Podcast Transcript

Risk Never Sleeps
Episode 94
Phil Davis

Ed Gaudet: Welcome to the Risk Never Sleeps Podcast, in which we talk to the folks on the front lines delivering and protecting patient care. We get to learn about their stories, and I am pleased to be joined again, once again, by my good friend, Phil Davis. Phil is the healthcare IT, cybersecurity, and privacy attorney at Hall Render in Indianapolis. Did I get that correct?

Phil Davis: You did.

Ed Gaudet: Yeah. Awesome.

Phil Davis: Hey, how are you doing?

Ed Gaudet: Hey, Phil, good to see you, man.

Phil Davis: Thanks for having me back.

Ed Gaudet: Happy Friday. You bet. Always a good time to talk to you. And yeah, happy Friday. Any plans for the fourth?

Phil Davis: I think we're gonna find some fireworks somewhere around town. That's usually the plan. ... the dogs, stay in the house, and have a nice insulated fan noise, and home we go.

Ed Gaudet: White noise for them to calm themselves. Yeah. Yeah. Well, very good. Yeah. We're, I don't think we have any plans yet. So this is going to be, we usually are on a boat heading up to Provincetown. They have an amazing parade and set of festivities, fireworks, etc. there.

Phil Davis: I can imagine in the northeast that they have quite a fine time on the July 4th holiday. That's the birthplace of July 4th, if you will.

Ed Gaudet: That's right. Yeah. And it can get a little crazy there, for sure, with the festivities. So always a good time though. And a little slice of Americana right there in Massachusetts. I personally love going, so I don't know if we're going to make it this year, but I'm still hopeful. All right, let's get into it. Gosh, last time we spoke, I think a lot's happened, right? Change Health, Ascension Health.

Phil Davis: Yeah. There's certainly been no shortage of headlines highlighting third-party risk and business continuity and a lot of the things that we talk about a lot, right? And it just goes to show that none of this is solved yet.

Ed Gaudet: None of it's solved. And why do you think that? I have my theory, but what's your theory on that?

Phil Davis: Well, I'd love to hear your theory, but especially in healthcare, right, I think we talked about this maybe in the first, the first time I was on the show, and healthcare is so complicated and so complex in terms of the number of outside vendors and the number of advanced, really advanced technologies that are all pieced together and constructed to deliver what we call the health care service. Right? Like health care, really, if you zoom out is just a collection of vendors that a health care provider has assembled in such a way that allows its employees to provide care services. You've got medical devices, you've got software, you've got some cases, staff, outsourced staff that comes in. And with all of that just comes in an incredible amount of complexity and an incredible amount of an attack surface and risk. And health care is just so hard to guard from all angles.

Phil Davis (cont'd): And I think that's how you see just so many of these large-scale attacks happening is a lot of times it's a vendor that's getting the attack, right, the Change Healthcare situation or, you know, a potential vendor solution that you use to either secure your environment or deliver care that takes down your own internal systems. And so it's just this patchwork of advanced technologies that has a lot of capability, but also just leaves a lot of risk by definition with it in healthcare that I think creates this environment that is really just ripe to be disrupted in a negative way.

Ed Gaudet: Yeah. Great points. Is this yin and yang of good and evil that exists in everything. And so you've got this tension between I want to innovate, I want to drive innovation, I want to drive growth in my organization, I want to do the right thing for patients and outcomes, I want them to have the best experience, I want them to come back when there are issues, etc., with the challenges and risks associated with disruptive technology. And specifically, if you look back a decade or so ago, this wasn't that big of an issue because most of that technology was contained and constrained within the four walls of the health system.

Phil Davis: You didn't have the remote, you didn't have the work from home, windows that needed to be opened up, the remote access, right? You can access your internal resources from anywhere. Well, is that a good idea? In a lot of cases, maybe not. But you're right, ten years ago, when I was a CISO in an organization, ten years ago, we couldn't get to our email without the VPN on. Right?

Ed Gaudet: Right, right.

Phil Davis: That concept is gone. You can, everything's in the cloud and widely accessible.

Ed Gaudet: In the notion of applications in the way that they're developed, it used to be this, you'd have this monolithic on-premise application that did the majority of the things you needed, and now it's distributed across several SaaS applications. So you get this sense of microservices and micro business processes now that are being driven through automation and technology, which in the past didn't really exist.

Ed Gaudet (cont'd): And so this notion of things that we used a decade ago to manage risks like certificates like, tend to be outdated insomuch as things change so often, you need to take much more of a continuous and more dynamic approach to monitoring risk. And I think that adds to the complexity, obviously, because.

Phil Davis: Absolutely. And you can't throw out the threat actors, right? They have certainly advanced their tactics. And obviously, the advent of ransomware in that concept of creating the most amount of destruction possible in the target environment really makes things difficult in the health care setting, because our bar in health care is so high in terms of what we're willing to withstand in order to still provide care, and it just makes that pain point so much higher. And so when you reach that level, when an attacker has gotten into that, to that degree, you now have a whole lot of pain that, that you're having to withstand because your bar was so high, right? We're critical infrastructure service. We're a service that society needs to have performed. And all of that comes together to create that perfect storm.

Ed Gaudet: Yeah, exactly. And so as we receive technology and innovation to do things better, faster, cheaper, etc., they also get the benefit of technology. And they're leveraging technology, obviously, for the wrong reasons. And also the fact that they can hide now, dark web, the ability to basically disappear, and be anonymous, also drives to that level of complexity from not only managing the attacks, but catching the attackers. And then lastly, they become much more organized. So they've realized that they could also create these microservices, if you will, for things like ransomware, where, you know, one person or entity goes and collects the money while another one does the attack while another one communicates, etc. so.

Phil Davis: I continue to be amazed at. So now, having been in the cybersecurity kind of attorney role and dealing with ransomware incident response and the negotiations that you have with these attackers, I continue to be amazed at the level of customer service and sophistication of some of their operations. Right? They have literal teams in the same way that a healthcare system might have teams of, you got supply chain people, you've got purchasing, you've got sales people, you've got, they've stood up a lot of that same infrastructure and have processes even, and standards built up about what we're willing to offer and what we're not going to offer.

Phil Davis (cont'd): And it's just, the world has evolved so much, which is where we started with this conversation just to, it's gone where the incentive is, unfortunately. Right?

Ed Gaudet: Yeah, it always goes where the money is.

Phil Davis: As long as people are paying ransoms, that's a never ending debate. But as long as people are paying and there's a revenue stream for those nefarious individuals, unfortunately, I think that's what you're going to continue to see.

Ed Gaudet: Yeah, it's the old Willie Sutton adage, I rob banks, because that's where the money is.

Phil Davis: It's where the money is. Exactly.

Ed Gaudet: Oh, well, I think we hammered that topic. So let's talk about.

Phil Davis: Let's talk about how to manage some of this.

Ed Gaudet: Yeah. Let's talk about how to manage it, and then we'll get into some new technology. So White House administration's been doing a lot, been very active in this area; driving regulations, accelerating the rulemaking process when it comes to the cybersecurity performance goals. What's the latest update from your perspective there?

Phil Davis: Yeah, I think so, actually, when you bring that up, was actually in DC within the last month or so and got to meet with Representative Bhushan, who's from here in Indiana. And this was in the heat of the Change Healthcare hearings and all of the various revenue impacts that the government was having to step in and help with. So obviously, this came up, right? And I think the feedback that we're getting from the Hill is that there is a lot of appetite for creating increased standards, let's say, for minimum cybersecurity requirements. Now, that could look a lot of different ways, right? Whether it's a carrot or it's a stick, I think, is still up in the air.

Phil Davis (cont'd): You continue to think that there is a lot of value in creating some sort of a meaningful use type of incentive for where you can demonstrate that you have multifactor authentication in place, you know, for remote access or critical application access, whatever that standard you know, we can agree to set is, if we can set some sort of meaningful use like incentive program to where you get either dollars back, or maybe that's dollars for setting up that technology on the front end versus, you know, the HIPAA model of, well, you get punished if you don't have.

Ed Gaudet: Yeah. And they have the ONC, which is really good at the sort of certification process, obviously, through meaningful use, have them administer that as well.

Phil Davis: I think there is some appetite for that. The feedback that we got is that's very expensive and I, certainly, am understanding that. But I think there's a critical mass of incidents that really have driven the conversation there in terms of, Okay, how do we as an industry and government plays a role certainly? How do we all collectively, as an industry, come up with an acceptable method of ensuring that our healthcare data is minimally protected by certain technologies. I like all the cyber performance goals. I like pick up the standards that that 4 or 5 D group is coming out with. I think these are all really great, really great ways to get that conversation going to to collectively decide what those standards are. Because at the end of the day, we do need to decide what the technologies need to be and how they should be implemented, the economics behind that.

Ed Gaudet: Yeah, and the economics behind that too, because as you stated, it can be very expensive for these smaller rural critical access hospitals to meet that, meet those standards, given that every dollar is, they manage like manhole covers. Right? So.

Phil Davis: It's so true. We've seen a little bit of drippings from that. Right? I think there was a $50 million fund that was announced for rural health care entities to invest in improved cybersecurity. That's obviously maybe a little bit of a drop in the bucket, but it could be a good test case on how do we distribute these dollars and what's the audit and compliance angle that needs to be there to ensure that those dollars are being used appropriately, right?

Phil Davis (cont'd): I think that's hopefully test case of how we could step in to start helping rural facilities. Because you're right, those are the facilities that probably have the most roadblocks to getting these things in place.

Ed Gaudet: Yeah. And be deliberate and purposeful on how we help them achieve those essential and ultimate enhanced cybersecurity performance goals. Because again, if we, and then also that's only half of the problem, right? The other half exists outside of the four walls. It's the third parties. And right now the third parties even, aren't even brought into that conversation. What's your thinking on that? What do you think we need to do there?

Phil Davis: I'm encouraged, I think, by the cyber performance goals, and I think there's been some, kind of some breadcrumbs dropped in some of these announcements by HHS that those standards are eventually going to make their way into being the new security rule under HIPAA, the technologies that undergird the updated security rule. And I think what that would do is bring in the business associates, right, the vendors to covered entity health care providers because they're subject to the HIPAA security rule the same way that providers are. So I think if they can develop those standards into, obviously, it's hard to scale that, right, to all entities throughout the nation. But I think that work has started, and I think that kind of evolution of the security rule will help get the industry as a whole that's holding protected health information to include covered entities and business associates. I think that would go a long way to creating that incentive program. That obviously exists within the HIPAA infrastructure. And so you have a little bit more stick there than carrot.

Ed Gaudet: In a mechanism that's already in place that you can just append to.

Phil Davis: Exactly. But I think that the writing's on the wall, though, that we are going to get updated security rule technology standards, and it's going to be less what I've talked about in the past, where it's a nebulous requirement that you're left to determine what works for you, and it's going to be a little bit more prescriptive from a technology perspective.

Ed Gaudet: That's great. In your role, you get visibility into a number of health systems and what they're doing and what their priorities are. What are you seeing in terms of patterns of priority over the next 12 months for health systems?

Phil Davis: In terms of kind of this third-party risk, there's been a concerted, I want to say, refocus on the third-party risk policies and procedures and what customers in the health, so the covered entities whose PHI, that all of this data is belongs to the customers here, what they're willing to accept in contractual settings and creating some of their own standards about, Hey, we're going to require that a vendor has at least this minimum level of technical control in place, and we're going to need them to commit to that in a security addendum or something like that. So that's on the one side of things, the contractual side. But there's also very real process improvements that are happening on the third-party risk side. And I've had conversations with clients recently, several conversations, on the theme of well, let's really think about why do we have a third-party risk program? Why do we do that? Because after Change Healthcare, they obviously had massive operational impact because of a vendor's event. I think that makes you question, Why am I doing these third-party risk assessments if I can't prevent an attack in my vendor's environment? Right?

Ed Gaudet: Right. I'm curious to hear what they said because again, I have my own thoughts on this topic.

Phil Davis: Yeah, every organization I think approaches that a little bit differently. There's several buckets, I think, of incentives and goals of the third-party risk program. At the top of the list generally is we're required to do risk assessments by, you know, HIPAA, for example; you have to assess your risk. And our patients and our customers expect that of us, the regulators expect that of us. They expect us to do appropriate due diligence when we're engaging. And so it's a little bit of a standard of care; that gets you in the door. Right? But then I think that there's other benefits of doing that outside of I'm trying to prevent all cyber attacks in my vendors. I don't think that's a reasonable goal of your traditional risk assessment process sort of going in and taking over their SoC or putting your equipment in their environment, which is probably not going to fly with most vendors. But sort of that. I think your risk assessment process can uncover certain things that you can then handle in a contractual negotiation. Right?

Phil Davis (cont'd): You can say we found a certain number of red flags, if you will, in our risk assessment. So we want to have some contractual coverage, whether that be remuneration from a business impact standpoint. It gives you more leverage to have those conversations under the data. So that's a still a real benefit of the third-party risk process. And I still continue to think that the rising tide has lifted all boats in the industry.

Ed Gaudet: That's a great point. That obligation that a vendor takes on also is going to make them better for the next customer that they work with, because their program will have matured based on the feedback of the prior.

Phil Davis: I tend to think that all vendors in the healthcare space now are very used to getting these questionnaires, or at least some manner of third-party risk assessment vetting. And that's caused the vendor community to collectively ensure that they have answers to those questions when they get them. And I think that has, is that rising tide from a security perspective that has helped bolster the industry. So I think there's a little bit of a kind of communal benefit that we're all doing these cyber assessments more than just, hey, it helps our own organization meet our requirements. It also helps the community as a whole lift its level of practice.

Ed Gaudet: Yeah, yeah, that's a great point. I think on the Change Health side of the world, it was the question about: We did all this work; how come we didn't see it, how come we couldn't prevent it? Because it was different than every other type of assumed attack or threat that you were dealing with. And I think the learning, I talked to several health systems during the time of the attack, and I kept hearing this repeatedly: we had no, the biggest learning is we were surprised. We had no idea the level of concentration that Change had within our organization for a critical business process. And the fact that the other thing you're exposed is the amount of cash on hand these health systems had to be able to weather that storm of that event. So I think that was a wake-up call for organizations to start to look at that concentration and develop business continuity and disaster recovery plans that include alternatives. So if I do have that concentration for the right reasons, efficiencies, or the wrong reasons, it happened to me because they acquired a bunch of customers and companies and I lost sight of that, right?

Ed Gaudet (cont'd): I always thought it was distributed, and then I blink and it's not; it's all coming through one organization, which is now part of a larger organization, or two steps removed from where I thought it was. So I think that, again, goes to the dynamism of this problem and the complexity of this problem.

Phil Davis: Yeah, I agree with that. And I don't think organizations should be too hard on themselves or their teams for necessarily missing that one. Right? I think the Change scenario was such a, it was so unique in that to what you just mentioned. I think that they amassed such control under the radar a little bit, right? I don't know that your regular health system really realized that was such a single point of failure in the whole system. Because it's not like they necessarily signed some contract to be exclusive for all of their claims processing. Generally, they thought that they had many different organizations that these things were routing through, but turns out with acquisitions and things they didn't. And so every now and then you get an event like that that shakes the whole industry. And it's not necessarily something that someone missed necessarily. And I think this is where the federal government can step in a lot of time and help provide some guardrails and some controls around that concentration of power. But all that to say, when you're going through your business continuity plans, I think that highlights a lot of that expanded business scope that we've been talking about on the IT and security community for years, that this is much more than an IT problem. You're talking about going into days cash on hand, right? How many business continuity tabletops up to that point had considered what's our cash on hand, right? And so you learn things as you go through these events; certainly. And it's not necessarily about, Hey, we miss this. We have something wrong. It's about, Let's take the right lesson from this and also then try and extrapolate a little bit and take the next step down the line of where else do we have single points of failure like this? I think a lot of organizations have a single point of failure with their supply chain purchasing, right? They'll have one durable goods heart that hardware equipment suppliers medical supply supplier that they buy the vast majority of their medical equipment through things like syringes and gloves and gowns and things like that. What are their backup processes there? Going down the line and saying, How can we take this concept that we now?

Ed Gaudet: Laundry service. If I have one laundry service that can handle my health system because of the size and that gets hit, what happens because I can't operate a hospital without lunch?

Phil Davis: Yeah, exactly. One exercise that we've recommended organizations go through is take, literally take your purchasing department should be able to pull you a list of your spend, right, with vendors, sort it by dollars. That gives you a very critical list of vendors at the top of that list, where you can think through, Okay, if they go down, what's my backup vendor? What's my, maybe 2 or 3 other vendors that I can reach out to make up if something happens with these top $5 amount spent types of vendors? And so recommended that as a piece of your business continuity planning to just get some other ideas of where this may come up and bite you and how to be a little bit more prepared for it.

Ed Gaudet: I love that. That's great advice to listeners too. So hopefully, a lot of folks are listening to this podcast in particular. Let's switch. Let's talk about AI, my favorite topic. I'm sure yours too. So what are you seeing from a governance pattern, from an adoption pattern. How are your customers or folks that you talk to thinking about AI or actually implementing some type of cybersecurity program or governance around AI.

Phil Davis: Yeah. So let me start with the governance piece. I think generally most organizations have started at least, if they haven't published one, they've started drafting their AI governance policy. And some of the decisions you have to make when you're going through that is do I block certain AI tools, like kind of the public? Do I block those or do I allow them and just communicate training out to my organization? You don't put sensitive data in here, or do you want to take maybe the more restrictive approach and block them, whitelist them if there's a business case, things like that. Those are the types of kind of practical decisions that I think organizations are fighting through in those governance policies. Obviously, you need to have solid data governance, data classification, procedure in order to pull this off, right? Because all of this is about what kind of data are you comfortable with your thousands of employees putting into these tools. And so if you have data classification already to a point where you can classify your data, it makes that much easier, right?

Phil Davis (cont'd): You can say no classified, no private data; only public, right? For example, so that's another kind of trend area. There's various degrees of maturity regarding data classification because it's a very hard, admittedly a very difficult concept to operationalize. And it takes a long time.

Ed Gaudet: It doesn't, I don't think it takes a long time from a strategic framework perspective. It's the going and finding and then labeling the data that's more difficult. So it's more, it's like, you can set the framework to say data that looks like this is classified this way. And so you use your best judgment initially. But then if we want to automate it and really drive the inspection of it, that's the hard part I think.

Phil Davis: Absolutely. It's the communication to your organization that, Hey, we have this new scheme of data classification. And here's the examples, and here's how, you know, when you're looking at a piece of data or a document what to do with it based on this, right? And there's, there are, you're right, technologies that can help you crawl your file shares and your office 365 environment and automatically apply. And that's, obviously, probably the preferable way to go. But that's not cheap. And there's a runway there in terms of deploying tools like that, but it does certainly have a tie-in to this AI conversation, I think, was the original point. But in terms of how organizations are implementing AI, there's, obviously, it's a lot of vendor-driven product conversations in terms of, Hey, this tool we've already been using now has an AI component, maybe it's EMR, maybe it's the dictation platform, right? These vendors that you already have in place now has this AI capability. All right; well, let's perform this new risk analysis and risk assessment on this new functionality and see maybe if we can deploy it in a limited set to start testing it out. Seeing a lot of that. There's a lot of contract issues that take place when you're purchasing these AI tools like data training and data ownership. And that's from the legal side of things, how we get into the weeds and in the AI conversations. But I think vendors understand a lot of these risks and have been willing to work through a lot of the organization's concerns in terms of if I put data into your platform, we have a VA in place and we know you're required to protect that data, but AI's got a mind of its own, right? In today's day and age, how do we ensure that data is not going to be churned out to somebody else, right, who's not able to see it. So those are a lot of the conversations.

Ed Gaudet: And do you think this is a problem? And if so, how do health systems manage this as it relates to legacy vendors and products that you're working with and then bringing in AI capabilities through updates or patches and maybe not being as visible to the organization that's occurred? Have you seen that and have you seen policies or governance associated to to manage for that?

Phil Davis: Yeah, that's a great point because I think that does happen, right? In a SaaS, an environment where you're receiving an update automatically, and now there's, Oh, whoops, there's a new generative AI tab.

Ed Gaudet: Adobe did it recently with PDF and it was nefarious the way they managed it. I couldn't believe it. They kept throwing up the banner. They wouldn't allow you to say no, and then eventually they just accepted it in the application directly, which I thought, which is. So I think as we think about government regulations, these things need to be considered too, because vendors should not be doing this.

Phil Davis: Yeah, I agree. When I was a CISO, there was a number of situations where it was like someone a call to the help desk really who was the flag? That new SaaS tool. I have this button. What does it do? Or something like that. Right, Ed? Alert you to, okay, well there's an a change that happened over the air without me being able to vet it, press the button to go live. And I think there's some vendor relationship management kinds of things that need to take place there.

Ed Gaudet: Certainly that's a.

Phil Davis: If you're in the contracting phase, grip in a little bit of that. But to your point, these are vendors that have been in place for ten years.

Ed Gaudet: Yeah. But to renewals, you get renewals that are coming up. So as you take an opportunity to renew, make sure that you're building that language into the contract, right? If you're doing reassessments, make sure you're asking the question, right? How do you manage that? Or have you already done it to us and we just don't know about it?

Phil Davis: And your lawyers, I'm sure, can go back at the contract and probably find some ways that's already addressed in the documents that you have, maybe as confidential information or things like that. But the point that you're talking to a lawyer about it, right? Something's already happened. Right? So I think there's a little bit more proactive actions that organizations can do just in their regular roundings with their vendors and ensuring that they know what's coming up, that they know how the system deploys updates and they make it known that we have certain standards here. Will you work with us? And generally, vendors are cooperative at that stage, right? Once we're talking to all the lawyers to look at the contracts, things are generally gone a little bit sour.

Ed Gaudet: Yeah, this is great. I have a couple more questions for you. I love you to put your attorney hat on for a second. Are you seeing a rise in these class action suits related to data breaches?

Phil Davis: Yes, I think that's an unequivocal yes. It's it seems like there's a certain section of the plaintiff's bar that just watches for headlines and then starts drafting. It gets in word right away and copies their last class action suit and paste it into a new document, find and replace the organization names. It's funny, to be honest, we have seen several initial complaints for data breach cases that have mentioned other hospitals and other health systems that are not associated with the instant case, it just indicates that there's a very quick trigger finger right now on data breach headlines. It almost will automatically, to a certain degree now triggers a suit. And you'll get three, 4, or 5 of them right out of the gate. And it just, it's a shame in 1-in-1 respect because the cases are not obviously very informed at that point. There's incorrect information in the complaint, and it just, it creates a real overhead burden of now having to go fight that from the organization's perspective to say, Paragraphs nine through 15 are factually incorrect. And then you have to argue about that and do motion play. So from, just from the litigation cost perspective, it certainly can be significant. We've seen a lot of insurance influence in terms of how those cases may, obviously, the settlement conversations are generally insurance has a role to play there. But to answer your question, I think when you do announce your regular data breach as the result of a malicious attacker, we are seeing almost an immediate filing of a handful of cases.

Ed Gaudet: And what's in it for the plaintiff? Like, how much are these individuals getting on in some of these cases?

Phil Davis: To be honest, it's a little bit to be determined, right? Because I think a lot of these suits, their challenge is have you stated sufficient damages in your claim, right? Have you as the plaintiff, have you been able to demonstrate that you were harmed? And in a lot of those instances, they may get nothing. They may get the suit thrown out. And we've seen certainly a lot of cases where that's happened where after a year of litigation and motion practice and discovery back and forth, it gets thrown out and they get nothing.

Ed Gaudet: And of course, the lawyers always end up getting more, right?

Phil Davis: And that's the truth. Right? And I think that's why you see a lot of the plaintiff's bar jumping at these opportunities is because they may get a class of 200,000 people. Everybody gets, you know, $4.38. But attorneys that are working the case, they get 33% or 40%, whatever the thing is. And so I think there's a lot of incentive right now with those settlements that do happen before they ever get to a trial. If you're getting a settlement, I think that's always the goal with these plaintiff suits is to get a settlement and then to take a cut of it, and it's just the incentive structure that's been built up around these data breaches.

Ed Gaudet: And there are some states that are obviously trying to thwart this with their own efforts. There's the Senate Bill 2018, 20818, that is also trying to prevent these class action suits without lawful or gross negligence, which I think is good. Should we have a national amnesty program or immunity program for folks that are doing the right thing by actually reporting the breaches, but then are getting, obviously, getting challenged with the effort to respond to these class actions?

Phil Davis: Yeah, I think that's interesting. I think it gets back to that initial conversation I think, that we had about what are the minimum, what's the minimum standard of care that you should employ as a health care organization from a security perspective?

Phil Davis (cont'd): And if you're doing those things, if you're doing what we as an industry have said is the minimum, should you be held accountable, right, for something that happens while you were doing what you were supposed to do? And I don't know that we could get there necessarily from the national legislative standard states, you know, may be able to carve some things into their data breach laws or consumer data privacy laws, but these cases are generally very creative about how they use state laws to leave their claims in the court. Right? These are generally, they're not citing HIPAA other than as the duty that was their, right? Because HIPAA does not have the private cause of action part. So these are generally state laws, claims that are being asserted. And 3 or 4 of them will get thrown out. But every now and then you'll have one that may stick, right, in a certain circumstance.

Ed Gaudet: Yeah. And the dirty little secret is there's a single click fragility, the whole house of cards, right? It only takes one user to click on that link, right? You could do all the training in the world, you'd be doing all the right things. And that attack, that phishing attack is so well done. At that moment in time, that click happens and then everything comes tumbling down.

Phil Davis: Yeah, absolutely. And this is something that I try to think through, obviously, when I was in the CISO role and still trying to help clients walk through is, there is that one click, but generally there are 3 or 4 layers behind that click, right, that may have failed or may have, you know, weren't just, weren't in place, right? Things like URL filtering or all the various kinds of technologies that you can put in place to anticipate that someone's going to click. There's probably a patch that's missing somewhere along that chain that allows that in the background executable to happen, right? It's that click, but there's so much behind it: your patching program, your, the various firewalling technologies that you have. I mentioned URL filtering, right? There's so many layers that you can think through in terms of I know someone's going to click; What can I do to prevent that click from having the impact? And it goes all the way down to data segmentation and the blast radius and things like that, right? It just gets so deep and that's that health care and really any modern enterprise environment problem of one little thing can trigger and be associated with 15 other actions and systems. And so understanding your entire attack surface is really difficult thing to do, but something that I think is a key part of a security program.

Ed Gaudet: Yeah. Managing this healthy level of paranoia about everything.

Phil Davis: You don't have to worry about that. And the security community, I don't think.

Ed Gaudet: Oh, no, but just outside of it, I think it's transitioned to and transcended to the house, right, to the home. And we come home and we take a deep sigh of relief that it didn't happen on our watch. But then we come home and it's still happening, right? Your kids and your parents and spouses that may or may not have that maturity of cyber that we have. And then you're dealing with it during your off hours, if that even exists. I don't think it exists actually in the cyber world, does it? Notion of off hours I used to always tell people. Keep your phone next to your bed. It's 24 over seven. It's health care; risk never sleeps.

Phil Davis: Risk never sleeps. It's the name of the show and it's the name of the game I think, too a lot of us in in the arena.

Ed Gaudet: That's right. Well, Phil, as always, thank you for your time. A pleasure to catch up and talk to you. Wish you the best on the 4th of July weekend and we will talk soon. This is Ed Gaudet from the Risk Never Sleeps Podcast. If you are on the front lines delivering patient care and protecting patient safety, remember to stay vigilant because they're out there, Phil; those hackers are out there. 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