CYBER SIP

*Barclay Damon Live Presents: The Cyber Sip Podcast*

**Episode 2: "Ransomware With Mike McCartney, Part 1: Threat Landscape, Protection, and Response"**

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 Cyber Sip, practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

**[KS]:** Hey, everyone. Welcome to episode two of the Cyber Sip podcast, and I am so proud that we have as our very first guest Mike McCartney of Avalon Cyber. Mike is the national director of cybersecurity for Avalon Cyber, and he's also a highly decorated 22-year veteran of law enforcement. Just a couple of highlights for you as: a senior investigator of the New York State Attorney General's Office, Mike founded the Computer Forensic Unit, and that unit remains in effect to this very day. And as the assistant chief investigator, Mike McCartney oversaw all of the digital forensics and internet investigations for both the civil and criminal divisions of the AG statewide. Along the way, Mike was assigned to the FBI's Cyber Crime Division. We're going to talk about that in a little bit, Mike. But in 2007, Mike co-founded Digits, a computer forensics, cybersecurity, and incident response firm. And he served as president and CEO of Digits until it merged into Avalon Cyber in ... 2015. Right, Mike?

**[Mike McCartney]**: That's right ...

**[KS]:** Mike McCartney. So happy to have you on as our very first guest.

**[MM]:** Happy to be here, Kevin. Thank you. Appreciate it...

**[KS]:** So let's talk about your experience with the FBI. I understand you had a top-secret clearance. What do you need a top-secret clearance for?

**[MM]:** Well, you know, after 9/11, you know, unfortunately, the FBI you know, maybe missed a few cues. I think that's still in debate. But you know, at the end of the day, they were looking for any help they could get trying to connect the dots and keeping people from flying planes into buildings in this country. And so they reached out. They realized that at the federal level, it wasn't going to be enough. And so they reached out to state and locals to kind of bring everybody together and say, Hey, let's get ears on the ground. Let's figure out what's going on out there. Let's bring in taskforce, what's referred to as TFOs or task force officers from state and locals and put everybody in a room and figure out how to connect the dots. And so... but in order to do that, obviously everybody needs to have TF clearances. And we had to work on things that were pretty confidential. Lackawanna Six investigation—many in that ... in the local area that we may be broadcasting to remember the Lackawanna Six investigation. Those were internet wiretaps, internet email wiretaps, a lot of, you know, electronic surveillance that went into those types of cases, but that was the type of stuff we were looking at to try to help, you know, protect America essentially.

**[KS]:** And, Mike, along the way, you've authored a fair amount of publications put out by the Department of Justice. I want to ask you about one in particular, and that is the Forensic Examination of Digital Evidence: A Guide for Law Enforcement, which came out, I think, in 2004. I know that's still in use today. Can you talk to us a little bit about how important it is to have a series of concrete guidelines that law enforcement can use across the board?

**[MM]:** Yeah. So it's interesting, Kevin. Because the evolution of digital forensics really came along from the mid-'90s, late '90s into where it is today, where lawyers and law firms and corporate counsel use forensics to do all kinds of investigations. You know, employee cases, whatever. But back then, it wasn't even called digital forensics. It was called like the "extraction of digital information from a spinning magnetic media" or whatever. Like, nobody knew what this was. And so there came a point where the forensic community needed to get their arms around digital forensics. And the people in the white coats and the forensic labs, you know, there used to like a very strict forensic process, right? If it's a white powdery substance, we run it through a process. It's either cocaine or heroin, and we could test its purity. But the green vegetable matter, right we could run through a process that we can help determine what you know, what kind of THC level.

**[KS]:** Makes it easy ...

**[MM]:** ... With computers. It was a very, you know, the forensic sample was so dynamic, right? It wasn't just the white powdery substance, it was a Windows machine. It was a Macintosh machine. It was a Unix machine. You know, it had different applications and software that was running on it. And nobody in the forensic community really knew how to deal with ... How to extract the relevant information out of all those applications and those different platforms or operating systems or systems. So NIST (the National Institute of Standards Technology), which is one of our governing bodies of all things. Brought in a bunch of stuff. Yeah, right. All things everything, really. I mean. From weights and measures to gasoline.

**[KS]:** Right, right.

**[MM]:** Brought in a bunch of subject matter experts and said "Hey, guys, we need to figure this thing out. Like we need to try to figure out how to apply some standards and some consistency to what we're calling digital forensics. So I was one of the ones that was involved. There was many of us. It was what we call consensus authoring. So we consensus authored. That's actually what the one book you quoted is one. It was actually two and there's some other publications, but it was a way to get our arms around. Like this thing is, this is the best practices in how to approach processing and extracting digital information from computers so that it can be used in court.

**[KS]:** And we're going to talk about getting ... getting our arms around ransomware today. And it seems as though whatever evolution and growth over time we've had in our ability to get, get our arms around digital forensics, that the threat actors always seem to be a step or two ahead of us.

**[MM]:** One-hundred percent.

**[KS]:** So Mike, let's turn to ransomware and before we get started, since I think in the cyber world, we often all use terms that we think everybody knows what they mean, but they often don't. So give us a good definition of "ransomware." What is it?

**[MM]:** It's really just a piece of malware, virus malware, that can get injected into a system, computer system, that essentially will then run applications to encrypt data. Lock data from access. Right? And then the user that that deployed that application is the holder of the key. And so in order to unlock that data. And this is encryption D.O.D. standard, like you're not going to break this encryption right. That's like ...

**[KS]:** D.O.D., you mean Department of Defense standard?

**[MM]:** That's right. Department of Defense data. You either need ... to be able to recover from backups. And if you can't, you're going to have to get the key because there's really no other way around it. There are some, some of the malware ransomware variants that are out there have been out there for a while. So if you're lucky and you get encrypted with an older version of a piece of ransomware, there might be a key readily available that you might be able to be able to pull down and use to decrypt, but most of the time, you're pretty much reliant upon the adversary to unlock your stuff.

**[KS]:** And we're to talk about the encryption keys in a little bit when we cover the vexing question of whether you should pay the ransom. But Mike, how do you know you've suffered a ransomware attack? I think many people know, but some don't. How does that become apparent?

**[MM]:** Well, it's pretty easy because you can't access anything. You know? Usually it comes in at like three in the morning or on a Friday before the fourth of July weekend. You know, I mean, I think our adversaries plan that and launch their attacks on the most inconvenient time for companies. But typically, you're going to get a call from your IT provider, either it's a third party provider, internal IT department, that's going to say, "Hey, we can't get access to any of our stuff, our file servers down, our domain controllers down, our web accounts are down, like we cannot access anything" and it's showing an extension on the end of every file that's indicative of like a ransomware variant or when a ransomware type of ... type of software that has taken over that account.

**[KS]:** So I pulled some statistics before we went on today, I want to run those by you and then ask you a question about it, so...

**[MM]:** Sure...

**[KS]:** According to Verizon, 10% of all breaches are ransomware now. In the last year and a half, about four in ten global organizations tell us that they have been the victim of some form of ransomware attack. And according to the FBI, the number of ransomware complaints through the first six months of this year alone is just under 2,100, and that represents a significant, I believe it's a 60% increase over the same period in 2020. So why are we seeing such a significant uptick in ransomware attacks? Is it the remote work that's come as a result of COVID? Or is there something else going on?

**[MM]:** I think it's both, Kevin, to be honest with you. It's the opportunity has gotten greater as we've expanded our attack surface. So when I talk about "attack surface," right, when you know, pre-COVID, most people were in corporate offices, right? So you had a corporate infrastructure that your IT providers, and if you had enough to have an information security provider, right, you could protect, right? It's all in kind of under one roof, so to speak. So your attack surface was limited to that corporate environment. But as coronavirus came and we jumped to this remote workforce, we've expanded our attack surface exponentially. Right?

**[KS]:** Right.

**[MM]:** And so now you have people all over the country, all over the world that have access to these corporate environments. Right? We say, "Hey, go home and work on, by the way, you can log into what used to be under our roof that we used to protect," right? And so that's number one.

**[KS]:** And the computers they're using ...Forgive me for interrupting, but I just wanted to ask you about that. The computers that we're using when we work remotely are often not nearly as secure as those that are in the office environment.

**[MM]:** Sometimes they're personal computers. If the corporation can afford to give everybody a corporate-owned laptop or something, great, and then the IT department in that corporation could do some, some control and some monitoring and some oversight of those assets. But when you just say, "Hey, go home and just here's an account to log into," right? That just further expands your attack surface. The other thing is that ransomware pays.

**[KS]:** Yeah.

**[MM]:** It's lucrative. If it wasn't lucrative, the adversary wouldn't do it. So it's a very lucrative business, and it's a very fluid and entrenched organized crime syndicate. You had different people doing different pieces of this. You got the... the original hackers that are out scraping credentials. You know what we call the harvesters, right? And then you have them selling those credentials to the people that go in and actually hack and steal information that they sell that to other people that use it for identity theft and credit card fraud and, you know, whatever. And then you sell it to the adversaries. That are doing the ransomware for money. And then they come back in and use those credentials that lock you up. So it's a multi-tiered organized crime syndicate. And it pays. If it didn't pay, they wouldn't do it.

**[KS]:** Yeah, and you say that it pays and it really does. I mean, the statistics differ depending on the organization, but I think Verizon tells us that in the first six months of 2021, ransomware has been responsible for about $590 million in business, and all of last year was a little over $400 million. So you can see in those numbers the dramatic increase, and some of it, as you say, is foreign state, often Russian, sponsorship of the ransomware attackers. In other places, it's the lax cybersecurity, which we're going to talk about a little bit later. But as you say that that third reason is so important: it is lucrative. So let's put a pin in that point about how profitable ransomware is and let's let me set the table for you. Here's a scenario: You're the CEO of a mid-sized business and it's Sunday morning, 5:00 a.m. You get a call from your CFO who tells you that your computer systems are locked, you have no access to the data, and you've suffered a ransomware attack. I know we're going to talk about the incident response when we have you back for another podcast, but what's the goal at that point? What does the organization have to do to get back up and running?

**[MM]:** So there's a couple of things like immediately, you know, when they get that call like, "Holy cow, our systems are shut down. We cannot go to work Monday morning and actually perform and provide the products and services that we do for a living. This is what we do." So the first thing is in my ... in my experience and recommendation is to call your attorney. These become legal obligations. This is not just the "Oh, it's an IT issue. And if I could work through my IT issue, I can just get back to work and everything's fine." No, there are significant corporate legal obligations that get triggered as a result of these things. And I'll let you speak to that—if you want to do a podcast, we could flip the seat and I'll ask you questions.

**[KS]:** Right.

**[MM]:** But, but the point is, is that like the first call is to your counsel because they want to start looking at what kind of insurance coverages you have. Do you have cyber liability? Does it cover ransomware? Do you have an errors and omission policy that maybe has a technology provision that may help you cover some of the stuff. Do you have an incident response firm that's going to help you figure out, and work with your IT team, to figure out really three questions: How did they get in? Right? What window or door did they crawl through? Where did they go once they were in your network? What were they after, were they after HR data, were they after financial data, what were they after? And then the biggest question of all is what did they take, right? Or what did they access, depending upon what state you're in. And I think we'll talk about more of that if we talk incident response.

**[KS]:** Right

**[MM]:** But but. Really, it's, it's a, it's a major sort of "all hands on deck" to say, OK, first of all, we need to isolate the damage, right? We need to figure out where the attack vector was, what machines, what we call patient zero or patient one, right? Where did the attack come in? And where did it go from there? It's kind of like cancer. Well, I got cancer in my thyroid, and now went to my liver. It went to my, you know, whatever. So where did the attack vector come in and where did it go? And then how do we contain that? Like, we absolutely need to stop the bleeding and contain that threat and that bleeding. I mean, the biggest thing after that is, you know, ratification, or remediation. Like, how do we start to get systems back up and back on-line?

**[KS]:** Right

**[MM]:** Hopefully, you have backups right as you recover from. If you don't have backups, then it's a big-time decision to determine whether or not you need to pay to get the key to get back in business. I mean, that's a whole 'nother conversation.

**[KS]:** Well, let's turn to that conversation now because it is an important one. And we're seeing increasingly, I think, at the federal level from the ... from the White House to the FBI and other law enforcement agencies, the message is sent that you should not pay a ransom. And I want to talk to you about that. But let's again, let's, let's continue to set the table. So you've ... you've, you've called your lawyer, you have a forensic expert that is investigating the attack vector, what's been accessed, how to get back online. And let's say for a minute that you do have backups, but they're not complete. So maybe you're able to restore your systems from backups over two-to-three-day period, but you can't restore everything. You know that a certain portion of your data, maybe it's your customer data, maybe it's personnel or health records, they're not coming back. How do you make the decision whether to negotiate with the threat actor for the decryption key? What are the some of the factors that an organization needs to be thinking about before it makes that difficult decision—we know it does get made, ransoms were paid, JBS paid, I believe, an $11 million ransom earlier this year; at least told us that it did. Colonial Pipeline paid a $4.4 million ransom earlier this year. How do you get to the point where you decide whether or not to pay the threat actor?

**[MM]:** It depends on how important that data is to you? You know, I mean, it really comes down to a business decision. Right? And you know, you know, we've talked about this before, Kevin, you and I are friends, we've done a lot of work together. But it really comes down to the information, governance. And data retention, right, so, it's all that kind of preplanning. You know, in advance of a cyber incident, right? To understand kind of where your data is, where all your important stuff is, and how long you have to keep it, you know, and what you need to do to recover if you lose it, right? I mean, those are the key elements to these types of questions. So when it comes back to like, can I recover from backups, or maybe I can only partially account for backups? Well, what am I not able to recover from and do I need that today? Or can I, can I recreate that ... You know, I just had a case the other day where the client was like, "Well look at, some of that. I can recover the rest of it. I'm not going to pay these guys to give me a key to recover this. I'll just pay my internal staff to re-key it." Right? I'd rather pay them 20 bucks or 25 bucks an hour or whatever to re-key and reenter all that data and ...

**[KS]:** Right

**[MM]:** Pay this knucklehead.

**[KS]:** Yeah.

**[MM]:** ... you know, ten grand to give me a key. You know what I mean? So it comes down, it really comes down to a business decision as to, you know, how important is the data to you? How long can you live without it? And what's it going to take to recover it?

**[KS]:** Yeah, no. I think that's exactly right. And we had an experience recently with a client where the client did have reasonably broad and sound backups and was able to get back online within a few days. The client was concerned for his customers that he do everything possible to recover and protect as much data as he could. So one of the questions we had to answer was sitting here now, knowing that we're thinking about negotiating a ransom, does it make sense for us to do that so that we can say later to our customers, our employees, whoever it may be, "We did everything possible to recover and safeguard your data." How does that factor into the consideration as to whether to pay?

**[MM]:** Well, I think it goes a long way. Kevin, actually. Because there's ... there's a lot of downstream things that come, as you know. Right? So, you know, all the work you can do in advance of these things, you know, having board meetings, bringing in experts, having committees that talk about cybersecurity, like being attuned to all of these risks, whatever. When something like this happens and you are, then in the midst of an incident, right? Keep in mind again, as I started this conversation, you have legal obligations to disclose and notify to Attorney General's office ...

**[KS]:**... is absolutely and the data [illegible]. Right? Sure.

**[MM]:** Right, so, so the more you've done in the advance and the more you're done in the process of the incident is going to help you negotiate with the Attorney General's Office and the consumer fraud protection bureaus, and the Homeland Security Department. And whether you're in a regulated body like Department of Education or Health and Human Services. Or whatever other layer of regulatory oversight you're in, right? All of those things are going to seriously help you. So I guess my point is, is that it's just important to do some advance work, do some preplanning and get some of your ducks in a row. But when it comes, when the rubber hits the road and you have to like, figure out how to negotiate this incident, anything you could do to kind of manage and mitigate your exposure is going to be helpful.

**[KS]:** So you're talking about a situation where you of an organization has had a ransomware attack. It knows through its forensic investigation that PII (or personally identifiable information) or PHI has been accessed, it has to provide notice not only to the affected individuals, whether they're customers, consumers, or employees, but it also has to provide notice, depending on state law, to regulators. So, you're providing this notice to regulators, and you may be at the same time struggling with this decision, whether or not to pay a ransom to recover whatever you couldn't restore from the backup. Those regulators—federal or state—are going to strongly discourage you from paying a ransom. 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.

**[MM]:** 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 been right. 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]:** like Russia, China. India, Ukraine, North 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]:** Hope you enjoyed part one of our episode on ransomware with Mike McCartney. Coming up in our next episode, Part Two with mike, we'll talk about potential criminal liability and sanctions you can face if you do pay a ransom and we'll also talk about the steps you can take to reduce the risk of ransomware to your business. That's next time on Cyber Sip, we will see you