



Podcast Transcript

Risk Never Sleeps

Episode 7

John Riggi

Ed Gaudet: Welcome to the Risk Never Sleeps podcast. I'm your host, Ed Gaudet, and today I'm joined by my good friend and colleague, John Riggi. John is the National Advisor for Cybersecurity and Risk with the American Hospital Association. John has spent nearly 30 years as a highly decorated veteran of the FBI, thank you, John, for your service. And serves as the First National Advisor of Cybersecurity and Risk for the American Hospital Association and their 5000-plus member hospitals. Well, welcome to the program. We got a lot to talk about today, and you have a phenomenal background and set of experiences, so let's get right into it. Our listeners are really excited to learn more about what you do every day for the American Hospital Association. So maybe just take us up to speed. What's going on in your world?

John Riggi: Well, first of all, thanks for having me on the podcast today. It's great to work with you and Censinet as always, because as I always tell you, and you know it, Ed, we say that we want to partner with firms that are in the position to serve our members, not just sell, but serve our members. So in my role here, the AHA, I deal a lot on national policy, advocacy issues related to cyber, government relations of course, I deal with all my current and former colleagues across all the government agencies. And of course, the most important thing I do is help members directly. When they have a problem, when they have a cyber incident or ransomware attack, I often do get those late-night calls and asking for some guidance and assistance.

John Riggi (cont'd): And ultimately, that helps me do my job because I'm there with an inside perspective to help transmit best practices and lessons learned and encourage them to share without attribution, what happened, what worked, what didn't work, and work with the government? Cooperate with them so they can understand who the bad guys are and help warn the nation. So I get a tremendous amount of satisfaction in doing that job and still having a mission.

Ed Gaudet: Excellent, excellent, and no pun intended, but there's been a lot of buzz going on about this recent hive takedown. I'd love to get your perspective on that.

John Riggi: So there's a great example of private sector working closely with the government, within the government, understanding what the impact of these ransomware attacks on hospitals. As you know, Ed, I've been a very vocal public advocate for several years encouraging the government to take offensive action against these groups, just as we did when I was in the FBI when we work in counterterrorism operations, same set of facts. You get bad guys that are beyond the reach of handcuffs of the FBI, so we have to utilize the capabilities of military intelligence services as well to go after them and disrupt them. So great example of the FBI working with victim organizations, including hospitals. Attorney General Garland mentioned right at the outset of his press conference how they had worked with hospitals, help defend them against cyber attacks, and then utilize that information to then penetrate the HIVE ransomware organization, really dramatic, to get inside there and penetrate their organization and be embedded in an undercover operation for seven months and steal the decryption keys. As Attorney General Garland said, hack the hackers, steal the keys, and give them to the victims before the victims pay. I mean, really, really great work. And then the coup de gras was to actually take down their cyber infrastructure, their servers, networks that they were using to launch these attacks. So that's, again, great example of victim cooperation, exchange of information with the government to enable an offensive operation against the bad guys, which ultimately helps defend the entire system.

Ed Gaudet: Great example of that inter-intra-agency collaboration and coordination, right, to do basically what the bad guys have been doing to us for the last five or so years, coordinating at the dark web level and creating that level of microservices to distribute, if you will, the workload of those attacks in a coordinated way. So great work by everyone involved there. Tell us how you got into healthcare and specifically how you got into cyber.

John Riggi: Yeah, it's a long journey for me, actually, because when I started in the FBI in 1988, cyber did not exist. I think I got my first laptop, which weighed about 25 lbs plus in the FBI was probably 1992 or 3. So ultimately, when I first entered the FBI, I was working a lot of the traditional violations in the high priority violations at the time: drug trafficking, international organized crime, drug money laundering, and then post 9/11 in New York City, of course, working counterterrorism issues. And then got a stint over at the CIA as a senior representative on counterterrorism issues there. And then all of that, which I didn't realize at the time, was actually just preparing me to work cyber, where ultimately that's where my last assignment was in the FBI to run national cyber outreach programs and develop these mission-critical relationships with private sector, including healthcare. And the reason why I say it was helping me prepare for my assignment in cyber is that it really was all the same bad guys, international organized criminals, nation states, terrorists who had evolved to use cyber as a means to accelerate their plans and their attacks against the US. So having the background on these humans who are using cyber as a means to conduct their criminal activity and spying was very helpful.

Ed Gaudet: So the equivalent of a cyber Whitey Bulger.

John Riggi: In a sense, I guess in a sense or a lot of the other organized crime guys and the Russians that I was working in New York City at the time. But again, as technology evolved, the bad guys also began to implement technology in their operations as well in cyber.

Ed Gaudet: Excellent. What keeps you up at night? I imagine a lot these days.

John Riggi: Besides your phone calls, Ed? No, there is quite a bit, right? So what I'm always most concerned about, and I'm not just myself, but all of us professionals in cyber and of course the American Hospital Association are these high-impact ransomware attacks which disrupt and delay care delivery and risk patient safety. When I'm called about a hospital that has ambulances on diversion or strict bypass with stroke, heart attack, and trauma patients, when I'm aware that a hospital which has been hit by ransomware are delaying cancer treatments for patients, in the emergency department, waits went from one hour to 12 hours, those are the things that not only keep me up at night, but let's just say highly motivate to continue on this in this role and to call out the bad guys and to encourage government to go after them. Ed, you've heard me say this many, many times that we view ransomware attacks on hospitals not as economic crimes but as threat to life crime. And the government is now responding as such.

Ed Gaudet: Yeah, I know you and I were some of the first to connect on that topic. I remember years ago, four years ago.

John Riggi: While the work that you would do, great work doing on 405(d) Taskforce.

Ed Gaudet: And it's really interesting and scary because we're all patients and we know patients and it's very personal. If your mother, father, sister, brother, grandfather, cousin are hooked up to one of those machines or on their way, like you said, in an ambulance and it gets diverted because of an attack, it's a life-threatening event.

John Riggi: What I think what's lost on a lot of folks inside government, outside government, perhaps even it's lost on the adversaries, that they don't realize the risk to public health and safety they pose, is that they're not only attacking the hospital, the organization, the financial entity, they're attacking the patients that are inside the hospital because of the lack of, the denial of the availability of the technology, delays their care delivery, but it is also an attack on the entire community, which is serviced by that hospital. When that emergency department is no longer available, that means the entire community that emergency department serves is at risk. That means those ambulances are going to be diverted, and the patients, to another hospital or health system, which may be much further away, and again, creating that delay.

John Riggi (cont'd): So if you, God forbid, suddenly find yourself in a heart attack or a car accident and your nearest emergency department is no longer available, you're a victim as well.

Ed Gaudet: That's right. And typically, like in wartime, it's kind of a shared understanding. You don't attack those hospitals right on either side. And so and yet.

John Riggi: It's a war crime.

Ed Gaudet: It's a war crime, right? So it's a war crime. Why is this any different, right?

John Riggi: It's no different. When you're attacking a civilian target whose sole function is to provide emergency treatment, care to patients, to provide medical treatment. Again, that is, if this was wartime, would be equivalent to a war crime. But again, that's why, and we're very encouraged to see the federal government to adopt an official policy that they treat these attacks on hospitals as threat to life crimes.

Ed Gaudet: Maybe we should try them in The Hague.

John Riggi: Well, that's another policy discussion, to have a declaration of war somewhere. But we're encouraged to see the cooperation between the FBI and Europol was actually very instrumental in the takedown of the hive ransomware. So there's.

Ed Gaudet: Oh, interesting.

John Riggi: There is great international cooperation.

Ed Gaudet: That's great.

John Riggi: ...



Ed Gaudet: So let's switch gears a little bit and let's get a little personal. Sorry, this is as personal as it gets.

John Riggi: Okay.

Ed Gaudet: So what are you most proud of over the past year? I know it's been a rough couple of years for everybody with a pandemic, and we're sort of coming out of it, 2022. What are you most proud of?

John Riggi: I think the work that the association and I have been able to do to help government understand the impact of these attacks, to help facilitate the change in official government policy to view these as threat to life crimes, to encourage them to go on the offense against the bad guys, and to help defend the sector, hospitals, and health systems by facilitating the exchange of cyber threat information with hospitals and health system between Hospitals and health systems and the government, and then helping hospitals better prepare to defend against these attacks and be better prepared to respond to them once they occur and help them recover quickly from these high-impact attacks.

Ed Gaudet: Yeah, Excellent. Outside of healthcare and cyber, what are you most passionate about? What would you be doing if it wasn't this?

John Riggi: Well, first I have to say I'm most passionate about that flag behind me, doing the right thing for the country, helping defend the nation against bad guys, continuing to have the privilege to be in a role, to serve, to serve and help defend folks. Other than that, my spare, 10 minutes per day. But I've got a little extra spare time. I do like to work out every day. I try to work out and I get a pretty good record of working out just about every day. I think that keeps me going and gives me energy. Family, of course, spend whatever spare time I can with family. For a little bit of recreation, I do enjoy driving sports cars a tad fast.

Ed Gaudet: Oh, very nice. So, I love that.



John Riggi: I'm not saying I'm breaking any speed limits.

Ed Gaudet: No, no, no, no. We didn't say that. We could edit that out if we need to. What would you tell your 20-year-old self, which was like three years ago? What would you tell your 20-year-olds?

John Riggi: Come on, Ed, you're so generous.

Ed Gaudet: What would you tell your 20-year-old self?

John Riggi: I would tell my 20-year-old self that in the nineties there's going to be a company called Amazon that's going to go public, and a company called Google. Funny name, but buy as much stock as you can.

Ed Gaudet: That's my answer.

John Riggi: So it's so dramatically different, your perspective, I have to tell you honestly, even at 20 years old, I had the distinct clarity that I wanted to be an FBI agent as soon as I could. So I was very blessed and privileged to be able to fulfill that dream. Ultimately, would tell myself that the world is a very complicated place. You can't solve all the problems yourself. You're going to have to work with people very closely and ultimately that you will perhaps not solve the issue, but hopefully make a significant contribution to helping solve whatever the issue is and hopefully, of course, helping defend the nation.

Ed Gaudet: I love that. Where do you think that comes from? Like you have a family that were serving in the military or in public service or.

John Riggi: No, I don't actually. My parents are immigrants, came from Italy, and hardworking folks, very humble, blue-collar folks. But what they instilled in me was a love for this nation and being a good citizen and contributing. And it wasn't about making as much money as you could, but doing something noble, honorable, and being tough with honor and all of that. So I think it came from my parents.



Ed Gaudet: Well, we appreciate you and we appreciate your service. This is the Risk Never Sleeps podcast. So I'd be remiss if I didn't ask you this question. What is the riskiest thing you've ever done?

John Riggi: Work-related?

Ed Gaudet: It could be anything, John. Just keep it clean, please.

John Riggi: So. Well, of course, it's always clean. Well, first, let me just say that folks would have to read my bio to kind of understand a lot of the operational things that I did over my career. I was very privileged to work with a great team of agents, international partners, and intelligence officers. Probably the riskiest thing I ever did, honestly, is classified. I can't really talk about it and involves foreign operations, but I won't be able to really get into that. The other piece of my resume or bio, if you notice that I served eight years on the FBI, New York City SWAT team. So that was fun. As I told my wife, it's all about no harm there. But there's we get bigger guns, more guns, better training. So it's actually safer to be on the New York City FBI SWAT team. So let's just say that I was in a lot of high-risk encounters, gunpoint encounters, and thankfully was able to complete the mission without getting hurt or killed.

Ed Gaudet: So any interesting stories you do any work with organized crime during that time or?

John Riggi: Ed, you see my last name, right?

Ed Gaudet: I do.

John Riggi: All right. So in 1990, after my first assignment in Birmingham, Alabama, I am 100% Sicilian, and I was immediately assigned to the Sicilian Mafia drug trafficking squad in New York City in 1990, where I stayed for several years working that. So I did a lot of work, ran undercover operations.



John Riggi (cont'd): I ended up doing a little bit undercover operation myself later on against Russian organized crime, but worked very, very closely with Italian national police and others against the Sicilian Mafia and US-based organized crime. So a lot of fun in those days, but had the opportunity to work with some tremendous heroes on both sides of the Atlantic.

Ed Gaudet: Well, any interesting stories about that time that you can share with the listeners? I know I'm putting you on the spot.

John Riggi: Well, there's one humorous story I can tell, so I won't use all the names, but. And one of the arrests that I made of an international Sicilian Mafia drug trafficking figure, he's Sicilian about my age. So at that point, I was probably in my early thirties or so, and somebody I had encountered on the street a couple of numerous times, we introduced them at midnight to coincide with 6 a.m. in Italy, where they were doing we were doing a big international takedown. These guys were really bad guys, international heroin traffickers involved in multiple homicides as well. So I have him in handcuffs. He's in the back of the FBI car. We're taking him in to be processed, and I'm speaking to him in Sicilian dialect, our mutual combined native dialect. And I remember him as he's in handcuffs with his head down looking at me, saying to me, so let me understand this. You're Sicilian like me, and you're in the FBI. I said, that's correct, thinking that, boy, our lives are really different and he's thinking of reflecting on our different situations. He then looked up at me and said to me with a straight face. He said, where did you go wrong? Again, this was the mentality at the time that he just couldn't believe a Sicilian guy working against other Sicilians. But happy ending. I went home that night. He went away for 20 years.

Ed Gaudet: Well, that's terrific. John, thank you so much for sharing your time with us today. And our listeners will appreciate your stories. Thank you for your service and everything you do with the American Hospital Association and protecting us and protecting patients' safety. This is Ed Gaudet for the Risk Never Sleeps podcast. For those of you on the front lines of patient care, thank you for your service. And remember to stay vigilant because risk never sleeps.









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