Podcast Transcript

Risk Never Sleeps
Episode 97
Jigar Kadakia

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 pleased to be joined by Jigar Kadakia, the Vice President and Chief Information Security Officer for Emory Healthcare out of Atlanta. Welcome, Jigar. How are you, sir?

Jigar Kadakia: Thank you, Ed.

Ed Gaudet: I think this is your one-year anniversary here, joining Emory. Is that right?

Jigar Kadakia: Yes, it is one year. It has been one year.

Ed Gaudet: Happy anniversary.

Jigar Kadakia: Thank you very much.

Ed Gaudet: Let's start off with telling listeners a little bit about your role in the organization.

Jigar Kadakia: Emory Healthcare is a large academic medical center based in Atlanta. So, I'm the chief information security officer for Emory Healthcare. So, as typical with a with a lot of CISO roles out there, responsible for risk, third-party risk, security operations, training and awareness programs, biomedical device security, as well as cyber operations as it relates to the cloud environment and then security overall. So risk management, risk assessment, the key tenets that you would expect that a security program. ... job.

Ed Gaudet: Yeah, and you have a university attached as well, which is a little different. How does that, how is that different from some of your previous roles?

Jigar Kadakia: The university has different sets of issues. So they have student, they have graduate programs, postgraduate programs, undergraduate programs, etc. So, their ability to protect student data, intellectual property research data is a slightly different animal when it compared to the core healthcare data. In general, university data is in many locations. Healthcare data is supposed to be in one location, but as well it's in many different locations. But the level of scrutiny and the amount of data that you have on the university side is governed by different sets of rules, mainly FERPA, among some other regulatory requirements associated with kind of the research data.

Ed Gaudet: Yeah, and you spent about nine years at Mass General Brigham; which part of your role was privacy officer? Talk to us about the combination of those two roles. And do you think that's a good idea for other organizations to consider, or do you think they should separate security and privacy?

Jigar Kadakia: As one would say, you can't have privacy without security, but you can have security without privacy. The two are very intertwined. There is a lot of legal interpretation as it relates to the privacy aspect of it, especially with many of the burgeoning privacy laws that are occurring. So, GDPR has been a big one that a lot of individual organizations have had to face. But China, India, the UK, Australia all have different types of privacy laws that are very similar in nature, and quite frankly, probably a little bit more specific and more widespread than maybe the US version of privacy law.

Jigar Kadakia (cont'd): California has always been the spearhead or the leader as it relates to patient or privacy rights in general, including patient privacy rights. And as California has developed its set of privacy laws, other states around the country have also adopted new and different privacy laws. So, the privacy environment has changed significantly, which has caused the security professionals to maybe change their approach on how to support and protect data because certain requirements require certain levels of protection, certain data elements are considered sensitive, etc. So it's really morphed how security professionals protect data within their own environment based on where they're located, the types of data they have, and how they operate.

Ed Gaudet: So a lot of regulations to crosswalk. Do you think we'll ever get to a national privacy law like GDPR?

Jigar Kadakia: I don't know, I don't know. That's, that'll take an act of Congress literally to ... to create a federal law. And then, on these types of issues, at this stage in the game, they have deferred to states to create their own requirements as it relates to privacy. They have also created their own set of security requirements in some instances as well, depending on the state, the legislative body, etc.. I don't know if we'll have a national requirement, but there is movement to come up with more prescriptive guidance, not law, but guidance around security as it relates to healthcare entities. With the HICP and those type of laws, there's cybersecurity laws in place, and now the government is contemplating recommendations or more prescriptive guidance around AI and AI technologies that all of us are facing.

Ed Gaudet: I remember when CASB, the California breach law, came out; I think actually this is the anniversary of it back in the early 2000, 1386, I think, was the, you probably were dealing with that when you were at Deloitte or even earlier.

Jigar Kadakia: Yeah.

Ed Gaudet: Tell us about your background and really unique coming out of the big two of the big four, I think.

Jigar Kadakia: Yeah, I started out my career at Accenture. System administrator, high availability data center type person, and then moved into Deloitte. I think for cyber professionals, the ability to understand and manage risk and risk management, I think is really critical to be in the cyber professional because security is black and white in some instances, right? Either you're attacked or not attacked, there's a malware or not a malware, you're logging, not monitoring. It's the interpretation of what you do and how to manage the level of threat that drives you into the risk world. And quite frankly, the business understands risk better than they understand we have vulnerabilities that need to be addressed, what's the risk of those vulnerabilities, and what's the risk of those vulnerabilities and their impact to environment, to our financial well-being, our for our case patient. But some other industries that may be their products or consumers, etc., so I think it's important to understand risk. I also believe it's important to understand audits. Having been at Deloitte, we did a lot of audits in our time, especially during the Sarbanes-Oxley period, and I think it was a very valuable experience to learn how the audit approaches the audit methodology because you have risk assessments; you have outside audits and cyber or in IT. And it's good to be able to have the skills and the understanding of what that means, whether it's sample size or the auditing approach so that you can better prepare yourself or prepare your organization as they go through those types of audits and whatnot.

Ed Gaudet: I got a glimpse, I think, at one of your reports that you did for a local Boston health system years ago, and I was really impressed with how just detailed it was, but identifying gaps and really laying out this roadmap for CISOs and CIOs to close those gaps over time with obviously requisite investments. Yeah, obviously, part of the toolkit that every CISO has the audit function. How did you get into healthcare, and how did you get into it? What drew you there?

Jigar Kadakia: So, I'm a chemical engineer by undergraduate degree. I was doing my co-ops in Midland, Michigan, the home of Dow Chemical, and I realized as a young college student that I didn't want to be single living in Midland, Michigan. And no fault of Midland; it's cold in Michigan, but there's just not a lot of people and not a lot of young people. And having gone to school in Cincinnati in a big city but not like Atlanta or New York, but a bigger city there was a nice population of young professionals around. So, I decided that I wanted to not move to a chemical plant, and the opportunity came about.

Jigar Kadakia (cont'd): At the time, it was Andersen Consulting able to work at a number of different clients, travel and visit and live in different cities, mostly major cities across the US. That led me into technology. And then from there, as I mentioned before, I moved on to Deloitte and really focused in on audit and Cybersecurity. At that time, it was called information security before the buzzword cyber came about, but focused in on information security, and I worked for a number of healthcare clients at the time. And then, at the same time, Obama passed the Aura act. And then we had the HIPAA act and all these things that happened in the 2000s, 2006, and '04 time period. Meaningful use came about, and that's when there was a big focus on moving to electronic health records, meaningful use. And I did a lot of work around meaningful use, which kind of drove me into the healthcare space, which led me into cybersecurity or information security. That's when healthcare started to adopt what financial industry had already adopted, which was a CISO or director of information security, but someone to manage kind of the information security aspects of a IT program and led me into being a CISO at an organization and then continued my path as a CISO here at Emory Healthcare.

Ed Gaudet: It's amazing to think that the role is not that old.

Jigar Kadakia: Not in healthcare. The financial industry, it's been there probably 30 years or so.

Ed Gaudet: Yeah, which isn't that old in the scheme of things. All right. Great. There's a lot that's been happening. Obviously, we had Change Healthcare event. We had the.

Jigar Kadakia: CrowdStrike this week.

Ed Gaudet: CrowdStrike. It's just, it's the cyber. It's the gift that keeps giving, right? Were you affected by the CrowdStrike, and what did it look like, and how easy was it to recover?

Jigar Kadakia: Yeah, so we were one of the customers. I think they had 26,000 or 27,000 customers impacted by the blue screen of death. We were able to react and mobilize fairly quickly and ensure that we had full patient care by Monday morning.

Jigar Kadakia (cont'd): We had armies of people over the weekend starting Friday, touching keyboards and doing command line stuff that many people never did and some people did but hadn't done in years ago. And as the weekend progressed, there were different options that became available to speed the process. But at the end of the day, you still had to manually touch every device. Someone had to touch the device, whether it was an IT professional, a volunteer, a nurse, a doctor, but someone had to touch the device. And by the end of the weekend, with all the different updates that were pushed and the options available, in some cases as simple as just rebooting the device or having someone reboot the device versus going in and doing the code and those kinds of things, yeah. While it was impactful, it was very impactful for two days. I think, for some, it's a silver lining. Part of it in cyber management of endpoint devices is a typical reboot cycle. Typically, most organizations don't have a scheduled reboot cycle. A reboot device cycle and endpoints helps clean the memory, helps performance, helps reduce staleness, connectivity, etc., so having been able to reboot everything for the first time, probably ever, we probably saw some devices come online that we hadn't seen because they were stuck or broken and just needed the reboot. In other cases, probably got better updates to these devices over time because updates got pushed and probably got cached and didn't get rebooted at some periodic cycles. There are some silver linings out of this. Clearly, this was very painful, and I don't want to underestimate that. It was a lot of work, a lot of effort by a lot of people, and we had a group of team members and volunteers mobilized to assist in touching the keyboards and doing all the things that we needed to do to maintain and help our patients. But post-incident, there's always, what are you going to do and how do you improve the discussions about resiliency? I saw, CrowdStrike now is thinking about a metered approach or a rolling approach for updates and not.

Ed Gaudet: To be smart.

Jigar Kadakia: ... Big Bang. Something that most organizations would have followed would have been a rolling update approach. And so, by having the ability to roll out update approach, you can control the number of devices impacted. So, if there is something bad that you can stop and wait till the fix comes in before you roll out.

Jigar Kadakia (cont'd): So some things that CrowdStrike has learned is that some things that we'll be able to apply in our environment, and some other things that were positive with regards to health and hygiene of our endpoint devices; we also found old ones that we replaced as part of this process. That probably would have taken some time, but now, in the height of the emergency, we probably were able to we did it much more quickly.

Ed Gaudet: Yeah, you always got to look for the silver lining in these events. The good news is most people were able to recover quickly enough. I was hit with it, so I had to deal with it personally. It was frustrating. Once I figured out the path to recovery, it was pretty quick. So, let's talk about AI. It tends to be on everyone's list. What are you doing at Emory, and what are you thinking about doing over the next 12 months or so?

Jigar Kadakia: As I mentioned before, AI is a burgeoning topic. The government is trying to get ahold of things. We have a school of AI at Emory University with a bunch of thought leaders in the space. We're trying to get ideas. There are multiple facets of AI that people have to be aware of and dealing with that has been it's quite complicated. So there's the security concerns. There's the privacy concerns. There's the ethical concerns. There's bias concerns. As a university, we have obligations to students. So, students use it and not use it. It professors using it, not using it. What are the rules? What are the approved solutions? What can you do? How do you denote it? How do you document it? How do you reference it? Like all of these questions are out there, there isn't strict guidance on any of it. So everyone is trying to talk to their peer groups, talk to experts, quote unquote experts in the space to figure out what the best approach is and then implement something that lets us harness the power of AI but in a safe, secure, and private manner trying to balance that going forward. I think, hopefully, in the next couple of months, I think people are going to do things today, and then in six months, they're going to have to modify because either the technology changed or got improved or there's is some kind of guidance that people should follow, or maybe some type of law or rule that we'll have to modify. So I think for the next few years, every, you know, six months, we'll have to modify our approach until things even out to a kind of a baseline.

Ed Gaudet: And have you created a cross-functional governance committee?

Jigar Kadakia: Yeah, we have a cross-functional team. We have created a policy via the cross-functional team. It's going through the review process. We have a set of AI approved tools that we have, and we continue to look at new tools and approve those. Some tools are baked into existing processes, and others are add-on tools. And so, determining which tools that we want to allow and approve it's been part of our workflow because we want to provide solutions to the end users. And if we can provide them a wide enough selection of tools, then there's a less likelihood of them going and buying something different that we haven't had a chance to review, approve and put in the proper controls to manage it.

Ed Gaudet: Now that makes sense, and we see that pattern quite often across health systems. What other strategic initiatives are you dealing with or priorities over the next 12 months, other than AI?

Jigar Kadakia: Clearly, improving the resiliency. So CrowdStrike and Change Healthcare both highlighted the need for improved business continuity, disaster recovery type. I think most organizations have done some work around this, but with back-to-back incidents, I think it's heightened the focus of we need to shore up these processes and make sure we properly test, and maintain, and train our people on those processes, clearly a focus on business continuity and disaster recovery. As I as we talked earlier, AI; what are we going to do with AI? How are we going to handle AI? We have governance in place, but what else can we do? Is there things that we need to be aware of? I think is on the docket continued evolution of cybersecurity. The threat landscape in cyber continues to escalate. The threat actors used the CrowdStrike incident to try to do scams and phishing and whatnot. How do we stay on top of that and move things forward? Identity, at the end of the day, is the crux of all things in cyber. How do we continue to move to a zero-trust model? How do we improve identity? How do we make it easier for users? Those are all big-ticket items. I think over the next 12 months, that will look to try to move, make progress against.

Ed Gaudet: Excellent. When you think about working in passions outside of your day job, what would you be doing if you weren't doing this? What are you most passionate about?

Jigar Kadakia: So I would like to do something maybe where I didn't have to use my brain as much.

Ed Gaudet: Say that now. But then when you're doing.

Jigar Kadakia: ... Parts of my brain, right? There are a lot of activities that, we're on a Zoom call right now, right? There's a lot of activities, especially on a day like today, that I'd like to be doing outside. Any type of activity outside would be cool. As a profession, as you age, it's harder to do some of the activities that you like to do outside, but I think anything ... uses a different part of your brain, building something, constructing something; maybe that's a little bit of my engineering background. That would be something that would be of interest for me, other than maybe sitting on a beach.

Ed Gaudet: My dad would build, when we started having kids, he would build dressers and all this furniture for the grandkids. So, do you envision yourself?

Jigar Kadakia: Have you built something that you have that's tangible, that you have pride in building? Part of it is a learning experience, and part of it is what the, what the opportunities are and what you can do. So it's just using a different part of your brain, using your hands and those type of things is just, it's different than typing in a keyboard and talking on a Zoom call all day.

Ed Gaudet: Amen. You go back in time. What would you tell your 20-year-old self?

Jigar Kadakia: I don't know, I don't know what I tell my 20-year-old self. I'll tell my 19-year-old twins all the time, take the opportunities that they have in front of them, and don't be afraid to take risks. I think I grew up, or a lot of folks grew up, a little bit risk averse, and I that was probably how people were brought up, maybe in the 80s and 90s. I think the attitude is a little bit different today, and I encourage my kids to try new opportunities. Don't be afraid to fail. I know they're going to fail along the way, but you can learn from failure and take those opportunities.

Jigar Kadakia (cont'd): Right now, there's so many opportunities for 19 and 20-year-olds that didn't exist when we were 19 and 20, and there's also a little bit of a you can try it and fail and move on to another opportunity where I think we are 19 and 20, we had to stick through it, and we are less about trying things and failing and moving on because if we failed at it, it was considered a failure. I think today, it's considered a learning experience. And at that age group, you can do a lot of learning experiences and be successful.

Ed Gaudet: Yeah, and it felt like back then, you didn't have the safety net of your parents to fall back on. You were out of the house. You were gone. You were out.

Jigar Kadakia: Yeah.

Ed Gaudet: It was very rare that you'd come back where...

Jigar Kadakia: Boomeranging back.

Ed Gaudet: It's, yeah, there's a lot that happens. All right. You're on a desert island, and of course, you come from Cincinnati, WKRP, the greatest rock station ever. What five records or movies would you bring to your desert island?

Jigar Kadakia: So I think I would want a chair or some kind of chair and umbrella. Movies. I like a lot of movies. I don't know what, I like, once I watch a movie, it's hard to watch it again for me. So I'd love to see any new movies. So I'm probably not as, I'd like really, as I've seen a lot of movies. Huh?

Ed Gaudet: You like horror movies or thrillers?

Jigar Kadakia: I don't like horror movies, so I like, clearly I like Star Wars, but I like action movies or mystery-type movies, and I'm not opposed to documentaries either. Comedies are funny depending on the time, of the time. Albums or books, so a huge Jimmy Buffett fan, and I always have some Jimmy Buffett music, probably, and it works well on an island, right?

Ed Gaudet: It works great, perfect.

Jigar Kadakia: Books. I would take recommendations on books. There's a lot of books out there. I haven't, I wish I read more, but I don't read as much because you can podcast it and stream it and do those things. But I would take recommendations on books for the island.

Ed Gaudet: All right. Hardest lesson in your career?

Jigar Kadakia: Admitting when you made a mistake and accepting what you make a mistake. So not every decision we make or I make is good, and so, accepting the decision was misguided, and accepting that and then learning from it, but being able to quickly come up with a different decision or a different approach, I think, has been a learning lesson for me.

Ed Gaudet: Good advice.

Jigar Kadakia: Yeah.

Ed Gaudet: The riskiest thing you've ever done?

Jigar Kadakia: I like to scuba dive, so it's risky. When you're 100ft under the water and/or swimming with the sharks.

Ed Gaudet: Yeah.

Jigar Kadakia: So it's fun. Scuba diving at night is even more different experience. So, different types of fish light up at night versus during the day that you can't see, so it's really cool. And then being able to swim with the sharks, the sea turtles, and other creatures and animals 60ft, 70ft, 80ft below water is pretty cool.

Ed Gaudet: Where's the most interesting place you've had to dive and where would you like to go?

Jigar Kadakia: Most interesting is Fiji, and the next place I want to go is the Great Barrier Reef. I hear it's wonderful there.

Ed Gaudet: Yeah.

Jigar Kadakia: A lot of sharks there, too.

Ed Gaudet: Yeah, for sure. As a cyber professional, we swim with sharks every day, right? Last question. What advice would you give to someone coming out of school that wants to get into cyber or healthcare or both?

Jigar Kadakia: Look for opportunities. I don't think you have to have the healthcare knowledge. I think you have to have a good, solid tech knowledge. At this point, someone coming out of school, a knowledge in the cloud I think is important, and how to do cyber in the cloud, I think, is probably very important compared to your traditional on-prem areas. As I mentioned before, it would be good if they had a baseline knowledge of risk and or the ability to audit because you can quickly get a job in cyber around risk and then move within an organization or move into another organization and focus in on the technical aspects of it. You don't have to be a coder to get into cyber. You don't have to be a developer to get into cyber. Clearly, those skills are important and will help you accelerate, but you can do it from any position. If you look at the marketplace, there's millions of cyber jobs available, so you just have to want to try it. You have to have the ability or want to learn, right? Ask questions, learn. You're going to have to do some self-study to get yourself brushed up on the concepts and the approaches. Things are changing so quickly. What you learned in school two years ago may not be applicable today, but clearly, you have a baseline knowledge.

Ed Gaudet: Yeah, great advice. This is Ed Gaudet from the Risk Never Sleeps Podcast and we have been speaking to Jigar Kadakia at Emory Healthcare. If you're on the front lines protecting patient safety or delivering patient 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