system, a small clinic, a plan, and payer, or a health IT company, all those subsectors suffer from similar cyber security threats and challenges, but they are often manifested in different ways, So how do we develop some kind of cross-cutting advice to the sector? And so the best way to do that is to rely on the owners, operators themselves. And so, the Sector Council organized itself around a number of task groups that are focused on some very specific functional aspects of cybersecurity. I mentioned some of them: medical device cybersecurity, workforce development, hospital cybersecurity.



Greg Garcia (cont'd): And we develop, we built these task groups co-chaired by different representatives of different subsectors to bring that cross-sector view, populated by anywhere from 30 to 130 organizations, generally at a fairly senior level, providing their expertise, the best practices that they use in their big company or their big hospital, bringing them to the table in a collaborative way, saying, here's our best judgment about how the healthcare industry can be applying leading cybersecurity practices to their own cyber risk management programs. And so the result of those efforts where some task groups were working for two years to put together some guidance document. The result is from the beginning of 2019 to today, we have published 21, I believe, documents, some in partnership with HS, you mentioned, 405(d) that is the health industry, cyber practices, or HICP, how hospital systems need to better secure their data and operations to medical device security to supply chain cybersecurity, which you've been so helpful and contributing to, about how you secure the cybersecurity of your supply chain, your providers, to many others that the, all your listeners can access freely available to you on our website HealthSectorCouncil.org under the publications tab, and these are, I say it repeatedly, these are by the sector for the sector. And our expectation and our hope is, and our challenge is, to get these into the hands of the stakeholders who really need them, particularly small and mid-sized organizations, to know that they have a place to start with our publications, with our toolkits, and to get those to be implemented so that collectively we can raise the bar of security and resiliency across the sector. And we'll be spending the next five years doing our best to market them, raise awareness using a force multiplier of our industry associations in our membership of our government partners. So they're there, and all they need is to put them to work. They don't always require big investment, but they require some attention and some commitment.

Ed Gaudet: Yeah, and it's such a rich corpus of knowledge and experience that's presented there, and every organization should take advantage of. It's freely available, and it's developed by your peers across the industry. And it does have that nice balance of what it is, why it's important, and more importantly, how to actually put it into practice. I think there are a number of health delivery organizations and providers that are leveraging those documents and best practices in their own organizations today. Really excellent work that everyone does across the sector. You also brought to market a series of educational videos, which I think is really getting some really nice traction in the marketplace. Tell our listeners a little bit about that.



Greg Garcia: Yeah, that is, that was great. That was put together, conceived of by our Workforce Development task group with the understanding that yes, we have chief information security officers and threat analysts and vulnerability assessments, but what about all the frontline users? We've always said that whether it's in healthcare or anywhere else, one of the biggest threats is the insider threat. And by that, we really mean just a lot of inadvertent mistakes from well-meaning employees just doing the wrong thing or clicking on that link when they shouldn't or opening that attachment, and that goes for frontline clinicians as well, doctors and nurses and surgeons and office managers. And we realized that we need to speak to them, to the frontline users, in ways that they can understand, it's not technical, but they have a role to play, they have a responsibility as well. Help out your CISO, just, here are the basics. So we developed a series of eight videos. None is more than six minutes each, so it's about 48 minutes in total, and each one is on, each video is on a different related topic, whether it's understanding password management or how do the hackers get in and what's the impact on the organization. Here's what you need to do, and here's what you need to don't do. And our on-camera talent has become a bit of a rock star in our community.

Ed Gaudet: He's so good.

Greg Garcia: He's Dr. Christian DeMuth, he is an emergency physician at UC San Diego and a professor there as well, but, and a self-taught hacker. So he can hack the computer, and he can hack the human, and to have that combined skill set, he imparts credibility. And we wrote it in such a way as to be non-technical, and it's a great video series. We had great video production. We took up collections from the members to finance it, it was not hugely expensive, but very professionally done. And the good thing about it is, why should a busy doctor, I don't need to see this? A lot of the healthcare systems are building it into their learning management system as part of their requirements, and for good measure, we throw in one continuing medical education credit or continuing education credit, so there's some incentive there as well. But yes, the feedback so far has been almost universally positive, and the uptake is increasing. And in fact, next week we're going to release a new and improved version, which has some new features to it which will make it even easier to use for everybody. So available on YouTube as well.



Ed Gaudet: Yeah, if you're listening, you're a clinician, go check out YouTube. Go check out the Health Sector Coordinating Council website for more information on this video series. That 40-minute investment could be the, make the difference between protecting patient safety and having to deal with ransomware attacks.

Greg Garcia: Yeah, you can either get it, you can go to our website HealthSectorCouncil.org. There's a tab specifically for the video series. It's called Cybersecurity for the Clinician, and it's there so that you can either receive the specific file for the learning management system that you can implement in your LMS, or you can simply go to YouTube and search for Cybersecurity for the Clinician, and off you go.

Ed Gaudet: Excellent, excellent. So we're going to switch a little bit, and we're going to get personal, Greg. It's been a rough couple of years for a lot of us. What are you most proud of this past year, over the last couple of years, either personally or professionally, or both?

Greg Garcia: Both. Professionally, I'm just constantly proud of the work the Sector Coordinating Council is doing. I came to the table with a vision and articulated the vision, and it made and makes sense to so many people in the healthcare community at very senior levels, and if you have their buy-in, then things are going to get done. And I'm not doing the work, it's you all. It is the stakeholders, you are the owners and operators. And the fact that we have built a community of collaboration and pure energy motivation to work together to collectively conquer this challenge, I am proud of that, and there are no signs of it attenuating. Every week we get new members coming in. Every week, somebody is saying you should be involved in the Sector Council. I don't know what it is, but I know I'm supposed to be here, and I'm, and then I tell them why they're supposed to be here. And the momentum is building, and it has been over the past five years. So I'm very proud of that professionally, quite frankly, I think one of the highlights of my long-toothed career for sure now. And personally, the pandemic significantly improved my guitar playing and my repertoire of both classical pieces and singer-songwriter stuff. But yeah, I fulfilled, almost fulfilled a lifelong dream of getting, of trekking to Everest base camp at the beginning of May. I think probably since I was eight years old, I've wanted to see Mount Everest, and I finally did my own two eyes, my own two feet. What an extraordinary experience that is.



Greg Garcia (cont'd): As an elder folk, I didn't realize the extent to which I had some arthritis in the hip, and about halfway up to Everest the joints just said, nope, you're going home. And so didn't make it up to Everest base camp, but my brother-in-law did. And it's, I've got some extraordinary pictures and videos to document it, and I'm elated by that, so I'm proud of that.

Ed Gaudet: Yeah, absolutely. Halfway is better than no way.

Greg Garcia: That's right.

Ed Gaudet: And most likely, that's one of the questions. What would you be doing if you weren't doing your current job? What are you most passionate about? And wonder if you just kind of.

Greg Garcia: If I weren't doing my current job, I would be a professional golfer. That was my aspiration in college.

Ed Gaudet: Okay.

Greg Garcia: I was good, but not good enough. You don't appreciate how extraordinary professional golfers are when they get to their level and how good I was, and how no damn good that really is.

Ed Gaudet: Were you a scratch golfer?

Greg Garcia: Oh, yeah. Oh, yeah, I was, scratch, but that's not good.

Ed Gaudet: That's not good enough, right?

Greg Garcia: That's nowhere near good enough. These guys are machines and I was not good enough, but it was worth a try. Yeah, that would be a dream.

Ed Gaudet: You still play?



Greg Garcia: Yes, I still play. Yes, I do. But of course, that's put on hold right now until my hip recovers, but most of my time is spent cycling. I used to race. I used to be a bicycle racer. Got pretty good at that until the homeland security job came along, and that was 24/7, and all the training had to stop.

Ed Gaudet: So you thought you were going to say the next James Taylor.

Greg Garcia: Yeah, I'm learning a couple of James Taylor tunes and a bunch of others.

Ed Gaudet: So do you know Noah Kahn? Have you heard of Noah Kahn?

Greg Garcia: No.

Ed Gaudet: You should look up Noah Kahn. The cool kids are in the Noah Kahn. My daughters introduced me to his music. He's a phenomenal singer-songwriter, similar to Ray Lamontagne. Do you know him?

Greg Garcia: Yeah, yeah, along those veins, I think I would say one of my favorite singer-songwriters, and I would venture one of the most covered singer-songwriters is John Hiatt.

Ed Gaudet: Oh. John, yeah.

Greg Garcia: Absolutely, and not well-known name, but his music was responsible for some comeback of careers from people like Bonnie Raitt and absolutely B.B. King and Eric Clapton.

Ed Gaudet: John Prine?

Greg Garcia: Yep.

Ed Gaudet: Cool. What would you tell your 20-year-old self if you could go back in time?



Greg Garcia: Oh, follow your gut. That's all, that's all I ever did. And I might have had some advice from my father, who I respected and loved deeply, or other mentors in my life who would say, get your five-year plan, know exactly what you want to do. I know generally what I want to do, but I also want to be opportunistic, and that sometimes means waiting until the right thing comes along. Unless you're in misery in a particular job. And I've only been in misery in one job in my life, that was my only career mistake. Everything else, I'm proud of my career, what I've accomplished, but also the choices I made to make each career step, and that's because I followed my gut. I remember when I took a role, a very high profile coalition job, managing a coalition, Team 98. It was at the height of the encryption war, behind the National Security Agency wanted to put a clamp on both the sale and the export of any high technology that had encryption built in, of course, because it hampered their ability to do surveillance, primarily on either criminals in the United States or foreign terrorists and such. And that was just a non-starter for the high-tech industry, and there was assembled a very well-funded coalition of high-tech companies, an unholy alliance of civil libertarians and Republicans and Democrats. And it was very clear it was going to be no more than 1 to, 1 year to a year and a half if we were going to be successful. And one of my colleagues from one of the companies I was a trade association executive at the time, he called me up and said, what are you, nuts? This is fraught with risk. It's going to be over in a year or so, and where are you going to be? And I said, that's exactly why I'm doing this, because it's fraught with risk. If, what am I going to do with my career? I shied away from something that was intriguing but had an uncertain future. Now I'm going to do this because I'm going to get something done, and it's exciting. I'm going to learn a lot, and I'm going to make a difference. And I did, and by the end of the run, we had succeeded. And that gave me enough visibility and credibility that I was fairly quickly snapped up by another company and achieved what, by then at that time, was my biggest career objective, was to be the chief lobbyist for a high-tech company run by the Washington office, and I did.

Ed Gaudet: Now, think you're referring to the CFIUS law.



Greg Garcia: No, CFIUS was, that's the Committee on Foreign Investment in the United States, which reviews whether or not a foreign company can purchase a, you can purchase a majority stake in a United States company that is deemed to be of national security significance, that you don't want any of your national security or military assets to be beholden to a foreign company.

Ed Gaudet: Back during that time, and I know because I was selling one of the companies that I worked with to a foreign company, and we had encryption software, so we had to go through the CFIUS process because they didn't want necessarily this country owning this type of encryption software.

Greg Garcia: Exactly, it was, where this was an issue, there was, there are two major issues. At the domestic level, there was something called the clipper chip, and the FBI said for all computer chips that included encryption on them, we, the FBI, want to install what's called the clipper chip, which was a backdoor in the encryption algorithm through which FBI could enter with a warrant. And the high-tech industry said, if you do that, you destroy our industry because now we know we've got Uncle Sam inside of our computers. And the other law was export controls, so if you wanted to sell that computer, there weren't cell phones at the time, but if you wanted to sell that computer or any other device that had encryption in it overseas, you had to get a license. And encryption was considered, was included on the munitions list, the munitions list as a weapon. So that's what we were trying to beat back during in that coalition, saying this makes no sense and it's going to undercut. This is where the, that interesting intersection between business, government, and national security, economic security, business and government, that sensitive intersection where we said that, if you do this, yes, we understand national security, but you're actually undercutting by national security, by undercutting the strength of the US high technology industry.

Ed Gaudet: Yeah, I think they refer to the was it the MYK 78 chip, or the M Y K 78.

Greg Garcia: Oh, that one's, that one I don't know.



Ed Gaudet: Oh, okay, that might have been on the phones when they were thinking about adding the clipper chip on the phone way back when. Interesting. Cool. So last question. I'd be remiss if I didn't ask it. This is the Risk Never Sleeps podcast. So Greg, what is the riskiest thing you've done in your career or your life? Maybe life is better than career.

Greg Garcia: Riskiest thing I've done in my life. Probably, I'm a black belt in taekwondo, and I used to compete a lot for my school. And when you're a black belt, there's violence, always the risk of getting knocked out and brain damage and that kind of thing with a spinning kick to the head. So that was probably consistently the riskiest thing I've done. When I was on the golf team at UC Santa Barbara, I owned a motorcycle at the time, and I had to go down the freeway on the, on this little Honda 200 motorcycle to practice about 20 minutes away with my golf clubs over my back going 65 miles an hour down the highway wearing golf cleats. And so I had golf cleats, in those days were metal, they were metal cleats, and so I had fun dropping my feet down to the pavement as I was going 60 miles an hour and watch the sparks fly up from the friction of the cleats on the concrete. I suppose that wasn't particularly smart, but.

Ed Gaudet: No, but if you combine those two, if you did like the crane kick wearing your cleats, that would be probably the risk.

Greg Garcia: Oh, I never thought of that. Oh, that would really do damage.

Ed Gaudet: Yeah, that would be bad for the person receiving, at the receiving end of that. Greg, thanks very much. This has been terrific. You've given us a lot to think about. And if you are listening and you want to get involved with the Health Sector Coordinating Council, go to the website, reach out to Greg. There's a lot of work that obviously, we're in the process of managing through, but we always need volunteers. And Greg, I'm sure you'd be happy to have more folks join the HSCC.

Greg Garcia: Absolutely. This is a great partnership, and it's growing, and we need all hands on deck.



Ed Gaudet: Terrific. And thank you, this is Ed Gaudet. We're signing out the Risk Never Sleeps podcast. If you're on the front lines protecting patient safety, stay vigilant because risk never sleeps, and we are out.



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