Podcast Transcript

# Risk Never Sleeps Episode 124 Carter Groome

**Ed Gaudet:** Welcome to the Risk Never Sleeps Podcast, in which we talk to the folks on the front lines protecting patient safety and delivering patient care. I'm Ed Gaudet, the host of the program, and today, I am pleased to be joined by my great friend, Carter Groome. You are, you've made the great list, Carter.

**Carter Groome:** Oh, boy. Thank you. Thank you, Risk Never Sleeps. You are prolific, and I appreciate what you do for our sector.

**Ed Gaudet:** Oh, I appreciate you as well. So, let's talk about just remind people a little bit about your organization you were on about a year ago, as it turns out, I think.

**Carter Groome:** Wow. Yeah, a long time. Yeah, that feels like a decade, last year, that's right.

**Ed Gaudet:** It does. But I see you often at the conferences and other sector meetings. And so I feel like we just talk every, you know, every other week. But so just remind the listeners a little bit about yourself, a little bit about your organization, and then we'll kind of kick it off from there.

**Carter Groome:** Yeah, sure. You know, First Health Advisory, I am the CEO. The company started, in fact, as an electronic health record optimization and integration firm.

**Carter Groome (cont'd):** And about ten years ago, we started getting opportunities in medical device security, and it became a practice, which became an identity, which became who we are today, which is all things security, privacy, risk management, and compliance as advisors and consultants specific to the healthcare market, which includes providers, physicians, practices, government health entities, health technologies. I just absolutely love what we do. There is a challenge every day in this field, and the folks that you know are involved in this are, you know, my dear friends, including yourself. And boy, it has been a battle, and there are certainly days where I say, why in the world would I want to be in healthcare cybersecurity? And everybody on the outside thinks it's great, and we're making money hand over fist, and it's just the easy work and, you know, just sleep every night, no problem, but it's a battle. But that's part of the challenge which draws me, and I'm sure you, to what we're doing because the mission is important.

**Ed Gaudet:** Yeah, I think that shared mission is what keeps us sane and focus on the things that matter, right? And industry over profit, although profit is important, we need profit to keep fueling the business and reinvesting in the business, however, not at the expense of doing the right thing for healthcare. And I think that's what sets us apart. Certainly, vendors that continue to serve in healthcare continue to deal with some of the frustrations that you've alluded to because it isn't easy, which again, for some people, I love a challenge. So bring it on. For others, they want the easy route. And, you know, they're they're doing something else, so.

**Carter Groome:** Bring it on. You know, we talk about resilience from an industry perspective. But I think those individuals like yourself and myself and you know, the colleagues that we work with day in and day out have a certain level of resilience themselves as people, you know. I've had the conversation before that it's almost a tolerance for suffering, right, that could also probably be a definition for resilience. But, yeah, I mean we get beat up all day every day.

**Ed Gaudet:** We're getting kind of philosophical here, but you know, for our listeners, we serve in the shadows of those that actually give themselves every day on the front lines. And I think that's what's inspiring to us is, while we have our challenges, we look at those challenges and go, wow, right? I mean, that's what keeps me going.

**Ed Gaudet (cont'd):** It's like, I mean, yeah, my day is hard, but, you know, the folks that were serving their communities during COVID, the folks that do the, you know, the 30, you know, the 36-hour, you know, three straight 12-hour days, right in the OR, right in the recovery units and the surgical units. I mean, they get the respect.

**Carter Groome:** No doubt, no doubt.

**Ed Gaudet:** All right. So, is our pity party done? Are we done with our?

**Carter Groome:** Ed, you know, it's funny. I know there are people listening to this laughing right now. Like, but no, it's.

**Ed Gaudet:** And I think that's what makes the relationship, so immutable. Like you form these relationships with people, and you know you're going to battle every day, you know, with that same shared mission. It does make it, it does make it easier. And certainly, you know, sharing dinner and a cocktail also makes it easier too, which is why we're often doing that. So 2024, let's put a stamp on it and to clear it over, okay? What a crazy year.

**Carter Groome:** You know, we've said for the last decade at least since WannaCry, which is what, '17, that, oh, this is the worst year. This is the worst year. This is the worst year. I think it's just like every election said, this is the most important election. 2024 was the worst year, you know, depending on the lens, right? But it was more than ever a wake up call for the leadership and the boards and those that can make a difference in our sector, right? And I distinctly saying this is our Colonial Pipeline moment, and that still holds true today. What Change Healthcare went through woke up a lot of different parties that can influence the resilience in the security and the privacy and the overall risk that our sector is facing. So you can't, you kind of look at it two ways, right? I mean, there were a lot of long weekends and late nights in 2020 for those of us that do what we do. But there, I think, is some good that has come out of the awareness, the education and what needs to be done overall to put our sector in a better posture going forward.

**Ed Gaudet:** Well said. I think, yeah, it was like last year, right around this time. Well, in another month, I guess we were all at ViVE when the proverbial stuff started to hit the fan, and we were all looking around going, we're all at ViVE, and this is going down. And yeah, it was just amazing to see the reactions of people initially that thought, oh not me, I'm good. And then they realized, like, probably within the next 24 hours, oh no, I'm actually affected because I use a particular product that I didn't think was part of that overall organization.

**Carter Groome:** Is this going to be back up tomorrow or?

**Ed Gaudet:** No, I know.

**Carter Groome:** This week? And I think.

**Ed Gaudet:** When you start, when you start talking about cash on hand, you know, it's not, you're not in a good place when people are looking at how much cash do we have on hand to weather this storm.

**Carter Groome:** And not, you know, and I'm glad you brought that up, right? Because we talk about cyber safety as patient safety, and unequivocally, I believe, and that is so important. But these are still businesses at the end of the day in what really and this. So I don't want to be cynical, Ed, but what really got the attention of boards and leadership is, wait a minute. We're not dropping bills. You know, we're not checking eligibility. We're not able to generate revenue.

**Ed Gaudet:** Yeah, yeah.

**Carter Groome:** Boy, that really got the attention.

**Ed Gaudet:** Yeah.

**Carter Groome:** That need to know.

**Ed Gaudet:** Yeah. And hats off to, and again, I'll, you correct me if I'm wrong here, but hats off to the organizations that provided, you know, some relief while we worked through this incident and recovered because there were some organizations that were really in need of that financial relief until we got through it. And so I think that was primarily was that UnitedHealth and Optum that provided that provided some funding for folks?

**Carter Groome:** Yeah, absolutely. There were others, right? And we can sit here for the whole time we're talking and you know, look at the negatives of that and yeah, the tax and everything else. But yeah, I mean, that event alone short of, you know, an incident from CrowdStrike, you know what Ascension went through, what's you know, essentially everybody was looking at that and saying, what are the indicators of compromise? We are in a hot situation here because we need to make sure our environment is clean. So, you know, that was, you know, a national event, what Ascension went through.

**Ed Gaudet:** Yeah, yeah. No doubt. And it just seems like it's the industry that keeps on giving. Like like 10 years ago, 20 years ago, you never had this. And you fast-forward it, and from a healthcare technology perspective, like there's no more. I used to think about healthcare, as always, 5 to 10 years behind everybody else technology-wise, that's not the case any longer. In fact, you could argue that they're either on par or maybe even a little ahead of some industries, especially as they start looking at AI and the use of AI across the business.

**Carter Groome:** I believe that, and I also believe if you do security well in this sector, you know, fintech, manufacturing, retail, I'm pretty sure you could get a handle on those industries if you're doing it well in healthcare, right? Just kind of wish healthcare would pay a little bit better to retain the talent that we need, and we absolutely need it.

**Ed Gaudet:** Yeah. I was talking to someone today about the workforce challenges. And, you know, how do we, as a sector help really bring in the younger generation into not just cybersecurity but into healthcare when there's so many options available at that collegiate level, right? As they're thinking about their career path, how do we bring in all the good things that come along with the things we do every day, albeit the challenges modulo the challenges that we have to deal with?

**Ed Gaudet (cont'd):** And how do we do that at scale so that it's not an after-effect, but it's actually a cycle like we've got now universities working for us? They're aware of the opportunity. And the next set of graduates are thinking about, I'm going cyber healthcare, like it's a path, and people talk about it as a path. It's not like a, oh, did you know healthcare has cyber, which is where I think it is today a little bit. I think we suffer from that.

**Carter Groome:** Right. In a sadistic way, I think we can thank 2024 for some of that energy, right? I'm seeing these programs announced and curriculums developed, you know, from, you know, that undergrad and graduate level stage that could certainly be a pipeline for that talent that our sector absolutely needs.

**Ed Gaudet:** Amen, yeah. All right. Let's switch topics to something near and dear to our heart. Something that we were on the ground floor of creating, and now we're actually dealing with the monster doll. I'm just kidding. We're dealing with the next phase of that creation, which is the HIPAA rule being opened up, right? What is it, the MPVM, or I forget, the NPRM. Thank you. NPRM. And all 300 and something pages of that thing, digesting that, understanding how they synthesize all of the work. The Health Sector Coordinating Council, the 405(d) through HHS, did to get us to this place we are today.

**Carter Groome:** First of all, I want to say thank you to you, Ed, and everybody that had input into this thing, right, over many, many years. And so you think about what Health Sector Council was doing. You think about how CPGs were put together. You think about all the dialogue and all the conversations that the task groups had. That is absolutely seen in this document. It's unequivocal that, you know, those inputs were taken account for and there's all kinds of commentary now sort of reacting to the content of the proposed security update. And some of that's good, some of it's, you know, against it, you know, it's too burdensome. You know, we're already strapped in the system of care. You know, it has to be done to better defend critical infrastructure. You're seeing it's all over the map. And we are literally just in the starting block, in my view, of an ultra marathon, when we look at historically changes of this magnitude that have come and could just go back to high tech. In 29 when it became a law, 2013 was when it actually became enforceable. And that was just to make business associates comply with the HIPAA security rules. So, almost four years.

**Carter Groome (cont'd):** So this is something that is super important, Ed, and I believe everybody needs to pay attention to what's in there. But I would caution, one, on you know let's let's look at this as a starting point, and it's a great starting point. And two, obviously, with a new administration coming in, we need to start getting some signals from that administration on their posture, right? You know there's going to be inputs that come from HHS, the new DEP Jim O'Neill presumably. How does he feel about this? How does Senate feel about this? Cassidy is going to be the chair of the health committee. Rand Paul is going to share his GAC. How does he feel about CISA? Is CISA going to be the SRMA? Because we saw the, you know, OMB come out and beat the crap out of HHS just back three months ago. So there's so many little tangents that we don't have signals on right now that could impact what we've just seen in terms of the notice of proposed rule. So that's just to start the conversation.

**Ed Gaudet:** Yes, yes. And just to give people sort of a historical view of this. You'll keep me honest here, Carter, HIPAA dealing with the confidentiality, integrity, and availability of electronic protected health information, i.e., your health records, right? Using a digital form starts off in 1996, and then it's updated in 2003, I believe was the update.

**Carter Groome:** That's right.

**Ed Gaudet:** And then HITECH comes along with EHRs and meaningful use. And there's another security update that follows that you mentioned. Was it '14 or '13?

**Carter Groome:** I think '13 is when it became enforceable, and then there was a 21.

**Ed Gaudet:** And then there was the 21 update as well. And in between that, there is a law that designates 405(d), right?

**Carter Groome:** That's the 21. Yeah.

**Ed Gaudet:** The 21 Act to basically, where there's a public-private partnership to come together to create a set of tools, and processes, and best practices that the industry, the sector can use, right? In a meaningful way to protect protected health information and other.

**Carter Groome:** That's it, right? So that latest one, you know, sort of known as Safe Harbor, right?

**Ed Gaudet:** Yeah. Well, that was the what was that. What's the third is, I forget now, was it like 1386 or.

**Carter Groome:** Yeah. Public law, right? But that's, again, it's already codified, right? It's saying follow these practices and OCR will look favorably upon you if you're doing it for 12 months, right? So yeah, there's this whole sort of argument out there, Ed, to say, listen, you know, it is imperative upon the health systems, the business, the regulated entities, which is an appropriate word, right? It's not just covered entities, the regulated entities to protect EPHI, which is also the right thing to do here, not, you know, not the organization, but where that data is, and wherever it resides. So, you know, there's a lot of good that's coming out of this, but do we need, and I'm not stating a position quite yet, I want to get those inputs that we talked about earlier. But do we need something like this when you could follow a framework like NIST, which is flexible and prescriptive enough to already do some of these things, and it's codified? So, you know, there's that argument, right? There's a big group saying, hey, we don't need to be regulated. The business and the business leaders should, as an imperative, take on this type of activity to protect and safeguard their businesses. And if they don't, they should be out of business.

**Ed Gaudet:** Yeah. And to your point, and this is really interesting, right? Because these things are coming to HICP creates the cybersecurity performance goals. So out of hiccup and the work we did as a sector with CISA and CMS and others, where we looked at a bunch of research, and we said, hey, we're not doing great as a sector. What we really need is a minimum set of security standards that can be applied across the sector to keep us out of trouble. Because when we created HIPAA years ago, we didn't have this thing called ransomware. This is a relatively new phenomenon, and it's bad. And so we have to think about it in the context of that, the change that occurred, technology or otherwise, right? And we have to be able to react to that change.

**Ed Gaudet (cont'd):** And that's really what HICP, HITECH, CPGs, the new HIPAA, NPRM, are all designed to provide the sector with a way to protect itself in a meaningful way. I mean, I wrote about this in for a couple years ago about creating a meaningful protection standard. And so what I love about, I mean, there's a lot to not love about, but what I love about the intent of it, if we keep the intention pure, the intention is create a minimum set of standards that everyone should be following: enforce, don't make it voluntary because no one will do it. Enforce it because it's the right thing to do. Modulo. We got to figure out how to pay for it, right? So there's, that whole thing that we got to figure out. But if you think about the intention, I think the intention is right. Now, how it morphs from there, like if we add too much to the HIPAA or whatever you want to call it now the security rule ..., if we add too much to it and it doesn't make sense, then it's going to cause more trouble. It's going to cause more confusion. It's going to cause, quite frankly, more stasis. Who knows what the new administration will do because they're not regulation-friendly, which, depending on your persuasion, is a good thing or a bad thing, right? Irrespective of all of that, we have to solve the problem of protecting patient safety, patient care, and the services that we all now rely on that are electronic.

**Carter Groome:** Unequivocally. So we are in agreement on that. And in fact, if you use the word minimum, right? And in CPG, you call it essential, right? In this document and in the proposed updates, my view, there's nothing minimum about it. It's, you know, look, we would probably know some of the authors and architects of this. We don't have to talk about them, per se, but I'm sensing they're like, this is our Hail Mary, right? We did a lot of work over the last couple of years, and we're going to make sure it's documented and we're going to go for the moon and the stars in the universe here. I mean, you break down some of what the requirements are. If you just took the asset management requirement, Ed.

**Ed Gaudet:** It's not possible.

**Carter Groome:** Yeah. Following EPHI, but then any CIA activity that could impact EPHI, right? That's just one line of 394 pages, or 393 pages. That is a massive, massive lift, right? So we're not talking about just small rural critical access will have challenges meeting this standard, right?

**Carter Groome (cont'd):** This is not just a minimum standard we're talking about here, right? Like do MFA make sure it's deployed. You know, like encryption for, you know?

**Ed Gaudet:** I mean, I was talking to our mutual CISO friend recently, and we were talking about the analogy. Yeah, I could keep my house safe by locking all the doors and boarding up all the windows, but it's not practical. Like, I could do the same for my business, but it's not practical, so I have to assume some sort of risk. And I think that's the thing they're missing, is that you have to assume some sort of risk with data today because it's fluid. There's no such thing as unless you, by the way, this is a little biased, but years ago, I had a company where we put security controls around the actual data objects. So, in that context, you could actually solve for this problem. And I thought it was going to solve for this problem. The problem is it's too hard practically to implement because it changes all of the infrastructure. It changes the paradigm. People's minds explode when they think about managing entitlements. How many people? When's the last time you heard the word entitlement used in a technical context, right? So I think that it's just, it's a good idea on paper, but practically it's going to be near impossible to implement. And so, therefore, you're wasting a lot of money versus taking some level of risk that you're going to have to deal with regardless to operate the business. Otherwise, it just doesn't make sense. So I agree with you, but I think, again, I tend to be the eternal optimist. I think this will work itself out based on the comment period. I'm hopeful.

**Carter Groome:** ..., right. This is, you see, there's a lot of buzz. And I think, you know, even our clients and people that we talk to are like, oh, what do we need to do now? Let's, like have some patience here, right? This is first draft, right? This could be a years-long process. I know they put in 180 days to compliance, right? These are the things I'm talking about, Ed. Like they're just asking for the world knowing that's not going to be the end result of this, right? And, you know, they make some cases for incentives out there that's not even close in terms of what's needed in my view, and that's where Senate Help Committee, the committee comes in from a funding perspective, but this right now is a proposed unfunded mandate. And when you look at the numbers that were put in there, 9 billion for the first year, and then you divide that by the 822, sort of, you know, a guesstimate of regulated entities. What is that per entity? $11,000. And so you think you do all these things in your organization for $11,000, right?

**Ed Gaudet:** Maybe a month.

**Carter Groome:** Right, but my point is, if you're not already sort of on the path here, doing some of these things that are truly best practices, I'm not arguing with that, right? There's a lot of good in here. But if you're not on that path and all of a sudden you're like, well, now we're going to be regulated. Boy, it could take you two, three, four years even if you had the motivation, your leadership team, your board said, okay, we're going to completely change how we view this risk.

**Ed Gaudet:** Does it sound like minimum. Does it?

**Carter Groome:** Yeah. It's.

**Ed Gaudet:** To your point. Coming back to your point earlier, it really doesn't sound or feel like minimum, yeah.

**Carter Groome:** That it's not. But I can also see the positioning of let's put it all out there and then yeah, you know. Yeah, it'll sort out, right?

**Ed Gaudet:** And yeah, no, and I suspect that that is the case, and I'm hopeful that's the case. I know hope is not a strategy, but you know, I suspect we're going to, it's either going to get delayed because of the administrative challenges I mentioned earlier, or it's going to get shaped into something that is actually consumable.

**Carter Groome:** And look, I'd put my house that it's going to get shaped somehow, or right, there's ten different paths this could take, right? I mean, honestly, HA could walk into RFK Jr's office and said, this is our position on regulation. I think it's good, and kill it. It's not, right? Which they probably will, because if it's not funded they're not going to accept anything that's going to put the hospitals at risk, which is right. That's why they're there. That's what they should be doing. Just that. Imagine that meeting alone. It's, you know, Rick Pollack, right? President, the American Hospital Association walks in. You know, he can get an audience. Done. Okay. No problem. We don't like regulation, so but also think about other downstream effects, right?

**Carter Groome (cont'd):** I don't believe that OCR is all of a sudden going to triple or quadruple their funding. And so, how do they administer what's been put out there as a standard. And then, is it still kind of self-assessment in a way. I've hired a third party to do our assessment and attest that we meet this standard. So this this is big. This is not just some, you know, we're going to fly under the radar, push a little, you know, regulation in the final seconds of the fourth quarter, and see if we can punch it over the goal line. I mean, this is a big task, Ed.

**Ed Gaudet:** And yeah, this, I mean, I don't suspect this is going to get done anytime soon either. I do like the fact, though, that it is, we're thinking about the right things. Again, I think the intention is there still fairly pure. I think it would be great if there was some type of remediation that was, you know, financially viable, or there were incentives like there were with meaningful use that could get the smallest of the small there in a meaningful way, right? It doesn't mean that they're going to have the best level of protection compared to someone that can afford it, but it's going to be better than they are where they are today, which I would posit, you know, in some of these hospitals is just it's there's nothing there. There's, it's a no-op like they might be able to cover HIPAA maybe.

**Carter Groome:** Maybe.

**Ed Gaudet:** Maybe.

**Carter Groome:** Now I know this is interesting. I'm literally refreshing the HHS site the new site every hour today. And I'll do it tomorrow. Why? There is a rumor that HHS is going to put a draft rule out that is going to apply CPG essential goals to CMS participation in potential reimbursement.

**Ed Gaudet:** Oh, wow.

**Carter Groome:** Now again, I don't know when this gets published, Ed. We are essentially a day away from this administration being done, but there is a rumor that the current secretary has signed off on a draft rule.

**Carter Groome (cont'd):** Now, again, I don't know all the sort of the political, you know, the risk of change, you know, the risk of, it's just like everything's frozen, but that that's something that may come out right. And I've been talking about that. Do you tie some minimum standard to reimbursement and or, you know, maybe not conditions of participation in Medicare and Medicaid, but to reimbursement? And is that a longer-term and more viable incentive for organizations to meet that standard? And I, absolutely believe that's a, you know, probable, you know, in good way to do it. So that's what I'm watching for. Is this thing actually going to hit, or?

**Ed Gaudet:** That would be that would be in direct conflict with the NPRM.

**Carter Groome:** It would be, it would be. So, yes, I suppose I'm still here advocating for some incentive, right? I mean, and I don't want to see a big stick at least early on in this if it's enforceable. But you've got to incentivize organizations to do something here. Yeah.

**Ed Gaudet:** I don't know. I mean, it's a lot because it's, you know, it truly is a people process technology consideration in order to even to meet the CPGs, you've got to have all three, and a lot of the challenges with rural hospitals is they don't even have the resources. So they would either have to hire a free-up, a FTE for security officer, although by HIPAA laws, you're supposed to have a security officer. So, like, not sure that makes sense, but they need some help. They're going to need some help to implement.

**Carter Groome:** They need a lot of help. And you know, listen, I don't want to be self-serving, you know, in any way, shape or form. And I think that's part of trying to be disciplined and not put a bunch of sort of stuff out there right now until we get some more inputs. But, you know, part of the issue is you can't just have a virtual CISO or person that's going to be able to cover all the different disciplines and subject matter requirements that are needed in this proposed rule. There's a lot of different expertise that's required to do this stuff from a networks perspective, a framework perspective, an infrastructure perspective. I mean, across the board, you can make the case that there's easily, you know, ten different disciplines within security that might be needed at least to consult again. Not not trying to be self-serving here, but it's not just one person.

**Ed Gaudet:** No, no, no, no. And if it is, you know, there there has to be. Well, what? Anyway, before I go there, what's interesting to me is, in a world where we're outsourcing a lot of that. and there's an event, how does one reconcile the liability? So if you're a rural hospital and you are using a third party as your vCISO, and that person has attested to supporting the new rule, whatever that may be, and there's an incident, what happens from a liability perspective?

**Carter Groome:** Great point, right? And I've already seen the conversations. When you think about class action, you think about claims, right? That is probably more of a stick certainly than OCR finding, you know, someone 30,000 or 10,000 or 90,000. We've seen a lot of activity in the last month, right, for events that were four and five years ago. Yeah, that's not necessarily a motivator for an organization to do something, but a class action suit that hits you three months after you get breached, and you're paying serious dollars. And now this is going to give more tangible sort of evidence, right, needed, or at least fuel for those class action suits to actually succeed. Yeah. And so, that, therein lies a big stick to protect your organization with or without regulation. But I'm sure a lot of the law firms I'm not picking on them are going, oh, we're going to love this. See, right? You know, you didn't every year check with every business associate and get validation that they are following the same requirements that you're following. I mean, just I mean, you think about the burden, right? I mean, like. You can help them with that, Ed, but, right? Like there are jobs going.

**Ed Gaudet:** Oh, no. Yeah, no. Absolutely. Like years ago, I had referred a client to a friend of mine, a lawyer at a law firm, and I'd heard rumors that there was, you know, a lot going on at that firm, and I was called up to basically apologize. Oh, I'm really sorry I referred you to them. I heard, like, a lot. He goes, what are you talking about? That's, those are our favorite clients where there's a lot of chaos going on. That's where we make our money. And I just thought that was great. I'm like, oh, I hadn't really thought about that perspective before, but you're right. Like, there's going to be a feeding frenzy from that sector because of all of the ambiguity. And, you know, and, you know, issue of liability that'll be new. We're going to have to deal with that the minute the first incident hits, right? We did everything you told us to do.

**Carter Groome:** So ..., like there's so much to unpack. To your point, Ed, there's a lot of good in here. There's a lot of learnings for organizations that maybe don't follow it as closely as you and I. And, you know, those members of the community that we've worked with, even to build out 405(d) and HICP and CPGs. So there's good in here, no doubt. And I would just urge generally the sector to have patience as we go through the process of getting this to a point where it's not such a huge burden. And organizations say, okay, I understand we need to do this, you know, not only for our communities and patient safety, you know, but the greater good of our sector.

**Ed Gaudet:** Yeah. Well, there's an opportunity to I think they should hold hearings on this. This is a big deal. They should hold hearings on this.

**Carter Groome:** And I would not be surprised, frankly, you know, because a lot of the public comment period, they'll then hold open forums or town halls. Yeah.

**Ed Gaudet:** Are you submitting your own comments under?

**Carter Groome:** We will be. But again, I'd like to see a couple signals from new administration so I can, I just, last week or the week after to see if there's anything you know that that would signal, right? Just yeah, anything that has the R-word related to it is just forget about it, or we're going to review it, or, there are certain things that when we think, yes, there is bipartisan support for better cyber protections. Absolutely. It's just in how it's enforced. It's, you know, in how ultimately it's implemented and sort of just how the prescriptive rules should be, how prescriptive they should be. So yeah, I think there's going to be some form of, but it's going to take some time to get there.

**Ed Gaudet:** May live in interesting times. And then you throw AI, let's go to AI. What are you seeing from, are you implementing it internally? Are you helping organizations think it through from a governance perspective?

**Carter Groome:** Yeah, mostly from a governance perspective, a responsible use perspective. You know, I can tell you, yeah, I'm seeing, right, because there's still a lot of ... around bias, but that's starting to work its way out, right, in terms of the bias.

**Carter Groome (cont'd):** But you know, when you think of the use cases that are concerning to us from a security perspective, right? You know, deepfakes and those things. Yeah, there's high concern from a social engineering perspective. I think that's what we're starting to see. That worries me. You know, I think when you think offense and defense. And does the adversary have an advantage with AI or reverse engineering zero days and things like that? I don't think so. You know, I've heard that, but I don't think so as much. I think it's helping the good guys, right? Just as much as it may be helping the bad guys. So there's a balance there from AI and look, you know what I've said, you know, throughout this whole hype cycle of AI, right? And I think it's going to settle a little bit is listen as security and privacy and risk advisors, we need to figure out a way for the healthcare organizations to continue to invest in what is going to meet their business goals. We cannot be a roadblock, or the Department of No. When we say to a leadership team, yeah, you know, you can't, you can't do this. You can't implement this tool, this technology, this platform, this application. We need to be able to say, yeah, you can do this. And we've done an assessment on it and go forth with your strategy and meet those organizational goals. So it's, that's really important that those organizations feel like they can maintain their competitiveness. And AI is at the very center of that.

**Ed Gaudet:** Yeah. Amen. Yeah. Agree. Yeah. It's like I said, it's an interesting time to be in healthcare for sure.

**Carter Groome:** Security. I mean, like, I almost feel like this could be the golden era, right? I mean, sort of. And you could point to, maybe when that started, it's kind of started a little bit where in the beginnings, but the golden era of awakening, if you will, for understanding it is an imperative, not just a regulatory requirement, but an imperative to protect your business and do right from a security perspective or privacy perspective or risk management perspective.

**Ed Gaudet:** Yeah, this stuff matters for sure. Yeah. All right. Thinking of, and I know we're going long here, but I always enjoy talking to you, we haven't even gotten even to the personal questions, although we did that in the first run of show here. But, you know, you and I share a common love for music.

**Carter Groome:** Yes.

**Ed Gaudet:** And I think, in the late 80s, early 90s, we may have crossed each other's path in a field somewhere, maybe in upstate New York or somewhere in New Jersey, we might have been dancing together. Who knows, right? Yeah. So I found out you were a Grateful Dead fan, and I was very, very happy to hear that. So let me ask you just a couple of questions because I always find this fascinating. What was it that brought you to the Dead? I remember this is a family program.

**Carter Groome:** Well, listening your story might be the same, right? It is. You know, I had thoughts when I was younger of what the scene was all about. But I had a friend, and they said, listen, hey, they're coming to RFK Stadium in D.C. and just come, you know, it's just, you know, you'll have a lot of fun and you can hang out in the parking lot and just do that. And yeah, so I sort of reluctantly agreed. And this was, I think '89, maybe '90. And I'm telling you, I had such a great time at, I had a ball. Everybody was just obviously so friendly, and it was just a, I don't know, like a culture in and of itself that I thought, wow, this is, I love this. I just love everybody's very optimistic and, you know, just loves each other and the whole, right, right? You know, all the stereotypes that you could think about, I fell in love with, right? And beneath this, you know, jacket, and it's not what we do in all the other things, I am a hippie at heart.

**Ed Gaudet:** I love that, I love that, yeah I know. You're so right. There's something so magical about a Dead show that, it's hard to explain to people that have never been there and never experienced it. And now, you know, you can obviously do it through the cover bands, the plethora of cover bands that exist. Jrad, DSO, you know, and others, right? There's a bunch of them. And then the newer bands that are coming up, Billy Strings, that have been influenced by the Dead, weather, there's this interesting crossover and fusion. And then, of course, the Dead and Company, Dead Ahead, those, those projects that continue to persist with people like John Mayer. When I tell people that John Mayer is in Dead and Company, they first go, John Mayer? What? No. Like, like, it's amazing how many people don't realize that. But even that experience, I mean, it's not the Grateful Dead. It's not Jerry. But, man, it's a close second.

**Carter Groome:** That's for sure. It was hard to deny the influence that that band had on sort of jam bands, right? And there's so many influences. There's probably bands that do stuff that don't even know that they were influenced by what they did.

**Ed Gaudet:** Yeah, yeah. And that, like you said, that sense of community, which is interesting, that we're in our professional lives. We deal in a sense of community. So I wonder, I'm just thinking, I'm thinking in real-time here. I wonder if that has to do with how many folks in healthcare are actually Deadheads. That's an interesting survey.

**Carter Groome:** ... to admit it. So I'm putting it out there in the public domain that Carter Groome.

**Ed Gaudet:** That's right, that's right. If you're listening to this podcast, get to LinkedIn. Take a picture of yourself with a Deadhead concert t-shirt and post it. Come out. Tell us you're a Deadhead.

**Carter Groome:** Come out!

**Ed Gaudet:** Does that mean you and I have to do that? We're gonna have to, all right. So here's what we'll say. If we start seeing people do that, Carter and I will do that. We will put our Dead paraphernalia on.

**Carter Groome:** Boy, watch out.

**Ed Gaudet:** My hat, my rings, t-shirt, and we will take a picture. We'll post it on LinkedIn. How does that sound?

**Carter Groome:** And then I'll make burritos in the parking lot. That's how I made my money at the Dead shows: burritos and grilled cheese sandwiches.

**Ed Gaudet:** Whoa. 2 for $20 or 3 for $20.

**Carter Groome:** ... never sleeps.

**Ed Gaudet:** Yeah, well, and if you're really interested and want to see them, they're playing at the Sphere in April, May, June, I think, or March, April, May, something like that.

**Carter Groome:** Gotta get there. That just looks like such an amazing experience. I know you have experienced that, and you've motivated me.

**Ed Gaudet:** Did I tell you I'm going to six shows?

**Carter Groome:** You did.

**Ed Gaudet:** Yeah, well, I'm gonna see you at one of those shows, I hope, maybe two. Maybe two. All right, Carter, thank you, as always, it's good to catch up with you on many important topics. This is Ed Gaudet from the Risk Never Sleeps Podcast. And if you're on the front lines protecting patient safety and 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