#134 - Ransomware Response (with Ricoh Danielson)

[00:00:00]

[00:00:00] **G Mark Hardy:** Hello, and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy. I'm your host today and we're excited to have a show about how to respond to ransomware. Now I know we've done a couple ransomware shows in the past, although that was a year and a half ago, but today I've got a special guest, Ricoh Danielson, and he is here going to talk about his experience helping companies.

Respond to ransomware and come up with an innovation ideas that you probably not have thought of before. So it should be interesting. But before we get going, let me share with you a word from our sponsor. Our sponsor Risk3Sixty has recently developed a new ebook entitled The Business Case for Penetration Testing. Downloaded today to learn why it matters, the financial risks and investments associated with the pen test, potential [00:01:00] cost reductions and more. Also, this ebook provides templates for developing your own business case. Visit Risk3Sixty.com/Resources today to get your free copy. That's r i s k 3 s i x t y.com.

And thank you Risk3Sixty for sponsoring our CISO Tradecraft podcast. Please support them and look at the great material. Now back to our show. So on CISO Tradecraft show, we do a lot to help cyber leaders get smarter about protecting their companies from cyber attacks. And one of the things we're observing in today's environment is just a huge dichotomy in cyber capabilities between small companies and large organizations, for example, Fortune 500 companies typically have a CISO and a cyber organization with dozens to perhaps hundreds of full-time employees, and they'll run programs like a SOC, a security operation center.

Now, these programs may not always be run internally with their own organic resources. They might outsource it to a managed security service provider and outsource soc. Sometimes the contractors, but they do have them. [00:02:00] Now, compare that to a small business. If you're a company between, let's say, two and 2000 employees, you mostly focus on profitability and staying afloat and providing the business goods or services that you deliver to your customers.

Now, if you think of a small business, like a local dentist or a lawyer or tax accountant or something like that, these small businesses will store your personal information or protected health information just as well as a large company, except the small businesses only have a small IT shop, if any at all.

And they don't spend money on cyber when they don't hire staff that specialize in cybersecurity, and they certainly don't have a full-time CISO. Now, if you don't spend money on cyber and you don't have people looking into preventing cyber attacks, what do you think? Bad stuff is going to happen. And that's exactly what we're observing.

We're seeing a lot of successful ransomware attacks against smaller businesses. Now. Today I'm excited to introduce our guest speaker, Rico Danielson. He's a man of many talents. let me share with just a few of them before you learn how to respond to [00:03:00] ransomware Rico, you were a tier one special operator in the US Army.

You are a US Marshall Posse member out of Phoenix, Arizona. You led global incident response at Charles Schwab, led cyber ransomware negotiation for many cyber incidents. You've been a CISO at multiple companies. You also have a law degree from Thomas Jefferson, and you're under a hundred years old. Is that all right?

[00:03:21] **Ricoh Danielson:** Absolutely. Absolutely. And you're missing the three master's degree as well, so, but yeah, absolutely.

[00:03:27] **G Mark Hardy:** Yeah, you've got the, I love you all on the back and I've looked at, but I can't, my vision isn't quite that good. But I mean, that's awesome that you've done had a chance to have such an interesting background and been able to contribute in so many ways into our career and our profession as well as for other organizations.

So today I wanted to talk with you about incident response and then what actually happens. When small businesses, well find out they got ransomware. So we'll start with a fictional example. We'll take a small business and I'd love to get your thoughts on how a company, like when you started first responder, would help them dig [00:04:00] out of being a victim of cyber crime.

So let's imagine the fictional companies a small medical clinic. It's got roughly 500 people, a few offices in a regional area. They have an IT shop of five and they install Microsoft Windows in every laptop. They're using E3 licenses and oh wow. You get Windows Defender, great. And they might do quarterly patching, but no one's really looking at cyber activity because they've got to focus on connectivity and availability of software applications.

Now let's say the CFO gets an email saying, We have stolen all of your 2022 tax information and your client protected health information, and the ransomware asks for a hundred thousand dollars in Bitcoin, or the ransomware group is going to publicly disclose all that protected health information and potentially harm all that clinic's customers.

Now if I am this fictional company's CFO. What should I do first? Am I immediately calling the FBI? Am I calling local police department? Do I call my insurance company? Do I update my resume? What should I be doing first?[00:05:00]

[00:05:00] **Ricoh Danielson:** All of them, all the above. That's what you want to do. Definitely the resume part, but no joking aside in reality situation is it's your choice if you want to call your insurance is really up to you. You're more than likely you're going to have to call your insurance. I highly recommend because remember, they're your partner.

Even though you're paying them a lot of money, they might not cover certain things. They're going to try to bring in their own IR firm. I've seen it to where people have their o bring in their own IR firm like us, where we show up and we help guide them through the negotiation, the process to, to work with their cyber insurance.

And then also, I've seen the other side where they brought the cyber insurance and they still bring us in. From the cyber insurance side and we help them out. Right? So there's that aspect of it. You know, from a tactical, technical perspective, you want to get the threat act on the outside. So I've seen drastic measures all the way changing into DNS domains, all the way to resend passwords, implementing multi-factor authentication rolling creds on a 24 hour basis kerberos creds and whatnot.

And, you know, all the way to. Just taking networks [00:06:00] completely down off the grid offline. And that, that's one of the things you don't want to do because then you have to start up all over again. And remember, remember the, the common number that a business is set up in has been in business for 10 years. So, and you know, all the intricate things of like the network and we got this thing working.

I like working with network engineers. I used to be one and it's like, Hey, it works. Don't touch it. Right? It might not be secure, but it works. It works. Just don't touch it. So that, that's one aspect of it. The other aspect is you're going to have to engage law enforcement. If not, they're going to show up.

They're going to, they're going to make himself very well known. On a most recent one. We're actually engaged by the Secret Service and they said, Hey, we saw the recount happen a week ago. Here's a specific person. Here's kind of what we're looking at. And they already knew it was about to go down and it went down very quickly.

The best things, it's, it is those moments of hours within 35 minutes, an hour, two hours of what you do will reign in the histories of cybersecurity forever. You need to be [00:07:00] agile and, and I'm talking to like an executive leader here. You need to be mindful and put your ego aside and say, my IT team can handle it.

No, they can't. IT and security are two different things. They run in parallel, but with two different professional skill sets. And you need to bring somebody in. So bringing in consultants, bringing in your insurance, bringing in the FBI, you now you're going to have this thing called the war room. And now you got to set up a war room and you start driving it.

And if you don't know how to do the incident command and war strategy around this you might want to bring somebody in. You know, that's what I would recommend. That's how it would look like the first six hours.

[00:07:35] **G Mark Hardy:** Yeah, so it seems like there's a couple things that organizations could do. One is to practice at war room, which is what we call tabletop exercises, and you probably do those. I do those things for my clients as well. But the other one then is to have these points of contact. Identified in advance. You don't want to be going through the yellow pages.

F f F A, f A, F B, F B oh FBI. There we go. Let's give them a call and they call the 800 number. But if [00:08:00] you engage in InfraGard or something that's a local chapter, you may have an opportunity to meet these professionals in advance. And so heaven forbid something goes wrong, you call him up and it's not hi.

Yeah, this is G, letter G, then Mark. No, not Mark G, but he'll be like, Hey G, Mark, how are you doing? Like what's going well? Yeah, we need you this time. So, so that's one possibility. But let's assume for example, that we've done our homework like that. And so something big hits the fan and we have our emergency communications plan.

So we'll go ahead and we'll notify the relevant departments. We'll call up key personnel but as soon as they, after I do those initial calls, right, you need to kind of wake somebody up at two in the morning. It might be the ceo, it might be whomever it's supposed to be. What do you do first? You. And you've mentioned a couple things.

You just pull the plug and disconnect your network from the rest of the world. You go ahead and spend time to confirm that it's not a false positive, even though the clock is ticking. What do you do in those first few minutes before you get to those critical hours that you talked about?

[00:08:58] **Ricoh Danielson:** Yeah, so the first thing I would do then, [00:09:00] this is just me thinking outside, you know, I'm thinking strategically, right? Immediately I would engage my executive leadership and then I would bring everybody to round table. And then I love bringing a cyber attorney to the table as well to immediately make everything on under client confidentiality.

So you can do what you need to do and, and where you can, because. Your cyber insurance or a cyber insurance may not agree with your methodology or approach on strategy in regards to how you got the threat act on the outside, but the reality situations, you have to get them on the outside. Once you bring everybody together at 2:00 AM.

Chant, let's just say hypothetically, the threat actor put a ransom note and did not execute any encryption. Now you know who you're dealing with, right? So now that we're starting to see the trend going back and forth of a threat actor, just kind of doing a snatch and grab and trying to extort you versus the whole extortion and encryption.

Now, you know, your, your threat actor, a little bit of research might help you out a little bit in regards to understanding how they got in, what they use, what vulnerabilities, their TTPs and the IOCs. And then you can determine. You're talking about the golden hours, right? [00:10:00] Four to six and now 12 hours.

You have to make the critical business decision. And this is a business decision with cyber attributes to it, what you're going to do, because there's going to be user, user impact, healthcare impact, customer impact, patient impact. So the bigger thing we have to say is, okay, if we pull the plug on the network, what does that really look like?

And I've met very few people who've done that. And it's catastrophic. You're, you're talking about taking, in this case, a, a medical clinic, completely offline, right? So that's one. And number two is, okay, have we done, I've always correlated to jiu jitsu. I'm a big jiu jitsu guy myself. You know, you can actually do a lot of, a lot of hip movements and whatnot in this small little things.

Okay, did you roll the creds? Did you implement mfa? Did you close down all the ports? What do we know? What do we don't know? And these little things, these little jiu jitsu moves you're doing with the threat actor can kind of get him on the outside very quickly instead of having that knee jerk reaction.

Where you're just actually having to, to pull the plug and, and start from scratch. You know, so little [00:11:00] things slow and steady, even though you're on a golden, golden hour timeframe. And then from there you can actually start engaging the threat actor from hand to hand combat, if you will. Because they're going to come back around.

They already, they already got their foothold, right? Yeah.

[00:11:12] **G Mark Hardy:** Well, if you take a look at the typical, I mean the Verizon data breach report just came out, but take a look at other sources and things that to talk about. Time for dwell time inside your environment. And they vary across studies. Verizon's very different than Larry Mann's study, but then the time for lateral movement, and in some cases we're talking minutes, not hours, and that's a snatch and grab.

And yet by the time you figure it out it could have been significantly time late. So there's, there's two scenarios. One is you just happen to get them as the glass breaks and you hear the alarms going off and they're running around inside your store, grabbing stuff out of the merchandise, so to speak.

And the other one is they've been low and slow in there. They've been sneaking in every month or every night for the last month, and now you just happen to stumble into it. So probably different levels of response, but not knowing right away. [00:12:00] Because typically what happens is we get alerts. We remember it's a small organization, maybe they had Windows Defenders Alert that someone opened up a malicious document.

It had some macros in it. But then you didn't see anything and you went on to go ahead because somebody else needed that, or he had to set up for lunch or whatever, and you forgot about it. And it seems to me in those first several minutes, if not first few hours, that one of the things that's not on the list is, Hey guys, what were the alerts that we had in the last few months?

And oh, by the way, depending on your license with Microsoft, you may only have 30 days of logs. And so if this thing started 31 days ago, you're out of luck, you're out of log anyway uh, unless you're using a third party tool. So, so thoughts on that? When do we, you know, when do we decide that we have to go high order in our response versus, Hey, this could just be a script kitty, or this could just be as you had said, somebody who sent a note but they didn't encrypt anything.

But the clock's ticking. What, what are we, what are we doing here?

[00:12:56] **Ricoh Danielson:** Yeah, so the one thing I would kind of like approach it is I [00:13:00] always treat everything equally. I think a red alert is a red alert and I'm going to go in there guns and blazing. This is what we're going to do. And it's almost like a standardized process and methodology of saying, okay, let's go ahead and capture a lot of, you know, let's just say, you know, velociraptor logs, trying to figure out where the lateralization of the movement's going.

If there's any PowerShell movements, if there's any obfuscation of PowerShell, cause that's very noisy as well. And then also we look at it from a tactical, technical perspective of a timeline. Okay, what are we missing? That's what I always ask because. When, when a threat actor shows up, you're going to see, okay, January, January where, where's the end of January timeframe and where did that go?

And then all of a sudden, we're back in November or, you know, February and we're back in business. This doesn't make any sense. So what happened or what can we deduce from there? And then we start looking at network logs and stuff like that. So these are, these are the more tactical level type deals. But at the end of the day, you're going to have to make that critical decision and actually really, really lean into.

Everything is more than likely [00:14:00] an alert, especially at the golden hour. But the problem with that, and the counter to that is you're going to get alert fatigue, if everything's an alert, you're going to get, everything is an alert, right? So the best thing is you can do of, of qualified masses. That's what we always usually use when, when in Iraq and Afghanistan.

Instead of saying personnel who are qualified masses, I need alerts at a qualified masses. Now that we know the threat actors, TTPs, IOCs, what they're after, more than likely, It's going to be the crown jewels you know, your servers, your different ehr EMR systems. Now we have a, a parameter we can kind of focus and model after, and then that's what we go after.

It's going to change. It's going to change for sure. Because threat actors love to just go around doing different things and go in different places.

[00:14:43] **G Mark Hardy:** Yeah. And I think a lot of these smaller organizations, which you're we're looking at, may not have continuous monitoring going on. They don't have a soc. If they don't have the advantage of somebody looking at all the network traffic, they're not going to spot lateral movement very quickly because nobody's looking [00:15:00] at that.

And in fact, one of the dilemmas is, is that when you finally realize something is going on, you're figuring that either A, if the logs show what was going on, and often it's a little bit like, well, wait a minute, you could reconstruct what they were doing the last three weeks. How come you didn't do anything?

Because it's buried down in the logs and you don't have any SIEM to go ahead and distill this thing down. And so as a result, do we have this perpetual situation of smaller companies being behind the power curve where they just can't get there from here? Or is there some, some magic deus ex machina that can come down and say, you know, we, this descends upon us, you know, put disc one into drive A and hit click enter and you secure your entire enterprise.

[00:15:45] **Ricoh Danielson:** I think Staples made the easy button a long time ago. So you just hit that thing, hit the easy button. But, you know, one thing I, I found you're right, you're right. There's a lot of things you can do during the moment. Incident. The other thing is, you know, if you're a big sophisticated organization, you should be SIEM tuning and you [00:16:00] should be log tuning, what's important to your organization.

It's different what versus. An IT shop you know, there's some very powerful tools out there. And one of the things I would have to recommend is it when in doubt EDR out, right? Just throw the EDR in, you know, just like in the infantry, when in doubt frag out, just throw a grenade out, right? Same thing like you're going to hit something when you throw an EDR out.

And if, if, if time is of the essence and professional professional services and is very budget times. Constraints. I would just definitely just use the EDR and you're going to have to figure it out from there if you're in a smaller IT shop. If not, there are professionals out there like us, like we're tool agnostic, we're just ninjas and we do whatever we need to do and just run in there and just get after it.

So I mean, I, I think that's one of the heavy hidden tools you can definitely do for sure.

[00:16:47] **G Mark Hardy:** Right now in our fictitious organization way, set it up. They had E3 licenses and defender running, is that going to be enough to be able to capture the information we need? Do we need to crank it to E5? Do we [00:17:00] need Defender++? What is, what? Is there anything, if we will, if we're just in a, a Microsoft shop, I'm not trying to pick on them or, or, or, or promote them.

I'm just trying to say from many smaller organizations, they're not going to have a diversity of tool sets and so can they, if they just use the tools that Microsoft provide, a, have enough information that they can see what's going on, but B, potentially construct alert scenarios so that they find out earlier rather than later what's going on.

[00:17:24] **Ricoh Danielson:** Absolutely Abso Microsoft Defender is actually a pretty good tool. If you have the E3 license and also Microsoft Defender going, or E5 or Microsoft Defender plus plus, I mean that. These are fantastic, but just remember, just like any other tool, it is a point of reference of tool. Hey, that threat actor went over here, right?

Anytime you clear a business, you, you have the blueprint. You know which route you're going to go. You're going to kick in the door, I'm going left, you're going right. Type deal. And then you stack again, right? Same premise in combating the threat actor with Microsoft Defender is a great point of reference for a blueprint, but then you have to follow the trail and go hunt that threat actor down.

[00:17:57] **G Mark Hardy:** Right. So you got a clock ticking. You've [00:18:00] got a ransom note saying, send us Bitcoin. I always used to say an executive trying to buy Bitcoin is like a grandmother trying to buy heroin. They dunno how to start. They dunno what to do. They're like, what do we do guys? But more to the point is that we take a look at the logs and we find out that.

Although they claim they stole all the health information for the patients, we go, I don't know. I'm not seeing that boss. What, what do you do at that point? Do you, do you simply call, say, we're going to call your bluff. Do you assume that maybe the logs have been modified or erased or they were not looking at them correctly, or they came out with some other way to exfil?

At some point in time you have to go ahead and declare a threat, either benign or hostile. It's either false positive or true positive, and you've got the alert. But now what do we do? How, how do we go about that? Again, you haven't shown up on the scene yet. We're, we're waiting for the cavalry to come over the top of the hill.

[00:18:49] **Ricoh Danielson:** yeah, so absolutely. So whenever, whenever you've determined that, hey, there's some data that's been. You know, possibly, possibly exfiltrated. The best things you can do is, you know, en [00:19:00] engage an incident response firm. You have evidence now, even if it's an allegation in the state of Tennessee and also the other states, they are saying even if there's an alleged of possible data that has been leaked, you have to do some sort of reporting.

Now, the reporting process is going to be encompassing of. What have you done for this incident? So you're kind of mandated to kind of bring somebody in. Once we show up, you know, we, we start doing the digital forensics on all sorts of devices. We deploy agents we start getting our network telemetry, and then also start getting everything else in between all the metadata that we really need to start responding.

And then from there, We have to make a business decision to either engage a threat actor or not engage a threat actor. I don't recommend a lot of my, my clients to engage a threat actor just because there's a lot of legal weight that goes with it. And a lot of attorneys do not understand the, the ransomware or threat actor engagement process.

They're like, oh, absolutely. Now there's too many laws. And when the reality situation is you can or you cannot, really depends on how it fits your business model. Now when we [00:20:00] engage in the threat actors, That's a whole different dynamic. The idea is never to pay. And, and a lot of people will disagree with me.

I can tell you right now from one specific person, from a specific cyber insurance company, he, and I don't agree but I said, you don't ever need to pay. And I, he has clients who pay and, and that's really your preference. It's really up to you. But, Just remember this, if you're going to pay, you have to run it by the FBI, your attorney, and make sure you're not conflicting with some sort of OFAC regulation.

Confliction, right? And if you pay a known terrorist organization or a known terrorist state God to help you, right? So,

[00:20:36] **G Mark Hardy:** Yeah, and it's interesting if, if you go through the fine print, when it talks about OFAC and paying ransom, it's a little bit nebulous, and I think it's deliberately that way. It's one of those lawyer things where it says, well, it depends. But if you're in a situation where it might be life safety if we can't get the system back up, but the ransom's going to an OFAC entity and it's there and it's listed as one of the do not pay.

That's an interesting dilemma [00:21:00] where you have. Send a you know, card to run over one person. You'd take it on the tracks and run over different people. And is my reading of it, and again, I'm not a lawyer and I don't play one on tv, is that if you call the FBI early and you play your cards, face up with them, and then they realize you're in this corner, they say, well, your damned if you do, damned if you don't, it's one of these Hobson's choices.

But if you do choose to pay the ransom to do this life safety, particularly in healthcare maybe the judge will go easy on you or maybe the paperwork will get lost and going. You don't want to anticipate that, but at the same time, you should never get there at all. robust defenses, having redundancies, having ability to go ahead and look at exfil being able to stop everything, all the great things that I'm sure this organization is going to invest in after they get hit.

[00:21:52] **Ricoh Danielson:** they always do.

[00:21:53] **G Mark Hardy:** part, it's like the wallet, it opens up and there's a half-life of awareness of a board of directors of a cyber incident [00:22:00] seems to be to be about 45 days. Within 45 days. Something else is big going on. Hey, we got production problems over here, or it's the weather, the stock market or the, or whatever.

But during that interval you have an opportunity. So yeah. So let's, let's back up a little bit and think about notifications. So when we. We realize that something's going bad. We have keyto stakeholders we need to notify. And is it a lot of variance in that? Is it a matter of getting everybody to assemble in one place and getting the word out at once?

Is they doing a, a call tree like we used to do in the military where you call Charlie, calls Bill and off you go, what's, what's the best anything that works better than others?

[00:22:39] **Ricoh Danielson:** Yeah, so usually pen flare works pretty good, right? But I don't say that jokingly. Don't ever put a pen filler out. One thing is I would say, you know, you definitely need a matrix, right? You want to get really super fancy with it, get a matrix going and say, Hey, who's who responsible, whatnot. But, You got to have a short list, you got to have your, your list of heavy hitters, CEO, CFO, and then they start going from [00:23:00] there.

You want to bring everyone together as much as you can, if you're going to do it via the, you know, the internet or, you know, different go-to meetings or anything like that. One thing you have to be mindful is more than likely your internal components are more, are compromised and the threat actor has visibility in it.

So setting a GoTo meeting out and then threat actor joins on their behalf, you know, that's really amazing. I've seen that happen before. One

[00:23:21] **G Mark Hardy:** The ultimate Zoom bombing, right? Yeah.

[00:23:24] **Ricoh Danielson:** Like, Hey guys, how's it going? You know, one of the things I would recommend is, you know, go taking your, set your tabletop exercise a step further and doing unsecured communications.

Like go, go to the exercise of going to Walgreens, buying a burner phone. Standing up a, a war room in a coffee shop and kind of going through the exercise, that's where a lot of people lose it, especially at the medium to small business level. They don't, they think this is a game, but the threat actor is never going to go away, and they're probably going to come back over and over again.

[00:23:53] **G Mark Hardy:** Yeah, that's a good point because as you had indicated, you don't want to be doing in band communications when your [00:24:00] communications are likely being monitored, and so that's one of the things we used to talk about, about the only real benefit of setting up PGP keys in advance. Is that okay? Yes. I guess you could still do it in band, but the problem is, is that if the bad actor all of a sudden sees a huge spike in internal encrypted stuff for like Yeah.

They know. And, and so the whole idea is there's a couple things. You don't want them a to know that, you know, if they are trying to be low and slow, and then if they've notified you that they're there you don't, they don't necessarily, you don't want to tip your hand to them to say, We know the extent cause are they bluffing?

Is the game of poker necessarily not a game of chess where all, all the pieces aren't visible on the table? And it's not a matter of outthinking your opponent, sometimes it's a matter of out psyching your opponent and things like that. So if we can't send in band communications and we have to use, as you said, perhaps burner phones and get, get together at at the Starbucks or something like that, [00:25:00] How do you go ahead and collect that information, collect that audit trail of information?

I'm sure the insurance company's going to want to see it. And potentially, if you end up with that OFAC dilemma that we talked about before FBIs want to read your thought process, et cetera, because you don't want them to say, oh, we just decided to do it. Screw the law. You want them to realize that this was a very deliberate decision, ways that we could do that other than, you know, good old pen and paper and take notes.

[00:25:25] **Ricoh Danielson:** Yeah, that's the whole thing of the first thing I ever, ever brought up was bring your attorney because, you know, they're, they're going to represent you. They're representing the best interest. The FBI, I think, is a very interesting group of people. I, I have friends who in the FBI for cyber ransomware negotiation and cyber incident response.

A lot of people might not agree with me, but I've never found them very helpful. They're a one way communication type deal. They gather information, they go dism, rehearse amongst themself. That's just my opinion. But you know, that's just me. The best things you can do if you're in a really, really compromised communication and also a different type of organization where you can't use inbound [00:26:00] network.

You might want to. Start bringing around different terms, host it at their, their office, or a, a possible neutral office. And you're going to have, you know, sworn statement, you're going to have to go old school sworn statements you know, sworn documents and stuff like that. At the end of the day, whenever you go back to your insurance and you say, Hey guys, you know, here, here's what we got.

There's no way we can fabricate. Here's a best, here's our best just effort, and here's our best foot forward. Here's a reality of the situation. And we've arrived to. Having to pay this OFAC or this, this OFAC sanctioned organization, there's ways you can do it. I don't recommend you do it. I recommend that you hire an organization to do it.

You can, you can hire an organization like us or you can hire like an organization, like another organization that comes to my mind. And they'll do, they'll set up the Tumblr for you. They'll set it up in a, in a foreign organiz foreign country. And it's a very white glove services and it's very good to do.

But try whatever you can do not to get to that point of decision.

[00:26:56] **G Mark Hardy:** Yeah, I, I mean, I remember, you know, look at what's happened with Bitcoin over the [00:27:00] years and. Having some Bitcoin early on and I sold all mine to clients who got ransomware and they didn't know how to get Bitcoin and they said, we'll give you 15% over market. And it's like, okay, great. So I made few hundred bucks because this Bitcoin was like a three digit value I put on my taxes.

I I, I was business profit. I made almost a thousand bucks selling Bitcoin. Never bought anymore. And of course Alpha went up by, by a hundred fold. But you, you look at things and recognize that. I can't pay it properly. And if I'm a consultant, I'm brought in. One of the questions I'm going to ask is, well, if it's an OFAC entity, and for those who aren't familiar with the Office of of Foreign Asset Control, it's a treasury department puts out a list and it's updated on a regular basis of any entity that they consider to be an adversary of the United States.

It could be a nation state, it could be a particular state actors even include a lot of Bitcoin addresses, although you'd think. Somebody you knows what they're doing will never use the same address twice and it'll still end up in the correct wallet. But I, I digress. [00:28:00] But there was one client where they had asked if I could help out and that was when I pulled the string and said, yeah, it's an OFAC thing.

On the end of it, it's like I can't help at that point. But yet you indicated that you can using foreign stuff, and I'm not asking you to self incriminate or anything like that, that's not the purpose. But you're saying that there basically are ways to do it and maybe people should ask you for more details and not necessarily on this public call.

[00:28:23] **Ricoh Danielson:** Right, right. There are ways, there's always ways and there's actually formal correct ways of doing it. Also there are organizations that actually have a process a little bit better. We do it as well, but one of the things we, we suggest is, hey, notify everyone. You can within your organization, law enforcement, cfo, legal counsel, and the F B I and the secret server, whoever you're working with, and let's just make sure we're on the same page.

I understand, I hear what you're saying that we shouldn't pay, but we have to pay. So here's what we got, you know, so,

[00:28:52] **G Mark Hardy:** Yeah, if it, if it were your daughter and they were going to kill your daughter, unless you send them money I would pay

[00:28:57] **Ricoh Danielson:** yeah, absolutely.

[00:28:58] **G Mark Hardy:** matter who the bad guy is, it's [00:29:00] like you're going to, you're going to save that person.

[00:29:01] **Ricoh Danielson:** You know, it's very, very interesting you brought that up. I met a director of education for a state. I can't say who. She was so brilliant. She goes, you know what? I earmarked a hundred thousand dollars budget every year to put aside to pay for ransom. And she's like, I know it's coming.

And, and sure as sure as a bet, man. She called me up not too long ago. I was like, Hey, remember what I tell you? I was like, yep, I see it. And she paid. And I said, okay, perfect.

[00:29:28] **G Mark Hardy:** Yeah. And if, if you don't pay it, you use it for the Christmas party at the end of year. Again, worked out well. Okay. Let's, let's get serious again. So when we're looking at things, for example, We go back and we look at our tooling. You said get EDR in there. We, we light off the EDR, it goes through and we get some hits, say That looks malicious.

This is a binary that just doesn't belong. There. There's a process running in memory whether or not it's left any record on the hard drive, but assuming we can see that stuff, we go through there and just start trying to act [00:30:00] like we're at a shooting gallery at the arcade and charge shoot, you know, Blasting all these things out one at a time.

Do we try to go ahead and just disconnect from the internet? Do we isolate systems? Do we pull, you know what? What's the best approach? Particularly if you can't go down, if got to stay up and running for life safety, or you're a government entity, or you've got health stuff so you can't turn it off, you've got to keep going, but yet you've got to fight in, in urban warfare, so to speak.

[00:30:27] **Ricoh Danielson:** Yeah. So to me there are no rules at this point. Anything goes. So any, anything and any devices a target. So what I like to do, I, I'm a very, very different creature when it comes to an incident response. I'll actually have a war room and almost kind of run a purple team exercise right then and there.

Hey, get the bridge going. Do you see this? Do you see that? And these, these working sessions are, you know, anywhere from like four to 12 hours going, right? And they're revolving. So you have a live security operation command. You're running the war room, you're running the TTPs, you're running the threat hunting, you're chasing down the [00:31:00] threat actor all in one time.

And the war room does not go down. You're going to have to create shifts. The problem with the other, the inverse of is, you know, hand it off to a soc. Remember, there's a ticket that's going to be generated. Somebody at a junior level is going to go chase out, which is okay. But right then and there at the incident response level, you need an incident responder to be hands-on in it, in your environment.

So the best way for the way I've found is even an attorney will sit in there and be like, Hey, because you know, they get paid per hour, obviously. They'll sit in the war room and they'll say, Hey, sure, why not? I'll hang out with the guys and you want to bring them in and say, okay, does this work for you? And you're going to go through the whole network and it's going to take you.

You know, it depends on your network. Or let's just say you're a small medical clinic, you, it'll take you anywhere from 24 hours to 72 hours or 84 hours. I mean, this the nature of the beast.

[00:31:45] **G Mark Hardy:** Yeah, and, and so at that point in time we say, okay, fine. We've identified that there's been stuff in our enterprise. We have, we think we've isolated it, or at least identified it. What do we do then? Do we, as I said, we go then try to whack a mole you. [00:32:00] Take a system offline. Do you re-image from a gold image, assuming you have one?

Or do you use Microsoft as its own gold image and you say, I'd like to download a copy of Windows 11, please, and then let all the patch. How do you go back and reconstitute your enterprise? Do you do it one at a time? Do you do a department? Do you set up temporary computers for people to work in the, so, you know, those are at least good.

So while you're fixing the stuff any strategies that work better than others.

[00:32:25] **Ricoh Danielson:** So every strategy is different for each organization I've seen where they take them offline, one individually, re-image them, deploy a go golden standard. I've seen that done before. The most recent one that I've done in the last four weeks, where we actually took 1100 devices completely offline and we started re-imaging there.

We actually had an assembly line in the conference room. You bring them in, you sign them in, get blown away, you get a new image, and go back to work. The network took for us to bring back up was 84 hours. And for the whole process of the image, we worked about two and a half weeks to get 1100, over 1100 devices re-image in one sitting.

[00:32:58] **G Mark Hardy:** Yeah, it, it's [00:33:00] amazing when you think about what they were able to do at Aramco a decade ago where they had over 30,000 machines and these things were all able to be redone very, very quickly. But I remember when I was over there and I asked them, I said, how did you guys get concurrence? He said, we only have one shareholder.

It's the king. And so when the king issues a royal decree, you do what he says. And they went ahead and they fixed it, and they, and then they made stuff happen. But again, most of us don't have those resources or that clear chain of command, all like they do. So now organization, they've been hit, they've been burnt.

There's this 45 day plus or minus half-life of awareness where you can pretty much get whatever you need on a budget. These companies will buy technology. They'll pay for consulting, they'll pay for legal help and things like that. But do you often see them then create a more ongoing relationship with someone like yourself or you know, someone like a virtual CISO or the like to say, Hey guys, we kind of wandered into the street because we didn't have adult supervision.

Let's make sure we don't wander that way [00:34:00] again. Is that a pattern that you see or do they pretty much go back to business as usual after 90 days

[00:34:04] **Ricoh Danielson:** There, there is no bi business back to usual. There is none. You've, you've been in a jiu jitsu fight with a black belt or red belt, and you got, you got tossed around. So I mean, this is the tough one to go with, right? So what happens is we have an ongoing relationship with them, not only as the incident response firm, but also as a VCISO and we now you have a chair.

Now we have a chair at the board level, right? And we say, okay, guys here, and it's brand new to them. It's brand new to these organizations. They have no clue what. A true cybersecurity entity looks like or later looks like. So you bring that to them. I've done this for a while and I've been offered multiple jobs and I'm like, Hey, that's cool, but I, I appreciate it.

I'm good to go over here. So you'll be surprised, like whenever you develop those relationships and you're in, in the, in cahoots with them, how quickly they look to you and say, what do you think? What is, what is our level of expertise here now? So don't be surprised if, if that actually just matures into that naturally.[00:35:00]

[00:35:00] **G Mark Hardy:** Right. And I, and I find some of these relationships where you get in there and they, they appreciate it. I had, I had one client, they, they said, Hey, we want to extend your co. We want to expand. They said, well, this is great. And it was really good when you got all the paperwork done, they said, Oh yeah. By the way, we just had a major breach and you get to brief the board because you're now the, the Chief Scapegoat Officer.

Yeah, you got it. And it, it was pretty straightforward. I mean, if anybody ever has to do that, you basically go in and said, here's what happened, here's why it happened. Here's what we put in place as controls to keep it from happening, and here's why we believe that we'll be okay in the future. And like, okay.

And the people who you know, we're like, that's, yeah, that's how it works. Because at the highest level, you're really about managing risk. And one of the things we have to do in cybersecurity is we're in the business of revenue protection. We want to ensure that the organization's core lines of business keep going.

Now, one of the things that ransomware used to take advantage of, and if what I call Gen one ransomware, Which is an attack on availability. Hey, your files are encrypted. Oops. You got to get them back. We set up a lot of [00:36:00] robust backups. OneDrive will do that for Microsoft, even for individual systems. We could go ahead and have redundant backups and multi-generational backups and things like that.

And so Gen two ransomware comes in and says, we'll do a confidentiality attack. We stole your stuff. Oops. Your files are encrypted. Ah, Take a hike, we've got to back up. Okay, well guess what? We're going to go ahead and tell somebody what we've got. And then at that point it comes down to a matter of being able to validate that claim.

If you could see that yes, you had two terabytes exit your enterprise in the middle of the night last night, there's a good chance that it got popped. But if you don't have, if you have telemetry and you don't see that, they might say, Hey, here it is. And we, we say, sending you a sample record or two.

But it might be almost like the bluff of the United States did in 1945 with Japan. You know, we're going to drop 10 more of these things. And they had dropped every single one that existed, at which point they're like, okay, fold, you win. So if we take a look [00:37:00] at our telemetry, And say, you know what? We did not have a two terabyte exit, and our database is two terabyte and Health and Human services requires us to report a breach, and then the lawyers and everybody else are going to come after us and the stockholders, et cetera, et cetera.

Is there a situation at which point you go back and say, we just think it's a bluff. There's no way they stole all the records. There's no, they couldn't have gotten it out of the system. Not only are we not going to pay them, but we're not going to report. Now that seems to be a risky thing, but have you seen that situation occur?

[00:37:32] **Ricoh Danielson:** Yes, I've seen both I've seen it to where threat actors say, Hey, we have all your data. And you're like, oh, shoot. And then they say, we have one gig. I'm like, well, okay. That's interesting. That's, that's not a lot. Okay, let's talk about that. And then you, you have to line up the logic for the executive board, executive board who is good at what they do, which is executive steering and getting us to the revenue and whatnot.

You know, so we as technologists have to show them and say, Hey, check this out, man. Here's how we're going to go about, line out the information and [00:38:00] whatnot. The other part is to make sure that we have all the facts that are in a row. Sometimes they're the facts. Are the facts. When I look at things and I see the letter of the law and I read as an attorney, it says, do you know for certain you've been breached?

Well, I can't tell you that. I can tell you that somebody was here. So there was an in you know, inadvertent or unauthorized access. I don't know if it meets the breach notification. Okay. Do you know if anything has been le been exfiltrated? I, at this current time, I do not have anything showing that these logs that's been exfiltrated.

Okay. So then the best, the best effort you can do or you should possibly do is say, Hey, you know, We don't know if we've been breached, but we're going to do the best thing for our customers, our patients. Let's go ahead and do a breach notification now to the extent of what that might look like. You might offer credit monitoring or you might do some other stuff or might not do anything.

Just release the statement and say, Hey, this is the bare minimum. So it's really up to you and, and how you see it, how good your attorney is, right.

[00:38:55] **G Mark Hardy:** And I think you raised a good point is that sometimes these breach notification laws is written, say, oh, you got to [00:39:00] tell within 18 milliseconds or 48 hours, or whatever. But the answer is, well, it might take weeks or even months before you're absolutely certain that that's been the case, because it could just be anomalous information.

It could be a, so again, that's kind of the area of lawyers and I try not to play in that area, but

[00:39:17] **Ricoh Danielson:** one, one thing you, you brought up with that, that, that's a specific example. When I was working in the financial industry, there were, I think that was the fcc, the FRB was like, we want a five hour notification. In the event an event happens. And I'm like, okay, well, I mean, there's a, there's tons of events in our SIEM, so I mean, you might as well just keep you on speed dial y'all.

And they're like, well, we need to know. And I said, guys, like, this is just unreasonable. You're being unreasonable

[00:39:41] **G Mark Hardy:** You say, give me your home phone number and

[00:39:44] **Ricoh Danielson:** yeah,

[00:39:44] **G Mark Hardy:** Good luck. Yeah. Call me in three days and let me know if you got any sleep.

[00:39:47] **Ricoh Danielson:** yeah, I'll just hit the forward button, all these emails, alerts.

[00:39:50] **G Mark Hardy:** If we kind of wrapping up here a little bit, anything you would suggest, small business, let's say who've not been hit but are going to say, okay, we got a little bit of religion. This Ricoh guy says, it's not a matter [00:40:00] if then, but when, and we really don't want to go ahead and end up you know, putting in stitches when you could have worn a seatbelt or worn a helmet or something like that, so, so what precautionary measures could smaller organizations do that are within budget but are still going to give them the Pareto principle, you know, 20% of the money giving you 80% of the benefit.

[00:40:20] **Ricoh Danielson:** Sure. One, if you can, if you can afford insurance, go get it. Go get insurance by default. Two, put a tool in place, even if it's a inexpensive tool, do something. Because when the, when these lawyers come out, they're going to be like, well, what did you do? What is the bare minimum? It shows something, even if it's an AV and it doesn't do well, just do something.

Three, do an incident response plan, even if it's on the back of a napkin at Buffalo Wild Wings, having beer. Please do that. Right? And then four tabletop exercise, you know, dry run war game, you know, something like that. You, you got to do that. These things, I know they sound very boring, but at the end of the day, this is, this is a fundamental level.

This is how you hand a hand combat with a threat actor. And [00:41:00] these are the fundamental things. And the last part is this. If you don't know an incident response firm, Call them. You don't have to buy anything. You don't have to because they're going to try to say, be like, Hey, let's sell you this retainer.

You don't have to buy anything. Keep their phone number handy. In the event something happens, then you buy it. Okay? If it's not covered by your insurance, you don't have to do anything. Just stack the deck in your favor.

[00:41:21] **G Mark Hardy:** And that's some very good advice, and one of the things also is I would say get a copy of the contract and get your legal department to look at it in advance. Typically, the idea of a retainer is we work out all the legal stuff, so if something hits the fan, you pick up the phone and we get started right away.

The alternative, as you had said, is. Go ahead and at least know whom to call. I would say there's a middle ground, which is you already know what the T's and C's are, and you say, well, you know, paragraph six and paragraph nine might need to change, but otherwise we could do business. The only difficulty may be is that if it's just you getting hit, you're probably okay.

But if it's a enterprisewide or a galactic attack, they're going to prioritize their existing [00:42:00] customers first and they're going to say sorry, you're on the wait list. We'll call you back in three to five weeks if you're still around. If people aren't get ahold of you, if they say, Hey, this Ricoh guy is the real deal, how will they get in touch with you?

What's the best way to do so?

[00:42:12] **Ricoh Danielson:** I mean, I can give you my phone number if you like. But

[00:42:14] **G Mark Hardy:** It's, it's going out to the world. It's going to be on the internet for the next 400 years. So you decide.

[00:42:18] **Ricoh Danielson:** Perfect. Yeah, just give me a call. It's 480-747-5970. You can always email me at ricohd@1stresponder.us, or go to our website first 1stresponder.us

we always welcome conversations. The one thing I always try to tell people is, I'm in the business of you.

I'm not in the business of sales, so I'm going to probably, I'm probably going to talk myself out of quite a bit of business when we engage. So my biggest thing is, you know, what's best for you and your business. That's, that's the bigger thing.

[00:42:46] **G Mark Hardy:** That's very good. Good idea. That's a great way to wrap up the show. So, Ricoh Danielson, I'd like to thank you very much for being part of CISO Tradecraft. For Audience thanks for listening in or watching on YouTube. And if you're watching on YouTube, do me a favor. Click that subscribe button. I always wondered [00:43:00] why other people would say click subscribe.

Click subscribe. And I realized it actually does help. It helps us get rid of unwanted ads and allows us to get better control of the content. It doesn't cost anything either. So now I find myself being a subscribe, begger. Never thought I'd be there. If you're listening to us on podcasts, of course you get us on all the channels that are out there, and we have links in our show notes.

We get transcriptions. If you go to the CISOTradecraft.Com go to our GitHub page and you can look up past episodes. All this information is available for you out there to make your job better to become a cybersecurity leader. So until next time, I said, this is your host, G Mark Hardy. Stay safe out there.