-- Speaker 0   00:01   <inaudible>
Speaker 1   00:03   welcome to the trade security podcast. How frustrated do you get when your computer won't do what you want it to do? Or how do you feel when you're standing in line at a retail outlet and the cashier says the electronic payment system is down and now you have to pay with cash. Imagine if you came into work one day and all your computer systems were blocked and there was a message that said something like, pay us and we'll open your system. Think it doesn't happen. Think again. Since 2015, cyber extortion has become one of the most significant exposures for most organizations and the number of attacks and costs has been growing at an incredible pace this month. On the trade security podcast, we talk about the cyber extortion threat and how businesses can protect themselves. My guest is Cassandra long. She's an associate broker, cyber and privacy at Ayaan and she joins me from Toronto. Cassandra, really nice to meet you by podcast.
Speaker 2   01:01   Nice to meet you, Janet. Thanks for having me.
Speaker 1   01:04   My pleasure. Um, I had never really thought much about the cyber extortion situation because you think it only kind of happens in movies, right? But this is a very serious threat. So let's talk about how serious the extortion threat is to Canadian businesses.
Speaker 2   01:23   Great. So that is very true a lot of the times then we have clients who reach out to us. They may be under the impression that because they aren't a health care provider or um, a large bank or retailer, they think that they aren't at risk for an extortion attack. But really there's not really any prejudice in the market for this. Hackers are looking to get a quick dollar and sometimes that might even be an easier route to go if they are looking to attack someone who doesn't have as sophisticated systems as say a retailer, a large bank or healthcare provider. So really everyone in the market who either has personal information that is sensitive to the public that they need to protect or if they rely on technology, they are at a risk. It just depends on how large your risks or your exposure is when it comes to that.
Speaker 2   02:13   So we have seen that ransom demands have been increasing since, I would say around 2016 there was a study that was done by a cyber intelligence company that found around 2.6 million organizations globally encountered a ransomware attack during a 12 month period between 2016 and 2017. So this is growing largely globally and a lot of these cases are still, a lot of these cases are still going unreported as well because if it doesn't involve personal information, we may never hear about it because it's not required by <inaudible>, um, the privacy commissioners of Canada to report it. So some organizations may be handling this in house just paying the ransom or hopefully trying to resolve the issue at hand and restore their information as possible. So there's probably a lot larger number than that. That's just the number that we have for what's been reported so far.
Speaker 1   03:10   <inaudible> so you said something, you said if you weren't a healthcare or a bank or whatever, um, there still is a threat. It's basically anybody who uses technology well unless you're a black Smith or something, I think everybody kind of uses technology now. So really there is, there is a possible threat to, to anyone. So let's explain the possible extortion threats that a business might encounter. What are the actually look like? I mean I explained a couple there, but am I on track or what do they look
Speaker 2   03:42   exactly? So, um, essentially what an extortion or a ransom demand is, is it's essentially a third party who enters into an organization system and infected with malware. So screen will pop up on your computer, which has instructions on how to pay the demand and has the actual demand that the hacker is asking for. One of the scarier things that organizations see, and this is when they start to panic, is a timer counting down until the hacker either wipes the systems or releases data. You cannot click off of the screen or do anything except pay or speak to the hacker. And typically that counter that is taking down the minutes every 30 minutes or every hour, the demand increases. So if you don't pay on time or in a timely manner, your payment is going to increase drastically because they may be asking for two or three Bitcoin. --

--
Speaker 2 04:38 You may think that's cheap, but actually one Bitcoin can be anywhere from eight to $15,000 Canadian depending on how the crypto market is doing that day since it's constantly fluctuating. So there is exactly, so there is four main, um, types of threats that we're seeing. So one of them is an opportunistic extortion, so it's typically a malware with a small payment demand, um, that you would need to pay in order to receive an encryption key. So it's usually a generic attack and it sent him multiple organizations without a targeted focus or recipient in mind. So one of the most popular ones that we've had recently was one to cry. So that affected more than 200,000 computers across 150 countries and they were only demanding about 300, um, to a $600 maximum of USD. So they just sent it out widely and blindly. And they did receive in turn a large amount of funds since it was such a small amount, but it was so widespread that worked for them as well.
Speaker 1 05:46 Hmm. Okay. So yeah, go ahead. No, no, no, you keep telling me. So
Speaker 2 05:54 another one is targeted extortion, which commonly involves a mission critical system or sensitive data. So this is where you would see those large retailers, healthcare, um, large banks. And it is someone who is coming in and real threats to public publicly released data. So these would be things like education law firms where you know that you are storing sensitive data and you do not want that to get out into the public and risk a possible lawsuit or fines and penalties by the privacy commissioner. Um, with the critical system. This would also be detrimental to companies like manufacturers who can't run their systems, critical structures like energy or power. Um, without that ability to access their network and operate their systems, they are essentially down and cannot provide their services to a large group of individuals.
Speaker 3 06:49 Yeah.
Speaker 1 06:50 So who's behind this and, and why are they doing it? I mean, I get it, there's money involved, but really who is it?
Speaker 2 06:59 So it is a global threat. Hackers are from all around the world. Most commonly the attacks are stemming from outside of North America, but we don't know who it is. So what's the nature of this business to hackers are left anonymous. We don't know who they are besides their hacker tag that they'd given themselves. And cryptocurrency is untraceable so anyone can procure, say Bitcoin and authorities have not yet found a way to track where the transfer of Bitcoin is going. So we don't know who is behind it, but there are repeat offenders. So, um, that's the great thing of having a forensic expert or someone to assist you that when they see where the, the hack is stemming from, who that hacker might be, although we may not know exactly who they are, their identity, they can recognize their hacker tag and say that, Oh, this, this hacker is um, a little bit more honest and they will release your encryption key if you pay them. Or Oh, we have a relationship with this hacker. We can negotiate
Speaker 1 07:59 <inaudible>
Speaker 2 08:00 man down a little bit. So it's, it's very, yeah. So there is some loophole that we can try and get in there, but we don't know who was behind this and I don't see, um, anything in the near future of us developing some way to find this because this has been going on for years now and there hasn't been much development on discovering who these people are and how to stop them.
Speaker 1 08:25 Wow. Okay. So we've talked about the impact on a business that's going to cost them money. Their systems are down. If they can't pay, you know, who knows what awful things can happen. But what about down the line in, in your supply chain or with your customers or whatever, even if it isn't your own business set that is attacked, can this have an impact on you?
Speaker 2 08:48 Absolutely. So, um, with extortion there's typically a business interruption that does occur. So with no access or limited access to your systems or your information can cause your or your operations to be slowed or at times at a complete stop. So recently a client of mine was a distributor and they suffered a ransomware, their residual effects of that attack left their business interruption for more than a hundred days, um, which they did have coverage for, for their loss of income. And that depends on what is cons --

-- idered to be a business interruption for them for those a hundred days. Is that fully shut down? Is that only operating at a limited amount? So depending on what exactly is going in to your business daily, that's where it's important to find out if you do have a backup plan for a business interruption. If you do have an incident response plan for something of this nature so that you can respond quickly.

Speaker 2 09:45 So with the growth of supply chain, there's almost a guarantee that an organization may suffer some, a dependent business interruption caused by another's extortion event. So for example, if I was a glass manufacturer who suffered an extortion event and cannot gain access to my systems to run my assembly line, I can't manufacture my product, which means I can't provide my glass materials to say Apple to manufacture their Mac books. So now Apple is behind in production and they can't provide say, a thousand units to best buy in time for black Friday sales. So although it's only the glass manufacturer that separate the extortion attack directly, it may impact more businesses down the line as operations are at a halt. And there's also that privacy aspect to consider. So once access to systems are restored and investigation must be made to find if sensitive information has been compromised. So in the unfortunate event that it has additional costs and requirements are likely going to be incurred as well by that affected in the organization.

Speaker 1 10:45 <inaudible> so you mentioned a hundred days as a possible sort of timeframe for recovery. So I'm thinking about this scenario you just gave us and said, okay, Apple wants to supply all these Mac books to best buy or whatever and they need to do that because it's part of their revenue. So they go looking for another supplier and you could lose your business connections and and opportunity with apples. So like can be a fairly ugly picture candidate.

Speaker 2 11:12 Right, exactly.

Speaker 1 11:14 So let's talk about how a business can actually protect themselves. What's involved and what can insurance do as far as cyber extortion?

Speaker 2 11:24 All right, so there's two main ways that I've suggested business protect themselves. One would be proactively and the second is reactively. So to be proactive, it's, it's smart to invest in your company security, be that hiring an individual with expertise or experience in the cyber and privacy space to help educate the rest of the organization on how to protect themselves with proper procedures and employee training. Other ideas would be to allocate a healthy budget to system controls, things like firewalls and UpToDate systems. Um, and having policies in place in the event that something does happen. So that incident response plan I mentioned, um, it really helps an organization reacting more effectively as a cohesive unit when something does happen. And then reactively, of course, it'd be an adequate insurance policy. So in the event that an extortion attempt was made on an organization, those without a proper cyber policy policy are usually ill-equipped to handle it.

Speaker 2 12:19 So I had mentioned that the tag names of hackers had given themselves, um, with a proper policy that provides expert, um, forensics they can help you with speaking to those hackers, negotiating with them, actually procuring the Bitcoin, which, um, I would think that most individuals or organizations wouldn't have the first clue on how to do that. Cause you can't just go to CIVC or Bemo and ask to transfer your Canadian dollars into Bitcoin. It definitely does not work like that. So, um, and in the event of a breach, you, you need to have that money to begin with. So most recently I had another client, um, of mine who received an extortion demand of over $2 million Canadian. So with their forensic experts and their policy, they were able to negotiate this down by 90%. So I wouldn't guess that typically organizations have $2 million at hand to just pay out whenever something were to happen. So that will really help them there.

Speaker 1 13:21 So you bet. Go ahead. Sorry, go ahead. No, no, no, go ahead.

Speaker 2 13:26 Um, and then once you have your friends who are experts that have helped you get the hacker out of your systems and make sure that there's no chance of getting back in, there's also the chance that your data or your systems have been destroyed or, or altered --

-- and you would need to restore those systems and data as previously, um, to how they were before the breach. So that can also be very costly. So with that and everything else with the policy, it provides sort of a handholding to organization. So one of the most critical services provided under our policy is a breach coach, which is otherwise known as a privacy lawyer. So they are professionals in the market. Um, they're experts in their fields and they handle multiple reported incidents daily. They're available at a moment's notice, which is crucial with extortion attempts since you have that clock constantly too came down. So with so many things happening at once, I breach coach will act as the organization's mediator and we'll walk them through all the necessary steps to recovery. They'll ensure that the correct protocols are being followed in order to comply with many privacy laws. And they will also work with all the other service providers under the policy so that the organization, um, in question isn't being stretched in multiple directions and they can focus on getting their organization to that same state prior to the attack.
Speaker 1   14:48   Right? Like I can't even imagine being a business or a business leader and having something like this happen. And then you would just sit there going, I have no idea what to do. But if you have this support, um, that comes as part of your policy, then you just go, okay, you guys are the experts handle this and I'll figure out how I can maintain my business going forward as, um, as you look into this and get me sorted out. That's, um, I think that's a crucial factor, isn't it? Okay. So, um, to my next question, I guess Cassandra will, like what factors do businesses need to consider when they're thinking about getting coverage?
Speaker 2   15:30   Right. So one of the main things I would suggest is hiring a knowledgeable firm. So fiber is still a new coverage when you compare it to things like property and DNO. So there are new threats happening almost daily. So coverage is constantly evolving. It's important to have an expert on your side to ensure that you have adequate coverage for your unique risk and that your is providing all the bells and whistles, um, that are popping up constantly. Secondly, I would consider what types of limits you may need. So on average and extortion attack can be upwards of $3 million, which includes the actual extortion, demand, business interruption, forensics experts, and that system and data restoration. Now, this nimble, this number will vary based on the amount of demand and how much your business is impacted. And I also had an organization recently who chose to restore their systems from backups rather than pay the demand and their total loss, still more than $5 million due to the business interruption and extra expenses they incurred as a manufacturer.
Speaker 2   16:31   So they were completely shut down. There was no way that they could work through their systems, be a paperwork. So, so they didn't pay that demand. They were still extremely impacted by the event. Another thing I'd suggest is to really review your policy to ensure that there's no hidden exclusions. So some insurers have preferred vendor panels that they wish to use and they will not pay for costs incurred by a non-approved vendor. That's not always a bad thing as preferred vendors will most likely be experts in the field. And this is a stipulation that is more to help the organizations more effectively. It's in the insured's best interest to remove the threat in recovery as much as it is the organization. And another is to review the insuring agreement and actually understand how it is triggered. So there may be a limit to the amount of rents and monies that an insurance willing to pay.
Speaker 2   17:23   There may not even be a willingness to pay at all. So some insurers, most notably FM global, who does provide a cyber solution, um, well not pay the actual extortion demand, but they will restore your system. And another is to see if the trigger for coverage is broad enough. Does it include a denial of service attack where they're demanding an action instead of fund. So one of the most popular ones with that is Ashley Madison. They received a, um, extortion attack, but they weren't actually being asked to pay any demand for money. They were being asked to shut down their systems. They did not want them to provide the service that they were and di --

-- dn't believe that it was moral. So when the hackers requested that they shut down their systems and Ashley Madison failed, they actually released over $30 million, or sorry, 30 million gigabytes of data, um, which included people's names, their addresses, their phone numbers, their email addresses out into the public.

Speaker 2 18:23 And that resulted in, um, dozens of lawsuits that actually Madison settled on since they did not meet the requests. And I do believe that all or all organizations can benefit from a cyber policy. Let's see. So typically most organizations don't have thousands of dollars of Bitcoin stored away or are willing to test their backups and reset their system. So the service is provided under a policy or priceless as the average individual wouldn't know what to do. When that very blank screen pops up with the timer counting down, um, and large global corporations have suffered breaches such as, um, Equifax Bemo target these companies of that size and prestige are vulnerable. Then really all organizations are at a possible risk.

Speaker 1 19:06 Wow. How do you sleep at night, Cassandra? My goodness. How do, how to any of us sleep at night? Um, you said something that I thought was very interesting. You said that there are companies that actually have relationships with these people who are trying to extort money from them and they go, yeah, we can talk this guy down. So I guess my question is, you mentioned, you know, the one company that refused to pay and then you mentioned that, you know, people actually have relationships with these hackers. So w is there an answer to don't pay or do pay and try and bring them down. Is this something that it's just the cost of doing business and you're going to have to pay these guys? Like, do you have thoughts on that or is it just like, who knows?

Speaker 2 19:52 Yeah, so it's, um, the, the choice to pay or not pay is really up to the organization. So it is at your discretion if you believe that it's better to just restore your systems and have, um, your data restored or even recreated if it's, if it's unable to be restored, that is completely an option if you prefer to pay it because you don't want to take the risk or you are holding frontage sensitive information, we can do that as well. So I have seen both. Um, and typically people choose not to pay the extortion because they must be compliant with their organization. So sometimes with public sectors it may be seen as negotiating with terrorists, um, with others, they just don't want to take that risk. So I have not seen that one is better than the other because with my example here of not paying an extortion, it still costs $5 million.

Speaker 2 20:48 Um, and then I've seen other ones where they've paid a little bit and then they have their systems and everything is running smoothly again. So it is at their discretion. I would still always suggest that we try to negotiate and see how it goes from there. Um, but it is great to have those forensic experts who can tell you that this hacker we dealt with before and they doubled it. They got a, and they found another way and, and they demanded double the, the amount of, um, extortion the next time. So that's why it's great to have experts on your side. If you have no idea what to do next, then it's better to go in with a team of individuals who are there to help you. It's in their best interest as well to get you up and running. It's costing them dollars as well as you. So they are, um, the team at your hands. That is the most important thing when something like that happens.

Speaker 1 21:42 Right. So I guess I have a final question for you and that would be any key takeaways that business owners should think about when they, they are considering whether or not to get started with this is maybe, maybe the key takeaway is just call and ask. Right? And investigate. But I mean once a couple of key takeaways that you have for us.

Speaker 2 22:04 Yeah, I would definitely um, make sure that the organization as a whole understands their risks. So if they as a construction company may think that they're not at risk because they don't have any information, but if they are, um, operating automated machines or if they're like mining or something like that, that is something that could be detrimental if they were to have an extortion event. So I would first consult with their it people and discuss how heavily reliant they --

-- are on technology. I would check in, they make sure that they have an incident response plan, a backup plan, something in the back of their mind so that when something happens they know what to do. And for a lot of organizations that plan is call our broker or call our insurance provider, which is completely fine because you want to get them on the phone as soon as possible.

Speaker 2 22:59 And if that is your plan, then that's a good place to start so that you do have something as a backup there. A third thing I would suggest is just filling out an application. A lot of the times, um, in comparison to other lines of insurance, a cyber application can be a bit daunting. They are quite lengthy, maybe anywhere between five to 10 pages. And the questions are very it related. Now when completing that application, if you feel overwhelmed or you aren't sure, that's why you have your broker to assist you. And if you are overwhelmed then that probably means that you are more odd risks. Because if you don't understand the question, you may not understand your organization and the that are at hand. So I would definitely just complete that application, get a quote. Even if you're unsure, if you have someone to walk you through the policy, it can help you realize things that are possibly a gap in your organization and where you may be more at risk. So there's many solutions out there and there's definitely one that can fit your unique risk and tailor it to um, what you need. Exactly. So it's not a one size fits all solution. Definitely. So I would absolutely explore the options that are out there.

Speaker 1 24:19 Wow. Cassandra, this has been honestly a fascinating conversation. Thank you so much for presenting the landscape for us on cyber extortion. I think we all have a lot to think about, whether big or small. Right, so thank you very much.

Speaker 2 24:33 My pleasure. Thank you for having me.

Speaker 1 24:36 Cassandra long is an associate broker, cyber and privacy at Ayaan. You might want to do some investigating on your end if you are a business leader and a business owner. That's our show this week and this month. Please check out our Twitter, LinkedIn, and Facebook feeds and subscribe and share this podcast with your friends and colleagues through iTunes, Google play, and Spotify. Until next time, I'm Janet Eastman. Thanks for listening to the trade security podcast.

Speaker 4 25:01 The trait security podcast is brought to you by the receivables insurance association of Canada, whose member companies help Canadian businesses succeed and grow securely.

--