Managing Cybersecurity Threats in 2025 Episode 2

[00:00:00]

PLUS Staff: Thank you for listening to this PLUS podcast, Managing Cybersecurity Threats in 2025. 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'm pleased to turn it over to David Shannon.

David Shannon: Thank you Tyla. Yes, as Tyla said this is David Shannon. For those of you who don't know me or might be listening in for the first time, I chair the Privacy & Data Security group at Marshall Dennehey, we're an insurance defense law firm, based out of Philadelphia.

We have a large practice, obviously, like a lot of firms do now for cyber-related matters. And this is our last podcast of the year with PLUS. And I'm really pleased to have Billy Cordio from Surefire Cyber with us. And I'll let Billy introduce himself and then we're [00:01:00] going to talk a little bit about the differences between remediation and a forensic investigation and why they're so important, not only the investigation, but the remediation that's going to happen afterwards. So, Billy, why don't you say hi to everybody and give them a little bit of your background.

Billy Cordio: Absolutely. Thank you.

So, my name's Billy Cordio, Director of Incident Response here at Surefire Cyber. I do an engagement lead type of role, right?

So, I help facilitate the first call all the way to the last call that we have with clients. I'm a key coordinator for restoration and forensics. We obviously want to run those in tandem, so we just want to make sure everything's moving smoothly. My industry knowledge comes from about 15 years of technology and cybersecurity, a digital forensic world for the last about seven years.

And so just helping clients, like I said, kind of deal with the worst business days that they're probably dealing with and get through them.

David Shannon: That sounds great, Billy. Thanks for being with us here today. And as I said, and you were just mentioning, when a cyber event happens [00:02:00] for one of the businesses that might be listening or for the insureds, for the underwriters and claims individuals that are listening, you know, we immediately kind of jump in and have an incident response scoping call, and then we start with the incident response investigation.

Why don't you explain though, what's the difference, you know, from the way Surefire Cyber sees it, as for the incident response and then the remediation, and kind of how they can go hand in hand or be a little bit different depending on the circumstances?

Billy Cordio: Yeah, absolutely. So, from Surefire Cyber's perspective, we're one of the firms in the industry that run forensics and restoration in tandem.

You have a lot of firms that just do forensics, a lot of firms that do restoration, and sometimes one of those two will pause the other. Obviously in our world we want to end business interruptions. That's usually the biggest cost of these types of investigations and incidents, and so the fact that we can run everything [00:03:00] in parallel helps obviously speed up that business interruption piece and get critical systems back online sooner than if you have two separate firms kind of involved.

David Shannon: So, when you guys come in, are you looking for that right away, or does it just really depend on the circumstances, which I think it probably does, as to what you have to do first or what you're going to do in tandem? And how does that work – are you having the same groups or are you going to have separate groups that handle each phase of that?

Let the underwriters and the claims professionals that might be listening understand how you guys come in, and what you're looking for, and then how you set it up.

Billy Cordio: Yeah, absolutely. So as far as the incident type, I think that kind of dictates what groups are involved and how we approach it, right.

If it's a ransomware event, our team's going to be involved. It's going to be restoration immediately, usually day zero. After that, forensics gets involved pretty quickly there. Once we start to see systems come to a point where we can

start bringing them [00:04:00] back into production if we have pre-ransomware cases, right, so some type of malware incident or something that was detected early on, our forensic team gets involved way quicker, usually day one as well, because they obviously have a lot more to figure out and try to determine right off the bat. So, the clear difference or sometimes what we do is what we call quarantine network.

So, we're going to lock everything down coming in and out of that network. And that's really where the time crunch comes in. When it's ransomware, a little less critical just because everything is down, right. And now we have to start bringing things back up. But if it's pre-ransomware, we want to push through as quickly as we can to get those guys running.

And so, a lot more forensic work needs to happen immediately to determine root point of compromise and what type of back doors, what type of malware may exist in that environment so that nothing bad further happens as the network relief starts to come back into play.

David Shannon: Gotcha. [00:05:00] And what do you see when you come in?

What's a big help for you from, say the businesses, you know, the insureds that the underwriters and the claims guys here are working for, you know, are there some things that you're like, “Hey, this is great they have it set up this way.” Or that they understand their system better?

What makes it a little easier for you to get right in there and start restoring as soon as you're engaged?

Billy Cordio: Yeah. So, one of the biggest things I do is coach clients through is going to be is the MSP IT, right. When you have an internal team, they often want to be involved, but a lot of those IT guys and MSP guys, like they aren't dealing with broken things, right.

That's kind of the glory of what we do. Those guys are maintaining the systems, right. They're keeping them running smoothly. They're making sure that updates are happening and everything is in a production state, right. Things aren't broken. What we're doing is kind of a crash fix, right.

Everything is broken. [00:06:00] I've told a lot of people in this industry, in the recovery side of it, that in terms of what they can do to make things worse is just don't delete things. That's about the only piece that can make things worse from our perspective because everything is already broken. And so, often times

when you have an incident response recovery team involved, you have broken things and we're just fixing them, getting them back into state, but also securing them.

And that's where that forensic piece plays into it, right. We don't want to just restore a client and have them up and running. But they can have the same threat actor come back in two days later, three days later, and do the same exact attack, right. We have to run that forensic investigation in tandem so that way we make sure that they're secure.

VPN, MFA, right. One of those configuration pieces that MSPs may not be keen to or may have misconfigured, right. And those are the pieces that we will look at in detail because those are [00:07:00] the specifics that we learn from the industry as we do see these ransomware events and pre ransomware events day in and day out.

David Shannon: Right, you mentioned something there that I always find important too, is that it seems like when a forensic team gets involved, that's one of the first things they want to know is what they can look at. And when they hear that stuff's been deleted, that's a real problem, right? These businesses think, “oh, let's just delete everything, get the threat actor out of there.”

But then it leaves you guys in a real bind, right? Because you don't have the information, so to speak, to be able to investigate, figure out what happened, and also figure out how you're going to restore stuff in a safe way, right?

Billy Cordio: Absolutely, right. At that point, we're just more implementing best practices and security measures that we get from day in and day out of dealing with the same groups.

But obviously, there are new tricks that come out between these groups every other week that if that forensic evidence is deleted, it makes it a lot harder to keep you guys protected. So, yes, [00:08:00] making sure that they don't delete is a big piece of allowing the forensic team to do their valuable work.

David Shannon: I know it obviously depends on, you know, the business and the amount of systems they have, et cetera. But how long do you guys see on average, say, for small, mid, large businesses to get them back up restored and running? You know, is there any kind of timeline that you're trying to work on for each of them, or is it really just, you know, case specific as to the amount of work that needs to be done depending on the systems?

Billy Cordio: I wouldn't say it's case specific, but it's very situational. And what I mean by that is, "Are there backups?" That's usually the biggest piece that separates the people that are going to be running in day two, day three, versus people that are going to be running day seven to day ten. If we have backups to work off of, that is the kind of big piece that we can restore and get things running quickly with a forensic investigation on top of it, right. As we do those restorations, [00:09:00] we have a forensic team come in that sweeps machines to make sure that there's no back doors, there's no underlying malware that's going to be repeating the same incident. Now if you have a decryption, right.

If they have encrypted systems and deleted backups, that is the long-term one that unfortunately we can try and get things out as operational as possible, but it's very situational depending on what type of encryption they have, how they were impacted, and more importantly, how the business can operate without systems, right.

Some businesses, like a manufacturing plant, we see they're able to keep producing things that are pretty standardized. They can just continue to run their productions, whereas if it's a law firm, they have files and file systems they need access to immediately.

David Shannon: What are you seeing when say you've had, you know, a ransomware attack and I know more and more people are not paying the ransom, which we all think is great, [00:10:00] but when you are having cases where the ransom is being paid and you're getting the de-encryption key, what are the differences there then on how you're restoring and remediating as opposed to when you're just going in and getting the backups up and running?

Billy Cordio: Yeah, so, when you have to have a decryption key, it's always advised that you don't decrypt without a backup. And what I mean by that is we are taking a copy of your encrypted extinct to make sure that if things go wrong, we have a reverse method to get back to at least where you were when you were encrypted.

Oddly enough, these threat actors will help troubleshoot those decryption tools if they don't work correctly, which is just odd to say, right. You wouldn't expect tech support, but you do get tech support here and there. But that is one of the biggest time crunches sometimes coming into play, is that I now have to make a copy.

And when you have terabytes of data, those copies can take two, three, four days before they're even in a state that it's ready to [00:11:00] do a decryption.

David Shannon: Yeah. That I think is the issue, when the businesses want to pay because they have to, they kind of expect, “oh, well we can just, you know, have the insurance carrier write a check, so to speak, um, the next day.”

And then, you know, you get the key and they're up. But it takes a lot longer than that, obviously. So, what you're saying is you have to get everything backed up first, then you're going to get the key and try and go in there and de-encrypt at that stage, right?

So, it's not something that's done in a 24-48 hour period.

Billy Cordio: No, absolutely not. Decryption is not a magic wand. It's not like you can run a decryption tool. And weirdly enough, like encryption process usually runs, oh, I would say five to ten times faster than an actual decryption process. And then when you decrypt, you still have those underlying threats, right.

There still could be an encryption malware somewhere, there could be backdoor somewhere. And so, you still have to perform that forensic investigation. So almost [00:12:00] always that decryption method is going to take a lot longer than if there's file backups.

David Shannon: Yeah. And what have you seen lately with the de-encryption keys that you're getting?

You know, are they reliable now? That's always been the concern - that you're going to get a de-encryption key and the client asks you, “Well, does this mean that we're going to get everything up, not an issue?” And you have to let them know, “Hey, we're dealing with criminals. We can't guarantee anything. We can just give you our experience.”

And like, we would go to you and have Surefire Cyber say, “Here's our experience with, you know, Qilin or Akira or something like that and tell you these are the percentages as to what we think will happen if we get the key from them.”

Where is that right now? Is it mostly good encryption keys, you know, you could say, or are you still having some problems with some of the cases?

Billy Cordio: For the most part, I think it's gotten really well that the more known groups, uh, the Akira’s, the Qilin’s, those groups, those are the ones [00:13:00] that have viable and reliable decryption.

Usually the only ones that we will see problems with when it comes to those bigger groups that have good tooling is going to be tied to databases. That's always the one tricky piece. And that's not necessarily because they're not decrypting, it's just because of the interruption process that happens, right.

Like when you think of a SQL database, they have to be shut down in a very specific manner and they're usually not right. Those threat actors are just terminating processes, so there's a lot of corruption that happens there. So that's usually the one piece that sometimes we'll see some bad encryption or bad decryption happen.

Outside of that, the unknown groups, the newer groups, those are the ones that can be a little bit unreliable as well. And there's just, as you said, it's not a guarantee ever that you're going to actually get decryption that is very successful.

Usually though it's about 95-98%, somewhere in that range that most of your data will come back. [00:14:00]

David Shannon: Oh, that's good to hear because the clients always want to have some kind of percentage or some kind of guarantee, or at least you're telling them what you think's going to happen.

So, we're always kind of covering ourselves a little bit, as you said, you have to let them know you're going to have corruption, et cetera. You know, I was just thinking, Billy, as we're getting close to the holidays, when people are going to hear this, what do you guys see? Over the holiday period, do you see a substantial increase in attacks?

You know, the threat actor's thinking people are on vacation, they're not following, what's going on as much. Are you able to say, “Hey, yeah, we're going to see a 10%, a 15%, or even more increase in the ransomware attacks, over that December time period when everybody's, you know, not, not working as much. It might not catch everything as quickly.”

Billy Cordio: Yeah. So, Thanksgiving I think is a kind of a bigger holiday that we normally see attacks on. So probably Monday of next week, since we're recording this right before Thanksgiving, you're [00:15:00] going to see a lot more influx of people reporting these attacks.

They absolutely attack in early mornings - usually, 2:00, 3:00 AM is when those attacks happen, or on holidays, that is a very prominent piece that we do see.

Now, the weird one is Christmas. Christmas doesn't normally see a huge influx after Christmas. It's usually before, and that's because of a lot of, weirdly enough to say, it's like it shuts down from like Christmas to mid-January.

It's one of the slower parts of our season, and a lot of that ties to the Christmas spirit and just that kind of holiday. But usually right before Christmas, we'll see a little bit of an influx, and then mid-January is when it starts to get busy again. But yeah, between Christmas and mid-January it slows down.

David Shannon: Yeah, it is interesting. I guess, you know, you probably, without having stats, think, well maybe in Eastern Europe and in Russia, you know, they're celebrating the Christmas holidays too, so they're all going on vacation for a [00:16:00] couple weeks. And which just kind of shows, you know, how they're run like a business like everybody else now.

So let me just ask you this Bill, just to tie it all up there at the end, so to speak. So, the remediation is something that maybe the insurers aren't thinking about right away. Not thinking, "Hey, we're going to have to do all this. We just got to get the forensics done."

But the best way to kind of attack it is to have you guys come in and you're doing both at the same time, right? And you're having the same company, you know, that's going to handle both, and you can kind of work together and then see what problems occur and you can handle them. On both sides, both the forensic and the recovery to make sure it goes as quickly and as efficiently as possible, right?

Billy Cordio: Absolutely. The communication from our internal teams, between our restoration side and our forensic side really helps step up and push that process of getting clients running quickly. And so, the fact that we can coordinate, "Hey, we have a triage that was delivered. Immediately, we need this cleared as soon as possible."

You lose [00:17:00] out of the time of having to send emails or having to contact another business and trying to get things prioritized. Whereas, when you have a firm that has both of them internally, you don't generally have that miss of timing. You have people that once again work in parallel. There are firms that go out there and won't start doing restoration until a forensic investigation's done.

And sometimes forensics can take three or four weeks, right. Like the thought of a business being down three to four weeks is kind of crazy in today's standards.

And so, you're often better off with a firm that is going to run in parallel, right. And that's where kind of the historical information that we know because we do this day in and day out really plays to our advantage. If it's a group that we see every day, we probably know that root point of compromise before we're even on that scoping call to discuss with you guys what happened because it's so standardized right now that these groups just constantly abuse the [00:18:00] same metrics over and over.

David Shannon: Yeah, it does seem like that, you know, I'll get a on a call with you guys and, and you'll know right away now, depending on the threat actor, more than likely, how they got in, what the weakness is, what they would've taken, and what you're going to have to do to get the company back online.

And that is, you know, I would let everyone know that is really comforting when you have that experience and you can kind of just go to one company, one firm, and they're jumping on everything right away for you and get everybody moving. And the client really appreciates that too, because they're not having different people giving them, you know, different instructions and questions from different people as well.

So, I appreciate it, Billy. Yeah, so Tyla, I think that's it. And to everybody out there, if you have any questions, certainly feel free to reach out to Billy at Surefire Cyber or myself at Marshall Dennehey. I've worked with Billy and his team a lot. They do a great job and I'm really glad that he was able to come in here and give us this advice as we finish out the year.

So, thanks again, Bill. I appreciate it. [00:19:00]

Billy Cordio: No, absolutely. Thank you for having me.

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