Managing Cybersecurity Threats in 2023: Mid-Year Data Breach Trends Episode 3

PLUS Staff: [00:00:00] Welcome to this PLUS Podcast, Managing Cybersecurity Threats in 2023: Mid-Year Data Breach Trends, episode three. 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 to everybody. This is David Shannon. I'm a shareholder at Marshall Dennehey based out of the Philadelphia office. If you haven't listened to us before, I chair our firm's Privacy and Data Security group. I've been defending clients when they are faced with data breaches and data incidents probably for over 10 years now.

Today we're going to talk about mid-year data breach trends – what we've seen at this halfway point for 2023 and anything that might be a little bit different than the previous years. And then we will touch on what we might see before the year ends. With me today is Brendan McGann from Arete.

Brendan McGann: Yeah, so I'm an incident response lead here at Arete so, [00:01:00] I really kind of run a team of about eight to nine individuals who run into those open fires in incident response. Anything from ransomware attacks to insider threats and investigations such as that with the guidance of breach counsel-helping a client through kind of their worst potential day here.

David Shannon: Okay, great. Thanks, Brendan. And as I was saying we'll look at where things have gone so far in the first, say, six months of the year. I know there's been a few reports and memos, et cetera, that have gone out. I get all the emails from everybody telling us those things. And I think I actually got one from Arete yesterday, from Lynn.

If I was to say--someone's asked me, what do you see is the big thing this year? Brendan, what I would probably say is a lot of what we've seen, for example, the MOVEit breach, and anything similar to that, where we're seeing a lot of

breaches where they are exfiltrating the data and then contacting individuals, directly. Not going to the breached entity, with a ransom if they've encrypted it, but more just saying, “hey, we've got all your data and we're going to start contacting your clients or [00:02:00] your customers and tell them that all this data is going to be put up on the web.”

And boy, then they pressure you to pay, et cetera. How do you feel about that? Have you seen that a lot more this year? I think MOVEit is obviously the big one, but even beyond that, there's been a lot of other ones where I've seen that as well. What's been your kind of thoughts and what you've seen in the last six months?

Brendan McGann: Yeah, I think MOVEit really brought it to the forefront, brought it to everybody's attention. Just that potential to affect 400 organizations and over 20 million individuals. That breach was a really well orchestrated big event that took a lot of effort to pull off and only over a two-day span. But we have seen those step-ups of data exfiltration-only gangs coming to the forefront here. Things like Karakurt, BianLian-organizations, which are no longer going to do encryption. People are getting much more savvy with backups, immutable backups.

So, we're not looking at paying for the restoration of data, so much as sensitive data being prevented from leaked. We have seen that uptick for sure. I think [00:03:00] we've seen about a 45% uptick. Just a very quick kind of review of the cases I've seen in this year versus last year.

David Shannon: Yes, that was one of the things that I may have seen on one of your weekly reports from Arete – that the ransom demands have really increased, and the numbers that we’re seeing now are so much higher than even three or four years ago. I can even remember five years ago, when it first started, I was like, wow, I just paid $500,000 to some threat actor in Romania for all I know.,

So, the numbers have really gone up, but I think the stat that I was just alluding to is that the payments have really gone down because of, I think, as you mentioned, there is a lot better security, a lot better backups, so people aren't being forced to have to pay. I've obviously had some situations representing clients this year where they just say, “hey, we have to pay.” Last night I was on a call with a client and they're going to consider it.

It wasn't we have to pay it, but we're going to look at it and see what we want to do which is opposed to what we saw maybe in the last few [00:04:00] years.

Have you seen the same thing that those numbers have gone up, but the numbers of payments g have not gone up but have actually decreased.

Brendan McGann: So, I think if we look at the whole total number of data exfiltration only events versus data encryption events, the overall average has increased-just the market has become a little bit higher. We are seeing a bigger ability to decrease and talk- down those prices on those only data encryption events.

Because there's always that concern. And I think the market's always very sensitive. Look at Clop and what they put it in their ransom note. They actually have a written warranty about preventing the data leakage, whether anybody really believes these warranties is up to them.

But I think, yeah, that paying for data deletion is always a very sensitive topic for anybody.

David Shannon: one of the things I know when we talk to the clients is, and they'll ask about that, and was a specific question from the client last night on a call , "what guarantee can you give me that, we're going to get this key, and that we're going to be able to use it , and the Negotiator for paying the ransom was saying"

I can't guarantee you that you will get the key [00:05:00] I can tell you these are my percentages of getting a key from this specific threat actor, which was Lock Bit. We think with LockBit now being kind of as a service. We're not sure about getting the key, since you know do not know exactly who it is, but it was interesting, the client is asking the same questions as before.

Only now, it seems that companies like yourself have a lot better data. A lot better statistics that you're able to give clients that answer. For Lock Bit 83% of the time, we get the key, it's not a problem. Something like that. Is that something say with LockBit, are you seeing now more with ransomware as a service that it has affected the numbers this year that, you're not getting the keys as to oppose to that you normally would when it was just that one main entity threat group?

Brendan McGann: I think definitely with Lock Bit, but especially in my own experience just recently, there's a little bit of a breakdown in so far as, let's say customer service. I've seen multiple key events. I've seen events where I've had to go back and push back additional times for working decryptors.

I have an event right now personally that I'm [00:06:00] going back a third and a fourth time for functional decryptors, whereas before LockBit was a very easy to produce, decryption/encryption method-we knew that it was going to be efficient and fast. We're now seeing breakdowns there and it could be because either the affiliate or also it sounds like there may be some internal breakdown within LockBit itself.

David Shannon: And have you seen that, you use the word affiliate, have you seen that more in these last six months, that we're seeing a lot more affiliates? That it's become more of a service, as people say, as opposed to just specific groups that are doing the attacks and then encrypting for the ransom, but now they're basically selling that service so that others can see it?

Have you guys really seen that as an increase in the last six months?

Brendan McGann: I think we have, and I think the scary part about that is we never know who, and especially anytime we get into discussions, if it's strictly for intelligence gathering, or if we're going to go down that full path to decryption and proof of deletion, you never know who that other person on the other side of the keyboard is going to be. We could have somebody who's going to be very rational and easy to talk to or we could have a cowboy on the other side, and we can have somebody who's [00:07:00] going to be irrational and sporadic and it's going to drive that conversation either way.

So that kind of skews the percentages we have. I think we have to be sensitive as to, “hey, this is the average, but we never know who that other person is going to be.” Maybe they're having a bad day today and they're going to take it out on us. So, we have to be ahead of that.

David Shannon: Right. And I think, since we're talking about where are we six months into 2023, I think one of my takeaways would be it just seems to me that there's more affiliates, if you want to use that word, as you did.

I get that a lot, and I'm getting that from people like yourself when we're on the calls, or if we're on the call with Digital Mint or one of the other negotiators, is they are really talking more about the affiliates now, as opposed to in prior years, it was more the specific groups, and it really seems like they've broken up a bit.

Do you guys, in any way, and I don't even know how you would track it, but do you think that the ongoing Russian Ukrainian war has affected that, has that

kind of led to even more of these affiliates being out there, or you just can't [00:08:00] tell?

Brendan McGann: I don't know that I have a statistic on that per se. I know that we did notice that when the war started, we did see a potential dip in business.

We did see an impact. We're starting to see it come back to life and I personally feel very busy at times. I think the rest of my colleagues would agree that there are definitely--like any industry- you're going to have ups and downs, but I think we're back to normal.

I can't really say with any real certainty, we're seeing that war is having an impact on the affiliates or not.

David Shannon: I think I'm the same way. It's like people will ask me that and it's not like I have any kind of secret geopolitical analysis or know what, the NSA knows as to who's doing this work whether they are Ukrainians, Russians or whatnot, who now aren't on the front lines anymore.

But as I say, you would think it would affect it. And we'll just have to wait and see. I still believe that once that war finally ends. My concern is you're going to have all these people who have way more computer tech savvy skills after doing all this work with hacking and the drones and everything [00:09:00] else we see over there.

It's where are they all going to go to work? And they're going to be, there's going to be a lot of money that can be thrown at them to come work for these threat actor groups. I think that's something down the road, I think could be a real concern when it finally ends. You know, right now they're Ukrainian military hackers or the Russian military hackers. Where do they go to work when the war's over? And I think that could be a real problem.

Brendan McGann: I think if you're dealing with geopolitical issues where they're attacking each other, it can stay between them, and then now that if the war starts ending, what do they do with the remainder of their time? Are they going to start attacking everybody else? It'll be interesting to see if we see a huge uptick after it. That would be a kind of really interesting topic to talk about at some point.

David Shannon: Right. And another thing this year, can we get your thoughts on AI, which has been all over the news. It's like all of a sudden, the major

media just discovered AI, at the beginning of the year it became such a big deal in the news media. Do you guys see any of that where you can say that's affecting cyber security or cyber-attacks.

Or is it more right [00:10:00] now that we assume the cyber security companies, who are developing security software are going to use that to try and better enhance defenses? And on the other side are the threat actors using it anyway? I don't know. What are your thoughts on that? Have you guys gotten any kind of data or any thoughts on that?

Brendan McGann: So, I think it's interesting. like any tool that's out there that can be used for good, is going to be used for evil- we just know that. So EDR platforms have been using AI for threat detection, scanning purposes, and at the same time, I imagine, that's also being used against us.

So, there are many articles out there that have seen that they're using AI to write ransomware code. So, I think what will happen in 2024, will this spill into next year? Will we start seeing AI being used maliciously? That's one of those amazing things that we'll see what comes in 2024- we've seen big data breaches this year and what spills out. It could happen. Again, I wish I had more in-depth information on that. That would be a really interesting topic.

David Shannon: I think that's going to be a topic that we'll see on panels at every cyber conference for the next few years. [00:11:00] It's like, five years ago, all of a sudden ransomware started being the hot topic, and everyone went to that panel group discussion.

We'll then see if that happens with AI as we go forward.

Brendan McGann: Oh, absolutely. And then there'll be a next hot topic as we're talking about AI, what's going to be the next problematic event for the future? So, for sure.

David Shannon: Absolutely. I always use the analogy when I'm talking to people. I say, my son was born in 2007.

He's only 16. You know what? That's when the first iPhone came out. It shows you how this industry, just the computers and the data and the mobile phones and everything, it's just so young. It’s just in its infant stage and Lord knows where it's going to go over the next 10 years, 50 years, a hundred years.

Brendan McGann: And the adoption to it. I think I knew as I was going through school, I would lose points if I didn't have a typed paper written on a computer. Now, they're issued computers at early ages and classes. And I think, the adoption of technology at a much younger age is only going to become more and more proficient as we see performance throughout the environment, but we're [00:12:00] becoming much more attached to the technology environment, just all around.

David Shannon: Yeah, absolutely. As you said, it can be used for good, it can be used for bad. Another note I was going to bring up with you just in the last, say, six months. Are you seeing more? And I think I've seen some articles on this, of the source code for the ransomware, that it's more accessible now.

It's either been leaked onto the web or the dark web, or it's being sold now, so it's all over the place. Has that really been something that's more of an increase this year than we saw in prior years?

Brendan McGann: I think we have. I think we've seen a little bit of that kind of pick up and increase. I think, as affiliates--and that's going to be another issue.

With affiliates is, are you potentially looking at disgruntled employees? Are you looking at splinter cells? Because, hey, they're not thinking they're getting a big enough cut of the affiliate market space. So, you may potentially see some breakdown in the affiliate structures. Are you going to see more backlash to the admin organization?

And I think that's a real potential because we're not dealing, like I said, with threat actor communications, the [00:13:00] most rational people- sometimes we're dealing with people that are obviously coming from criminal organizations.

David Shannon: Yeah, absolutely. I see that is the big problem.

The more it splinters out, the more uncertain it is, the uncertainty that we have, then that we're actually going to be able to get good keys, multiple keys, as you said in some instances and incidents and that they're going to work and there's not going to be problems. I had one earlier this year that you know, a good ransom was paid, all the keys came back as far as we knew, but there was one server that just could not get up.

It was just gone. It was wiped out. And it was a huge problem for that business not getting that back. So, after all of the hard work, everything that had been done, we ended up having a huge gap and hole in their operations getting back up and running. And I think with all the source code out there even more in the Wild West, so to speak, all of these affiliates, I think that's one of the big takeaways so far this year is it's just splintering out so much and we'll have to see if that continues and what it affects.

A couple other issues I just [00:14:00] wanted to mention, Brendan, before we would close out from my standpoint, because I'm a lawyer, I think there's been a lot more law firm breaches in this year. It just seems to me that way. I think I saw a stat somewhere in the last couple of months that was true.

Now, a lot of that may be the MoveIt breach because there were a lot of big law firms in New York that were hit with that. But how about you guys? Do you have a stat or a feeling on that as to if there are more professional services that were hit this year so far?

Brendan McGann: Yeah, so I ran this too and I looked at it and I do see a very real increase within the professional services side. So, and I'm not sure if we can chalk it up to MoveIt, or if we can chalk it up to just a real targeted attack against the industry. We're dealing with organizations that, in the criminal mindset potentially have more income.

-they have more money coming in the front door. Whether or not they understand how IOTA accounts work and client fund accounts work that may be a very different discussion and trying to explain those processes that just because we have the money, doesn't mean we can give it out for ransom.

That's a very hard discussion to [00:15:00] have to try to talk these people off that. But I would agree with you, I really have seen an uptick in professional services throughout the year.

David Shannon: that's a good point. I had one with a small to midsize firm that did mostly estate work, wills and estates.

So somehow, if you looked at those IOTA accounts, some of the others, it was a lot of money in there, but when that ransom came in, the managing partner just laughed and said, “God, if we had that kind of money, I wouldn't be sitting in the office, six days a week.” So that is an issue they don't understand.

Brendan McGann: No, and I think it's the same thing when they get a copy of the insurance policy, and they think we know that the value of the insurance policy is XYZ and they just assume that's going to be the ransom demand. Trying to explain how coverage works to a threat actor is almost impossible as trying to explain how client fund accounts work or operating costs.

David Shannon: We had one where we had to explain that insurance policy the hackers had was four years old, and there has a lot more exclusions in the policy, from where we were now.

The last one I wanted to mention was just, obviously it's always still there, the business email compromises we see those with large [00:16:00] numbers too. We see a lot with small numbers. There's these small little, threat actors that do all these Microsoft scams with the security alerts, the PayPal scams. I haven't seen those as much this year. That was more last year, I think, but still seeing a lot of these little Microsoft security scams where, that pop up comes up and they have got people running around either to their bank or to get gift cards or God knows what else, to pay these things.

Is that just because it's all splintered out that these are all just low level hackers who figured out how to use that code, and they're just sending it out to thousands and thousands of systems and then see what happens?

Brendan McGann: Yeah, I think the shotgun blast approach is really efficient with that, they're going to go and just see what they can get. They'll a target tax season too because they're going to try to get people to log into to give them any kind of information they can. I think that BECs are just going to be something that we'll see perpetually.

The big Exchange, zero days are a thing in the past is everybody kind of migrates off of the Exchange environment, moves into Office 365. They're going [00:17:00] to utilize what they can. So, I would anticipate BECs being a thing for perpetuity, make it more and more refined. Stealing the passwords and redirections to potential Office 365 mimic sites.

But I think we're going to see maybe a little bit more refinement in the future. Maybe it'll make it look a little bit more professional. Stop misspelling words in the spam messages would be good, make it look a little bit more believable.

David Shannon: I think so. Some of them are really good and some of them are just, almost pathetic that I hear about.

But, when they started, I guess it probably was last year when I first started seeing someone, they started like passing people over to other individuals. That was when I was like, wow, they're really getting sophisticated. They're like, let me tell, let me connect you with someone in our customer service on another thing.

And next thing you know, the client's telling me they talked to two different people as part of this whole scam. My own personal feeling is that until the banks are somehow found liable for this that it's not going to change, but I think if we had some lawsuits somewhere where some banks got hit for not [00:18:00] having proper security or not being able to change their policies and procedures so that they're responsible for multi-million dollar, scams and compromises that sends the money off to China.

I don't think it's going to change.

Brendan McGann: You would think that there's at some point going to be some recognition, especially with these ACH transfers, if they're seeing multiple ACH transfers being completed to accounts that have just been recently set up, that there'd be some type of red flag that would go off in the banking system.

Hundreds of thousands of dollars being migrated to an account, which they've never done transactions with in the past, which was only created within the past seven days. You think that the banking system would pump the brakes here and go, “whoa, hold on. I think. I think we need to flag this and potentially consider this as, something nefarious.” But yeah, I think that would be a change in the banking policy.

David Shannon: I think that's the issue on those is how it's going to change. Okay, Brendan, anything else? Any thoughts on, in the next six months, anything that's going to pop up? You think? Or do you think it's just going to be this continued kind of issue with these ransomware for service type events?

And obviously, the big [00:19:00] one is more and more where we're just seeing the exfiltration and they don't even dump a ransom encryption malicious code in there. They just take the data and say, you're going to have to pay for it.

Brendan McGann: Yeah, it's going to be tricky to say. I think as we see backups get better and better, we may see the market switch to more of just data exfiltration and, we've seen Akira decryptors come out, we've seen Hive decryptors come out, and then they have to retool themselves. Are we going to see bigger breaches like the MoveIt case? That was well orchestrated,

organized. They waited very specifically until there was a UK bank holiday, and Memorial Day, to attack these networks across such a broad spectrum.

Are we going to see threat actors really organize themselves to go after not just singular targets one by one, or maybe potentially a larger exploit, and go for much more targeted large-scale attacks?

David Shannon: I think that'll be the interesting thing to see is, if I had one kind of takeaway, it's just more and more of these incidents where they're not dropping, the ransomware malicious software, but just doing [00:20:00] the exfiltration and then writing a note.

So, we'll see how that goes over the next six months. And I'm sure we'll have another one of these at the end of the year, for a year-end roundup.

Brendan McGann: Yeah, I think a year-end wrap up would be really interesting to see what the biggest breaches were. We started off early with the Midnight Group, who was scaring everybody, and then the takeaway, MoveIt just blew them out of the water.

David Shannon: it's amazing every year. There's something different. All right Brendan, I appreciate you getting on with us and we thank everybody for listening and we'll probably be back online with PLUS in 3 or 4 months.

Thanks very much.

Brendan McGann: Thank you for having me.

PLUS Staff: Thank you, David and Brendan for sharing your insights with PLUS, and thank you to our listeners for listening to this PLUS Podcast. If you have ideas for a future PLUS Podcast, you can share those by completing the Content Idea Form on the PLUS website.