Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 6: "When Your Number is Up: Responding to a Cyber Attack, Featuring Mike McCartney"

Speakers: Kevin Szczepanski, Barclay Damon and Mike McCartney, 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 Szczepanski. Let's talk.

[KS]: Welcome back to the Cyber Sip podcast. And welcome back to you, Mike McCartney. Thanks for coming back.

[Mike McCartney]: Thank you for having me.

[KS]: It was the first time we talked a little bit about ransomware and we touched on incident response. So I wanted to have you back so we could devote a little bit more time to that subject. But first I just want to remind everyone: Mike is the national director of Avalon Cyber and a highly decorated 22-year veteran of the law enforcement community. And Mike, do I have this right? You are the founder of the Computer Forensic Unit of the New York State Attorney General's office.

[MM]: Yeah, that's correct. And then we, uh, we ran that unit for almost 20 years, doing all kinds of digital forensic investigations under four labs that we created, as well as all kinds of internet crime and undercover internet investigations for a couple of decades.

[KS]: You've seen it all. And we're happy to have you back. And on today's episode, I want to talk to you about incident response. And why don't we start with a definition when we say incident response—and sometimes we shortened to IRP—what are we talking about?

[MM]: We're really talking about, um, conducting an investigation of causation investigation to some extent. It's not a true causation investigation like most insurance carriers would like to see. But essentially we're we're working for a law firm representing a company that has a security incident, and we're careful to call it an incident for a long time until we can actually determine it's been a data breach.

[KS]: Right.

[MM]: Because once you get the data breach, a lot of legal obligations start to get triggered and notification and disclosure and all kinds of things start to happen. So it's an "incident" and we're investigating an incident on behalf of counsel generally ... 99% of the time on behalf of counsel representing the company so that everything we do can be covered by the attorney-client privilege. But we're really hired by the attorney to answer three primary questions: How did the bad guys and the adversary get in? What window and door did they crawl through? Secondly, where did they go once they were in? Were they across the network? Were they after HR data? Were they after financial data?

Were they after competitive business intelligence data? Like, what were they after? And then the biggest question of all, I mean, the most paramount question of all that we need to answer is: What did they access or what did they take? Because each state has a different notification and disclosure obligation law. Some states are access law or access states, some are exfiltration states. And I know we're going to get into this a little bit more.

[KS]: Right now and you make very important points, right from the outset Mike and I just want to underscore them: first of all you're absolutely right, calling it a security incident. Sometimes I like to call it a cyber incident, although we should talk about the definition of cyber in cybersecurity sometime as well. But not every incident is … results in a reportable data breach.

[MM]: So that's right,

[KS]: …as we use the term "data breach" generically, and we really shouldn't, because we should if you have an actual data breach. You are obligated under the laws of one or more states, maybe even under federal law if it's a PHI or health care–related breach to make reports to federal and state authorities And in our experience Mike, I don't know about yours, but in our experience, often the investigation concludes that there was no reportable data breach.

[MM]: That's right.

[KS]: So you talked about the first three buckets that I think are very important. So let's say you have an organization that has experienced a cyber or security Incident. Mike, what's the first phone call that that organization needs to make and why?

[MM]: Well, I'll tell you, we generally will get the call initially, and I will recommend and tell the client to turn around and call their attorney. And by the way, not your contracts attorney or your real estate attorney—most companies have attorneys that do different factions of the business for them, right? Legally. But you need to call a data privacy cybersecurity attorney that understands the legal obligations that are here. You need to call them first because you don't want to hire us directly. I mean, you can, but it's not advisable. Like you really should get a lawyer that's going to hire us on your behalf so that we can protect the privilege and we can work through all the things; all of our all of our investigative reports, all of our emails, all of our conference calls, all of our forensic finding reports, everything is protected by the attorney-client privilege. And your attorney—because you're going to have notification and disclosure obligations under this incident (we'll call it an incident still for now) that you're going to want to be your attorney to be able to disseminate that information under their purview and under their control. You don't want to just hire us directly. And then if the AG finds out you hired us, and they subpoena me, I've got to turn everything over like I have no protection. So.

[KS]:So we need to be protective of that privilege that we talked about a moment ago. Very important. All right. So the business calls you, you say. That's great,happy to work with you.

[MM]: Call your attorney.

[KS]: …Call your cybersecurity lawyer first. And so they do they call. And what's the next step? What's the next phone call in the mix?

[MM]: Well, insurance. I mean, hopefully they already have cyber liability insurance. If they don't, obviously, you know, the lawyer is going to try to work through the policies they have. Maybe they got an errors and omission policy, has got a technology rider that the lawyer can maybe sneak some money out of. Maybe there's some general liability stuff, depending upon the way it's written or covered. But the key is … is, you know, looking at insurance coverages, if you have cyber liability, obviously that's the next call to contact your

... your claims adjuster. But then there, too, that's a whole 'nother conversation and that we can talk about is, you know, they might have preferred lawyers and vendors that they want you to use but understand you don't have to use them, right? There are ways to kind of work through and say, Well, I don't want to use an information or incident response firm out of California. I want to use a company down the street, I've used them for other stuff. It's one throat to choke—like I know these guys. Right? Can I add these guys to my case and they're going to be a couple of hoops to jump through, but generally we can do that, or you can do that same with your lawyer. Like, I don't want to use a Philadelphia lawyer... no pun intended or no, no insult intended. But you know, hey, I want to use the guys down the street that we use for all of our other stuff. So there is some leeway in some negotiation you could do there.

[KS]: Yeah, that's a great point, Mike. And it's a very important one when you're calling your insurance company you have two goals: First is you want to maximize your potential insurance coverage for the cyber incident...

[MM]: 100 percent.

[KS]: ...have that insurance in place. You want to make sure that your carrier knows about the incident as soon as possible so that there aren't there isn't some a gap that results in an absence of coverage. And, the second thing you're exactly right, Mike, there, at your earliest opportunity,you want to think about who you want your counsel to be, because if you are comfortable with the insurance company's panel counsel, you want to get that firm involved as early as possible so that they can hit the ground running for you. But if you're more comfortable with your own tried and true cybersecurity lawyers, you want to initiate the process of seeking approval from your carrier to use your own lawyer, and the earlier you do that, the easier and more efficient that process is going to be going to be.

[MM]: 100 percent.

[KS]: That's a great point. We've got the first call to the lawyer. Second call to the insurance company. And let's say none of these things happens immediately, right? So we have a lawyer in place. The company is protected. We're working on ... on confirming the insurance coverage but even as all of that's going on, Mike, there's a third phone call that needs to take place and it comes from the lawyer and who is that call to?

[MM]: Generally an incident response firm. I mean, you know, they're going ... your lawyer is going to have a call with the internal IT guys and folks, and it's going to be, Hey, what do we know? When did we know it? Right? But then at that point, they're going to be like, We have no idea. Uh, we're trying to figure it out. So generally, your ... your your legal team will engage an incident response team, which is not your IT team. There is a big difference between information technology, IT and information security, IS, two completely different things. We all have initials after our names are just different initials.

[KS]: Yeah, no. And that I think that's an important point. Mike, let's pause there and talk about it because I think a lot of folks think that the information technology professionals they have helping them day after day in their firms are also information security experts. But yeah, that may be the case, but very often it's not. There are two different disciplines. Can you talk about that?

[MM]: Yeah, for sure. There are absolutely two different disciplines... Now you might have an IT person who's also got an information security background and maybe a couple extra initials after their name that's security related, which is great. Fantastic. Most of the bigger, regulated industries have an IT department and an IS department. Think about Blue Cross Blue Shield, Health Now, you know, Independent Health how like all these bigger ...bigger entities that are regulated? They have a 100 person IT department, they have 100 person IS department, right?

[KS]: Right?

[MM]: Most smaller companies, small to midsize companies like us, and like you, or people that may be listening … to this 50 people, 100 people, whatever. They have an IT department. They maybe have one or two people. They don't have an information security department. And I like to analogize IT and IS much like the practice of law or the practice of medicine, right? You go to school, you go to med school, you learn about physiology and all kinds of body function and things. But then you come out and same with law school you learn, how to research and write and read and become an analytical lawyer. But when you come out, you become specialized, right? You got real estate attorneys, you got contract attorneys, you got criminal defense attorneys, personal injury attorneys; you got orthopedic surgeons, you got heart surgeons, you got brain surgeons…like, you know, like, I would no more have my real estate attorney represent me in a homicide case as I would have my orthopedic surgeon perform brain surgery on me, right? So it's the same thing with IT and IS. You really need to think about this, it's not just like, well, it's computers. I got a computer guy, right? That's not exactly the answer.

[KS]: And that's no, it's true. I mean, and to carry the analogy further. The cardiologist is a great doctor, knows everything there is to know about the heart and we need that we also need the ophthalmologist that kind of problem with our eyes. So I think that's a critical distinction, Mike, and it's no criticism of the IT warriors on the front lines every day. They do outstanding work and they … they take a lot of abuse from time to time because, of course, when something goes wrong with your computer, you need it fixed ASAP. And that's not possible or practical. So you've called now you've called your lawyer, your lawyer iss involved, your carrier's involved and your lawyer has contacted … or your carrier might have contacted a forensic cybersecurity firm. And let's say that's you, Mike. You get the call … and you've gotten that call from me and I I don't know how it happens, but whenever I call, you either answer the phone or call back within 60 seconds or so, and that's part of it to… to be available. So you're available, you get the call …and what's what are the steps that you are going to take as a forensic investigator looking into this security incident?

[MM]: So the approach most firms like us will take—and we're not unique in this—I mean, we like I like to think we are a little unique, but we're not. I mean, overall, it's really a, you know, a three-step process. I mean, we're walking through an incident response, right? This isn't a data breach—and by the way, you want to make sure that your employees aren't sending emails saying, "Hey, we were breached." And you know, the IT guys telling, you know, emailing the CEO, "Hey, we got breached last night. We got, you know, like, that's that's something for you lawyers to figure out later and kind of manage damage control where it's an incident…

[KS]: Right, right.

[MM]: It's an incident that we're investigating. And our main … our main objectives is really three… three … to answer three questions. One, How did they get in, what window and door did they crawl through? Where did they go? What were they after? Were they after financial dollars? Were they after HR dollars, were they after, you know, competitive business intelligence? And then the biggest question of all is what did they access or what did they take, depending on the state that you're in? Because some states are access states and some states are exfiltration states, so. And then we provide so, you know, in addition to answering those three questions, the first thing we're doing is isolation. We're working with the internal team to isolate the issue. Let's find patient zero. Let's isolate patient zero so we can stop the bleeding, right? Keep that from promulgating throughout the environment. The second thing is containment, right? Which is part of that. Let's make sure that once we isolate patient zero, that we can contain the rest of the environment. And then the third thing is remediation. OK, once we've contained or isolated and contained, now let's start to get you back to a place where you can get back into business. And that's a balancing act because we talked about, you know, backups and recovery from ransomware, I think one of our last pod callss.

[KS]: Right.

[MM]: But, you know, understanding that your backups could actually contain the same ransomware malware that infected you in the immediate instance.

[KS]: Right.

[MM]: So there's a whole process that goes into making sure that if you're going to recover from backups, that you're doing it in a safe and effective manner and you're not just kind of reinfecting yourself.

[KS]: No. Very helpful, Mike. Thank you. And you know, along the way, the... the forensic experts. The lawyer and your insurance company are working hand in hand with your own business's quarterback, if you will. Could be a CISO—chief information security officer if you have one; it could be your general counsel. It could be your CEO. If you're a smaller business, you may have that that task handled by... by the man or woman in charge. But ultimately, you're going to generate a very important report and you touched on the critical issue a moment ago. And that report is going to hopefully let your business and the lawyer know whether or not information has been accessed or exfiltrated. Let's assume that we're in New York, Mike, and that it's—which is now an access state—or that you're dealing with PHI, or personal health information, that is subject to an access requirement as well. What steps are you undertaking as part of your investigation to determine whether that protected PHI or PII has been accessed?

[MM]: So that's a great question. We go through a very lengthy forensic process to document and be able to report with a high degree of forensic certainty the number of records that were accessed and or exfiltrated. Now keep in mind, sometimes you just can't do it. There's not enough forensic data or forensic artifacts to be able to check all those boxes and be able to drill down with a high degree of forensic certainty that, you know, out of a HR database that has 2,200 records in it. Only 201 of those records were accessed and or exfiltrated.

[KS]: Right.

[MM]: That'd be awesome if we could do that in every case. Right. Some cases we can. But it depends on the the log-in and the verbosity of the logs in that HR database. It depends on a whole bunch of forensic artifacts that kind of lead us to that place and be able ... to be able to determine whether or not we can say that. But ultimately, the reporting is the key. And so, you know, any incident response cyber firm that is engaged in these types of things should be able to write reports—coming from law enforcement we have a very kind of structured reporting structure, and we write these reports for a much larger audience, right? The first ... in the first instance, the report is written for the client and the attorney that an executive summary, list of facts, kind of scenario of a timeline of events, right? Right. But ultimately, we're writing this for ultimately a court, internal and external auditors, the insurance company, right? There's a whole bunch of people that ultimately could end up with this report. So it's really important that the forensic findings are documented and well-articulated so that this document can live...and more importantly, one of my forensic investigators or even me can get on a stand in 12 months or 18 months or 22 months from now and look at this report and be able to regurgitate, like what we did, right, not like I have no idea what I'm saying there.

[KS]: That's so... ... right though and that's so important. What we tell our clients and I have talked about this...

[MM]: 100 percent.

[KS]: ...Before is there's a twofold purpose to doing what we do. We're doing it first because it's the right thing. We want to protect our data. We want to protect our customers and our employees. But the second reason we're doing it is equally important because...

[MM]: Down the road ...

[KS]: ...right? We want to be able to say down the road, if something happens, we took all the reasonable steps we needed to take to protect our data, to protect our business so if something goes wrong, you can mount your best defense and ... talk about the, the, the interplay between the legal team, the client team, and the forensic team as the investigation goes on, because it's really, it's a very cooperative and collaborative process, right?

[MM]: It has to be, it 100 percent has to be, you know, we're working for the lawyer who's working for the client, right? I mean, let's just understand the chain of command here. Right? So yeah, it has to be cooperative and collaborative. We need the support of the internal IT folks or external third party IT folks, whoever it may be. We have to collaborate on how we're gaining access to systems, how we're looking at ... forensically looking at stuff. And the cool part about the way forensics has evolved is when I was back in my law enforcement days is we can do almost all of this stuff over the wire, like we don't have to commandeer helicopters and rappel in our ninja suits with pelican cases and take over conference rooms, yeah.

[KS]: Thank goodness

[MM]: So we mean they that's right, because that usually costs a lot of money. I mean, that's the way we used to do it, although

[KS]: Some might still prefer to do it that way

[MM]: Yeah, and some actually still prefer to do it that way. But, you know, doing it all over the wire, it's, it's uh, it's a much more efficient and cost-effective way to do it. But we need cooperative, collaboration and cooperation to be able to get the information we need to get the information and to be able to document exactly what happened.

[KS]: Right.

[MM]: But keep in mind, there's times we can't. I mean, I ... I try to manage people's expectations. Like I'll say, you know, our ability to answer the questions your lawyer needs answered is going to directly relate to the availability of log data. And right, if you have no log data on your domain control, you have no log data in your firewalls. If we can't, like, go back in time, if you're only capturing logs for two days and this happened six weeks ago, like, I don't know what ... don't know what to tell you. I mean...

[KS]: And it's funny we touched on this in our, in our earlier podcast, and I think we need to have you back to to talk about...

[MM]: To do that..

[KS]: About data classification and the mechanics of logs so... and I may be oversimplifying it, but as I like to think of it as: if you have data classification and segregation, you know where the important data—the protected data is—in your system. And if you have sufficient log-in data, you know whether someone got in to that...

[MM]: To that data,

[KS]: ...and that can be really helpful. We love it.

[MM]: Extremely.

[KS]: Because then we can conclude yes or no, fairly confidently and as you say, to a reasonable degree of forensic certainty that although there was an incident, there wasn't an actual accessing or exfiltration of data. But talk a little bit about—in the time we have left—what happens or can't happen if you don't have that data segregation and logging set up on your system?

[MM]: So back to … it's a fantastic question, Kevin, and thank you for asking it. I mean, it goes back to information governance, right? It goes back to that pre-breach preparedness, right? Talking about incident response planning, you know vulnerability systems, then testing, you know, building out a plan, all that kind of stuff. But data classification, information governance, right, is so critical—and segregation… is so critical because I can't tell you how many cases we get involved in where we say, okay, we have 200 machines across the environment, right? 170 users, 30 servers. We're like, okay, where's what we call "protected data"? Right, when we refer to protected, they were told by PII, PHI, like, right, where's the stuff that's going to trigger notification? Where is your protected data, like, right? No idea. Can be … could be anywhere. I mean, HR people can access our third-party system, pull down spreadsheets, send them around and then their hard drive with an email is attached like… it's everywhere, right? That's a nightmare, because now all of a sudden, you just exposed yourself to a humungous potential risk of data exfiltration, right? Because you don't know if it was an email or if it was on hard drives or where it is. So having prepared data classification, information governance, data segregation so that when you do—and that's not if, but when you do have this thing—you can say, Hey, guys, yeah, we got an incident. We need you guys to come in and look at it. But here's where all our stuff is. And if you can tell us with a high degree of forensic certainty that nobody got to this bucket, it changes the game like a lot.

[KS]: It does and it does happen. And we're always happy when it does because as we've said, not every incident is a reportable data breach. In fact, many of them aren't. And the stronger your system is, the more confidence you can have in the conclusion that your forensic expert reaches right?

[MM]: 100 percent. And if we can say with a high degree of forensic certainty that we went through the systems, we went here, here, here, here, we know he went here and here. But this is where all the really important stuff is and he didn't go here. It's game over.

[KS]: And we love it when that happens. Sometimes it doesn't. And we're going to do… I think we need to do two podcasts, one on what happens when it doesn't. And we'll have someone come on and talk about how your law firm works with you to identify what reports you need to make and to what governmental authorities. And I think, Mike, we also need to have you back to talk about data classification and the structure of the computer system, because you need to know what data you have. You need to know whether you need it. You need to know who has to do it and why. Because you don't need all the data that you have, perhaps, and not everyone that has access to your data actually needs it.

[MM]: That's right. And you certainly don't need to keep it for 20 years.

[KS]: Right. And we see that as well. And that can be a huge problem if you have a ransomware attack or other incident. Well, Mike McCartney, thank you so much for coming back.

[MM]: You're welcome.

[KS]: Appreciate it. We talked about. Those three calls that you must make. We talked about the role, the central role that the forensic expert plays in isolating, containing ,and remediating the security issue. And I'm just so grateful that you come back. Will you come back again and talk to us about classification.

[MM]: I would love to come back, Kevin. Thank you very much for having me. I really enjoyed our conversation. Yeah. Please invite me back anytime you need.

[KS]: Oh, it'll be my pleasure. Thank you. We will talk again soon. And meanwhile, I hope everyone enjoyed this episode of the Cyber Sip podcast. We'll see you next time.

[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.

[KS]: 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.