Managing Cybersecurity Threats in 2026 Episode 1

PLUS Staff: [00:00:00] Thank you for listening to this PLUS podcast, *Managing Cybersecurity Threats in 2026*. Before we get started, we would like to remind everyone that the information and opinions expressed by our speakers today are their own and do not necessarily represent the views of their employers or of PLUS. The contents of these materials may not be relied upon as legal advice.

With the housekeeping announcements out of the way, I am pleased to turn it over to David Shannon.

David Shannon: Thank you, Bailey. I appreciate it.

And good morning or good afternoon to everyone who's listening in. We're here for another edition of our managing Cybersecurity podcast. We've been doing this [for]about three years now. [We will] try and hit some trends or some new issues that may arise each quarter for all individuals in the cybersecurity world, whether it be underwriters, brokers, claims managers or attorneys.

So, this morning Ryan Friel, who's a [00:01:00] partner in my group, and I are going to just talk about two issues that I think have gotten some play in the news a little bit in the last few months. Also, we've seen some uptick in handling these matters with our clients. That would be law firms being the subject or the target of the cyber criminals, the threat actors, and also financial individuals, advisors [and] broker dealers who are dealing with the implementation of an SEC regulation called Amended Reg S-P.

Ryan works in both our financial securities group and in the cybersecurity field, so he's handled a number of these matters involving responsibilities with this regulation. So, I'll just let Ryan introduce himself and then we'll talk about a couple issues.

Ryan Friel: Yeah, Dave, thanks for having me. As Dave mentioned, I work alongside Dave in the cybersecurity group. I also have a practice involving defending financial institutions, including broker dealers and SEC investment advisors, and also counseling broker [00:02:00] dealers [and] investment advisors on compliance matters, including the Amended Reg S-P, which Dave and I have spoken about previously on a podcast.

Since the last time we spoke, Amended Reg S-P has actually gone into effect for most large entities as of December 3rd, 2025. This material is very ripe. And these issues are real as of December 3rd, 2025.

David Shannon: Yeah. Thanks, Ryan. And we'll definitely talk about that a little bit and what it requires from those entities as well as what their counsel need to know when responding to data security events and breaches that affect these financial regulators.

But first [I] just wanted to talk a little bit about law firms that are becoming more and more the victims of data security events. I saw a number of articles in the last couple months that kind of mentioned how there was a real uptick in law firms that were being breached, whose names were being posted on leak sites with some ransomware groups.

We saw that as well. We handled [00:03:00] a number of cases for law firms in the past year. It would be both ransomware attacks and business email compromises. Obviously, law firms can be involved in the transactions where money's being wired. Someone, whether it be their firm or somebody else, that's in that chain of events for the payments, whether it be a real estate deal, a financial transaction or even fake clients and debt collection, [so] you're going to see that where the law firm gets dragged in.

A couple of things that I wanted to mention was, you definitely see the law firms being listed on some of the leak sites. There was a number of threat actors that were posting and seemed to be going after law firms more.

Silent ransomware was one. I know I was involved in a few cases with that group. [I] also have seen in the news their name coming up more and more when it involves ransomware and going after law firms. Particularly that group really goes after more just the data extortion [00:04:00].

I know in the events that we had, and in some things that I've read, they are not encrypting. They are just exfiltrating the data and then leaving the ransomware note saying "We're going to publish it, if we're not paid." That's a big deal for law firms. If their data is going to be posted up on the dark web on a leaked site, regardless of whether there was an encryption, it's a huge financial liability and a public relations liability for them and something that law firms have to deal with more and more like every business.

You're going to see not just when these threat actors get into law firms' computer systems, not just that they're going to encrypt, but some of them are

just going to take the data. With law firms, there's so much data there that is obviously customer or client related, whether it be financial or not. Whether it have specific PI (name, address, social security number, et cetera), you're definitely going to have that with some law firms. [For] others it's just going to be their customer's records, their customer's information. [It] could be their customer's intellectual [00:05:00] property [and] trade secrets, maybe, but certainly information that's privileged.

Having that go up on the dark web is a major concern for law firms. Whether it be the law firms themselves or their underwriters for the insurance carriers that they're working with, [you] have to really take a look at what your security is and expect that you're going to be targeted every day in some way, shape or form, whether it's [a] phishing email, social engineering, remote access, et cetera. You're going to see all of that with law firms, as victims.

It leads not only to the loss of the data and having to deal with a data breach but also the publicity as well. A couple of matters were in the news just in the last month. I was thinking about [them] when I was saying, "Let's have a podcast to talk about law firms." LexisNexis announced that they had a data breach and that there was data and information that was accessed. They had to publicly announce that. Their information, they stated, was just names, contact details and some account history. They were [00:06:00] stating publicly that there was no financial data or passwords that were exposed. In a lot of these cases, more information comes out later as to actually what was taken or what was accessed. We'll see if anything changes there.

That's a large, certainly major vendor for law firms. For any law firm that's using LexisNexis, they then have to go in, obviously, [and] make sure that their passwords have been changed [and] see if there's been any down the supply chain, so to speak, breach that's coming from that initial one. That was a big name that was mentioned in the news last month.

Another one was Jones Day, which obviously is a very large international, well-known law firm in the United States and throughout the world. They announced, towards the end of March, that they had a breach. Actually, the data was publicly exposed. I saw one article about how the threat actors even posted, to show which attorney in the firm they had gained access through, or at least they were alleging they did. It was a well-known attorney and partner in one of their offices on the East Coast [00:07:00]. There's a firm that certainly has, I would suspect, significant security [and] significant plans on protecting their data. They were the victim of one of these attacks and then [were] publicly being named.

[This] shows you that, not only do you have a law firm vendor in LexisNexis, but you also then have a large firm whose name is then publicly out there and they have to deal with everything that occurs with that. So, those were just some of the examples of some recent ones I saw in the news.

Ryan, I know we've also seen some BEC matters too, if law firms and that's always a concern.

Ryan Friel: Yeah, the BEC matters with law firms are concerning because when the data gets exfiltrated and once a threat actor gets into the system, there can be large sums of money that are moving in and out of law firms on a daily basis that can be subject to fraud.

That's always a concern.

David Shannon: Yeah, we see those and it's always a problem too in that if you're the law firm, it may not [be], and certainly in most cases is not, your money[00:08:00]. It's not your financial accounts that are being compromised, but it's phishing emails that are used. Then there are wire transfer instructions that are changed or ACH instructions that are changed. It's one of your clients, or maybe the client on an opposing side in a matter, that becomes the victim of the BEC.

But all parties that kind of touch that incident, in some way, shape or form, are going to then potentially be at risk for having claims made against them, lawsuits filed against them, et cetera. You can have both parties involved. You can have the banks involved. You can have investment companies involved, and then certainly the law firm. You're kind of looking down the whole chain of how it occurred. Who was responsible at the end of the day for realizing that there was a problem here? Was it more than one party? I think in most cases that we see the parties end up, I wouldn't say splitting the responsibility, but certainly looking [at], let's say, percentage-wise who was [00:09:00] most responsible [and] who was somewhat responsible. The courts are still dealing with these cases in a lot of ways.

The case law, as of right now, is the courts seem to be looking at who was in the last best position to determine that there was some fraudulent activity on that transaction. Now that doesn't mean that just that party's going to be found to be responsible or liable for the loss, but certainly the courts are trying to come to a position as to who are we going to say is legally liable for the incident. And as of right now, they're looking in some of the case law decisions as to who was

the last individual or had the best chance to be able to realize that there was a problem, that there was fraud there.

Those are ongoing legal decisions because these cases are still relatively new, in the grand scheme of things for legal precedent. For everyone who's listening, if you're [in] the insurance underwriting field, it's "What are you going to cover?"

There are now social engineering endorsements that are going on a lot of cyber policies. There are exclusions [00:10:00] certainly on a lot of the cyber policies for business email compromises. So, it depends on what the policy is going to cover or not cover from an underwriter standpoint and from the client's standpoint on what they're making the claim for. We've seen some where there is coverage, some where there's not coverage and certainly somewhere there's reservation of rights letters that go out and there's a real issue as to coverage.

Last month, or just towards the end of the month or maybe the beginning of this month, there was an interesting case that came out. I believe it was down in Alabama. It was a federal court decision down there where a law firm had a fraudulent client. The client contacted the law firm, and it was a threat actor, so to speak, [who] claimed that he needed to retain them to recover a debt. Signed an engagement letter and then the law firm went out and sent some letters, I assume, to the company that supposedly owed the debt and ended up getting money in return to cover the debt. But the company that they were getting the check from was fraudulent [00:11:00] as well, so there was fraud on both parts.

What the fraudsters did was they told the law firm, "Take out your funds and then just send me a check for the remainder." A check for about $150,000 was then sent to this fraudulent client. And after that check was sent out, later the initial check that the law firm received from the supposed company that the debt was being received from bounced. They had no money from that fraudulent client, and now they have just sent out a check to a fraudulent client themselves. There was fraud on both sides.

[In] the courts the claim was denied, saying that "You needed at least one valid client to have some sort of social engineering under the definitions in the policy." It was a little strange. I was surprised about it, but at the end of the day, the courts upheld that and said, "Yeah, under the definitions in the policy, the social engineering endorsement didn't cover this loss."

The law firm was out, I think it was about $150,000. Not a huge sum in the grand scheme of the cyber fraud [00:12:00] that we see. But certainly, if it can happen for that, it could happen for more. It's something to be aware of that any

time you're dealing with wire transfers, ACH transfers, et cetera, phone calls have to be made. [You] really have to ensure that you have the right people and the real people involved in the case before you just start sending wire transfer information or sending checks, in this case, to people that you've never spoken to. It sounded like it read that there was maybe one phone call but everything else was obviously just done on email and letters. Those are some of the big issues that we see a lot that I think are in the news a lot.

The other issue, as I said, which we are going to have Ryan talk a little bit about, is the SEC and this amended Reg SP which kind of puts a little more teeth into the reporting of breaches involving financial institutions and the policies and procedures that they have to comply with. Ryan, maybe you could just give us a rundown of what that is and how you're seeing it going into effect in the last few months.

Ryan Friel: Yeah. Dave, as I mentioned, last time you and I spoke [00:14:00] about amended Reg SP it had not gone into effect at that point. For larger financial institutions regulated by the SEC, the compliance deadline was December 3rd of 2025. For smaller entities, their compliance deadline is upcoming, on June 3rd, 2026.

To get back to basics, Regulation S-P was first implemented in 2000 and was not updated for close to 25 years. Regulation S-P is basically the financial industry's privacy role. It governs how financial institutions handle customer, non-public personal information. Its focus is on safeguarding customer data and providing privacy notices. It applies to broker dealers, registered investment advisors, registered investment companies, and transfer agents.

Obviously that 25-year gap between implementation and updating, Regulation S-P had not kept up with modern [00:15:00] cybersecurity threats. That's really what the amendments were designed to do. It's really recognzed, Dave, that data breaches are no longer hypothetical, they're inevitable. As you mentioned, across law firms the same things are happening across financial institutions, whether it's cyber attacks, ransomware, or just other unauthorized access [to] sensitive financial data. The compromise of such data is just a routine risk for financial institutions.

So amended Reg SP really just brought financial institutions closer in line with current expectations for incident response and data protection across the states and across other industries. I would say [of] the big changes, or the big amendments, the first would be that amended Reg SP requires mandatory incident response programs. In the registered investment advisor space, in the

broker dealer space and in the compliance requirements for those entities, they're now required to adopt written [00:16:00] policies and procedures designed to detect, respond and recover from unauthorized access to customer information.

While most firms likely had such policies in place already, now they're required to have such policies. Now those policies are enforceable by the regulators.

David Shannon: It would seem to me that a larger financial institution, or even a mid-size, is going to have all that. The same with law firms. The bigger you are, the more of a data security group or committee somebody has to get all that done.

I would think [for] these smaller broker dealers, the one or two-or-three-person shop, are they really dealing with cybersecurity and setting up policies and procedures? Those are the ones, because they don't have the best security, they're the ones that we see sometimes have the data breaches . When you come in, you see they don't have any real policy in place.

What happens if they don't have them in place? Are there some substantial fines? How's that going to be handled by the SEC or some other financial regulator?

Ryan Friel: Yeah, I think you're right, Dave. [00:17:00] I think that the larger entities that are already in compliance as of, or had, the required compliance deadline of December 3rd, 2025--. I think meeting that compliance deadline was probably easier for those entities.

[For]the smaller entities, as you mentioned the ones with the compliance deadline of June 3rd, 2026, this is going to be a significant undertaking for them. Partly because they probably don't have the procedures in place, but also because they don't have the information technology tools and the cyber security tools already in place to really protect customer data. So, this is going to be a significant ramp up period for them. We're talking about compliance in less than two months from today. Yeah, this is going to be a big change for them.

I can tell you that as a former regulator at FINRA, the first thing we do on any examination [and] the first thing the SEC is going to do on any examination is they're going to ask the financial institution for their policies.[00:18:00] That's where they're going to start. Does the firm have them? Obviously, the SEC or FINRA will expect to see a formal written incident response program. Does it align with amended Reg SP? Does it define customer information consistent

with the rule? Does it provide a requirement to provide notification to customers within 30 days?

Secondarily, the SEC or FINRA or any regulators are going to ask to see whether the financial institution is actually following their procedures, whether they're implementing them. Obviously, if the entity has had a data breach, a ransomware attack or some other event, that's going to be prioritized on the examination.

I think the low hanging fruit for these first rounds of SEC exams, particularly if there was a cyber incident, is whether the financial institution was able to comply with the 30-day deadline. That seems to me to be the most obvious place to look for any regulator. The 30-day deadline is a hard deadline now. That's a big shift from what the [00:19:00] original Regulation S-P required. It's basically just the mandate that if there's a breach involving sensitive customer information [you] first must notify effective individuals as soon as practical, but no later than 30 days after becoming aware of the incident.

As you know, Dave, that can be a tough deadline to meet under any circumstance. I've been discussing with my clients the necessity to quickly identify a breach [and] contact counsel or contact a forensic IT team so that the process of determining whether customer information has been compromised is sort of at the forefront of their breach response program so that we can try to meet that 30-day deadline.

David Shannon: Right. Yeah, it seems to me, if we can, obviously we're going to document why and show good faith reasons, et cetera, that you would show in a non-financial advisor breach.

Yeah, you're [00:20:00] right. When you have that 30-day deadline, and particularly if you have a ransomware attack, it's going to be a real problem to meet that in some circumstances. I think you're going to have to document it fully as to why you couldn't and how you did everything practical to get it out as soon as you could, under the circumstances.

Ryan Friel: Yeah. The other big change with amended Reg SP [is] it expands the scope of customer information [and] how it's defined and it brings more data under the rule. That’s an important aspect of it.

I think, finally, amended Reg SP requires that financial institutions provide service provider oversight. So, anything that they outsource, like third party vendors managing email or managing financials, IT consultants, anyone like

that [or] anything that they outsource away from the financial institution, they have to maintain appropriate safeguards on those entities. They can't just outsource the risk.

David Shannon: Right.

Ryan Friel: Under amended Reg SP.

David Shannon: Yeah, it makes sense. And then it just seems to me that it's just [00:21:00] one more layer for underwriters to take a look at when they're reviewing a potential company for underwriting. Do they have all these policies and procedures now? If they don't have the proper oversight of their vendors and all that, it gives you a red flag that this is a potential real risk for underwriting this company if they're not complying with the SEC regs, which are now laid out fully for all these companies to do.

I think besides the data breach response that we would be dealing with, it's on the beginning side for the underwriters to be able to go in. It's almost like a checklist now. "Alright, you're a financial advisor, you're a broker dealer. You're required under the, under this reg to have all this stuff. Show us that you have it." [This is] no different than, say, a medical provider being able to show what they have to be fully compliant under HIPPA/ HITECH.

Ryan Friel: Yeah, I agree. The other thing I would note is particularly in the independent broker dealer space I've already run into issues where the broker dealer or the individual [00:22:00] is duly registered with FINRA and the SEC. In those scenarios, the data compromised can be both the data of the registered investment advisor as well as the broker dealer. So, you can have many voices at the table trying to determine how to comply with amended Reg. SP.

That's certainly going to be an issue as the small financial institution deadline comes into compliance in June. How is data that an investment advisor and a broker dealer both have, both can lay a claim to, how are they going to deal with all the voices at the table when trying to comply with this rule?

David Shannon: Which always makes it more fun for us, trying to figure out who's in charge.

Ryan Friel: Exactly.

David Shannon: It's great to hear, Ryan, that at least we know what we have to look for now when we have one of these companies come in as an initial call or

initial meeting with a financial advisor. [This] lets us know these are the things we've got to deal with right away.

We'll see how it starts to play out, particularly [00:23:00] after the summer when everybody has to start having this compliance, no matter how big or small you are.

Ryan Friel: Yeah, it should be fun, Dave.

David Shannon: Alright. Alright, I think that is it for us today. As always, if anybody has any questions or comments about anything we talked about, feel free to give us a call or shoot us an email at our law firm.

We're always happy to talk to anybody about these issues. We hope we're able to give you a little insight into a couple of different things, whether it be legal or financial, regarding the cybersecurity field. Thanks very much.

PLUS Staff: Thank you for listening to this PLUS podcast. If you have any ideas for a future PLUS podcast, please complete the Content Idea Form on the PLUS website.