Risk in Context Podcast

Episode 19: The Evolving Threat of Ransomware

Tim Marlin:

Hello. I'm Tim Marlin, Cyber Product Development Leader here at Marsh.

Welcome to *Risk in Context*, which features conversations with Marsh colleagues, risk professionals, and others intended to help you better understand key risks, build more effective insurance programs, and think creatively about what's possible in a world of risk.

In recent years, ransomware risks for businesses have reached new heights. That makes it important for companies to understand the nature of those risks, and the considerations involved in decisions regarding ransomware payments.

This episode of *Risk in Context* features a conversation between me and two of my colleagues within Marsh's Cyber team, Susan Young and Stephen Viña, on the threat of ransomware.

=====

Tim Marlin:

So, this is a wide and broad-ranging topic, so let's jump right in here.

For good reason, ransomware is getting a lot of attention these days, not just from cybersecurity professionals and technology publications, but also from the mainstream media. So much so that some of our listeners might think that they have a pretty good handle on ransomware, but the ransomware threat is constantly evolving.

Stephen, maybe you can tell us a little bit about the current trends that you're seeing, as well as the evolving nature of these attacks.

Stephen Viña:

Sure, so over the last year, maybe year and a half, we've certainly seen an increase in the volume and severity of claims primarily from ransomware, and a primary method that's been used kind of true and tested from the bad actors is they'll send a social engineering, a spear phishing, an email that has malware in it with the hopes that someone in your organization — and really it only takes one person — to click on that link and then from there malware will enter the system, the computer network, and then just spread like wildfire looking for open doors with the ultimate goal of really trying to find those administrator privileges and from there to be able to really unlock where the real important information is.

And once they have that, then they really know that they have this organization where they want them, and then they'll start launching different types of extortion against the organization. And so we've really seen an increase in the volume and severity of those types of attacks.

But the attacks have gotten even more sophisticated than that. In many ways, they're still attacking organizations that haven't done a lot of the basics and taken advantage of some very standard to evolving techniques of security, and the bad guys in many ways are using now what we call ransomware as a service and this has kind of expanded the reach of the bad actors in that it's plug and play, so there are just a lot more actors that are that are taking advantage of ransomware and trying to get rich quick with these extortion schemes.

But the growing sophistication — and we've seen recent events where they'll attack the digital supply chain, so they're able to take advantage of maybe an exploit or a vulnerability or zero-day in some type of software that is then used across multiple organizations, hundreds, if not thousands of

organizations — where they kind of lie in wait with that vulnerability and then attacking that at a time of their choosing. Really what they're doing is they're taking advantage of that trust between organizations that work with each other and there's this unknown vulnerability that lies in these systems. And so we've seen these actors take advantage of that situation.

I think a growing trend, and really now it's a much more common practice, is what we're calling a double extortion, where not only do they lock up your systems, they're also looking to steal your data, and we're talking about data exfiltration. And they'll extort you that way, they'll say, "We've locked up your systems and we're going to release your data if you don't pay us X millions of dollars' worth of cryptocurrency." And so the bad actors are really, they're looking for just different ways to exploit and conduct ransomware attacks on the organizations.

Tim Marlin:

So those are really interesting points there, Stephen, especially noting that greater sophistication that the attackers are employing. I think a lot of folks tend to think of ransomware, especially if they've read a lot, maybe 12 to 18 months ago, were really thinking of this more as smash and dash type claim. Low levels of amounts of money that were being demanded. What kind of figures are you seeing that demands are today and in terms of payments as well?

Stephen Viña:

The ransom events, I've looked back and in 2019, 2020, we were talking a few million dollars. Maybe you would see one getting close to five and ten million and then really towards the latter end of 2019 into 2020 we started seeing easily double digits.

Now, you have to remember that a lot of these ransomware attacks, they kind of coincided with the increase in the price of Bitcoin. So as Bitcoin raised to 40, 50,000 dollars per coin, that same ransomware event where they demanded you know five coins just jumped up exponentially. So, these ransom events we've seen today are easily in double digits and, of course, that is the starting point. It is a negotiation that there's vendors that help organizations with. But they have definitely increased.

There was a slight pause, as you may remember, over the summer — there was increased scrutiny from the US federal government and regulators, and really globally you saw a large international outcry at this ransomware scourge that was happening here. And I think even this week, this administration announced bringing together over 30 countries to talk about how to deal with the ransomware issue and trying to come with some common consensus approach of how we'll attack this issue.

So, really, we saw this kind of growing issue and it really kind of crescendoed over the summer. And at that time then we saw — for some organizations, at least — they may have gone underground, they may have gone into hiding. Maybe they wanted to take some time to kind of reinvent themselves. There was a lot of pressure on them. A lot of law enforcement, very high pressure on these organizations and in some cases the law enforcement was successful. And so we saw somewhat of a dip, but now certainly we've seen a continued presence of ransomware just kind of where they picked up over the summer.

Tim Marlin:

Interesting.

So, obviously, a threat that's not going away. Yet even though steps are being taken to help mitigate it and the threat continues to evolve, as you pointed out.

So, Susan, I was wondering if you could talk a little bit then about who's being impacted the most here? Who's facing the biggest threat? Who has the biggest target on their back in terms of companies, entities, governments, who we talking about here?

Susan Young:

Well, thanks, Tim, and I think that was some great background, Stephen, and thanks for kind of really painting a great picture of the landscape.

So, Tim, really directly to your question, this is a problem for everyone. It's companies of all sizes, any industry and at its root this is a cyber hygiene problem. It's all about cybersecurity controls.

So, because of the volume and the severity of claims, what we're seeing is underwriters are just increasingly focused on controls. And this applies to all industries, all sectors, and companies of all sizes.

Now, obviously, there might be some companies and industries that may have more antiquated technology or companies with less revenue may have a smaller cybersecurity budget, which does tend to make them more low-hanging fruit than some of those organizations that may have more robust controls.

But when you think about it, again, from an underwriting perspective, pricing is going up in the cyber insurance marketplace and capacity and coverage are being restricted as underwriters really dig deep into this control environment.

So, if I were to dig in just a little bit to some of these controls some of the most critical are multifactor authentication. This is also sometimes referred to as MFA for short, and it's especially important for remote access and administrative access, especially for privileged accounts.

A few other controls, making sure that backups are secured, encrypted, tested — ideally, they're stored offsite offline. And then also looking for tools that support endpoint detection response and privileged access management, and really focusing on email filtering and web security to make sure that there aren't any bad actors that are putting phishing links in emails that an unknowing employee may click on.

So, those are really, I think, from a high-level perspective the top five controls that insurers are looking for. But, again, you know these are really minimum standards for underwriting and for companies that don't have them, insurability may be in question. So, again, this gets to all industries, companies of all sizes and it gets back to cyber hygiene.

Tim Marlin:

So interesting, so you note that tied to these controls, insurability becomes an issue. Maybe you can talk a little bit about that.

So, for clients that might not necessarily have those controls in place today, what are they facing in the market right now?

Susan Young:

Well, it's a good question, Tim, and it really depends on the organization but, in short, it's potentially restricted coverage if you don't have these adequate controls, but I think, honestly, the biggest thing is insurability.

So, if you think about it, let's take a step back. There are really a few different enablers here. If you think about how these ransomware attacks are actually occurring and being able to take advantage of those poor controls is one of them.

So again, if we're tying this back to the market, insurers don't want to offer coverage on a company that is perceived to have poor controls. So it is the insurability. It's potentially restricted terms. Obviously, it could have an impact on price but, again, I think that the bottom line is, Tim, it just gets back to insurability.

Tim Marlin:

That's really interesting there, because I think this is a sea change for a lot of folks who traditionally have thought that getting cyber insurance was traditionally, if not easy, there weren't going to be any questions about whether they would even be able to get insurance. And hearing this about the controls, it draws the market into stark contrast of where it was even 12 to 18 months ago.

So, turning back to Stephen here, so ransomware — clearly not a new issue, you were talking about things that happened in 2017, '18, and '19, and as Susan mentioned, there are some known controls out there that can mitigate the risks. Why is this still a problem?

Stephen Viña:

Sure, so, I think there are three or four primary reasons, and I think Susan hit on one of the main ones again, looking at those controls. In many ways the bad actors are looking for that low-hanging fruit — who doesn't have multifactor authentication? Who doesn't have some of these other basic cyber hygiene in place? And can those controls be exploited? And the bad guys know that and that's what they're looking for.

In other ways, though, they've grown in sophistication. As I mentioned earlier, they're looking for those, trying to take advantage of those zero-day exploits in a digital infrastructure that is used across multiple organizations and so they really spend time and attention trying to find out a way of how to exploit those vulnerabilities. So, there's a combination of those two.

Outside of that, I think there's a lot of discussion around cryptocurrency and Bitcoin and that it allows actors to move funds quickly without, in some cases, a lot of transparency or oversight. And so the bad actors are

able to move the money, funnel it through various exchanges, and then convert it into Fiat. And we saw in the recent OFAC guidance that was put out and the announcements by the Department of Justice where they actually put, for the first time, an exchange on the OFAC list. And so this was kind of a sea change in their approach where they're going after the exchanges that move the cryptocurrency from place to place.

The third thing I'll mention is safe haven. So a lot of these actors operate in countries that may tactically support these criminal organizations or they turn a blind eye to their activity, and as long as they're not attacking entities within their country, they will allow it to occur. And it doesn't help that we may not have extradition treaties with those countries and so to the extent we can fine the individuals and pinpoint them and name names, trying to extradite them and bring them to justice here in the United States is incredibly difficult.

So, the combination of those three or four factors have all contributed to why we're still with dealing with this issue after several years.

Tim Marlin:

Great, so, clearly, there's a lot for companies to have to digest and deal with there, and even more so once an event does happen.

So, Stephen, in your role here at Marsh, I know you work with a lot of clients who are actively going through ransomware attacks. In your experience, when an entity is hit with a ransomware attack, what are some of the best practices of how they can respond to that attack?

Stephen Viña:

Sure. So it is a crisis situation. A lot of these organizations are dealing with computers that are locked up and moving across the network, and so there are a lot of different factors to consider.

First and foremost, we generally will say do not engage the bad actors. There are vendors, there are third parties that will help you through that process.

What we'd like to see is that the organization will either work through us, through their insurer, and contact their insurer and seek those appropriate third parties that can help guide them through this process. And usually it starts with a breach coach or a counsel that can serve as a coordinator for that incident response in conjunction and to help supplement, or as part of, the organization's incident response plan.

So, taking a step back, I think before we even get to this point, it's critically important that organizations have an incident response plan that has been tested and exercised and regularly updated. It's one thing to say you have a plan. It's another thing to say that we've actually tested it and we know the parties that we need to call and have at the ready if an event happens.

And so really working through that incident response plan, you hopefully have all the different players that will be part of your response, including your counsel, including your forensic investigators.

And to the extent that there's PR, public relations, issues at play, you may want to have those types of services available as well.

And all of that will then help probably shape this question about: Should we pay or not pay a ransom? And in part with counsel and with your insurers and other third parties that actually help to the extent you want to pay or you are having conversations with the bad actors, to determine what is the amount and the history of the bad actor. Third parties can help with those discussions. And so all those factors together can help to really get to this question about whether you should pay or not pay.

Tim Marlin:

That's really important information. And I think underscoring that idea of making sure that incident response plan is fully tested too — I think it's the old Mike Tyson quote about “Everybody has a plan until they get punched in the mouth.” Really having a plan that's been tested and, as we've seen, also being able to have access to that plan, even when your systems are encrypted and locked up, making sure you have that is important too.

Stephen Viña:

Yeah. Tim, and if I might, that's a great point there. If I can make just two more things.

Particularly with the new OFAC guidance that came out, it's critically important that through counsel and through your insurer, you are having those discussions about the OFAC considerations. And in having discussion, in many cases you will have to report the incident to law

enforcement or it is considered a best practice to report the incident to law enforcement, and making sure that they are aware of the matter. I just wanted to mention those two things particularly because of the new guidance that just came out.

Tim Marlin:

Yeah. That's great insight.

And I think we're seeing other moves too. I think there was recently a bill put forth in Congress seeking to push companies to notify law enforcement anytime that they make a payment, which gets back to your question there that you mentioned before, the question of whether you should pay or not. And I know that there are a lot of differing opinions out there so I think I'll toss it to both of you. Every company that is facing a ransomware attack also needs to think about, should we pay or not? So I'll throw it out to both of you. Any thoughts about factors and ways to make that decision?

Susan Young:

Yes, definitely. Thanks, Tim and actually I think I'll punt to Stephen first, but I think there are a few things we can dig into here and these are definitely decisions that every business will need to make if they're faced with a ransomware attack.

Stephen Viña:

Yeah, so I'll hit a few considerations and criteria that I think organizations should weigh when they're considering whether to make a payment. And again, there's third parties that can help you track some of this information as well.

So one, you want to look at the history of the bad actor. Do they have a track record of releasing the decryption key to basically unencrypt your files? Will they negotiate? Do they have a track record of attacking you repeatedly? You might have made the payment and then, in a year, you're hit again.

So you know those are all things and there are different organizations out there, third parties that keep a running list of each bad actor, the average payments that they have negotiated, their propensity to do repeat attacks, the record of whether their decryption key works, so that history is incredibly important.

Number two, you'll also want to look at the sanctions. I mean, this is very, very clear that it's a prohibited transaction if they are on the sanction list. You also want to look at that nexus to a sanctioned entity. Perhaps this is just a new name for an entity that was previously sanctioned. You're going to want to do the due diligence to understand those implications. What is the organization that you're dealing with, the bad actor, and what is their history related to the sanctions list?

Public disclosure — so, if you do make a payment, are you ready to respond publicly about making that payment? Or, conversely, or relatedly really is, if you have a prolonged outage, perhaps you don't pay and now you have a degradation of your systems for a week, two weeks, three weeks, a month. What is your message, your public reporting going to be about your servicing? So, I think having all those responses ready and to think about those ahead of time is very helpful.

And the last thing I'll mention before I turn it over to Susan is, ultimately, you want to think about that operational impact. Is the cost of not paying — does that exceed the ransom demand? And really, we're talking about your business interruption, your impact to the systems or your customers. Think about potential liability, regulatory actions, and then the negative reaction that they may have on your business.

And, so, really, you're weighing all those factors when you're deciding whether you should pay or not.

Susan Young:

So great point, Stephen. And I think if I were to add on that, I think those are four awesome points to start with. I'm going to add on four to bring us home here.

So if I'm going to dig a bit deeper, number five would be backups. So thinking about: Can the company restore information from backups? If they've been attacked, do they need the decryption keys or can they actually restore from their backups? It's possible the backups have been corrupted, so they can't. And, again, this is something we touched on earlier as a key control that underwriters are looking for. So, ideally, those backups are segregated and offline so if an organization is attacked, you have the option to restore from backups if needed.

So the next thing I'd hit on is restoration time. How long is it going to take to restore data from backup? So this kind of gets to some of that operational impact that Stephen alluded to, but at the end of the day, how long

is it going to take to restore from the backups or the decryption keys or, if needed, to rebuild from scratch?

The next thing I'd hit on would be thinking about those attacks that Stephen referenced that potentially involved data exfiltration. What is the value and the amount of data? So thinking about that data that is either known or suspected to have been exfiltrated, what are the consequences of that disclosure? This could be from a legal perspective, a competitive perspective, just a commercial perspective with your customers, so it's really thinking about how many records are believed to have been exfiltrated and the threat actors and bad actors using this as that coercion technique to try to get organizations to pay the ransom demand.

And then the last one I'd hit on here, again — Stephen referenced this early on as well — is the double extortion, also sometimes known as a double ransom. Have they demanded that payment in exchange for not releasing stolen data to the public?

So, again, thinking about it, I think in one of the most recent reports we've seen from Coveware in Q2 of this year, 81% of ransomware attacks now include this data exfiltration component. So, when we're thinking about that, it should be a consideration as companies are considering whether or not to pay.

So I think all of these, I think eight in total, between Stephen and I throwing them all out there, but all considerations on whether or not companies feel that they need to pay or not pay the ransom demand. So I think, again, hopefully these are good factors to think about as organizations go through that thought process.

Tim Marlin:

Thanks Susan and Stephen on that.

That's a lot to take into consideration and it really does go back to Stephen's point earlier about having that tested plan, too. When you're going through a ransomware attack, having to be able to kind of take all of those thoughts in and be able to distill it, and come out, and make an informed, objective decision almost becomes impossible if you haven't thought about this ahead of time so thanks for kind of laying those out.

So, as we talk about this and think about the decision whether or not to pay, I think there's also a debate out there playing out in the media and elsewhere about whether or not ransomware payments themselves should be made illegal.

And while we aren't here today to take a position in the public policy debate, maybe starting with Susan, maybe you can discuss a little bit the arguments that each side is making here.

Susan Young:

Sure. So one side actually is, those who are saying that payments should be made illegal. Essentially, the argument is that cutting off the revenue streams for these attackers or these bad actors will ultimately help prevent attacks from occurring.

Stephen, what do you think on the other side?

Stephen Viña:

Yeah, so on the other side, banning payments means that companies will lose data, money, and operational capacity. And for some businesses that may not have a lot of backup capacity and capital, maybe it means they close their doors.

And in some very dire situations, particularly for critical infrastructure, maybe it means potentially a loss of life if we're dealing with the healthcare sector, particularly.

So, there are definitely some very serious issues if a company is down for a very long time, particularly those in the critical infrastructure sector.

Tim Marlin:

So clearly there is no easy answer on that debate. Any thoughts on how the insurance industry and how cyber insurance generally is playing into that?

Susan Young:

Yeah, I think that's a great point. And I think, generally speaking, while ransom payments still tend to be covered under cyber insurance policies, the best-case scenario is that you're never even faced with one to begin with. So this is where, when looking at the insurance industry, we've really turned around on this issue.

We're in an environment now that enables a lack of controls to be corrected. So, I think here we're seeing insurers do what they've done really well for a long time on many other risks, which is to mandate best practices

that buyers need to follow in order to secure coverage. And that all gets back to cybersecurity controls.

So, I think the bottom line here is, we're looking at the insurance industry as really acting as a catalyst for change.

Tim Marlin:

Susan, that's a great point and we've been talking a lot about ransomware attacks here, but the issue as you mentioned is not just the attacks, but it really is the cyber hygiene that goes along with that and trying to find a way to make sure that we stop these attacks because until we do, they're not going away. And we've been seeing a lot of progress on that front, and it's good to hear that the industry is making that change.

Now we just need to keep the pedal to the metal and driven by the insurance industry, government, cybersecurity professionals all working together to make sure that companies are in the right place to survive these attacks, but also be able to respond and recover when the attacks happen.

=====

Tim Marlin:

That's all for this edition of *Risk in Context*. I hope you enjoyed our discussion, and I thank you for listening.

You can rate, review, or subscribe to this podcast on Apple Podcasts or any other app you're using. You can also follow Marsh on LinkedIn, Twitter, Facebook, and YouTube.

For more insights from Marsh, please visit our website — www.marsh.com.

Until next time, thanks for listening.