UNAUTHORIZED ACCESS: TONY KIRTLEY
JULY 7, 2022

Sadia Mirza:

Welcome to Unauthorized Access. My name is Sadia Mirza, and I'm joined today by my co-host Kamran Salour and our very good friend, Tony Kirtley. In addition to being our friend and someone whose time Kamran and I waste often, Tony is the director of strategic business development at Secureworks. Tony, thanks so much for joining us today. Do you mind sharing a little bit about yourself and explaining what Secure Works does?

Tony Kirtley:

Yeah. I'm Tony Kirtley. I'm, as you said, the director strategic business development, looking after the cyber risk partnerships at Secureworks. I just came out of seven years with the secure works incident response team, so I've had a lot of experience with them about Secureworks, we are a managed service security services provider, and we have a monitoring platform we call Taegis. It is an XDR platform, and we have services that we can package along with that. And that is secure work's primary bread and butter. The incident response team specifically does about 14 or 1500 engagements every year. And so that's us.

Sadia Mirza:

Well, Tony, when we were creating our list of guest speakers, you were on the top of our list. Kamran and I have always enjoyed working with you. And I'm actually, I'm so glad... As we were prepping for this, I love the ideas that you brought to the table. So, today we're discussing the emotional journey people go through when faced with a ransomware attack. And I just want to say that I really loved this topic for two reasons. First, I think it's critical for all incident responders, especially breach coaches, which is the role that Kamran and I play, to know that ransomware attacks are really not just a business matter. A lot of victims of these types of attacks, I think they tend to feel personally responsible when a ransomware attack occurs. And at least for me, I think it's our job as incident responders to help them work through those feelings, which helps make sure that the investigation stays on track. And really the second reason why I thought this was so important is because nobody talks about this, but I've seen it come up in almost every single matter.

So Tony, when you propose this as a topic for discussion, and I think you've presented on this in the past, I was jumping out of my chair screaming, "Yes, this needs to be discussed."

Tony Kirtley:

Yeah, absolutely. And first of all, I'd like to give a shout out to Terry McGraw, a coworker of mine who came up with the idea. In my last role in the incident response team, I led a group of incident commanders. And we are the guys, as you know, Sadia, that work with the breach coaches, and we're the customer facing element of the incident response team. And what we've found over the years of working these engagements is that there are a lot of emotional responses, and some arrive at the desired state more quickly than others. And those that do have a much better outcome if they're able to manage those emotions early on.

Sadia Mirza:

No, I fully agree. And I'm just sitting here thinking about a couple of incidents that we've worked on in the past where the first scoping call, it's usually someone from IT is on the call, and you can... And especially now that with video conference calls, you can just see it on their face, the devastation. Sometimes I even go so far as saying embarrassment, but they don't need to feel that way, because unfortunately this is just the risk of doing business these days, right?

Tony Kirtley:

It is. And so what we tried to do is kind of put all of these emotions that exist in a ransomware incident into a framework that is mostly known by people. And that is the Kubler Ross grief cycle.

Sadia Mirza:

Okay. Tony, so walk us through it, because I don't know if everyone is familiar with the model. So, I'd love to tell us what stages we are and how you associate that with the different stages of ransomware.

Tony Kirtley:

Sure. Kubler Ross had five stages of grief that she had in her model. And those are... The first one is denial, the second is anger, the third is depression, the fourth is bargaining, and then acceptance. And acceptance is where you want to be, both when you're grieving something and in ransomware.

Sadia Mirza:

First, I think my reaction to that is, I think maybe some people who don't deal with ransomware all the time or helping respond to ransomware may feel like it's an extreme comparison, but I don't think that's the case, because I'm thinking about clients that we've worked with in the past, where you have some folks who are helping respond to a ransomware attack, who've been in their positions for the last 20, 30 years and responsible for IT. And I think it's at that level, the feeling of responsibility, the grief that this type of attack has happened, and now what the business is going through and everyone's under pressure. I think it's very fair to make the comparison, but acceptance is... So, based on those five stages, acceptance is where we want to get the team as soon as possible. Is that what we're saying?

Tony Kirtley:

That's right. That's right. Because when you can accept the fact that your business is down, you're going to lose money, it's going to be a matter of weeks before you're recovered potentially, then you can start being in it for the long game. Knowing what to expect, you can start to position the team for longer term, sustainable operations and you don't burn anyone out, and just putting yourself in that mindset of you can just make better decisions and set the expectations of the business so that they're not breathing down your neck every day, expecting unrealistic progress. So, it is very important to arrive at the acceptance stage as quickly as possible. Now, Kubler Ross, with respect to human grieving, said that these stages can be

experienced in any combination, in any order, and it shouldn't be rushed, but I'll submit that for a victim of ransomware, in order to expedite the recovery process, it does need to be rushed. We need to fast track the victim to the acceptance stage as quickly as possible.

Sadia Mirza:

So, let's say... Tony, in your experience, I know... Let's walk through the other stages. And I'm interested in your thoughts on what stage do we usually start at?

Tony Kirtley:

Well, we took it chronologically as Kubler Ross laid out. And let's start with denial. Last year, I wrote a blog that kind of frames up the ransomware situation, where the CIO gets called on a Saturday morning by his director of infrastructure who says, "Hey, we've got most of our systems down," and starts naming the applications that are unavailable. The employees can't do their work. They're losing money all the time. And the CIO is just having this internal panic attack, asking himself, how could this happen to us? What's the impact? This is the denial phase. How can this be happening? It's a disbelief. And in some immediate response is for them to just start taking action, start rebuilding systems, start resetting passwords, start shutting things down, not knowing what really they should be doing. The actions are unguided, and oftentimes they're unproductive. So, in the denial phase, it can be very dangerous if the organization doesn't realize that they should be calling the experts to get guidance that's going to be productive.

Kamran Salour:

So Tony, one thing that I notice in handling these incidents, when we're talking about the denial phase, a lot of times the clients will ask, why us? We're just a small organization. Why are we being targeted? Is there a way to extend this model? I guess, well, one way I'd love to extend this model, I should say, is to use it as a teaching tool where letting people know that it's not that you are a target for the type of business you run. You're a target because you have some vulnerabilities that are easy to take advantage of.

Tony Kirtley:

Absolutely. I've heard that same argument, Kamran, but I tell people that ransomware attacks are not targeted. They're opportunistic. And any company who has business, has data, has operations, IT operations that would hurt them if they were down, they're subject to ransomware. And you're absolutely right. It's a matter of how exposed are they, how vulnerable are they? And it's not hard to compromise some of these organizations. The objectives that we have in the first call with the victim is giving them a sense of calm, letting them know that we do have a process to get them through this, and starting to build their trust and letting them know what to expect. So, there's a survivability of the company at stake, in some cases. And in some people's minds, an emotional responses is, is my job going to survive this event? And so that leads us to the anger stage of the grief cycle.

And what we see here is some job preservation kind of action, some finger pointing, some deflection, jockeying. And I think the emotions these people are going through are, "This is my system. I own this. This is my baby." And so they get angry that's been violated, that that's

been compromised. And so it's hard to control anger in this situation. But I think the danger is for leaders in the victim organizations to not let that anger kind of leak to their staff, because it can affect their productivity. It can affect the morale. It can affect the loyalty of their staff if they let their anger get the best of them.

Sadia Mirza:

Tony, do you think this anger element, is it usually coming out from the senior leaders is what you see the most when on these calls?

Tony Kirtley:

Yeah, I do. In fact, the lower level administrators, they take a more ownership approach. They kind of feel guilty sometimes. And that's kind of the next stage, the depression, where they see a control that I didn't implement good enough is the reason for this compromise. And so they think it's their fault. They think they're going to get fired. They kind of fall into a state of despair, depression, that they should give up. But it's in these cases that we need to encourage them to keep going, that their leadership needs to encourage them that they're not going to get fired because of a mistake that they made or whatever, or negligence on their part. So, they need to implement a culture reassurance and assure them that every person is a critical part of the recovery team.

Sadia Mirza:

Kamran, it was making me think about my favorite topic, pre-breach services.

Kamran Salour:

Yes.

Sadia Mirza:

And I would imagine that companies that haven't done a tabletop have at least planned for this type of event. If they go... If a company gets hit for the first time and have had no planning or preparedness, I could imagine that a lot of these phases would come out a lot quicker and with a lot more impact, I guess. Right?

Kamran Salour:

Yes.

Sadia Mirza:

But think if companies... Right? If you've planned for it, if leadership knows that, "Look, this is a possibility. One day, this could happen. They've been part of those types of tabletop exercises," it seems like it might get us to that acceptance stage. Maybe part of tabletop exercise is getting us to the acceptance stage, actually, just knowing that this is going to happen, but there's a plan in place. Tony, is that what you're trying to teach us?

Tony Kirtley:

Yeah, absolutely. And that's why tabletop exercises are so important, because you may think, "Well, we're just talking about the issue. We're not really doing anything," but just getting people to understand what to expect in these types of situations is so important. We have a whole team of people in Secureworks who facilitate and plan tabletop exercises, and I was on that team for three and a half years. And just getting people in the same room together to talk about ransomware and the impact, the severity of the impact of it, is huge to get them to that state of acceptance, if it were to actually happen.

Kamran Salour:

This underscores a couple of things for me. And I guess first, I'm so excited, Sadia, that you are talking about pre-breach services, because that is so near and dear to my heart. But I think for me, one of the things that it highlights is having a very digestible and practical incident response plan, knowing that no matter how many times you go through a tabletop, it's never able to replicate the real thing. And so almost approach it with the understanding that when an incident does occur, no matter how long you've prepped, there is going to be some level of denial, anger. And with that, at the outset, that's going to likely cloud your thinking. And therefore to have a cheat sheet, or a very simple checklist of what to do immediately, if an incident does occur, I think that really highlights the importance of it, because I know, Tony, you mentioned at the outset sometimes, people will start to wipe machines, whether it's to get the company back up and running or to hide evidence, who knows?

To me, that's one very important takeaway on another important takeaway that I've seen on the anger side is really twofold. One, often I see anger from the impacted organization toward the insurance company, especially vis-a-vis, the timing of negotiations with threat actors. And it's important for us, whether it's council or the forensic firm, to really be cognizant of that frustration and anxiety phase where the client wants to pay the ransom as soon as possible, and sometimes too soon, before they know the status of their backups, and for us not to get caught up in that anxiety as well, and really exercise a lot of patients and make sure that we're not pulling the trigger on paying a ransom before we know if a ransom payment is needed.

Tony Kirtley:

Yeah, that's always a contentious time. Kamran, you're right. As an IR firm, we're always looking to determine a couple of things. One, like you said, if there's backups that are viable, and two, if the threat actor group is a name and shame threat actor group, which most of them are these days, if there is a proof of life, or if they've stolen data, and if they claim to, if they actually have. So, those are the two things we're looking for to inform the victim organization, advise them, or give them options on paying or not paying. The next stage in the grief cycle, we see, is bargaining. And this usually happens once the victim organization starts to gain momentum. Let's say they have containment achieved and they start recovering in earnest and rebuilding the infrastructure, and then start building applications.

They see some services come back online. And leadership wants to bargain with the staff with a hard push. "Hey, let's keep going. I promised the board we'd have this by such and such date." We're losing money every day that we're down. So, let's work some extra hours to get this going," but it's dangerous to do that, to burn out your staff. And what I always recommend for victims is to ask for help in those situations. We partner with recovery firms that provide people, skilled IT people that can help the victims out recovering their systems. I think that part

of the acceptance process is for the victim organization to realize they need the help and to go ahead and get the help.

Kamran Salour:

That's interesting, Tony, because for me, the bargaining side comes out more in the sense that the impacted organization, they're kind of close to... They're on the other end of things. They are close to being operational. And then I will find sometimes that the organization will kind of get very aggressive and creative with the threat actor in terms of suggestions of negotiation tactics, because they're almost playing with house money at that time. So, that's interesting. Your experience with bargaining is very different from what I've experienced.

Tony Kirtley:

Yeah. I've seen that too. I've seen some owners of organizations just take a high road and a hard stand against a payment, when the operational guys are saying, "We're going to go out of business, we have to pay, we have to have that data back." It's very interesting to see that push and pull. So then, the last stage is acceptance. And this is where you want to be, of course. This is where the real momentum in recovery begins. And I've seen one organization that had a b-line to acceptance, and I've only seen it once. And it was kind of a unique case. I responded to this one personally. The victim organization, their it director, it was a small company, had anxiety attack on day one, checked himself into a hospital. When I arrived the next day, he wasn't there.

I never met him. And he reported to the CFO, and the CFO turned to me and said, "Get us out of this." And so he pretty much gave me a blanket authorization to do whatever we needed to do to help them through it. I engaged the recovery partner right away, and it was easier to set the expectation with the CFO that I was working with. He could barely spell IT. He knew nothing and claimed to know nothing about it. So, he was very trusting, and almost an implicit trust in me as a third party expert. And so he was just like, "Yep, I understand. I'm in a bad place, and I want you to help me get out of it. What do you need?" And he signed the paper, and we went and got them recovered very, very quickly. That's just a quick example of how speed to acceptance really makes a big, big difference.

Kamran Salour:

Yeah. Sounds like that guy just sort of jumped over those prior four stages and just went to, "You handle it, Tony, right?"

Tony Kirtley:

Right. When I presented this last week, I got a question about that guy. And someone said, "Do you think it's because he didn't know what was going on that he was more accepting of the situation?" And I said, "No, I think it's more about attitude." Because he could have been arrogant and distrusting of me, thinking that I was coming in to take his money, but his attitude towards it was, "Hey, you're here to help us. So, I'm going to let you help us in the way that you think is best."

Kamran Salour:

Yeah. That's interesting. You bring up attitude, because sometimes these incidents are the results of not having adequate controls in place, and many times the organization entrusts an MSP to have those adequate controls in place. And so part of the process, depending on the situation, of course, is managing the relationship between the client and the MSP and the forensic firm, and letting the MSP know that the forensic firm here is not coming in here to point fingers. They are here to just fix the issue. But definitely, and I'm sure you've experienced this too, is sometimes the MSP is, or the relationship between the client and the MSP, is such that you're dealing with anger far too long and you're not getting to acceptance quick enough because there's a lot of finger pointing as to, "Why did you hire this MSP?" And the MSP saying, "Well, you didn't ask me to do these things." And that does definitely slow things down. So, I think attitude does play a big role in this process.

Tony Kirtley:

Kamran, you know, as well as I do, that we deal with a lot of different players in these situations. You've got the breach council, you've got IR firms, you have MSPs. Sometimes you have two IR firms, and so that kind of makes it very difficult. And you have third party support, like Microsoft or Cisco, or something like that. We've seen cases where there's jockeying among the third parties, and that's not healthy, but what we didn't talk about in the anger phase is the blame game. And it's so important to diffuse that nobody is to blame. We've all just got to work together. Regardless of your own agenda, we have to work together in the best interest of the victim.

Kamran Salour:

Absolutely. Right. And that's sometimes that's a bigger impediment than that other times, but a lot of that just depends on the attitudes of the players involved and the players involved. So, we talked about acceptance. A lot of times, in the incident response process, you get to acceptance. The impacted organization is very appreciative and happy moving forward. And a lot of times, they will say, "Well, we're going to look at security differently now. We're going to invest in a lot of different technology. We're going to migrate from a on-prem to Office 365. We're going to have endpoint detection tools throughout the network and a 24/7." So, sometimes somebody will respond that way. Sometimes people will be just, "I don't want to deal with this ever again, and I'm going to sort of take my chances in the sense that I've been attacked once, the odds of me being attacked again is lower." What are you seeing typically?

Tony Kirtley:

I'm glad you brought that up, because I wanted to kind of give a bonus stage of grief. And as a background, David Kessler, who was an associate of Elizabeth Kubler Ross wrote a book in 2019, called The Sixth Stage of Grief: Finding Meaning. And how that relates to these situations is, just as you're saying, Kamran, a lot of organizations, in fact most, take the experience, and a very emotional experience at that, and it sticks in their memory. And I always encourage security leaders to don't ever let that go to waste. The organization just went through a very trying experience. So, capitalize on that to get those security controls to prevent this from happening again, because it's not like a lightning strike. I mean, I think once you demonstrate

that you're capable of being compromised, you're at a higher risk of being compromised again, not a lower risk. So, it's not a round Robin here.

The threat actors don't care if they've gotten your money. And they'll go get it again if you don't plug those holes that they got into in the first place. So, I equate the finding meaning phase with never letting the incident go to waste and capitalizing on that memory.

Sadia Mirza:

And Tony, that kind of takes us back to the incident response planning and tabletops, and kind of documenting your lessons learned, right? This tracks, all of that, what we talk about from a preparedness standpoint really well, because we often talk about, once you do a tabletop exercise, you don't stop there. You take away your findings, you figure out the gaps and try to improve on it from that.

Tony Kirtley:

Yeah. And I think some organizations just hand wave tabletops. And I know it's bad to say that, but they do. It's a paper drill to them. They don't really internalize the recommendations and the results, probably because it's kind of like business as usual, just another meeting that's taking my time. But if they ever had to go through the real thing, they wouldn't think that way, because the emotions involved and the impact that it makes just stresses the importance of that preparation in an exercise. I mean, you guys do them, we do them. We collaborate with our proactive consultants all the time and share war stories with them about some of the things that we're seeing. And those guys take that to the tabletop to make the scenario more realistic.

We include, as I'm sure you do, very specific information from the organization so that it may conjure up those emotions to think, "Oh shoot, that application that I own is encrypted. What would I do if that happened?" And they start to put themselves in that situation mentally. And when they do, then that conjures up some strong emotions, and that's what causes that memory to trigger and them to remember that and internalize that.

Kamran Salour:

Tony, our producers are giving us the signal to wrap things up. And frankly, I'm going through those five stages right now, that I can't believe that time is coming up and I'm angry about it and I'm sad about it, and I'm trying to ask for more time here, but I guess we'll have to come to accept that we're going to have to wrap things up. But before we do, I want to thank you Tony for your time. And I really like this approach, because you're absolutely right. And it's easy to forget when we're talking about ransomware just in general and threat actors and IPS and data exfiltration. It's easy to forget that we're still, at the end of the day, we're talking about people.

And these are people's jobs, these are people's lives, their potential well being, and it's really important to put into context, the emotions that these people can be feeling, not only so we're there for those individuals, because we're in a position to be able to assist them, but I think it also helps us from just a practical standpoint, both on the legal and the forensic side, understanding where human emotions may come into play and making sure that those emotions don't impede the ultimate goal, which is to get the organization back up and running and really have those individuals returned to their "normal lives." So, I want to thank you again,

Tony, for bringing this to our attention. I think it's fascinating. And I hope our listeners find it fascinating as well. So, as our devoted listeners do know, we like to end every session or every podcast with a trivia question, because we will do anything we can to continue to have people listen.

So, this week's trivia question is, what is the sixth stage of grief, the sixth stage of grief? And you can answer that question by emailing the incident.response@troutman.com email account with your answer. And the first person to email with the correct answer is going to get not one, but two prizes. You'll get the customary hacker hoodie from Troutman Pepper, but Tony has been so gracious to include a North Face vest from Secureworks as well. So, the first person to respond will get two sweatshirts, I guess. So, I hope it's cold where you are and you can take advantage of them. But otherwise, I want to, of course, thank you again very much, Tony. And Sadia, always a pleasure to podcast with you. And we look forward to our next installment coming up next month. And thank you all for listening.