Managing Cybersecurity Threats in 2024 Episode 3

[00:00:00] Welcome to this PLUS podcast, Managing Cybersecurity Threats in 2024. 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.

And with the housekeeping announcements out of the way, I'm pleased to turn it over to our host David Shannon.

David Shannon: Thank you, Tyla. Appreciate it. And thanks for everybody listening today. This is our last podcast for 2024. Have another good topic to discuss that should be relevant to everybody who's involved in the privacy and cybersecurity and data breach response fields.

For those of you who may be listening for the first time, as Tyla said, my name is David Shannon, and I'm a privacy attorney with Marshall Dennehey located out of our Philadelphia office and have been working on privacy and cyber-related legal matters, data breaches for about, I guess now [00:01:00] 13 years.

And today I'm joined by Heath Renfrow, who's with Fenix24, have a good discussion to talk about data restoration and remediation after a data breach. And thanks for joining us today, Heath, and I'll let you just introduce yourself and let everybody know what you do and what your company does.

Heath Renfrow: David, thank you. Thrilled to be here. And good morning or good afternoon or good evening when you listen to this and everybody else on the podcast. I'm thankful that you're listening. My background quickly, I've spent twenty years Department of Defense active-duty United States Navy for nine years after that DoD civilian.

I was a CISO for all the Army installations across the globe at one-point, Chief Security Officer for the Army Corps Engineers at another station, and then moved on as the first CISO for Army Healthcare. Forty-eight hospitals, over six hundred health clinics, dental, veterinarian, research arm, twelve hundred plus personnel, just in the cybershop.

So, I've run massive global cybersecurity programs, Army healthcare alone had over seven hundred [00:02:00] thousand endpoints. So, I've seen a lot. I left the public surface after twenty years and went into the private sector, and I've been in the private sector since 2017. Been with a few startups, and one of those was the Crypsis Group, which is now known as Unit 42 out of Palo Alto, where that's a leading data forensic firm in the country.

I'm not a forensic guy, but I cut my teeth in the same spots, and then eventually left when Palo Alto acquired the Crypsis Group and came over to Conversion Group, my sister battalion. As their CISO and almost immediately we had a cyber security incident came in where they needed restoration help.

And we really did good with the engineers that we had, but they weren't built to do a certain response. We didn't hire them to do that. We eventually started Finex24 about 2. 5 years ago. And we're a pure play restoration company. We normally are brought in, after ransomware events and sit there and help clients be able to recover.

So about 90 percent of that's there, the other part is fleshing out threat actors in partnership with our data forensic companies. [00:03:00] If you've seen a major data incident or ransomware events over the last two years, we most likely were involved with it in one shape or another. And here to discuss the lessons I've learned and the way I look at security completely different than I used to before after being in this industry.

So thrilled to be here.

David Shannon: Thanks, Heath. I appreciate it. And yeah, we've worked with Heath's group and with a number of people there, and they do a great job, and I thought it would be a good idea to have him come in, because we've had a few forensic guests over the past year or two talking about how they handle the incident response and how they handle ransomware attacks, et cetera, but haven't really gotten into kind of what's just as important for the large companies, and for everyone involved with those incidents, which is the restoration when you have to go back to that.

I think particularly now with everybody not paying as much when it comes to these ransomware attacks, people are really looking to try and restore from backups or see other ways that they can get their data back up. So, I think that it's a great topic as we're seeing more and more of these events being [00:04:00] handled in house and with outside counsel and outside firms to try and restore their data without having to pay the threat actors. So, Heath, give us an idea

when we talk about data restoration, what exactly does that mean? You have an incident, you have some kind of, attack, malicious attack.

And then obviously, the key for businesses is how do we get back up and running and how do we get our data back, and be able to get back up and running with all that data? Give us an idea of when you guys come in, what exactly are you doing?

Heath Renfrow: David, it's a great question. So first and foremost, everybody assumes that you're going to be able to recover from backups.

Backups are always the afterthought. "They're going to be there. We can quickly recover." The truth is 95 percent of our engagements' backups do not survive ransomware attacks. They're one of the highly targeted situations, which does put clients in a tough situation. But I'll reverse back from this. The way these threat actors work is they'll get in your environment, they'll get administrator credentials to start changing passwords to your host environment, be it ESXI, Hyper [00:05:00] V, whatever it is.

Azure AWS and then they'll start moving. They'll move virally, take data from your environment, and then they encrypt. It's not a malware, keep in mind, this is just an encryption of data through the environment. We're starting to see destruction versus encryption lately because of people's ability to recover at times.

But in this situation, they encrypt everything. And then that's domain controllers. That's after directory. That is everything in your environment. And so, when you hit a domain controller, you're shutting off the brain of your IT operations. So, there's no functionality, no nervous system.

This is a reflection on internal IT staff, but 95 percent of recovery is going to be infrastructure based in individuals. And most organizations, no matter the size, don't keep a lot of infrastructure folks around. The reason is, once you've got an IT infrastructure, it's like a Ferrari, or a sports car. You drive it, you polish it, you put the wheels in it, it's good to go, right?

You don't need a whole bunch of resources to make it go. But when its nuts, bolts, engine parts thrown back in front of you after these threat actors, putting it back together is difficult. Humpty Dumpty being put back [00:06:00] together again takes some time. It's going to wear out the IT staff. They're probably not going to have the expertise.

It's not a reflection on their skill set. It's a reflection on, unless you do this day in and day out, you don't understand the little tricks of the trade, recovering a domain controller, not shutting them down, being able to replicate it, being able to build a clean domain controller, being able to get the forensic tool pushed out into the environment.

That's one of the main things I saw at the Crypsis group was clients going, "how do I deploy a forensic tool? My systems are down." And we come in there and get the bones and the structure put back together again, reconnect all the nervous system back to the domain controller that we've been able to save.

You can save a domain controller. You have to have a particular skill set. If you reboot your domain controllers or shut them down when they're encrypted, you're starting from fresh. You have to create an entire new brain. Create an entire new nervous system, and it really slows down the restoration across the board.

The assumption that a lot of people made, and even I made in my past role, is that I'd be able to recover quickly. And most recovery strategies and tabletop exercises really are focused on ransomware. They're [00:07:00] focused on natural disasters. When your infrastructure is completely torn apart, first, you got to get that backup operational.

That takes time. Even with all the engineers I have, I could throw 100 engineers at you. It's going to take time. "It's a marathon, not a sprint," is what I tell people to recover. And then from there, if the backups do survive, the assumption is you can just click your fingers and you're going to be back up again.

It's just not true. There are so many factors that come into recovery. Your storage can be blown away by these threat actors. First and foremost, if you have snapshots, unless you have immutable snapshots like pure HV. And then your backups, immutability is a weird definition being, for example, the definition of immutability is to two administrator accounts.

That's not hard for these threat actors to get and blow away your backups. But if the backups do survive, the return to operations in a disaster recovery plan, I've never seen one that actually is accurate.

So you have a pipeline that how much data you can move back across into the infrastructure and to be able to recover that. Keep in mind that 80 percent of

your [00:08:00] environment's encrypted, which means probably 80 percent of your storage capacity is taken up.

So, you have 20 percent storage capacity to try to recover it, and the amount of data, moving terabytes of data across a small pipeline to recover is very difficult. Cloud is even worse. This is on prem I'm talking about. If it's in the cloud environment, it's even a slower pipeline to recover. So, there's a lot of factors.

We have to come in and organize that. We do take over. That's the thing, David, that sets us apart is, I think over everything switches, firewalls, everything across the board. We execute. We're very 70 percent former military. We're very military like the way we attack this to allow the internal IT team to rest and handle the things they need to.

But ultimately, once we have the bones back together, the application owners had to get brought in to be able to help put the rest of the Humpty Dumpty back together. And so, we lean on them very heavily from their internal knowledge that we do not have.

David Shannon: You mentioned something that actually I was just reading about in the last week or so how the threat actors are now going to destruction more as to encryption.

And that I think one of the [00:09:00] forensic firms sent out a white paper on that, that they're seeing that more and more. And so probably everybody in this space is reading that, having to deal with it. Explain to us then, they're not encrypting the data there, they're destroying it. Explain from your point of view, what exactly are they doing in the kind of layman's terms? And how do you how does the data restoration that help when something like that happens?

Heath Renfrow: Yeah, it's interesting. The lack of encryption. I don't understand the methodology that they're going out because they're making things very difficult.

But they basically ripped everything down to bare bones, the bare metal across the board. And then, I see that they're doing that with the infrastructure, but they're still leaving the backups behind in encrypting those sometimes they're not actually destroying those. And if you do this all day, every day, like my team does, we have a lot of tricks.

We've learned a lot of things. There's always a way to be able to get the bare metal back and operational to the point where you can sit there and recover back into it. But it takes a highly skilled individual. Other organizations that don't use a professional restoration firm like ourselves, they most likely, David, will go [00:10:00] buy all new equipment.

All new software, all new hardware, all new storage and start from fresh. And we call that greenfield rebuild, which we don't believe in greenfield rebuild. We believe in brownfield rebuild, building back in the infrastructure that's already there. Because you do a lot of lockdown in these events and you reduce risk, but there's risk regardless either way, but quick recovery versus brownfield long recovery is greenfield.

So, this is very painful. The angle to be able to pay the ransom with this. I haven't fully understood with these threat actors. I don't know what the motivation is for me to pay you, and I have to do all this. You're not going to give me anything that's going to help me really. Other than the encryption key, if the backups do survive.

So instead of blowing away backups, they're encrypting the backups and then they're holding that ransom. But the recovery pathway is probably 10 times harder with the destruction method versus the encryption method.

David Shannon: Yeah. I'll see that a lot. I think you're right. When the internal people will say, "we're just going to go out and buy new servers, or we're going to bring in new hardware because it was on the list to be updated in the next two or three [00:11:00] years."

But you're saying, no, it's better to come in and take that, that hardware system that they have and restore that, recover that, and then get the data back that way or bring the data from the backups into those systems that you already have. Is that what I take from your feeling?

Heath Renfrow: Yeah. David, your spot-on. I believe in a lot of these instances that IT individuals are making business decisions that they shouldn't be making. Business interruption costs are astronomical for organizations, and sometimes they don't have enough capital to even make two or three weeks to be down. They had to make money.

IT, because they've never been this before, make the assumption, and there's some data forensic firms that are like this, they're like, "oh, we got to make it

completely clean, new zone, new production environment, new hardware, just to reduce all risk." Historically, ransomware doesn't really work like that.

They're not leaving time bombs behind in your environment. So, you have the structure, you have the bare bones, right? So, you can recover much quicker with the brownfield, drive down your business into rushing claims, and then from there you can strategize to go out, to sift through [00:12:00] and enhance your security.

They'll put Humpty Dumpty back together with maybe a few little tweaks that we can make. Keep in mind, insurance also, sometimes IT thinks that insurance is like a blank check for them. They're not going to do better than that. Buying all new software because you're going to upgrade it in three years, they're going to reject that, right?

When you try to invoice that in there. In the situation where IT wants to just do it themselves, it's a lack of understanding the business impact and senior executives are going to trust their IT team that they're making the right decision.

And that gap, there is no business executives to understand like long term recovery versus a short-term recovery, get operations back online, reduce risk. And then focus on the strategy to be able to make your security program better. But we very much believe in build back to the bone structure that's there, drive down business interruption cost.

That's why I started this company. To keep businesses and get them operational quicker. And to drive down the cost across the industry for BI cost.

David Shannon: That's what I was going to then say from my point of view and maybe from if we've got some [00:13:00] of the underwriters, claims professionals who may be listening to this podcast is that if you're going to look at that BI claim, and how you're going to keep that lower, it makes more sense, obviously not to just going out and spending, hundreds of thousands, if not millions of dollars on a whole new system, when you could get it back up and running on what we have, and having you come in to do that or a firm like yours, so that you're up, the BI cost is down, and then you're not getting into that big fight about as you brought up betterment, which, we'll see sometimes where I'm caught in the middle.

I've got a client that's gone out and bought all this software and hardware and they want to submit it and they want me to be on their side while the carrier

sitting there saying, "David, isn't all this betterment? They just went out and bought new stuff that's a lot better than what they had before."

I understand that point. I think it's a good point for people to understand as to why you would want a restoration team coming in early rather than later. So, you can start making those decisions. Ideally, I assume it's the obvious, but you want to get in there earlier rather than later.

So [00:14:00] you can start working with everybody.

Heath Renfrow: You're right on the point. I'm going to come in at the same time the data forensic program comes in. And the reason is because if you let a client struggle getting data forensic tools out, the faster forensics flows, the faster restoration flows. So, you want to get their tooling, the data forensic tooling, pushed out immediately.

We have the capability through our tricks and our tools to be able to deploy that even into a broken environment. Keep in mind the brain is shut down. You're tooling that deploy endpoints into an IT infrastructure are shut down, and they'd be able to recover those so difficultly.

The reason our data forensic partners partner with us is we speed up the forensic process by getting the data to him within hours versus days and weeks for most clients. What they'll do is their start hand delivering the endpoints or the data forensic tool to individual systems, which is time consuming beyond belief.

And from there, the business interruption costs. Yes, paying a data forensic firm like myself is going to give an extra cost on top of data forensic and outside counsel, but we drive down business interruption costs [00:15:00] over 50 percent driven down most of our claims for BI cost and we track it very carefully of what's critical systems come back online.

That way for a forensic account, they can see the money makers when they come back online. That's a huge challenge for most clients is asset inventory. It's just not there. They don't know their total assets and because they don't know their assets, they don't know the critical systems that need to be recovered.

So that's something we heavily focused when we first get in there. It's like, "listen, business leaders, what is the most important thing to get back?" Operational 2nd, 3rd, 4th and 5th doesn't mean I can't tackle 30 things at one

time, but we have a workforce. I have 100 plus engineers, right? That's all in house is all they do.

Keep in mind these clients. Maybe we have three or four, but they're defensive, right, in these situations. They think their jobs are on the line. They know their infrastructure. They think better than anybody else. "No, we can do this in house." They're worried about cost without being educated that their insurance policy probably covers a lot of the cost because restoration comes out of that business interruption side of their clause on that side of the house.

David Shannon: That was a [00:16:00] point I was going to make is sometimes you've got to, when you realize early it with a, you know, a midsize large size company, that you want to look at it and say to the insurance adjusters who are looking at the overall cost too, that while adding a firm like yours in there.

So, you've in some respects, they'll say, "Oh, we got two forensics teams." Not really. You've got two teams doing two different things. And that this costs for your firm is actually in the long run going to save money. And I find as long as it's explained well, and you can show some numbers that the carriers will be on board with having that restoration firm and fee be part of the first party coverage that's going to that's going to pay for this.

So, in the long run, it's better for them and it's better for the client.

Heath Renfrow: I have more and more insureds, they want us desperately to come into the engagements, but everybody does defer to clients, obviously, in those situations. I am a big advocate that policies in the future should mandate professional restoration to help in these situations to be able to drive down those BI costs. [00:17:00] Clients make the assumption they can do it.

They also make the assumption that their MSP can recover them. They're not equipped to do it. This is not what they do day in and day out, and they're going to make mistakes. They don't understand that they're going to charge outrageous hourly prices that the insurance is going to push back on. We're just in the industry right now where the client's right.

And I understand that and push back on that. But our goal is, yes, we're going to be a cost, but in the long run we're going to save a lot of money. We had one client, gambling industry, 300 million dollars in cyber insurance policy. They're probably losing 10 to 12 million a day. We recovered them in nine days, and they had told the industry that was going to take them 6-8 weeks to recover.

So, the business international claim is going to be astronomical. That's what professional restoration brings to the table. We also very much do everything remote. We do not believe in going on-site unless it is absolutely necessary. Getting on site takes time. It is not necessary in today's world.

I've worked in 93 different countries and done restoration in those [00:18:00] countries, mostly all remote. That really drives down the cost. Travel, food, airline tickets, being on site, wearing out the online site team. That's days to start that work versus hours of a scope and call where in a client's environment working.

David Shannon: Yeah, I think it's, I think it's a great point is that, and I think more and more when I talk to some adjusters and more of the managers, the claim managers, they're looking at those BI claims because those are the numbers that can really get up there. They can get a handle on what the legal costs are going to be, the notification cost, even the forensic cost to a certain extent, once you know how many endpoints, they're looking at things like that. Because they're all competing competitively for those budgets.

But I think the is the BI is the one that can be the outlier for a claim and a company that a carrier is using. And being able to lower that cost and to be more sure about that cost is only going to be for a week as opposed to, as you said, some circumstances, 6 weeks, it behooves everybody to really take a look at the data restoration and getting that done as early as possible.

What [00:19:00] do you see it that more and more, we could end on that as we've gone through this year, now we're going to get into 2025. Do you see you're getting more cases where the carriers and the clients are seeing that as well that, "hey, we really need to be looking at this data restoration early rather than we're three weeks into this and all of a sudden we're like, 'Oh, no, maybe we got to get somebody to look at restoring this stuff?'"

Heath Renfrow: I think it's improving with insurance and legal, most of my engagements do come from data forensic recommendations to clients that are knee deep in it. I think from a legal standpoint, it's a little misunderstood still that it's an extra cost of insurance. And I think counsel are being very protective of insurance as far as the costs that are going to them.

And it's just a little lack of that. And counsel and insurance are going to trust the clients when they say, "oh, we could do this." The key to the table is for us is, we speed everything up. We're not mother, may I? Some of my competitors or come into a client's environment like, "what do you need us to do?"

That's not the right approach. They've never been through this before. So, we [00:20:00] lead. We've automated. That's another thing, David, that we try to do is we automate a lot of our stuff. Scripts that can run through environment, PowerShell scripts. We want to drive down BI costs, but actually drive down our costs.

Our standard recovery rate a year ago, it was about 700 hours to be able to recover. Our standard this year is about 200 to 250 hours. That's how much we've improved and learned in the situation and automated across the board. I've done three times the amount of engagements this year as I did last year, but my revenue stream is exactly the same.

And that's a good thing for us because that means we're getting better at what we're doing. Restoration is probably brought in to maybe 15 percent to 20 percent of most ransomware cases. So, there's a long way to go.

David Shannon: Yeah, I think you're right. That's great to hear about how it's improving too, you're bringing down the hours because sometimes that becomes the thing.

People are just like, "how many hours is it going to take?" And they just want to look at those numbers without saying, "how much money are we going to save on the back end?" I think that's a great point for people out there who may be having these conversations with individuals in [00:21:00] the insurance industry or with their clients is to say, "we don't want to just look at the hours that we're paying for. We want to really look at the money we're going to save at the end."

And I think you're right. I've had a couple recently where it's the internal IT or their MSP who's like, "yeah, we're going to handle getting things done, back up and running" after they've had the ransomware where either you paid for it, or you've got the backups going and you're not paying.

It's something I think we're going to see more of as we go forward. It's just another part of these, the privacy and data security claims in the field that everybody's getting better at trying to not only protect their data, But at the end of the day, also restore it if they have the incidents that we know obviously are going to keep coming from all the threat actors out there.

But I appreciate it, Heath, we're getting there towards the end of our time. Thanks a lot for coming out. It's something that as I said, I think it's more and more we're seeing the data restoration. I think your firm does a great job, worked with a number of people there, know those people and I would

recommend anybody out there if you're going to have an incident where you're going to have [00:22:00] data that's going to need to be restored definitely consider getting that third party in there. And Heath and his team can help you out. All right, Heath anything else, last words?

Heath Renfrow: No, I appreciate it. Thank you so much. And if anybody needs anything, look me up and get ahold of me and anything I can do to advise or help out, let me know.

David Shannon: Okay. Sounds great. Thanks, Tyla. I think we're all done there for the year.

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.