Managing Cybersecurity Threats in 2024 S2 E1

PLUS Staff: [00:00:00] Welcome to this PLUS podcast, Managing Cybersecurity Threats in 2024, Season 2 Episode 1.

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. And now, I'd like to turn it over to David to get us started.

David Shannon: Thank you, Tyla. Good morning, everybody. Great to be back here talking to you in 2024. We had a number of podcasts last year. I think we got some great responses from it and I'm happy to be doing this with PLUS again this year. As we're sitting here at the beginning of the year, we'll talk a little bit about what we've seen as the year starts, and then how we think that'll play out as the year goes forward.

For all the first-time listeners, I'm David Shannon. I'm a partner at Marshall Dennehey in Philadelphia and I chair our privacy group. We handle incident response, class action suits, pretty much everything you can do with data breaches and data [00:01:00] security. I've been doing it for well over a dozen years, and I'm really happy to have with me today, Steve Ramey, who's a forensic investigator at IronGate Security, which is a new great company that's handling forensic work. I'll let Steve introduce himself and let you hear a little bit about what IronGate is doing these days. Go ahead, Steve.

Stephen Ramey: Thanks, David. Thanks for having me on the show today.

It certainly is a pleasure to talk about such great topics here on the cybersecurity spectrum. IronGate itself is a cybersecurity company that provides professional services for both proactive and reactive cyber services. Proactive to help set up programs, to assess the programs, test the effectiveness of those security controls.

As well as reactive to investigate the anomalies that occur as we deploy technology within our environment, we've seen a lot across our lifetime of ransomware and it's great to be able to give back through IronGate to

organizations of all sizes, both large [00:02:00] and small to help with these complex cyber services.

David Shannon: Yeah, thanks, Steve. I've known Steve for a number of years, worked with him on a number of cases or incidents and hopefully always had a positive outcome is the way we look at it at the end of the day. I'm really glad that he was able to join us today. As Steve just mentioned, ransomware continues to be a huge issue in cyber.

I still think that's the biggest thing we're dealing with now in the privacy field when it comes to cybersecurity, when it comes to cyber insurance and then into incident response. I've seen a number of them, obviously this week, last week, and all of last month, just to start the year.

I was reading a little bit about what some other carriers and forensic teams have seen as well. It was interesting, I read one article that was saying that January 2024 was a little lower than it was last January in 2023, which they attributed to the holidays just like us here in the United States.

They're celebrating the new year in some of the countries where we see a lot of the threat actors coming from, as well [00:03:00] as the Orthodox Christian holidays as well, which can affect that, which was an interesting point I hadn't fully thought through until they brought that up. But I did see a number of cases come in with ransomware that we've got from a number of different carriers over the past, say, five to six weeks of the new year.

My take on it and reading a few things is we're still seeing the same groups that we were seeing towards the end of 2023, LockBit, ALPHV/Blackcat, even with the FBI crackdown last year, and Akira is another one we saw last year that is coming forward again this year as well.

All three of them, I would point out when I talk to individuals, is they all exfiltrate data. They pretty much all have leak sites where they post data that they've taken. Some of them will do double, even triple extortion, whether it's for the data, or whether they're going to do some denial of service attacks, or whether they're going to go after your own clients.

But they really seem to be the three main ones that don't go away. It's [00:04:00] 2024, ALPHV/Blackcat's been out for, what, three years now? You now see LockBit 3.0. We've seen that on some cases where when we start talking to the forensic investigators, that's the phrase they're using for this version of LockBit that we're seeing.

And I've also seen pretty much the demands for the smaller ones are in that, $250,000 to $500,000, if it's a smaller company, a smaller entity. Pretty standard there. What I've gotten from the forensic investigators is, yeah, those are the numbers that they're seeing as well.

And working on a couple right now that are right in that range. So I think you're really seeing a continuation of what we saw in 2023, and you're even seeing with, say, Black Cat, that while they had some issues when the FBI came down on them in the middle of last year, they're back up and running, and it's a different kind of ransomware for service, but it still goes back to the same original entity.

So that's what I've been seeing, say, in the last five, six weeks. Steve, what do you think? Any points that you would [00:05:00] hit on those issues when it comes to ransomware and what you guys have seen as the new year has started?

Stephen Ramey: Yeah, David, spot on with those Akira, LockBit, and Black Cat.

To add to that, we've recently seen Medusa pop back up. We've also seen some activity from Snatch. All of which, the demands have been higher for those different groups comparative to last year. And what's interesting, what I think is actually driving the higher demands for these ransoms, is that businesses are getting smarter, right?

We've had since last year, actually since about two years ago, cyber insurance to qualify for that you need stronger controls. So, I think cyber insurance is pushing these businesses to be smarter. They then turn, take steps to implement these controls. And so, when they actually do get broken into, they get attacked, they're able to recover.

And so, they don't need to rely on paying for the decryptor to get back to their files, they can actually go to backups. So, there's a lot less businesses paying these groups, which in turn, by demand and those laws of [00:06:00] economics, you have to increase your price point to be able to keep your business afloat.

So, I think that's what's a lot of driving there, but, from a tactic standpoint, really, you know, these groups, while they might hit you with a five or six figure or seven figure ransom demand, at the end of the day, they do want to get paid. And so those that do take the time to negotiate with them, we do see a drop in price anywhere from 10 to 40 percent from that initial sticker.

For those that do have to pay, there is sometimes wiggle room with that initial ransom amount.

David Shannon: Yeah, I think so, too. And in some respects, I've seen a few where the client has said, “we have to get up as fast as possible.” It's just, there's no way that we can continue if we can't find some way to get their data back.

And then you're negotiating in a different way to pay more quickly. But I think you're right, Steve. I've seen that too, in that the companies that can get up in some respects with some backup, but may still have to pay for others, [00:07:00] because they still need the full data returns. If they're patient, they are going to see the number come down.

They'll hold steady for a while. I have one right now. They are holding incredibly steady on it. It's been surprising on that number. But you do see them come down. And, as I always say to my clients, we talked to you, Steve or whoever the forensic investigator is and have to let you let us know what you think about, the specific threat actors and what your numbers show and the data that you're collecting.

That's one of the reasons I always, point out to the claim professionals, the underwriters or the client, besides just being able to help negotiate the forensic groups can really give you an idea of what the game plan is going to be using your numbers and your stats as to where do we want to end up?

It’s like any other negotiation you would have in a settlement of a legal case. It's where do you want to end up? What's your pain point? What can you pay? And another point, I was making a note I wanted to mention, you know for the underwriters that are listening, [00:08:00] hopefully a lot of them, is really hammering to the clients that they've got to get that cyber insurance policy and make sure that they're properly covered for cyber extortion.

I see that with a lot of smaller entities where, you know, for lack of a better term, they're nickel and diming their cyber policy, and they can say they have one. But when you get into it, they get hit by a ransomware attack, which they never ever thought they would because of the kind of business they are, the size that they are, and then they don't have coverage for the extortion.

And that becomes a huge problem. Are they going to be able to pay it themselves? Or what are they going to do? Even though in a strange sense, they have the forensics under the policy for the first party, but they don't have cyber extortion, or they have a small sublimit for it. And that really causes, you know,

some issues obviously when you're trying to bring this client back online, whether either paying or at least attempting to do some negotiations.

So, something that I really hit all of my clients with is look at that policy and [00:09:00] how can you increase it? Because without it, you really have a problem. Particularly with regard to the Managed Service Providers (MSPs). Those are the cases that I think are really the tough ones to deal with now.

These managed service providers have so many clients themselves. If the threat actor is able to get in and encrypt their data it becomes a huge problem obviously, with just so many people who are screaming to get their data back online. And if there isn't a really good policy for that MSP, that can become a real problem.

And it's surprising how many of these MSPs, in my opinion, don't have enough insurance, even though they have so much data. So, I really think for the underwriters, that's something to look at. You really have to dig down. Your client, if it's an MSP, how many clients do they have? How much personal data do they have?

And what's their security? If someone's going to get into MSP A, what's that going to lead to? [00:10:00] Do they have the proper security to really keep it segregated from their clients? In my instance, obviously the reason I'm getting these cases, is they don't. And it becomes a big problem trying to deal with that.

And figuring out how you're going to pay a ransom when it's so much higher because of all the entities that are now involved. Steve, what do you guys see when you're dealing with an MSP and how are you dealing with those issues?

Stephen Ramey: It's an interesting perspective when we talk about MSPs or even taking a step back and looking at that hub and spoke, right?

Who are the data aggregators? MoveIt is a great example, in the middle of last year when that software was popped. As we think about our providers into our businesses who allow us to generate revenue, share information with our partners, our customers, and clients. We put a lot of trust in them.

That trust manifests in many different ways. We trust MoveIT to be able to keep us up, keep our data active and available so that we can share information as we need to. When we look at an MSP, we look at them [00:11:00] and trust them to keep our systems up, available, so we can conduct business, and keep our operations moving.

And one of the challenges that I've seen across this kind of MSP attack surface, even with businesses that use the cloud and rely on the cloud to store and back up their data is they say, “yes, my MSP is backing my data,” or “my data is being backed up to the cloud. And yes, I can recover. I have availability in the cloud to recover down to my on-prem systems.”

Nobody actually takes a look at and scrutinizes, how quickly can you concurrently restore your data? So, when you look at an MSP, say they have 1,000 clients, how many personnel do they have to service all 1,000 clients if all 1,000 clients go down at the same time?

Does the MSP actually have a IR plan to prioritize which clients have to be up and running? Are any healthcare? Are any in critical services or critical infrastructure? [00:12:00] Do they have that type of response plan? And then getting into the data piece of this, if there's 1,000 clients, how many servers do they each have?

How can they concurrently restore all that data at the same time to get those clients back up and running? Same thing when businesses have their backups in the cloud. It's less of an MSP, but it's still a managed service. Someone else is managing that infrastructure, but really that business is bottlenecked with their ability to download.

And you might have 10 terabytes of data stored in the cloud, that's available, that can be restored to your systems. But your ISP may limit how much download capacity you have. So, when you think about the 10 servers, those 10 terabytes need to restore to, you might be able to do only one at one time, and it may take five hours per system to get all that data back downloaded. Same thing with the MSP calculation. So, as you scrutinize from an underwriting application, MSPs and you look at their ability to [00:13:00] protect their customers information, we also have to consider the catastrophic situation that, yes, they will be breached. Yes, data will be affected.

Yes, data will need to be restored. We have to then take that one step further. How soon will all or a large majority of those accounts be restored and active? So that those end users can be back up and running, performing their business. That last step there, I haven't seen it taken into account often when we start talking about the availability of backups.

Taking that a step further, how soon can we get all these backups restored if all of our clients go down?

David Shannon: Yeah, I think you're absolutely right, Steve. I'm aware of a situation right now we're handling where a smaller MSP that just doesn't have the bandwidth, so to speak, to get everybody back up and running that quickly.

And then it's who are you going to prioritize? Which servers are you bringing up? How long is it going to take for each one? And it became a real issue. In the beginning [00:14:00] everyone thought, "okay, if we pay the ransom, we get to the encryptor and boom, we're all back up and running."

And it quickly became apparent no, that wasn't the situation because there's some limits with that client. And as the attorney, I don't always know how to ask those questions to start at the beginning. So, you must be careful when you're going to tell people that their data will be back, available, and back up and running.

And an eye-opener when you have that smaller MSP, that they start talking bandwidth and servers, as you said, and how fast they're going to move, and before you know it, just having the de-encryption key isn't enough. It's how are you going to handle getting everything going, getting it all off backups, getting it up so that everybody can get their data back.

And how long is that going to take each day? So, I think you make a really good point that there's more than just dealing with, getting either the data from the backups available or getting the de-encryption key and getting backed up and running. It really depends on the size of the company. And I found that the [00:15:00] smaller companies are the toughest to handle just because they don't have that expertise there, whether it's in house or outsourced, and they just don't have the size and the security, so it leads to a lot of problems.

I always preach that if they could just have more limits, it would make everything a lot easier. So, I'm seeing the same as you, these three main ones, there's obviously a lot of other threat actors out there, smaller ones with the ransomware for service, you can go on and on with the names of them.

And from what I've seen over the last few months, the numbers are staying the same. We're seeing a lot of health care incidents, as well as law firms and some accountancy firms in the last month.

So, it's still the professional services and the health care that we're seeing get hit a lot. The same for you, Steve? Is that what you guys have been seeing for the last couple months now?

Stephen Ramey: We've been seeing all across the board all different types of professional services. [00:16:00] We've seen some businesses from the automotive industry.

So really, it's been across the board and it's, you know, what's interesting between kind of the ransomware and BEC attacks, it's all different security configurations that have allowed these threat actors to come in. Recently we're investigating an Akira attack that we think the ASA, an outdated ASA firewall, is the source.

It's ongoing, so we haven't had a full conclusion. But when we look at BECs, what's interesting there is these tenants that have been popped predate, 2019 and I think 2020 was about the time Microsoft said they hardened their configuration for newer tenants but, the ones that predated that date still had POP and IMAP.

Employees get phished and MFA is enabled, but because of those legacy protocols, the attackers are still able to gain access through those legacy back doors. So, really even though we've seen the top, same ones here, [00:17:00] we're still seeing a wide array of entry points that have attributed to some of these attacks.

Also to note there, I think about 30 percent of our clientele do not have a cyber insurance policy. So, when we get engaged, the questions we ask, “oh, we don't have cyber insurance.” And so, it's not a problem for us.

We treat them the same exact way, but it still brings into question, “hey, there's a whole world here that could help transfer this financial risk. We can certainly set you up with those contacts should you want to.” And it changes the tone of the conversation when you have cyber insurance. Primarily, we serve a lot of the clientele, the insureds, but when you're dealing with a company that doesn't have cyber insurance, it's a vastly different conversation.

So, you mentioned sub-limits earlier for organizations that don't have cyber insurance and they're paying out of pocket for a lot of these services, especially when there’s less than 100 employees. And so, it's a different conversation when it [00:18:00] comes to a lot of that.

Long winded way to say, you know what we're seeing, yes, I agree with what you're saying, but still, some of these old kind of legacy protocols are still causing a muck when it comes to points of entry.

David Shannon: Yeah, that's a good segue there, Steve, because I wanted to touch base just for our last few minutes on, BEC, business email compromise. We're still seeing a lot of those, too.

I was reading some articles in the last few weeks that said, yeah, about a third of them, if not more, are just simply employees opening up the phishing emails. And the MFA can help, but it's not bulletproof, or it doesn't make your system bulletproof.

You're seeing these well-known brands that they put in these emails, Microsoft, PayPal, things like that, and people start clicking on them. And I know we do a ton of training on that at my firm now. But when you multiply that by the tens of millions, hundreds of millions of people out there working, the threat actors are going to get [00:19:00] through, somebody's going to click on the attachment, and they get in the system.

And if they do that, enough, sooner or later they're going to get somebody to wire some money by mistake. One of the things that I read, and I actually had one recently, was the phone calls, too. We have one where they made the phone call to double check because they had not paid by ACH before.

And sure enough, they thought they were speaking to their vendor, but in fact, it was the threat actor. So, they're putting in a phony phone number there and don't realize that it's not the right number. They make the call. They think, "alright, I went the extra mile, I, made sure that this was good."

And then they don't find out for three or four weeks that the invoice was never paid. And then that becomes a problem, because, trying to, if there's a third party claim there, trying to decide who's at fault if you made the phone call, you can say, "I made the phone call." And they say, "yeah, but you called the wrong person, you called the threat actor."

But I've seen a lot of these lately, they're all small too, Steve. [00:20:00] One was $24,000, one $125,000. I'm just thinking off the top of my head in the last month, there was another one that was like $260,000. It's not like they're out there hitting big companies and getting a million dollars, wired, which I've seen as well.

But it's these smaller ones. It's just surprising that, for $24,000, they're going to set up this whole phishing email scam. It's something that the underwriters really need to explain to the insureds, that you may think you're small, that nobody's going to come after you.

But it happens, and it's happening a lot. And, in some respects, it's easier for them. Because people in these smaller businesses, their employees aren't as well trained, and they're the ones that are clicking on those phishing emails and setting this whole system up. Are you seeing the same thing too, Steve?

We're seeing some larger ones. Those are the ones you read about, but it's all these smaller ones, these BECs that are coming through our door.

Stephen Ramey: You're spot on there, David. We're seeing [00:21:00] lower five digits, a lot more five digits, a higher frequency of them. And I still think that these attackers are getting the paydays that they want.

And they're getting crafty, right? It's not that they just get into an email, and they act. They sit in there for a while. A week, two weeks, three weeks, and they watch the email traffic. They actually map out who's who in the organization. Who are the people that have the ability to control financial transfers?

Who's that conversation interacting with external to that organization, who these buyers are? So, at some point, they will flip. They will create rules on the inbox that divert all messages, mark as read, to a different folder that user typically will not access. Then at some point, the threat actor then inserts themselves into the thread as that user to then say, "hey, change the wire instructions. We need to have that information sent to this account. Here's all the information, .pdf certificate, all that."

And then, [00:22:00] unsuspectingly, the individuals, they wire it. Of our matters, we did have a very low percentage something south of 10 percent, where they were actually able to pick up on subtle cues in these conversations where it made them question.

And those individuals actually picked up the phone and made a phone call. So, they were able to catch it before those transactions occurred. And then, we get brought in, we do the investigation and help map it out. You touched on the phone call piece of this, and it's absolutely critical that businesses set up an offline Rolodex.

So, break the Rolodex out. We know from the 90s - use that as your offline address book so that you have everything you need. It can't be tampered with, and when you have any doubt, you go to that. That's your bat phone. You go to that. It has the actual number in there that you need to call.

Don't pull from the email body because that's going to be tampered with. You suspect there's foul play in this communication. Don't trust the information in there until you [00:23:00] verify it, including the phone numbers. Go to the phone number source that you trust from the paper, from your cell phone, from your Rolodex, whatever that offline repository is.

The second point to call out here, too, are deepfakes. If you follow Jason Rebholz he had a really good post today about a deepfake scam that occurred, and this is just going to get more pronounced. They're absolutely elaborate, very tricky, and it could be getting folks on a conference call like this, and you're actually talking to a deepfake that you can't tell.

And so that is going to open up the book for a brand-new set of tactics from these threat actors. We really have to scrutinize not just the content, but also how we store information securely offline. So, when we detect something, we can go to that and have a lot of trust and confidence that we're calling and talking to the correct individual.

David Shannon: Yeah, absolutely. I think that's a great point, Steve. And yeah, I do follow Jason, did not read him this morning. Usually, I hit up his posts on the [00:24:00] train, but didn't get there today. I'll take a look at it. But, yeah, I think those are a lot of great points and, appreciate Steve adding his insight to these.

I would think at the end of the podcast, you're thinking about what to take away is one, as I always say, limits, but two is to really push that smaller entities need to be aware of this as well as large ones. It's just more and more these smaller businesses, professional services are getting hit just as much, and it becomes just as big of a problem for them as it is for the large corporations that get hit.

And then we read about it in the paper. But if anybody has any questions, feel free to reach out to me or to Steve at any time. Hopefully we'll see everybody at some of the conferences in these upcoming months. And we look forward to doing another podcast in a few months and see where we are mid-year.

Steve, I really appreciate your participation. Thanks so much, and we'll talk to everybody soon.

Stephen Ramey: Thanks very much for having us, David. Take care now.

PLUS Staff: Thank you to our listeners for listening to this PLUS podcast. If you have ideas for a [00:25:00] future PLUS podcast, you can share those by completing the content idea form on the PLUS website.