Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 3: "The Danger of Paying Ransom and How to Test and Train Your Way to Prevention, With Mike McCartney"

Speakers: Kevin Szczepanski, Barclay Damon and
Mike McCartney, National Director of Cybersecurity, Avalon Cyber

[Kevin Szczepanski]: Hey, everyone, this is a Barclay Damon Live broadcast of the Cyber Sip, practical talk about cybersecurity. I'm your host, Kevin Szczcepanski. Let's talk.

[KS]: Hope you enjoyed part one of our episode on ransomware with Mike McCartney. Coming up in Part two with Mike we'll talk about potential criminal liability and sanctions you can face if you decide to pay ransom. And we'll close with some important tips on how you can reduce the risk of ransomware to your business. All that coming up next on Cyber Sip. Stay tuned. So we talked about why you might need to pay a ransom. If you are unable to restore your data from backups, you may have no choice.

[Mike McCartney]: Why not?

[KS]: Right. But what are some of some of the countervailing reasons? Why are the federal and state authorities so stern in their rejection of ransom payments these days?

[MM]: And that's a fantastic question. It's a very unsettled answer at the moment. But the first instance. Is, as you alluded to, I mean it from a law enforcement background. We highly recommend you never pay. Because once you pay, you're considered a mark, right? You're considered a payer. And if you haven't fixed the infrastructure that allowed them in in the first place?

[KS]: Yeah,

[MM]: Right. And now you pay, there's a good chance they're going to come back in and do you again, you know, it's just it's, it's pretty common sense, but people don't really think about it that way. Plus, now you're being shared along the internet to all these different advisory groups and whatever. You're a payer, you're a mark. Right? Whatever. And that you're weak and insecure, whatever. The other issue besides not paying is the Patriot Act and other federal laws and regulations that say that if you're a company in the United States or you're an individual in the United States and you provide "material support" to an organized crime group or to a nation-state sponsored terrorist group, right? which a lot of these ransomware adversaries are.

[KS]: Right.

[MM]: They're like Russia, China. India, Ukraine, North Korea. You know, if you pay money, if it's just Kevin Szczepanski that pays money to North Korea, you could be in jeopardy for federal violations of the

Patriot Act. Or other ... other federal sanctions of providing material support to a terrorist organization. So we haven't seen—unless you can correct me, Kevin—we haven't seen yet any cases been brought by the federal government against a victim company. That paid ransomware that had to pay to get their key back. However, let's not think for an instant that that might not be possible.

[KS]: No, I think you're absolutely right to point that out. I think in the right situation, you could very well see it if you have a company that's trying to do everything right with robust cybersecurity that suffers a ransomware attack. If it's a company that that provides critical infrastructure like Colonial Pipeline ...

[MM]: Exactly.

[KS]: ... notifies the authorities right away, not saying Colonial Pipeline notified as quickly as it could have. But if you have an organization in that situation and then you're partnering with federal law enforcement, the situation could very well be different, in fact, in paying the ransom, the news reports tell us that Colonial Pipeline worked in concert with the FBI. You're not saying that the FBI told them they should pay the ransom...

[MM]: They probably told them not to, actually...

[KS]: Right? But they were aware of what was going on.

[MM]: I don't think they had any choice. I think I think they couldn't recover from backups.

[KS]: And I think and that's that was part of the issue.

[KS]: Right, but on the flip side, so you mentioned you may ... you become a mark, you may be you may be running afoul of, of criminal or international sanctions. But there's another problem I wanted to talk to you about, and it strikes me that you're dealing with threat actors, you're dealing with criminals. And there really is no guarantee that if you pay the ransom, that a) they will give you the decryption key. So let's talk about that. Is there honor among thieves? And then,n, the second part of it is, how well will the decryption key work? If you know, for example, that you've lost, you've been able to recover 80% of your data from your backups and you need that decryption key for the other 20%. How confident can you be that the decryption key is going to recover that 20%? Because it's ... it's very well possible that the threat actors took a portion of the data that you were able to recover from your own backups, right?

[MM]: Absolutely right. There's no guarantee and there's no honor amongst thieves. I mean that's the sort of the third reason why law enforcement recommend not paying. I mean, there's just no guarantee you're going to get the key, you're going to get your data back. And even if you do, that they're not going to come back and whack you again. It's just you know, the best solution to ransomware is robust backups. I mean, that's really the answer. I mean, you know, being in a position where you are completely dead in the water. You have zero access to the data and the information that you need to provide the products and services that you do to be in business, right? And if you can't do that right, you're in trouble. And if you're relying on some group of knuckleheads out of Russia to give you a key to get your data back, man, that's that's a tough position to be in for sure.

[KS]: There's also a risk too, Mike, isn't there that they even if they give you the decryption key and it works and you get the missing data if they have accessed or exfiltrated data from your organization, there's no guarantee that they're not going to sell that on the dark web anyway, so you are..

[MM]: That ... Go ahead.

[MM]: No. Yeah, I. Mean, that's a fantastic point because what we've seen over the last two years. Is what we call sort of like this double ransomware, this double extortion?

[KS]: Yeah, let's talk about that.

[MM]: Yeah, because I mean, that's where you're going. So what a lot of them ... the ransomware malware is doing today and what the adversaries and these organized crime groups are doing is, first, they infiltrate your environment. They get in, they start moving laterally. And they're going to fly low and slow for weeks, maybe months. I mean there's been some statistics out there to say that the average adversary is in an environment for 191 days before anybody finds out about it.
That's incredible, right? To think about...

[KS]: Looking at half a year.

[MM]: If you thought, looking at half a year. So if you thought... if you have a warehouse with all your inventory in it, right and you have alarm systems on there ... Or maybe you don't have alarm systems on, but you have an inventory with all your, you have a warehouse with all your inventory in it. And somebody is crawling around in there for 191 days.

[KS]: Yeah.

[MM]: Popping stuff out the back door. Like, that's incredible to even contemplate. Right? So the average is 191 days. They get in and they fly low and slow, they're in your environment. Then they start picking data, they start pulling and exfiltrating actual information. Right? Sitting on the side, then on the way out, they blow you up. Right? They lock it on with some ransomware, right? And then they say, "Here you go, pay me for the key. Oh, and by the way, pay me to not release this data. Oh, and here's a little sample of it. Just to let you know that I actually have it."

[KS]: Right.

[MM]: It's like proof of life, right. Here. It was the fact that I actually have your data. My proof of life is that I have it. And if you don't pay me, pay me once, great, pay me twice better. And if not, I'm selling the stuff on the dark web and you're just in it just as much trouble as if you did. Well.

[KS]: In fact, you mentioned proof of life. That's something that when we're involved in a ransomware investigation, we're asking for right away, right?Proof of life. Because we want to know if this threat actor actually has the data that it claims to have. And very often it does, but it's a strong sign in your favor if the threat actor is either unable to produce it or if there's some delay. And during that period of delay, you can take the time to rebuild your system from backups.

[MM]: Right. Absolutely right. 100%.

[KS]: So, Mike, you mentioned the backups and that leads me to a final thought. I wanted to talk to you about, about ransomware, and that is you've been in law enforcement for over two decades. You have been a forensic cybersecurity incident response expert for many years now. If you had to devise a wish list of safeguards that every business could implement to minimize the risk ... because we're not going to eliminate it, right?

[MM]: Right.

[KS]: What do you say? I love your phrase: This is a lottery that everybody's going to win at some point ...

[MM]: Your number will come up. This is not a lottery you want to win, but you are going to win this lottery. Your number will come up.

[KS]: So when you inevitably do win the lottery, what's your wish list? And let's talk a little bit about those safeguards that every business can employ that will minimize the risk of a ransomware attack.

[MM]: So it's all preplanning. It's getting ahead of this stuff. You can't wait until this happens, you got me, because once it happens you're, you're in big trouble. And this this this thing is like chickens with heads cut off. I mean, you're running around, you're trying to find a law firm that does this stuff. It's not your corporate contracts attorney. Not your real estate attorney, like you're looking at, not your IT guy. It's an incident response cyber forensic guy, right? You know, doing all this in advance. Making sure that you're actually spending some money on either your internal IT for robust backups, offline backups. I can't tell you how many times we get these cases where they're like, "Yeah, we got hit," and I'm like, "Well, where are you backups?" Well, they were there on the network and they got those too. Of course, that's the first thing they look for. And by the way?

[KS]: Right?

[MM]: Right. Why do IT people insist on calling their backup server "backup server"? Don't call it "backup server"!

[KS]: Drawing attention to it.

[MM]: Right? Yeah, call it "pink fuzzy buddy" or something like, well, you going to call it anything but backup server? Right? Or get that stuff offline. Right. So it's all about having robust, redundant systems from backups, for sure. Doing preventative, what I like to refer to as, you know, your annual physical right? Vulnerability assessments are like your annual physical. It's the only way to put one...

[KS]: Mike, what's a vulnerability test and what's a pen test?

[MM]: Right? Yeah. So a vulnerability assessment is essentially just kind of walking around the perimeter, kind of jiggling the doorknobs. Trying to see what windows we can ... which windows are wide open, which ones we can slide open, which doors are open. Which windows and doors have locks on them? Which ones don't have locks on them, which won't have locks, but maybe not the right locks, right? So that's, that's sort of a vulnerability assessment. Think about it in the physical perimeter kind of thing. Right. We're looking at ways people can exploit you or your environment. And get it right. The pen test is sort of the next step where, "Hey, we ... this window doesn't have a lock on it. We can slide it open. We can slither through it. Once we get through that window, we can make our way up to the second-floor office and to the left-hand drawer where you keep the checkbook." Right? So that's kind of the pen test to exploit those vulnerabilities. Get in and see how far we can go. And see if we can capture a flag. And see what else we can do there. So those are some of the preventative things that I like to analogize vuls and pens to your annual physical is really the only way to test for silent killers within your IT environment. Just like if you can, Kevin, if you ask me, when was the last time I went to see a doctor and I said, I've never been to a doctor, or I haven't been to a doctor in five years, Kevin, like, you'd think I was crazy, right?

[KS]: Right.

[MM]: But I can't tell you how many times I sit across from business owners say, what was your last vul and pen? We've never a vul and pen. All right. But you go and make you literally make your next annual physical appointment in the doctor's office when you're leaving your annual physical right?

[KS]: Right.

[MM]: And they draw blood and they look for high cholesterol, like liver enzymes, whatever. And if your cholesterol a little high, they prescribe a statin and they say, take this for twelve months and come back, we'll do this again. Same thing with the vul and pen. And it's like, Okay. Here, here's how we tested you. You got some issues, make some changes, do some remediation and we'll come back next year and we'll do it again. Right? So those are. Some of the things again. The other big thing is really monitoring. It's having systems in place that can detect and respond. I mean, you brought it up earlier. We can't forget. We've essentially punted on prevention about eight years ago. Right? We can't prevent. There's no way to do that.

[KS]: Forgive me. I just going to say I completely agree with you. And what I always say to myself is my clients have to be right 100% of the time to prevent an attack. The threat actor only has to be right once, once out of 100, once out of 1,000 or 10,000. And if that once out of 10,000 happens, if that lottery—if you win the lottery, then you could have a huge business disruption, financial risk, and reputational risk as well, right?

[MM]: Yeah, it could be company-ending in many instances. I mean, this could end your company... Like they say, 60% of the small to midsize. I mean, Colonial Pipeline not going out of business, JBS is not going out of business, Target didn't go out of business. But, you know, mom-and-pop manufacturing company with 150 employees, and they ... they could very easily go out of business.

[KS]: No, that's right. In fact, I think it was 2019 there was an Arkansas company that suffered, a small company, suffered a ransomware attack and 400 of its employees were laid off on Christmas Eve, and it was as a direct result of the ransomware attack and the loss of business.

[MM]: The ransomware. Yup.

[KS]: Yeah. Let's close on one important point, Mike, because I know you've got a run and really enjoying the conversation with you. But we talked about... you talk about physical safeguards to keep those servers under lock and key, and electronic safeguards that are promoted by [vol] and pen testing, as you said. But, let's talk about the, the, the employee, the sort of human safeguards, because at the end of the day, you can have all the protections in the world built into your network. But if your employees aren't adequately trained and don't understand what to look for, what to do and not to do, you can still suffer an attack. So what's the best way for an organization who may not have a robust training program to start thinking about that?

[MM]: Well, it's to actually employ a robust training program. You've got to test, right? And train; test and train. Test and train. Our employees are our weakest link. And so if you don't have a robust, you know, email, phishing kind of platform or some sort of a program if you don't have internal information security policies that you're testing against or having employees go through and check out of or test out of every six months or once a year, I mean, we do a ... we drink our own Kool-Aid. It's crazy. It's annoying because I'm like, I'm one of the cyber security guys. I gotta take one of these cyber security tests? Like, OK. But it's important. You know, when you have a bunch of employees to make sure that they know what to look for, how to identify a phishing email, how not to click on that Microsoft SharePoint password reset link...

[KS]: Right.

[MM]: ... when you have Microsoft SharePoint, but that just doesn't look just right, or when I click on it I get redirected to the Microsoft SharePoint link and I hover over the URL, it's a .RU!

[KS]: It's not the website that you think it is. Right, right.

[MM]: Right. So I mean, but that's education. Kevin. I mean, that's all training and education and testing. So it's, it's a critical component of any information security program. And we'll talk about this. I know. And maybe some upcoming podcast ...

[KS]: We're going to have you back...

[MM]: You know, this isn't just it this isn't just information security policy. This is an information security program. It's got lots of moving parts. It's got you know, email phishing, it's got training and education. It's vuls, it's got pens. It's got an endpoint, monitoring and detection and response. It's got, it's got all these different things, got incident response plan. So when something happens, you know, you got preapproved law firms on your list, you got pre-approved incident response firms on your list, you got another third-party IT or MSP that's going to help you remediate. You might have a crisis communications firm that's on your list in case you got a message. You know, what's happening out there in the in the world, so you know, having an incident response plan and other piece of that program. And there's lots of moving parts of that program.

[KS]: Well, Mike, as the sun seeps in through the windows here on this fall, Buffalo day. Thank you for joining us and look forward to having you back on another podcast.

[MM]: Thank you, Kevin, for having me. It was a great, great afternoon. Thank you.

[KS]: Thanks, Mike, and thanks to all of you for watching or listening. We'll be back soon with another Cyber Sip podcast.

[KS]: The Cyber Sip podcast is available on BarclayDamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share and continue to listen.

Disclaimer: This material is for informational purposes only and does not constitute legal advice or a legal opinion. No attorney-client relationship has been established or implied. Thanks for listening.