Rich Meneghello (00:00)
Welcome to The FP5: Five Things for Your 9-to-5. We help employers make sense of the fast moving world of workplace law and compliance by breaking topics down into five parts. I'm Rich Meneghello, Chief Content Officer here at Fisher Phillips.

Well, there's a sweeping new federal cybersecurity reporting mandate that's on its way. And today we're gonna share with you five things you need to know so you can understand what's about to happen and more importantly, what you should be doing about it. We have the best person in the firm to be talking about it: I'm joined today by Dan Pepper. Dan is a partner in our Denver office and he chairs our firm's data protection and cybersecurity team. Dan, welcome to the FP5.

Dan Pepper (00:47)
Thanks so much, Rich.

Rich Meneghello (00:48)
We're thrilled to have you. I know this is not everybody's most fun idea of a topic. To me, cybersecurity reminds me of like emergency dentistry: I'd like to know the options there for me if I need it, but I never wanna have to call the person. So I wonder if you have a lot of clients that treat you that way that maybe an ounce of prevention is better than having to see you when the crap hits the fan, but it must be an interesting job that you have doing that.

Dan Pepper (01:16)
It's an interesting job and a root canal is a great analogy, that's about right. I liken it oftentimes to, especially with the breach response work, like working in ER where you're sitting there and the double doors burst open, there's a gurney flying through, you have no idea what you're going to find on there. But you can be sure that the next several hours are going to be spent trying to figure it out.

Rich Meneghello (01:39)
And you were on your lunch break at the time, right?

Dan Pepper (01:42)
Lunch break, Thanksgiving, Christmas. Yeah, that's typically the times I like to do that. Yeah.

Rich Meneghello (01:47)
Yeah, the cyber criminals don't necessarily take holidays, do they? Dan you're definitely the most skilled person when it comes to data protection and cybersecurity in our firm. Before we dive into the five questions, what's your origin story? How did you get into this field?

Dan Pepper (02:02)
Yeah, you know, I, my background primarily is in in-house. So I was deputy general counsel and a deputy privacy officer at Comcast, before that I was in-house at Verizon as an assistant general counsel. You know, honestly, 30 years into this, the pattern really hasn't changed much. New technology shows up, you know, regulators scramble to catch up and clients get caught in between.

You know, with the old contracts and new threats, whether it's cyber threats or it's AI, it's really just the current iteration of that same story.

Rich Meneghello (02:38)
There you go. Okay, excellent.
Well, let's dive right in. We're gonna talk about five different things that folks need to know about the current state of cybersecurity. The first thing is, and it's really hard to have a conversation with me and not have it bleed into artificial intelligence, so let's start there.

The first thing is AI has changed what cyber attacks look like and how much damage they can do. And I think what this means when I think about it is that any assumptions that our audience might have had about the risk exposure that they have, based on, I don't know, information that they've learned any time prior to, I don't know, in the last year or so. It's probably not true anymore because the world has changed that much with AI. Can you tell us what's happening, Dan? Why are things changing so quickly?

Dan Pepper (03:28)
Yeah, I mean, I can speak to it in the context of cyber attacks. And, know, the question I often get is “Well, is AI already being used in real attacks?” And the answer is, yeah, it's not theoretical anymore. We've got documented cases. You know, the one I think that we would want to anchor on as part of this conversation is, you know, back in November of last year, Anthropic disclosed what it believes was the first AI-orchestrated espionage campaign at scale.

Chinese state sponsored actor, they jailbroke Claude Code and used it as an autonomous agent. And it did all the things that typically threat actors would do when they conduct some sort of a security breach: you know, 30 different global targets, tech companies, banks, chemical manufacturers, the striking numbers that the AI performed 80 to 90 % of these tactical operations and human involvement was measured in like in minutes, not hours. So this isn’t AI that's helping attackers. That's AI actually executing the entire attack.

Rich Meneghello (04:34)
And speaking of Anthropic, you just recently published an article, and for those listening, we'll publish a link to it in our show notes. You published an article just recently about Claude Mythos, released, well, not released by Anthropic, developed by Anthropic. Tell us about that. That to me was a both fascinating and a scary article at the same time.

Dan Pepper (04:54)
Yeah. April of this year, Anthropic disclosed another model, I guess we could call it a new model called Mythos, which on its own, autonomously discovered thousands of Zero Day vulnerabilities. And a Zero Day, just think of it as a vulnerability that hasn't yet been disclosed. No one really knows about it yet. And it found these things across every major operating system and web browser. And so, you know, one was a bug in a system that had sat undiscovered for 27 years. Another one was another exploit against what's called FreeBSD, but the point is that 99% of what it found is actually still unpatched. So Anthropic said, well, we're going to hold this back from public release just based upon the damage this thing can do. So it's restricted to just a handful of defenders under what's something called Project Glasswing.

But you know, what's interesting is independent researchers have already shown that smaller, cheaper, open source models can do the same thing. So the capability is diffusing whether we like it or not at this point.

Rich Meneghello (06:04)
I was thinking, I talked to a couple of our attorneys in the firm who are into AI and they're not coders at all, they're not tech folks, they're just lawyers. And they were talking about how they use AI and they feel like coders now because they can use different programs just with the basis of AI to make websites and do different coding. Made me realize in thinking about this in conjunction with the story we're talking about that anybody can use AI and learn how to be a pretty proficient cyber hacker, I'm guessing these days, that AI is just advancing the ball, not in terms of just knowledge spread, but actual weaponry. It's sort of scary.

Dan Pepper (06:40)
It's sort of scary. And you know, the skills that typically used to, you know, require an experienced offensive team to conduct these attacks used to be pretty significant, right? You'd have to have some pretty good coding skills, kind of like you mentioned, now with these tools that are available, even a poorly resourced threat actor with, you know, just a jailbroken model can run the same type of a campaign that these sophisticated threat actors do. And the tempo is truly superhuman, right? These agents, they don't sleep, they don't make typos. So they just go at such a speed and scale that it's just astonishing. So what happens now is when we talk to clients and we talk to boards and we talk to security folks and the last time that they looked at their cyber risk profile, just a year or two ago, that threat model is already stale. It's not philosophically stale, it's just factually stale based on what we're seeing.

Rich Meneghello (07:38)
Unbelievable.

Well, that leads us into the second thing, Dan. And if the first thing wasn't scary enough for our audience, the second thing might be, and that is that geopolitical instability also works to ramp up the cyber risk for companies. So, you know, back in 2022, when Russia invaded Ukraine, we published an article about how employers needed to get their shields up because Russian cyberattacks on American businesses were inevitable. And certainly that ended up happening.

But that same pattern seems really relevant right now, given the geopolitical instability we're dealing with, with Iran being a threat actor getting a lot of significant attention. Am I right about that? Is that something that employers seem to be worried about, or is that just sort of some stuff that you're reading in the news that might scare people?

Dan Pepper (08:33)
The parallel to Russia and Ukraine holds, but the moment right now is hotter than anything we saw post invasion in 2022. So let me give you the timeline, right? So February 28th of this year, U.S. and Israel, launched these strikes on Iran. On March 1st, Iran's Supreme Leader is killed and Iran retaliated kinetically with drones and ballistic missiles, but in parallel through cyber operations that are run by state-aligned groups and hacktivists. And within 10 days, we actually had a confirmed Iran-linked attack on one of the largest medical device companies in the U.S. So then a week later, FINRA comes out. They issue a cyber alert to financial services firms. We've got joint advisories coming out of CISA warning that Iranian-affiliated actors are targeting Rockwell Automation programmable logic controllers. What are those? Well, these are the things that control water utilities and energy facilities and other governmental stations. So it's active, it's current, it's still unfolding.

You know, it's pretty scary. But if you think about, well, who are these actors in practice? You know, there's a bunch of really kind of funny names like Seedworm and MuddyWater, right? But they've been active on U.S. bank, airport, software, nonprofit networks since February.

And these are the groups that are hitting the water utilities, you know, so they used to focus just on, you know, some other infrastructure elements, but, you know, now they're, they're shifting to these controllers that impact all sorts of different types of infrastructure entities. So really what they're doing is they specialize in these, these hack-and-leak operations that are designed to be more like psychological warfare than espionage, right? They don't care about stealing stuff. They're not financially motivated. They're just looking to create as much fear as they can. And that's the real difference from what we've seen from 2022.

Rich Meneghello (10:32)
Okay, and yeah, that was the thing I was thinking about here that employers have to worry all the time about cyberattacks, which very often are either the stealing of data or locking up of systems, and they'll ask for a ransom in order to free up your system. But I'm guessing Iranian threat actors are not looking to ransom right now. They're looking to just disrupt.

Dan Pepper (10:55)
They're looking to disrupt and destroy and it's to send a signal, right? That's really what they're doing. And now, you know, any organization in the U.S. can end up being on the firing line. It's not just the high value intelligence targets that we used to see. Now it's actual, you know, businesses that we all depend upon for all sorts of services and products. And the risk right now, you know, it's the defense industrial-based companies, especially those with Israeli research or defense partnerships. Those are, you know, prime targets now of these guys: healthcare, life sciences, financial services, anyone with deep third party vendor dependencies, right? So they're, they're dependent upon, you know, large supply chains to do what they're doing. The Iranians know that if they can get access and disrupt those, they can operate exponentially, right? So that one vendor may supply critical products or services to hundreds or thousands of customers. So instead of trying to hit hundreds of thousands of customers, hey, why don't we just hit that one vendor? We can do it much more efficiently and take them all out.

Rich Meneghello (11:54)
Yeah, wow. Okay, that's eye-opening. I hadn't thought about that.

Okay, the third thing, I'm not sure if we've sufficiently scared our audience here, but let's talk about a new federal reporting mandate, which is sure to send shivers up people's spines. A new federal reporting mandate is coming and the clock for reporting potential cyberattacks and cyber breaches is gonna start even before some companies know that they were hit.

Dan, the new law we want to talk about is called CIRCIA, the Cyber Incident Reporting for Critical Infrastructure Act. It covers more employers than most realize, and it also has an insanely quick reporting clock for lodging the report about these cyber incidents. We did also publish an article that you wrote about this, and that is also in the show notes. Can you walk us through CIRCIA and let employers know what they're going to be dealing with pretty soon?

Dan Pepper (13:02)

Yes, I think it's “sir-see-ya” or “sir-shah,” you know, make up your own, you know, pronunciation of this.

Rich Meneghello (13:08)
Hang on, is it “sir-shah”?

Dan Pepper (13:10)
I have no idea. I’ve actually never heard it spoken aloud.

Rich Meneghello (13:13)
Okay, well there you go folks. You just heard a potential editing feature right in real time there because neither of us know how to say it, so we're just gonna go with it. “Sir-see-ya” or “sir-shah” or whatever. Okay, “sirk-e-ya”, who knows? Go for it.

Dan Pepper (13:25)
“Sirk-e-ya,” we'll go with that, right? So yeah, quick background, right? So that, as you mentioned, that's right, that's the Cyber Incident Reporting for Critical Infrastructure Act. It was signed into law in 2022 and it required the Cybersecurity and Infrastructure Security Agency or CISA to write a rule that implements the reporting requirements. So CISA missed the October 2025 statutory deadline. So the final rule was pushed to May of this year.

And because of the DHS appropriations lapse that happened this spring that we're all familiar with, the town halls that they had scheduled got suspended. [The] rule’s very likely to slip again. But as you mentioned, Rich, yeah, once the rule is final, basic obligations are this: So there's a 72 hour clock from a reasonable belief that a covered cyber incident occurred. And then there's a 24-hour notice obligation to make or to notify CISA of any ransomware payment. And then you got ongoing supplemental reports as new information develops.

But when the clock starts, this is where I think almost everyone's gonna get it wrong. The trigger is reasonable belief, right? It's not confirmation. It's not, “hey we received our forensic report.” It's high-confidence detection in your security operations center that meets the statutory definition of a covered incident. So if your existing incident response playbook says, you know, “we'll make the reporting decision once forensics is done,” you're too late. You need to name right now the person who's authorized to make the reasonable belief call in the middle of an incident. And that decision needs to live in your playbook now.

Rich Meneghello (15:04)
Dan, who's actually covered by this? I know a lot of people will hear critical infrastructure and think that's not them, but how broad is coverage for this new reporting scheme?

Dan Pepper (15:14)
So CISA's own estimate is that more than 300,000 entities will be in scope. So the rule reaches any organization that operates in one of 16 critical infrastructure sectors if it exceeds the SBA's small business size standard, and I won't get into that because it varies by all these different sectors, but I think the takeaway is the list of those 16 sectors include things most people don't instinctively call critical infrastructure.

So if you're like hotels and retail and entertainment and healthcare, food and agriculture, right? So there's a lot here that you would typically not expect would get sucked into this. So if you, let's say operate a midsize hotel

chain or a regional bank or a food processor, you're probably in scope. So the employer who hears critical infrastructure in quotes and thinks “that's not me” is usually wrong.

Rich Meneghello (16:08)
Wow, okay. And let's say employers don't comply once this thing comes online. What are the consequences?

Dan Pepper (16:16)
So there's three escalation tiers. CISA will first issue a request for information. Ignore that, they're gonna issue an administrative subpoena. And if you ignore the subpoena, the Department of Justice files a civil action, including for contempt. And so on top of that, if you file an incomplete or a false report, that exposes you to false statement liability under federal law.

And if you're a federal contractor, you face debarment risk. So this isn't like a $5,000 fine regime. They've got real federal regulator enforcement mechanisms in place.

Rich Meneghello (16:52)
I'm going to encourage all of our listeners to look at our show notes and find the article that Dan published on this so that you are well familiar with it and also sign up to make sure you are subscribed to Fisher Phillips Privacy and Cyber Insights to receive them via email because we'll update this once the reporting system comes online, but I'm guessing Dan you're telling your clients not to wait, to start prepping now?

Dan Pepper (17:19)
Start prepping now, and I think this is probably the biggest piece of this, the rule delay that we're seeing, right? Whether the final rule drops next month or sometime later, it's not going to buy anybody breathing room. And there's three reasons, right? The 72 and the 24-hour clocks we talked about, they're in the statute itself, not in the rule. So they're not going to move. So CISA is already encouraging voluntary reporting today. So if the organizations that are going to ultimately be in scope don't build the internal workflow now, you're not gonna be able to stand one up in 30 days when the final rule drops. So what I have been telling folks is treat the delay as a planning runway, not as a holiday, because those numbers aren't changing.

Rich Meneghello (18:08)
This is the FP5, I'm Rich Meneghello. Once again, we're here with Dan Pepper, a partner at Fisher Phillips's Denver office, and he chairs our Data Protection and Cybersecurity team.

That leads us to our fourth thing. Dan, the White House is trying to push a significant shift in how the government is going to approach cybersecurity, aiming for more of a proactive stance instead of a defensive sort of posture. Back in March, the White House released two documents. There was a National Cyber Strategy and an executive order on cybercrime. And both of those aim to reduce some compliance obligations on behalf of employers and create more of an offensive capability in fighting cybercrime.

Once again, for our listeners, if you go to our show notes, we will include a link to an article that Dan published on this. What's the main takeaway regarding the White House's stance on cybersecurity and how is it changing things, if at all?

Dan Pepper (19:07)

The cyber strategy document, just for context, it's seven pages long. And compare that to the Biden 2023 strategy, it was 34 pages long. So the new one is deliberately high-level. It sets out six main pillars, basically shape adversary behavior, promote common sense regulation, modernize federal networks, secure critical infrastructure, sustain superiority and critical technologies, build talent and capacity. That's basically it.

The second document is the executive order on combating cyber crime, fraud, and predatory schemes. And that one is focused on transnational criminal organizations. So scam centers, sextortion, ransomware, business email compromise. And what that does is it directs a 60-day review of all the existing frameworks that are in place now. It's a 120-day action plan, and then a creation of an operational cell inside something called the National Coordination Center. And it also pushes for expanded information sharing between the federal government and commercial cybersecurity firms.

Rich Meneghello (20:11)
So, I mean, it sounds like on the one hand, the government is aiming for, putting it simply cutting red tape, fewer compliance obligations. It sounds like good news for employers generally and businesses, but what's your take on that? Am I reading that right?

Dan Pepper (20:25)
So, you know, even though the administration is shifting from a compliance-centric posture to more of a disruption- centric posture, you know, less of a “check more boxes here.” Is that actually good news for companies who are looking to reduce red tape? And so I would say it's sort of a qualified yes.

The good news is that, you know, the binary push to shift software liability and impose mandatory standards on critical infrastructure, that's being rolled back. So companies get some agility, they get some reduced audit burden. But here's the caveats: You still have state regulators in the field. You've got, you know, California, you've got New York Department of Financial Services, you got the state AGs, and then you still have the sector regulators, you know, the HHS, SEC, FTC, FCC. You got the state insurance and banking departments. They all operate independently of the White House posture. So the plaintiff's class action bar, they're not affected by this. And most importantly, I think when the inevitable incident hits, negligence theories look at an industry standard of care, not whether a specific federal rule applied to you. So really, fewer checklists doesn't really mean a lower standard of care at the end of the day.

Rich Meneghello (21:44)
Okay, and I'm trying to square and I'm wondering if employers are hearing the same thing that our third thing was about this new federal mandate from [CIRCIA] but we're also talking at the same time that the White House is trying to deregulate. So can you help square those? Like what sort of posture should I be thinking about big picture wise if I'm a business here?

Dan Pepper (22:09)
Yeah, right. So there's tension. So the administration, you know, they're deregulating on one side and, and CIRCIA is adding federal mandates on the other. So how do you square that if you're, if you're an employer? So I think three main points. So CIRCIA is statutory. The White House can't eliminate it by executive action. It can only narrow the scope and it can harmonize it through CISA's rulemaking. And then also the administration's deregulatory focus is on prescriptive security controls, not on visibility. CIRCIA is a visibility statute. Government wants data about attacks so we can act against adversaries. And that's actually consistent with the “shape adversary behavior”

pillar of the new strategy. And then the last piece I'd say is expect that the final CIRCIA rule is probably gonna be narrower in scope in the proposed version. But as I mentioned, the 72- and 24-hour clocks, they're gonna probably remain unchanged. I don't see that changing.

So I wouldn't read quote “deregulation” as “CIRCIA’s going away.” Plan for a final rule this year, there's probably going to be a narrower covered entity definition, but you're going to have the same reporting clocks.

Rich Meneghello (23:15)
Okay, I'm reminded, Dan, of one of the benefits of working for a national law firm with offices all across the country is you start seeing differences in regional differences in the way people pronounce and say certain statutes. And that's sort of the nerd in me that appreciates this sort of stuff. But do you know there's the Family Medical Leave Act? I've tracked, there are at least three different ways in which people in our firm pronounce it, depending on what part of the country you're in. It's either “fem-la,” “fam-la,” or “the F-M-L-A.” So I'm really going to be curious about “sir-kee-a,” “sir-she-ah, “sir-see-ya” to see how, whether there's a regional difference. I want you to track that for us, Dan, and let us report back please.

Dan Pepper (23:58)
If nothing else, I think that might be the most important element of this whole thing.

Rich Meneghello (24:02)
Agreed. Agreed.
Okay, the fifth and final thing, you know we've been not purposely, but scaring employers with a whole lot of new threats and reporting obligations and laws to consider, but, and we've also told them that their cybersecurity playbook is probably outdated. So let's do some good work here, Dan. Let's help them build a new one. From a practical question standpoint, what are employers commonly right now, most commonly doing wrong and where should they start when it comes to turning the page and getting to match the needs of this most modern era now.

Dan Pepper (24:44)
Yeah, maybe I can walk through the most common mistakes that I see and then we can kind of go into where to start.

First thing, incident response plans built from generic templates, right? Plans written for plain vanilla ransomware that don't contemplate AI driven attacks. They don't contemplate the OFAC sanctions exposure from state actor attribution. And they certainly are not capturing the new CIRCIA 72-hour reporting.

The second thing is assuming that the forensics report from an investigator that you hired triggers a notification obligation. I think organizations figured that's how we're going to build our obligations, both from a legal perspective and notification perspective. So if you're assuming that, it's gonna trigger the notification obligations, like I mentioned, it doesn't. So the reasonable belief is gonna trigger CIRCIA. State breach notification laws have their own clocks. The federal statutes like under HIPAA and Graham Leach Blyley, they each have their own. So by the time forensics is done, you're often already late somewhere.

Third thing, there's no designated decision maker for the reasonable belief call. So most organizations haven't named the person who decides in the first hours of an incident whether to pull the trigger on reporting.

Fourth thing, I would say tabletops that test the wrong people. So tabletop exercises are like your mock scenarios. So you'll have an IT team or a security team run the exercise, general counsel and the CEO, they reluctantly participate, but when the real incident hits, the muscle memory is in the wrong place, right? Board level, executive level tabletops are the ones that really move the needle at the end of the day.

And then there's no breach coach relationship in place before the incident. So entities that wait to engage outside cyber counsel spend the first 24 hours onboarding lawyers instead of actually responding. And then they start to lose the privilege benefits of attorney-directed forensics because they're still in the interview stage. Right? Talking to different lawyers.

Last thing I would say is, and this is probably maybe the most important thing now that I see, or at least one of the most important things is failure to inventory your AI exposure. Most organizations can answer three basic questions: What SaaS vendors are now training on your data? Which employees are being, are using unauthorized AI tools with sensitive company data and which of our vendors have bolted AI features onto their product in the last 12 months without telling us?

Rich Meneghello (27:08)
I think one of the cool things we can do with podcasts, Dan, is look from an analytical standpoint to see the points in time where the audience was most engaged and listened. I have a feeling that the last minute or so that you just talked, we're gonna have people rewind and listen to over and over again, because you just laid out an amazing playbook for the 21st century, and I appreciate it. I'm sure our audience will as well. And if they zoned out for a minute, I'm telling people right now, go back and listen to the last minute and a half or two minutes of what Dan said and you could probably have ignored the rest of the podcast.

Talk about vendor contracts though, Dan. That's the next step I'm hearing from people that they might not be up to speed or know exactly what they should be looking for when they're entering into vendor contracts for the third parties that might be assisting with cybersecurity.

Dan Pepper (27:58)
Yeah, most vendor contracts, require, you know, patching critical vulnerabilities in quote “reasonable” timelines. Sometimes 30 days, sometimes 72 hours. But recall, we talked about that new Mythos tool. Classes of tools like that compress exploit development from weeks to hours. So your contract language or your vendor is written for a world that doesn't exist anymore. The fix is to shift from these quote “reasonable timelines” based on severity to timelines based on exploit availability. So require emergency patching obligations when a working public exploit exists. Require the vendor to subscribe to threat intelligence that identifies exploited in the wild status, tighten the flowdowns to the subcontractors. And what we're now doing almost every time we're dealing and negotiating terms with vendors is adding a specific AI addendum which requires notice before vendor decides “I was going to bolt AI into the product,” and then barring the use of your data for model training without any consent.

Rich Meneghello (29:04)
Excellent. I'm guessing you probably get a phone call now and then from clients asking you about cyber insurance. What are your thoughts on that?

Dan Pepper (29:14)

Yeah, you know, I think there's a misconception that all the cyber insurance carriers provide similar coverage and similar types of limits, which is really not the case. We're starting to see more divergence there. I would say there's probably three things to audit with your cyber insurance policies.

First, look whether there is social engineering and impersonation coverage. We are seeing deepfake-driven wire fraud happening all the time now and that can often be excluded or sub limited in your policies. If you have a policy that was underwritten before 2024, they weren't thinking about AI-generated voice impersonations of executives. Didn't exist, right? So that's something to take a look at. Reread the crime and funds transfer fraud sections. See if that would potentially bring in this AI-driven social engineering type of activity.

Second, systemic risk and widespread event exclusion. So insurers have really been tightening these. An AI-orchestrated campaign that hits multiple clients of the same vendor can fall into those exclusions. So something to think about.

And then the third thing, vendor and supply chain exclusions, most incidents now they originate at a third party, right? And many policies will quietly exclude or sub-limit vendor origin breaches.
So at the end of the day, if you've got a broker, that's really the person to talk to. Ask your broker, you know, in writing, you know, does my policy cover these things? And get your broker to commit to that in writing so you get some comfort around it.

Rich Meneghello (30:47)
Okay, we've given folks a lot of information on this podcast and again, I encourage our listeners to check out the show notes where they're gonna find links to detailed articles that you've written on the various topics we've talked about. And like we said at the beginning of this thing five, you did a great job giving people, pointing out the biggest mistakes that you've seen and telling people how they can fix those. But, what's the first thing if I'm an employer or a business that's hearing this, and I want to do something about this to move the ball today, tomorrow. What's the first thing?

Dan Pepper (31:23)
First call is to the outside cyber council. I'm not selling you, I'm just telling you, talk to the breach coach and you want to do that now, not during an incident. Do it when things are quiet. The reasons for that is frankly, establishing attorney-client privilege, because an attorney-directed forensic investigation is how you protect that investigation and preserve privilege over all the communications about it. The case law isn't perfectly settled, but the framework has to be set up correctly from the start.

Pre-incident readiness, the breach coach relationship that you've got with your cyber counsel is the vehicle for reviewing your incident response plans, conducting your tabletops, picking your vendor panel in advance, right? So your forensic investigators, your crisis communicators, your ransom negotiators, figuring out the CIRCIA design workflow, right? All that is coming from the relationship with your breach counsel.

And I will tell you all of that is way faster and cheaper before an incident during one, you know, and speed at hour zero, right? When the alert hits, you don't have 48 hours to interview law firms. You need a phone number that puts a coordinated team on the line within an hour, right? And I would say if outside counsel feels out of reach for an organization, I'd say the order of operations for a resource-constrained employer, put MFA on everything, right? Multifactor authentication on everything and phase out any SMS-based MFA. So the SMS, think of like, you know,

the code that gets text to your phone. You want to start to phase that out because the bad guys have gotten really good at exploiting those. And write up an incident response plan with named decision makers, include the person authorized to make that reasonable belief call, do an executive level tabletop, look at your vendor contracts on patching the terms and the AI clauses, and then do that cyber insurance policy review. So even if you don't have the resources for outside counsel, start with those things. They'll pay dividends. If you can then engage your outside cyber counsel, that's great, but that's the order I would say you do it in.

Rich Meneghello (33:28)
Excellent. yeah, this is we're not attempting a sales job really on these kinds of things. But I will say Dan has an incredible team on his data protection and cyber security group. And I definitely would encourage folks if they haven't established relationships with him or someone on his team to do so. And yeah, hey, look, this is our podcast. We can do whatever we want with it. We're using it right now to pitch your services. So glad we got a chance to do that, Dan.

Dan Pepper (33:54)
Absolutely.

Rich Meneghello (34:03)
Well, Dan, before we let you go, one of the things we like to do on the FP5 is ask you five questions to get the audience to know you a little bit better. So are you ready to reveal all?

Dan Pepper (34:14)
I guess I'm going to have to be.

Rich Meneghello (34:17)
This is a requirement to be on this podcast, Dan, before you go. All right, we'll make them simple for you. First, are you a Mac or PC guy?

Dan Pepper (34:25)
Work or at home?

Rich Meneghello (34:27)
Like a lawyer, you answer a question with another question. Just answer the question, Dan.

Dan Pepper (34:32)
All right, I am a I'm a Mac guy. We'll go with that.

Rich Meneghello (34:36)
Okay, remote in the office or hybrid?

Dan Pepper (34:39)
Remote for sure.

Rich Meneghello (34:40)

Favorite way to spend a free Saturday?

Dan Pepper (34:44)
One of two things: either hiking the Red Rocks in here in Colorado or tinker around on a keyboard to try to pretend as if I'm actually a musician. So one of those two things, depending upon the mood.

Rich Meneghello (34:59)
Well, if our producer gets his way, maybe we'll get one of your recordings to add at the end of this episode so people can hear you tinkering around a little bit, we'll see. If you weren't a lawyer, Dan, what would you be?

Dan Pepper (35:13)
Oh definitely would be a rock star. Yeah. I'd be performing on stage, embarrassing myself and everyone else.

Rich Meneghello (35:19)
Playing the keyboards?

Dan Pepper (35:20)
Playing the keyboards or possibly playing bass as well, which I have, you know, sort of equal light talent on.

Rich Meneghello (35:27)
I like it, I like it. And those are both sort of behind the scenes though. You're saying rock star, but both keyboardist and bass player are sort of holding up the fort behind the scenes, not necessarily out in front. Is that, that's cool with you?

Dan Pepper (35:39)
Yeah, well, you know when you're not exactly an introvert or extrovert you fall somewhere in between those instruments perfect for that.

Rich Meneghello (35:44)
Yeah, I love it. Fifth thing, and maybe you already answered this question. What's a secret talent most people don't know about you?

Dan Pepper (35:51)
Secret talent. So I'd say that I have the ability to grow a conversation from what appears to be a very simple question and answer into hours of discussion far beyond anything that was expected or actually desired from the person I'm speaking with.

Rich Meneghello (36:07)
And we hope that the audience members don't feel that way about the podcast they just listened to, Dan, because it's been a really great conversation. I don't feel that way, but I look forward to the next time we get together in person so you can test out that superpower on me and see if we can do that.

Dan Pepper (36:22)
Yeah, we'll see if you got the kryptonite.

Rich Meneghello (36:24)
Right, exactly. All right, well, I'm really glad we got to know you a little bit better, Dan. Learned some fun stuff. You're not all doom and gloom and cyber risk. You have some fun stuff going on. So I appreciate you taking the time not only to be here and share your expertise, but to share a little bit about yourself. So thanks, Dan.

Dan Pepper (36:42)
Thanks so much, Rich. This was great.

Rich Meneghello (36:45)
And as always, everyone, thank you for listening to the FP5. For other insights from Fisher Phillips, go ahead and visit fisherphillips.com.

And for more about protecting your business from cyber threats, check out the insights that we've linked in our show notes, just you'll get all the good stuff that Dan has written on the topics we've discussed and more. We'll see you next week.

Listening to this podcast doesn't constitute legal advice. It doesn't establish an attorney-client relationship. For more information, visit fisherphillips.com/legal-notices.

And as a reward for sticking to the end, as promised, here is an original piece of music by Dan Pepper. I hope you enjoy it.