#190 - Lawyers, Breaches, and CISOs (with Thomas Ritter)

[00:00:00]

[00:00:12] **G Mark Hardy:** Hello, and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy. I'm your host for today, and we're going to have a little bit of fun by getting into some legal stuff.

Specifically, we're going to go over a range of topics relative to CISO, such as regulatory compliance, Until Managing third party risk, responding to data breaches, and the impact of things like MOUSC and all the other legislation and regulations that are coming out. But we want to provide some practical advice and some real world examples.

So our special guest today is Mr. Thomas Ritter, a renowned lawyer specializing in cybersecurity. And Thomas has worked with numerous organizations to help them navigate the complex legal landscape of [00:01:00] cybersecurity. Thomas, welcome to the show.

[00:01:03] **Thomas Ritter:** Thanks, G Mark. Excited to be here. Looking forward to our discussion today.

[00:01:06] **G Mark Hardy:** I am too. I mean, another buddy of mine, Mark Rasch, who was an attorney who was on our show a while ago and Mark and I spoke at the same event for years. And we're the type of guys that we get going. I think his record on a slide is never getting past slide two. I mean, he just went off in his own little direction.

So we're going to see how this one goes. But anyway, tell us a little bit about your background. How did you end up getting into cybersecurity law, which seems like a pretty specialized function. And, and again, it's a pretty neat opportunity.

[00:01:37] **Thomas Ritter:** Yeah, absolutely. So my journey in cybersecurity really started back in law school. I was in my third and last year of law school, and I actually took an elective, that was titled something like Big Data and the Law. It was taught by a renowned antitrust attorney who, had written

extensively about, [00:02:00] Big data and its implications, and continues to do so today.

And, I like to, also laugh over the fact that I was one of three people in that class. I've always been someone that kind of marches to the beat of my own drum. And I remember thinking at the time, this course may end up being either a complete waste of time or I might be on to something. So, I was really fascinated by a lot of what we discussed and, coming out of my law school experience, I actually started as a regulatory attorney, which segued rather nicely into, me then going and working as a full time, privacy and security attorney for a couple of different big law firms.

and then fast forward to. This year, and I actually left, a big firm and started my own boutique law firm, with one other individual here in [00:03:00] Nashville, Tennessee. And we are just solely dedicated to assisting clients with their cybersecurity and privacy needs. And as part of that, we're often working alongside CISOs and trying to find ways to help them with any of the challenges that they confront on the day to day basis.

[00:03:17] **G Mark Hardy:** Well, that's great. And welcome to the world of entrepreneurship. It's a lot of fun, a little bit scary, but it's something that I have done over the years, and I found that. At the end of the day, it's as much there as you're willing to work for, and yet, of course, you got to keep banging at it. So I think you're into a hot area and I think it's wonderful and, hopefully be able to provide some really good advice for folks.

But so as we look at cybersecurity in general, it's a hot topic. It's worked its way up to the board level over the next couple of years. We as CISOs and security practitioners, well, we've been doing it a long time, so we're kind of used to it. But from your perspective, what are some of the biggest legal challenges that CISOs are facing today?

[00:03:54] **Thomas Ritter:** Sure. Yeah. I think for starters, it's just. Constantly keeping up [00:04:00] with the ever evolving regulatory landscape. if you think about just in the last 12 to 24 months, you've had, you know, amendments to things like New York department of financial services, cybersecurity regulations take place. You've had the SEC amend their cybersecurity regulations.

you know, state breach notification laws are always being amended. And so. in all honesty and candor, a big part of my job is spending, I mean, at a minimum, probably an hour a day, just keeping up with all of this. Right. And so huge lift

and ask to have CISOs try to adhere to that responsibility. And, at the risk of sounding self serving, that's where lawyers come into play.

Right. and so I think that's a big one. Another one for me. Is really just managing third party risks. I'm hearing that from CISOs a lot. [00:05:00] you know, especially with the increase in outsourcing and, cloud services that, are part of day to day business ops and, you know, a microcosm of, you know, of third party risk is really this year, right?

If you look at some of the largest security incidents, thus far in 2024, they've emanated from third party providers like Change Healthcare, ConnectWise, Snowflake, we could go on and on. So ensuring that third party vendors adhere to the same cybersecurity standards can really be complex and, honestly should involve assistance from legal counsel.

[00:05:39] **G Mark Hardy:** Yeah, that third party risk is a particular troublesome because a lot of times you find out that it's outside of your control as a CISO. You don't control your third parties. And so as a result, we often depend upon policies for doing that. And I'm working with one of my clients where they have a large manufacturer who's kind of dinged [00:06:00] us in terms of going through their security assessment of the organization saying, well, you don't have a third party risk policy that goes down to the fourth, fifth, and nth party.

And I'm thinking, well, as a consulting firm, you can't, and it can't be very big unless you get ridiculous. Okay. Well, I got Microsoft and I'm like on a Dell computer. Well, then who manufactures the board for Dell is that's kind of out of scope. who is writing code for Microsoft or provide, you know, that's a little out of scope, but I can see if you're a manufacturer, you're making an, let's say an aircraft, and then you have to have engine assemblies of which you're going to have other component assemblies of which you're going to have parts, which, and, that could be four, five, six, seven, eight, and then like that.

So depending upon what industry you're in may determine the depth of that third party concern, but how would one effectively assess the correct depth? As a CISO, is that a call that the CISO should be [00:07:00] making? Is that something that the legal would make? manufacturing? Who, gets to say, yeah, here's how deep third party is?

[00:07:07] **Thomas Ritter:** Yeah, that's a great question. I think. In my opinion, it should be, legal in tandem with CISOs, right? And, you know, from a foundational perspective, Even just knowing, you know, numerous degrees of

depth is a great starting point. you know, I think the first and second and third degrees should, at a bare minimum, probably be the baseline standard when you're thinking about, you know, what's reasonable, right?

with respect to legal liability. but, you know, I also think Whether you meant to or not, you raise a great point too. Then when you're thinking about due diligence with third party risk, and you know, assessing third party vendors, cybersecurity practices, and, you know, if they've had a history of security [00:08:00] incidents, often a difficult thing to do because right, you as a customer and a client of that vendor may not be in a position to.

Negotiate or really, have much leverage in, in looking into those sorts of things. So it's very much a push and pull. it can be tenuous at times, but from an overarching perspective, I think just even demonstrating that you have a TPRM program, you have, you know, policies and procedures within that program and, you, that you have a vendor management program is a, great starting point and really trying to reduce the risk of future and subsequent legal liability.

[00:08:45] **G Mark Hardy:** That's a good point. And for those who haven't, know, TPRM, I'm the third party risk management. I always like to define acronyms as we go by. Most of us know that, but I'm just adding that for our show. But also you talk about vendor management program and the vendor management program typically is not managed [00:09:00] by the CISO.

It's managed by whomever's dealing with the vendors. So that suggests that somebody either needs to be in a lead and a support role and somebody else has to go ahead and decide How does that work out? One of the dangers I think takes place is that a lot of times we're asked from a third party, Hey, assess your security.

How are you? Oh yeah, we're good. check, check, check all the boxes and then done. And that self assessment is kind of what got things like the defense industrial base in trouble and why we're doing CMMC because a lot of companies were attesting, self attesting that they did stuff. Did I run my 10 miles today?

Anybody double checking? Nope, then yes I did. And from that perspective, we find out that breaches were occurring and things are going sideways and then it goes wrong. So if you want to go ahead and prove that your vendor management program does have enough due diligence to ensure that it's defensible, again is The other kind of the saying goes, anybody can be sued over anything, whether it'll be [00:10:00] successful or not is another, item, but in

general, barring nuisance suits and things such as that, we're really concerned about where someone is actually at risk from being vulnerable to a suit.

And so what would you do for a recommend for a vendor management program? With respect to due diligence, to be able to point to it and say, yeah, well, they kind of really were doing their job and this was out of scope.

[00:10:22] **Thomas Ritter:** Yeah, it's a great question. I think, in my experience of working alongside, large organizations that have, strong vendor management programs that exercise due diligence. There's a real simpatico between the folks in the procurement office, maybe general counsel and or external counsel. And then, the security professionals, right.

And security personnels, CISO being maybe at the top of that list and, you know, really wanting to, [00:11:00] Contractually sure some things up. you know, having everyone be on the same page with respect to the kind of security representations that maybe we as a client are expecting this vendor to make or even vice versa, right?

and, you know, I oftentimes. I just commonly see clients have a misunderstanding over things like, you know, when they're supposed to be notified of a vendor having a security incident, what the definition even is of a security incident, or maybe a breach, as I think we're going to Plan on maybe discussing a little bit later and the implications of defining something as a breach and so on and so forth.

So I think that's kind of my long winded way of saying, you know, it's great. If you can do things like conduct periodic reviews and assessments of a vendor, or even [00:12:00] ask a vendor to engage in something like an external audit. But as already mentioned, that may not be possible, right. When you're working.

with or, at the behest of like a Microsoft of the world. so I think, you know, at a minimum, having an understanding of, what's in the contract and trying to have everyone be on the same page about contractual expectations, should be at foremost a priority.

[00:12:28] **G Mark Hardy:** Let's, and you raise a good point because a lot of times people think, oh, we got legal requirements. Well, there's more than just the law. There's also, of course, statutory and regulatory and then there's contractual agreements. And then there's also things in the industry, for example, PCI, Payment Card Industry Data Security Standard.

It's not a legal, requirement. It's not a law, rather it is a business requirement that is set up for organizations that are going to process credit cards that they say, Hey, we'll agree that I will meet these principles and be able to be validated at that in exchange for the ability to [00:13:00] process credit cards.

So if we look though, at the legal and statutory obligations that are out there, as you had said at the beginning of the show, there is a number of them, potentially a patchwork at the state level. international level as well, but in general, what should CISOs be thinking about when they think about legal or statutory obligations?

[00:13:18] **Thomas Ritter:** Wow. Yeah, that's, that's a big question. you know, as you noted, the United States, I think, you know, Is a good starting point in that, you know, unfortunately, I think, to the detriment of businesses and organizational leaders, there's really no uniform framework, right? So, you astutely pointed out, it is very much a patchwork system, and it follows, you know, what's commonly referred to as a sectorial approach.

Right. and so. You are obligated to follow industry specific laws like HIPAA for healthcare entities or Gramm Leach Bliley for [00:14:00] financial institutions. And then you have the state specific ones too. you know, using the example of a statutory obligation or requirement that is oftentimes missed by businesses is, one actually that's based out of Massachusetts and that's their data security regulation.

I think it's pretty unique. it requires that any organization that possesses information on Massachusetts residents. must adopt a comprehensive written information security program or WISP. you know, NYDFS cybersecurity regulation, for entities that conduct or do business in New York. Also feature, you know, well enumerated security requirements.

and then, you know, as you pointed out, oftentimes, you know, business leaders and CISOs are kind of, you know, Left in the wind, so to speak on, you know, what are best [00:15:00] practices? you know, right now an ongoing debate in lieu of, you know, change and Ascension and some of the large healthcare breaches is the, omittance of the fact that there are no baseline security standards for HIPAA.

And so, there's a lot of talk and. Washington and under the Biden administration of, establishing baseline security standards, the American Hospital Association is pushing back on that. but it leaves people like CISOs in a tough spot if, you know, you're having to decide and oftentimes organizational leadership at the C

suite level is expecting you to decide, you know, what the right standard is, or, That you have implemented security controls that would quote unquote constitute reasonable security measures.

[00:15:54] **G Mark Hardy:** But you brought up something I kind of want to go and probe at this real quickly. So Supreme Court Chevron [00:16:00] recently and saying, hey, after about 40 years of the agencies essentially fill in the blanks for what we interpret a relatively vague or incomplete law. that appears to be a little bit, at risk now in terms of the Supreme Court saying, no, you don't get to do that.

Now, there's two sides of that I see it, and I'm looking for an expert opinion. One side of it says, hey, agencies can't just invent new ideas that are say, well, hey, nobody said we can't, so we're going to make you do that. And then the other side is a little bit of saying, hey, let's go ahead and try to make Congress do its job and be very little bit more specific.

And in the absence of that. they're going to probably get a lot of feedback saying, Hey, we ought to be doing something about it. Now, somewhere in between those extremes, there's probably a reasonable, medium. So what's your read on this, recent ruling from the Supreme Court with regard to Chevron, if you had a chance to look at it and what's the implication then in cybersecurity?

[00:16:51] **Thomas Ritter:** Yeah, I have had a chance to look at it and I've had quite a few conversations amongst, you know, peers within the legal [00:17:00] industry. And it seems as if you not unanimously, everyone is rather shocked by it, right? That the Supreme Court has reversed. a doctrine that's been in place for over 40 years.

you know, as far as where that leaves things, more questions than answers. you know, when you think about the implications of cybersecurity regulations. It's wide ranging. you know, I've already mentioned that the SEC has recently amended their cybersecurity regs. you know, you have the Federal Trade Commission that's kind of seen as the de facto agency for privacy and security that has, you know, regulations that typically are viewed through the lenses of, you know, industry standards and best practices and, With, you know, the Lopez Enterprise Bright v. Raimondo case, or Lopez case, [00:18:00] that was decided at the end of June, all of that has been called into question on future authority for regulatory agencies like the ones I mentioned, SEC, FTC. And so on and so forth to really promulgate rules and then more importantly enforce those rules. And so I've told clients by no means should it be viewed, as, you know, we suddenly should ignore these rules.

I think if anything, it'll probably be a slow and steady drip and that you'll see, you know, someone like Tim Brown, right? The, SolarWinds CISO who's currently being, by the SEC. I would venture to say that his attorneys, if they haven't already, are writing You know, a pleading that is saying, Hey, whoa, SEC, you need to pump the brakes.

but [00:19:00] I think for CISOs, for organizations, this isn't a reason to just suddenly put your head in the sand and not follow, agency rulemaking. I think you, you absolutely should. It's just. It'll be interesting to note that in the coming years, I would expect quite a few, organizations that are the subject of enforcement actions.

To push back against, what it is those agencies are trying to make them do. And the basis of that pushback is, going to be, you know, the dismissal of the Chevron doctrine or,

[00:19:39] **G Mark Hardy:** Yeah. So it's, not a get out of jail free. So CISOs can't look at that because obviously it's not the point, but it does suggest though, that it may be refocusing on things. But one of the important things. I think CISO should be aware of and should focus on is the concept of liability. And so what is the legal definition of liability, without getting too far into detail?

You know, maybe law school [00:20:00] 101 would be good enough for this. And then what's the basis for that? And how is that influencing companies? And what should we really be thinking about from that perspective?

Now, this is the Delaware

[00:20:10] **Thomas Ritter:** Yeah. So there's a couple different, ways to answer that. I mean, I think most simply, you know, lawsuits derive. More often than not from just statutory violations where a person who's been harmed brings suit, over maybe a company failing to enact adequate security measures that resulted in a data breach.

you know, strictly speaking, that's often predicated upon a negligence claim. you know, there are also state breach notification laws that provide what's called a private right of action to sue an organization. there's then a litany of laws that we've already mentioned that, allow regulators to initiate enforcement, actions against companies.[00:21:00]

you know, one of the best and most common examples pointed to would be the Office of Civil Rights under the Department of Health and Human Services and

how they routinely use HIPAA to bring enforcement actions against healthcare entities. And state attorney generals also do the same thing. you know, as far as like liability as a whole, you know, and, speaking to negligence. A thing I think is really interesting that isn't really talked about that much is, lawsuits that have been brought in recent years in Delaware over what's called Caremark claims. So, you know, as everyone well knows, the majority of companies choose to incorporate Delaware because of, you know, the tax implications of that and simplified corporate laws.

But in recent years, plaintiff's attorneys and always leave it to plaintiff's attorneys to find creative ways to try to sue someone have tried to go after companies board of directors using care [00:22:00] mark claims So the care mark standard has been around in delaware for I want to say 20 to 30 years, but it refers to conditions for Director oversight liability, under Delaware law.

And in the context of data breach litigation, Caremark claims have been used to support the notion that a company's board of director failed to prevent. a data breach from happening and therefore brought corporate harm on the business. you know, this was brought up after as many listeners and CISOs probably remember the Marriott breach.

It also came up again with SolarWinds. And while these lawsuits were ultimately unsuccessful, I think the biggest takeaway from these cases and something that CISOs and, you know, general counsel and external counsel should be thinking about that operate within the space is, I would expect it to become a bigger and bigger deal, especially, now that you have recent, you know, amendments [00:23:00] to the SEC regs.

And I think plaintiff's attorneys are going to just grow more sophisticated and nuanced in the future. bringing Caremark claims, but doing it under the auspice and aided and supported by, you know, some of these newer amendments.

[00:23:16] **G Mark Hardy:** Is this the Delaware Chancery Court, or is this some other

[00:23:20] **Thomas Ritter:** It is. Yes, it's been Delaware Chancery Courts.

[00:23:23] **G Mark Hardy:** got it. So there's risk out here, not only for them, perhaps. liability, with regard to negligence, as you had mentioned. Now the Caremark idea, at least for boards anyway, as CISOs, most CISOs aren't sitting on the board. They might report to a board or certainly should be briefing them on a regular basis, but any safe harbors or protective actions that, or companies

can do to help mitigate their risk, other than never make a mistake and do life perfectly.

[00:23:51] **Thomas Ritter:** Yeah, so it's actually a really timely question because right now, a number of states are either in the process [00:24:00] or have outright passed some safe harbor data breach statutes, right? And I think this coincides with, and I need to probably back up and first explain that there's been just this exponential, you know, explosion in data breach class action lawsuits in the last few years.

It's been felt on the insurance side. It's definitely being felt on the corporate side where nowadays, If you have a breach that requires you to report to regulators and individuals. depending upon how big the breach is and how many people you're reporting to, it's probably pretty safe to say that you're going to become a defendant in a class action lawsuit.

So, one state that actually just passed something a few months ago that My firm talked quite a bit about and have continued to have conversations with clients about [00:25:00] is Tennessee where I'm located and Tennessee actually passed a Data breach class action safe harbor some speculated maybe in response to change in Ascension Because of you know the large health care presence that is in The state of Tennessee, but essentially what this statute says is, you know, if plaintiff class action attorneys are going to bring a data breach class action and do so successfully, they're actually now tasked with demonstrating gross negligence.

So they've significantly higher, the evidentiary standard that plaintiff class action attorneys need to use, which in turn should make it. More difficult for these attorneys to bring these suits successfully. Ohio is another one that I think was the first. State, if I'm not mistaken, back in 2017 or [00:26:00] 2018 that actually passed something similar, which was actually, it's, an affirmative defense.

So, you know, if a company is sued over a data breach, they can actually assert as an affirmative defense and point to this particular statute, you know, and be provided some, you know, protection. All predicated upon if they can demonstrate compliance with some of the security frameworks and standards like, you know, NIST, ISO, and so on and so forth.

So, there are laws out there similar to what we were saying about, you know, the overturn of the Chevron doctrine. I've really cautioned clients and CISOs against relying on this too heavily. Particularly ones within the state of

Tennessee. I mean, it does not provide blanket immunity, but I think it's absolutely something that's worth knowing about.

And I think it should [00:27:00] be something that they can kind of. Use and maybe allow them to sleep a bit easier tonight if they're doing, you know, some of the things on the backend, like trying to comply with different frameworks and having that appropriate due diligence in place when it comes to security in general.

[00:27:19] **G Mark Hardy:** Got it. See, compliance is important. I agree. There's a lot of different frameworks out there. In the absence of one specific one, we find out that a lot of organizations choose the one. For example, if you're doing a lot of business in the EU or in the APAC region, often use an ISO standard because ISO is the international standard.

Kind of like the metric system, everybody but America uses it. And so, as compared to over like here, we're using NIST or something else like that. But in addition to complying with the standard, it's important that we comply also with reporting requirements and those reporting requirements, although they may not be tied to a particular standard, are nonetheless there and get you in trouble if you don't follow those rules.

So what are the types of reporting [00:28:00] requirements in cyber that CISO should be aware of and make sure that take place?

[00:28:05] **Thomas Ritter:** Yeah, it's, another great question. And it's, one that doesn't have an easy answer more often than not. because as I've already mentioned, reporting requirements are often largely dependent upon, what industry an organization finds itself in. So complexity can come into play very, quickly.

so let's just kind of, for purposes of having fun, engage in a hypothetical and that's, you know, you have a publicly traded. financial institution who undergoes an incident.

where does that leave that organization? Well, they could be subject to a litany of laws and regulations. They are subject to the SEC's cybersecurity regulations.

They are, they could be subject to NYDFS cybersecurity regulations. they're likely subject to Gramm Leach Bliley. [00:29:00] they then have to worry about state breach notification laws and those coming into play if they had impacted

individuals. You know, within states that would implicate that state's breach notification law.

So it's a patchwork and maze, as we both have said, of reporting requirements that make compliance really, difficult. but, you know, I think just from an overarching perspective and speaking about reporting requirements and timeframes, I first want to break it down by state, you know, states for the most part are pretty lenient when it comes to when organizations who have made the legal determination that they have had a breach and then have, obligations to notify individuals and regulatory authorities about that breach, can do so within, you know, a longer timeframe.

So. One of the bare minimums, 30 days, [00:30:00] you have some that go to 45 days, you have some states that are 60 days, and then you have some that leave it into a more ambiguous standard of, using the as soon as possible and without unreasonable delay language.

[00:30:13] **G Mark Hardy:** It's compared to SEC, which kind of puts the fire to your feet

[00:30:17] **Thomas Ritter:** yeah, so.

[00:30:18] **G Mark Hardy:** I don't know anybody can complete an entire investigation be authoritative in 96 hours or something like that. You just don't know.

[00:30:25] **Thomas Ritter:** agree. And yeah, you took the words out of my mouth. You know, you compare the states to some of the, you know, industry and regulatory frameworks like NYDFS and the SEC, who both feature 72 hour notification timelines. Based upon right, like materiality. and, it's just so difficult to do.

And as someone that's been a part of, you know, hundreds of security incidents, I mean, I can [00:31:00] tell you that there are very few maybe be, you know, probably I can count on one hand times in which. Within the first three days of the company and my client discovering that incident, they were at a point where they could capably make, and at our advice, have made a determination that it rises to the level of.

Of a reportable incident or a breach. so I think you make a great point. you know, another one to mention too is CISA's recently enacted. Well, I should say it's not actually in effect, but, CIRCIA. So the cyber incident reporting of

critical, you know, infrastructure act. and that's another, I believe it's maybe four days, but yeah, right around the 72 hour to 96 hour mark.

And so. Where that leaves organizations and CISOs is, in a tricky spot, right? And I think it [00:32:00] speaks to the need to really focus and, be strategic about preparedness and have tough conversations ahead of time and ahead of any incident with, you know, external counsel and really across departments, if you will, to, think through some of these things so that you're putting yourself, your business in the best position possible for when you inevitably do have something happen.

[00:32:32] **G Mark Hardy:** right now obviously from time to time things do happen and some cases go high order at least in terms of publicity and awareness and one of the things you can do is I remember reading something it said A poster, I think I saw it back in junior high school. It's like a fool never learns from his mistakes.

A smart person does learn from their mistakes. A wise person learns from others mistakes. And so if we want to put on our desire to be wise, what [00:33:00] if we take a couple of recent cases, relatively speaking, like SolarWinds or Colonial Pipeline, what, lessons can we learn out of that? And what is it that we could look at to go, okay, yeah, I'm going to go look to make sure that doesn't happen here.

[00:33:13] **Thomas Ritter:** Yeah. So for me, the first thing that stands out for some of the more high profile incidents, is just how unsophisticated, The root cause of those attacks were,

you know, let's start with Colonial Pipeline, right? The, bad actors leveraged, an exposed employee's password to access Colonials VPN, which in turn got them access to the company's network.

you know, this past spring, United Healthcare Group CEO, Andrew Witte mentioned that the root cause of Change Healthcare's attack was, a compromised Citrix portal. and so. amazing to me that [00:34:00] even as far back as like Target, right? And I think it was the HVAC vendor that had been given administrative access and privilege.

you know, We're,

[00:34:10] **G Mark Hardy:** Mechanical. I can remember the name, had to think about it a moment.

[00:34:14] **Thomas Ritter:** we're still seeing the same mistakes made over and over again, you know, and for me, it calls to mind, there's a Tony Robbins quote, that I often use in, presentations with clients when I'm talking about cybersecurity and it actually, you know, really supports, I watched a video you did within the last few months on complexity and how complexity is killing cybersecurity.

And the Tony Robbins quote is. That complexity is the enemy of execution. And I think that really speaks to, and I've seen it firsthand. idea that clients, you know, are throwing money at the problem and they're spending, [00:35:00] half their budget on the most sophisticated tool set. And then lo and behold, they're not even deploying those tools correctly.

Right. And they aren't focused on what I would consider like the essentials of, security, you know, the deploying multi factor authentication across your environment, you know, routinely reviewing administrative privilege, you know, looking at your password policy and how that's being implemented and used throughout an organization, really focusing time and energy on training employees.

Right. because more often than not, and a lot of the ransomwares I've. worked over the years. PatientZero starts with an employee who, you know, received a phishing email and clicked a malicious link that then starts the download of, you know, a ransomware executable. For me, it's like, I try to [00:36:00] really remind clients, you know, let's, think about doing The, essential security controls.

Let's implement those. and really, I think that'll help eliminate a lot of the risk. and then the second point I want to make about some of these, you know, high profile attacks is how they've informed. you know, subsequent law and policy that have come out of that. So, you know, both SolarWinds and Colonial, that largely informed CIRCIA that I had mentioned earlier that, you know, CISA was in charge of, promulgating.

And, you know, SolarWinds, I think absolutely informed the SEC's update and amendments to the cybersecurity rules, for publicly traded companies. So. I had mentioned this earlier. I think the same ultimately will be and can be said for, these healthcare attacks that have happened recently [00:37:00] and the soon to be updates to the HIPAA security rule.

so all of that to say for me, the two big things are just, you know, really focusing time and efforts on, the security essentials, if you will. And then looking at how those attacks have, informed,

policy making

[00:37:20] **G Mark Hardy:** Yeah. And we've talked about a couple risk vectors. One of the risk vectors being that of regulators, one of the risk light regular, vectors being that of. Lawsuits, but realistically, those two are almost subordinate to what I think is a greater risk, which is going to be threat actors. And in particular, if we take a look at where the money is, if you remember, the idea of Willie Sutton, the bank robber, when they said, why do you rob banks?

Because that's where the money is. we find that there's ransomware groups. And these ransomware groups, which operate outside of U. S. law enforcement, Jurisdiction are organized like businesses. They have a CEO, they have a HR department, they work [00:38:00] hours, they get a payroll. And this is big business. We're talking billions of dollars, and it's all operating obviously outside of US legal framework, but it is able to impact US organizations.

Is there any perspective on what, you know, we can't do a lot. You'd think you can't go ahead and just, Put a warhead on a forehead and I don't think U. S. government's going to do that. What's happening? Is this just going to be a scourge we live with? Right.

[00:38:32] **Thomas Ritter:** Yeah you rase a lot of salient points. Ransomwareis at this point unequivocally an epidemic that's just not going away. and I oftentimes, you know, unfortunately, after the fact for most of my clients. I have to remind them that these groups, they don't discriminate, they could care less about size and annual revenue of a victim organization.

Those are not metrics that are informing their decision making of, you know, [00:39:00] compromising a network and, you know, acquiring and exfiltrating a terabyte of data from that victimized organization. So it's all about, as you mentioned, just, the intent to get paid and do so as quickly as possible so they can move on to the next victim.

so I think that's just something really important to reinforce because, you ransomware incidents for mom and pop shop shops that, Unfortunately for many, put them out of business, all the way up to Fortune 500 companies, and it never ceases to amaze me that more often than not, a lot of the prevalent thinking is that, I just wouldn't have thought that they would have targeted me.

the second point I want to make about these threat actor groups, and it's one that you touched on is, you know, the challenges that law enforcement faces [00:40:00] and really trying to bring these criminals to justice. you know, I don't think most companies understand the work that's going on behind the scenes, or really give law enforcement enough credit and trying to combat what essentially is the 21st, you know, century version of modern warfare.

so they're fighting an uphill battle, oftentimes against nation state backed adversaries that, you know, are not. Capable of being extradited. I oftentimes encourage clients to let us liaise with the different FBI task force that are in charge of pursuing specific ransomware threat actor groups.

you know, one from a few years ago that, I got to know the, individuals of this particular task force really well, unfortunately, because, you know, We're [00:41:00] routinely having clients that were impacted by them, but it was the Conti ransomware group. and so, you know, the men and women that worked within this particular task force group, had really valuable intel for us, right?

And being able to, you know, Share, even if it was after the fact, things like IOCs or TTPSs, you know, was, helpful and not just from like the civic standpoint of, doing good and trying to prevent someone else from being victimized, I think too, it provided kind of a unique perspective in the sense of, you know, them being able to provide, you know, Some really good threat intelligence.

I will say it didn't happen or has not happened very often, but there have been instances where I've had clients when we've contacted these task force groups, actually be provided [00:42:00] a decryptor. And so, you know, I don't. I don't think that's something, an expectation that companies should have.

should you be hit

sometimes you lucky.

but sometimes you get lucky and you know, it reinforces the idea that, you know, there's a real misperception. If you ask me, around clients having a healthy dose of skepticism that The FBI is going to try to meddle in, you know, the resumption of, business operations and the FBI is going to try to, you know, dissuade them from paying a ransomware.

That's just, that has not been my experience. and I think, you know, the FBI more often than not, to speak for them or put words in their mouth, but, you

know, they, We'll tow the company line of like, you know, we don't encourage anyone to negotiate with terrorists or pay terrorists. But at the end of the day, it's a business decision and businesses are going to do You know, and oftentimes whatever [00:43:00] necessary to get back to being able to do business.

So, yeah, I think those are the two things I really want to bring up, you know, when you're talking about, ransomware in general.

[00:43:12] **G Mark Hardy:** Got it. Yeah. It reminds me of the flight attendant. I was on a flight a couple of days ago. The gentleman next to me, they're getting ready to land. He says, you go to the restroom. And he says, well, I can't tell you yes, but I can't stop you either. And it's like, okay, fine. You're not supposed to do it, but yeah, it's okay.

So I get that. Hey, you know what I'm thinking? We could, we're about halfway through the stuff I want to talk about and we're already almost at the end of an episode. So here's a couple ideas. Number one, how would someone get in the hold of you if they said, Hey, this guy is smart, he's articulate, he knows things that I care about, and I want to just get in touch with him.

how would someone best reach you?

[00:43:48] **Thomas Ritter:** Absolutely. So, You know, I would encourage them to go to our website, which is the name of our firm, RitterGallagher. com. we have a fillable contact form on the [00:44:00] site or they can just reach out to me directly, via email Thomas@RitterGallagher.Com. you know, I oftentimes love to hear from prospective clients that way.

And, and our firm, I think is really predicated upon wanting to form. a longstanding relationship with clients. Right. so, you know, anytime we can be of service to people, whether it's just talking about cybersecurity in general, or maybe doing more nuanced projects, we always love to help.

[00:44:33] **G Mark Hardy:** Well, got it. Well, I'm going to do it. I'm going to try to bring you back for a second show. We good with that? So we can go ahead and finish all the stuff we want to talk

[00:44:40] **Thomas Ritter:** I would love that.

[00:44:41] **G Mark Hardy:** Awesome. All right. We got it. That sounds like a commitment to me. I'm going to hold you to it. Okay. For our audience out there.

Hey, thank you very much for listening in. We've been talking about cyber legal tips with Thomas Ritter, an attorney who specializes in that area. He's down there in the Tennessee area. And you don't have, of course, have to be in Tennessee to be able to work with him. But I think this has been fascinating.

I've got a [00:45:00] lot more, so we're going to do another episode, but just not today. So this is your host G Mark Hardy. I appreciate you tuning in to CISO Tradecraft. Until next time, stay safe out there.