Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 17: "Four Keys to Prepare for a Data Breach, With Nick DiCesare"

Speakers: Kevin Szczepanski and Nick DiCesare, Barclay Damon

[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.

[Kevin]: Hey everyone, welcome back. I'm your host, Kevin Szczepanski. And today we are here with the founding member and co-leader of the Barclay Damon cyber security team, Nick DiCesare. He counsels his clients on best practices to securely maintain electronically stored information. And he serves as a breach coach, which, for those of you who are football fans, means essentially that he is the quarterback for the client in investigating and responding to data breaches and other cyber incidents. And he's here today to talk about four keys to preparing for a data breach. Nick, welcome to Cyber Sip.

[Nick DiCesare]: Thanks, Kevin. Happy to be here.

[Kevin]: Thank you so much. We've been trying to get you on for a while, keep meaning to get together and we're finally here. And I'm happy to have you. We want to talk about the four keys to preparing for a data breach. And first and foremost is knowing your data. And I think we both heard and those of us who have been in this business for a while understand that you can't protect what you don't know you have. So walk us through the importance of, first and foremost, knowing your data and what you do with what you know.

[Nick]: Yeah. So, you know, this this topic today is really all about, you know, the whole ounce of prevention is worth a pound of cure. And when we are called into breach situations, a breach coach to investigate it. The clients who have gone through these preparatory steps know what they have, where it is and have anticipated that something like this could happen are going to be miles ahead of clients who are just looking at cyber issues the very first time when something really bad happened in a ransomware attack and the like. And knowing your data is hugely important because ultimately, you know, you get hit with a ransomware attack everything is offline. You don't know, how are you going to access your data. How are you going to operate your business? Well, you know, what do we have, where are our key operational data? Where is that stored? How do I get to it? You know, up front, getting your business up and running if you know those things, know, this is the server that was impacted. We work around that this way. You know, that's huge right off the bat as you're trying to reestablish your business, get up and running. Find a way around whatever, you know, cyber incident has occurred. And that, again, you know, ultimately you're going to have a forensic investigation and they will hopefully be able to tell you, this is what the data point of that impact is, this server was impacted, these files. If you've done that work in advance to say okay we know this server contains all this data so we really aren't going to have a concern with all that data was...no private information was in there not real important from that perspective. And so we'll be able

to address the notification I'm required to provide notification was a lot easier and quicker and less expensively than someone who has to go, I don't know who is on that server, I guess we got to go find somebody who can look at it and that's assuming you can access that data to begin with. So vital step in knowing what you have, where it's stored. Again, an ounce of prevention in this case will save you loads and loads of time and money having to go through those steps for the first time.

[Kevin]: So let's break that down a little bit. I want to talk about that. You mentioned knowing your data, what you have, and where it is. You also want to know who has access to it and whether you need it, whether you still need to maintain it.

[Nick]: Again, there are other big things. You know, we run into situations where, you know, one of the major ways bad guys get in your system is through phishing attacks, of course. And for people who don't know what that means, those are the emails that look like they could be something real or not. You click on a link, you shouldn't have clicked on, all of a sudden someone gets access to that account. Now, you know, we dealt with businesses where every single person in that business has access to every single bit of data, every system, every account every everything that we access by every person from, you know, someone an assistant up to the CEO have the same access. And so one of the questions we ask when we go in to counsel clients, is will you control that access? If you have sensitive data, do the people that access that data really need to have access? You can limit who gets. You're trying to narrow down the window of opportunity for these criminals to get into your system, to get into sensitive data. And if you can say, yeah, this person really doesn't need to have access to this data or this system, you can try to create ways to isolate, you know, just who needs access to that system. And the other big thing you mentioned, of course, is data retention. And we're big on talking to clients about data retention policies. And, you know, it's not just who has access, but how long, you know, how long do you need to have this data sitting around and it's just sitting somewhere in some file that you're never looking in. That's just, you know, that's a bomb waiting to explode if a bad guy gets in there and all of a sudden is accessing ten-year-old data that you haven't needed or had any reason to keep. Now, you might have to go tell somebody ten years ago that, hey, we got out, we had a breach, we had your information still, and now you're notifying them ten years later. And the first question is going to be, why do you still even have my data? Why is that there? So controlling, you know, data access, controlling data retention...a gain, all great things to consider for preparation steps when, you're trying to reduce the risks associated with the potential for breach.

[Kevin]: Nick, I was thinking as you were talking about access and I wanted to run an example by you. So let's suppose that an organization has five employees and all five employees have access to data. That's five potential attack vectors that a threat actor can use. So if it turns out that only two of those employees actually need access to data, if you then prohibit access to the other three in a very real way, you are mathematically reducing the potential attack vectors, right?

[Nick]: Oh, absolutely. Yeah. Again, you know, five people receive an email you know, three of them don't click on it, two of them, right there. You know, those two didn't have access to the sensitive data. You've avoided the potential breach situation. So it's all about reducing that risk. We don't we don't like to go into scare tactics any more these days. But, you know, the cyber security professionals would all say, the years I've been doing this, it's not matter if it's a matter of when, you're going to have a cyber incident. So everything. Everything we're talking about is. Doing as much as you can to reduce the risk of it happening. Yeah, probably still going to have to do with something, but it's also about reducing the impact of what happens when something happens.

[Kevin]: Right. This is not a scare. This is really practical and helpful advice. If you do these things, if you know your data. I want to come back to that in a second before we move on. If you know your data and you are limiting access, as you should, and you're getting rid of old data that you don't need, that is going to increase your cyber hygiene, make it (a) less a less likely that you will suffer an attack. But when

the inevitable attack comes, it's going to make it a lot easier for you to respond when you limit the potential costs that you will incur in responding.

[Nick]: Absolutely. Yeah. Yeah. It's again, it's doing these little, you know, preparatory steps. Some of them don't cost you anything and they can save you again, not just money, obviously, that's very important cause you want to make money, like it saves you, you know, hours, minutes, you know, seconds that when you're dealing with the breach in real time is...are all vital.

[Kevin]: All right. So before we leave the subject of knowing your data, I just want to drill down on that a little bit for those of our viewers and listeners that may find a little bit more clarity helpful. So we're talking about knowing your data. Give us some examples of the data that we're talking about. I'll throw one out there. One would be emails, I suppose. Another might be customer information. What are the different types of data that you see in your world as a breach coach that will give our viewers and listeners some context?

[Nick]: Yeah. So, you know, typically. You know, most businesses maintain some information on their own employees, obviously. And typically, there's some database or file where that information is maintained. You're going to deal with customers and customer account information. Sometimes that could include financial account numbers or other...If you're dealing with individuals who might finance anything through your company, dealing with finance documents that would have Social Security numbers or driver's license numbers. Emails are emails are a huge issue. We've talked about this a number of times. These days obviously, everybody, you know, for ease is transferring everything, email. You know, you somebody needs a form filled out. You send them the form via email, they fill it out and send them back to you. And really, that that can turn into a big, big trap in a cyber incident situation. Because, you know, that's just sitting in an email account. It's there, bad guys could find it. But you also need to find it and determine if somebody has access to that. So if your business is regularly transmitting sensitive data, again, three big categories are going to be Social Security numbers, driver's license or other government ID numbers, and then financial accounts, if any of that stuff is being transmitted back and forth with customers, vendors, whoever, by email, you are really going to want to think about how that is, how that transmission is done, how that information even has to be done to transmit that information via email? You want to have some protocol for getting it out of email and erasing it from email, putting it somewhere else, preferably in a encrypted file of some sort. So even if somebody is able to gain access to your system, that has a layer of protection. Ideally, if you're going back and forth as you're transmitting this sort of data, via email, you want to do it in some secure way, secure portal, secure attachment to email, password-protected files, anything like that that you can do to protect the that is being transmitted. The last thing you want to have happen is to have a ransomware attack. And the forensic people are telling you, these mailboxes could have any access. There's some evidence that the mail was accessible to the bad guys. And now you're left with having to search through all of those emails to find all of the protected data that may have been transferred.

[Kevin]: So if I'm thinking about this, Nick, and I'm not a cybersecurity expert, I'm just running my own business. I've got a small, medium-sized manufacturing company, services company, and I'm thinking about it like it's my house. I wonder if that works. So my house has...I open the door. I've got a living room, dining room and a kitchen, and I've got bedrooms upstairs. If I know that my customers' financial information is kept in the kitchen, then when I have a breach and I, I bring in a forensic expert and the forensic expert tells me, all right, we know where they went. We're going to talk about risk assessment next. We know where the threat actors went. We know they didn't go into the kitchen. And I know that my customer's financial information is in the kitchen. I can draw a conclusion that the bad guy did not access my customers' financial information. So I sort of think of it with the analogy of a home. And I think that works because what we're really talking about is knowing what data you have, you have your customers' financial information, and where you keep it, where is it segregated in your computer system? Obviously, we don't have kitchens and living rooms in our

computer system, but we have the equivalent of dedicated spaces, sometimes servers, and if you know in advance you've made that preparation in advance, know not only what you have but where it's kept...I mean, how much easier does it make that for data breach response than in systems where you and I both been involved, where there's no segregation and there are no bedrooms or rooms in the house, you just open the door and nobody knows where anybody went.

[Nick]: Anybody with any. Right. It was a flat instead of a... Yes. Yeah. So that I mean, again, when you're when you're responding to a breach. You know, everything is, you know. We'll talk about some other time how the breach response actually goes. But, you know, the hours, the minutes, the seconds that they matter...You know your analogy is a great one. And if somebody broke into your house and you had them on camera, just going into the living room. And they didn't go into the kitchen. They whatever you had in your kitchen was safe. To be able to say that when you're dealing with the data breach. Forensic people are telling you that, you know, they can tell you hopefully if you've got some preparatory steps, they can tell you, you know, here is what we can tell. Term of art is "artifacts," Here are the artifacts left behind from the criminals that tell us where they got. And if they can say we can you know, we can say forensically they didn't get itintono the kitchen. Then that's that whole batch. You don't have to worry about what was there. You don't have to worry about looking at that data to see if there was anything important there. You know, the other.

[Kevin]: The other ...PII. PII or PHI.

[Nick]: PII

[Kevin]: In the case of we're talking about customer financial information in our example. So in all likelihood that is going to be PII and that could trigger a duty to provide notice under one or more state law. So that would be very important to know. They didn't go into the kitchen, for example.

[Nick]: Yes, absolutely. And it saves you...not only saves you time and saves expenses, the alternative is after the fact, you're trying to look through all that data, sort through all that data. And that could be its own investigation process, which could take days, weeks. How much data have? And not only that, but the time you spend, somebody's got to go through. You don't you don't have that data, if you don't know what the data is, where it's segregated, and you're just looking at the whole systems worth of data, that's an expensive process to go through and very time consuming when you're trying to answer questions about what happened after notifying people somebody's sensitive information potentially out there for bad guys. Bad thing.

[Kevin]: Sure. All right. So let's move on. We talked a fair amount about knowing your data. What do you have? Where do you keep it? Who has access to it? Do you really need it at this point? I think that leads naturally into our second key to preparing for a data breach, and that is conducting a risk assessment. So talk to us now, Nick, if you would. What is a risk assessment? And give us some examples of what a risk assessment entails. And if you could maybe start with system segregation, because that's really what we were talking about a moment ago when you talk about the different rooms of the house. So what is risk assessment? What are some examples of what an organization should be doing as part of that assessment?

[Nick]: So a risk assessment, you know, can mean a lot of different things. There is you know, there's no one size fits all response. And the risk assessment for one business might not look like the same as for another... the size business obviously is going to be different. The type of data that business deals with is going to make a difference in what your risk assessment looks like. Obviously, a business dealing with health care data is going to be a little different than somebody who just deals with customer data. Those are important to protect. But what you're going to do in evaluating risk is going to look a bit different. And, you know, one of the things about a risk assessment going back to your house analogy

and it's something that one of our forensic friends loves to use is a risk assessment is like a home alarm system. You know, what are, you know, you got windows and doors. Are those windows and doors closed or are they locked and somebody's been going in and out of them that you didn't know about. And so part of the risk assessment is looking at those things: how many windows, doors do you have open? Did you need to have them open? Should they be closed? Most likely, yes. But on top of that, a risk assessment is going to look at your practices, the things we already talked about, you know, have you... do you know what data you have, you know, where it's stored, you know, what sort of things are you doing to protect it? Do you have multifactor authentication. You have encryption, you have good, strong password policies, you have good, strong email use policies, one of my little pet peeves. So a risk assessment is you look at all that stuff, they can look at distinct parts of that whole equation. Some risk assessments involve what's called "penetration testing," where the company comes in and actually tries to get into your system and, if we can get in your system, the bad guys might be able get in, where are some of those vulnerabilities. So, you know, risk assessment is a broad it's kind of a broad term. But, it's something you really need to consider for your own business, what that looks like. And then, of course, we help people do that all the time. What things should you be looking at for your particular business? What are you dealing with and what sort of policies and protocols do that?

[Kevin]: Right. You're talking about our friend. I should tell our our viewers and listeners. The friend is, of course, Mike McCartney of Avalon, national director of cyber for Avalon. If you want to hear more from Mike about his analogy and the other topics we talked about, we've done three episodes with Mike McCartney and check those out on the Barclay Damon Live website or on Spotify or wherever good podcasts are streamed. So we talked a little bit about risk assessment. Let's turn to the next issue, which is training. So you've got we talked about key one, know your data, key two, risk assessment. Now key three is making sure that everything you've done envelops your entire organization, including all of your users. Right. Because you can have the best laid plans, but if nobody knows what your plans are or how to comply, you might as well not have them at all. So I know you've been involved in a lot of employee training in the course of your career. And as our cyber team co-leader, Nick talked to us about that training. What does it look like? Why is it important?

[Nick]: And so, again your technology is only as good as the people who use it. And you can have the best firewalls and best multifactor authentication and the best everything technology-wise, you still have to account for the human factor, which is in most cases, somebody gets an email, they click on a link or doc.. And all of a sudden they're in your system. So, you know, the training that we do is to try to help clients train their employees to identify the sort of tricks to the bad guys trying to do. What is a phishing email look like? What is some social engineering tactics that are used by some of the bad guys? And you know, we've done where you just put up examples. I mean, there's there are examples all over the place of, you know, what is this scam email look like? Can you share those with your employees? Hey, there's, you know, this largest email scam going around involving X and such, you know, company, whatever, Amazon, PayPal whatever, know Netflix, you know, whatever the scam is, there's some, you know. There's some information out there. You can share that with your employees. There are great training programs that are available that go through and train employees again and see, you know, technology-based training that you listen to some videos, they go through, some examples they answer some questions and the kind of hands-on training they do. When we when we're doing the training kind of go through those things, we also talk about best practices that employees should and employers should try to follow to avoid unnecessary exposure. Again, going back, I mentioned email. Email use policies. One of my big things I tell clients is you should have a policy that don't allow employees to use work emails for private accounts. Right. This way, they get some emails saying, Hey, you have an issue with your Amazon account, somebody who's charged $1,000. They know there's no reason I should be getting that email at this account so they know that's fake, delete that and there's no chance they're should click on that. And that's just you know, that's an easy way that bad guys do it and they'll send emails with "very urgent," big problems with some account. And a

lot of times it's tied to things that really don't involve work. Right. I use Amazon because they've been a target before. They scan your accounts, your accounts locked. You got to click on this, to unlock, it....

[Kevin]: And they provide your, you know, your password, your credit card or suits you. Look, there's that sense of urgency, often involving financial information, checking the email address, you look at the email address and if you hover over the email address, it changes to an address that you don't recognize. It's not someone from your organization or there are misspellings. It's really amazing when we talk about, you know, watch out for misspellings. Watch out for incorrect emails. Watch out for the sense of urgency. You say it and you think to yourself, well, of course, all this is obvious. Of course, that's not, why would anyone fall for that? Well, people do fall for it. And the threat actors use those techniques because they work a lot, right?

[Nick]: Yeah, absolutely. And again, I would say 50% of the breaches were responding to...have involved phishing attacks, successful phishing attacks, and. You know, a lot of times you can't. Can't trace the exact path. You know, somebody clicked on something. They execute this file on this person's account and now all of a sudden they're in your system, moving around, getting into other systems and things like that. So training people to spot those. And they're more and more sophisticated every day. But again, it's about reducing that potential risk. And you can eliminate a whole class of potential risk by saying, hey, don't use your work email for this kind of stuff so that you know what, you're getting in these emails and they look very urgent and, you know, reduce that risk. Right. One less thing you've got to worry about in the course of training people for things to look for, a number of items you mentioned. Misspellings, the different slightly emails, different addresses. Grammatical errors, you know, generic greetings, dear customer or those sorts of things. Signature blocks that don't really make sense on email, all those things, you know, to look for and avoid the phishing attack.

[Kevin]: Right. So we we've got one more key that I want to talk to you about in our remaining time. And that is something you alluded to earlier, which are policies. So talk to us in our remaining time about the written policies and procedures that every organization should have in place. I think one you mentioned was an email policy. So what are some of the other types of policies that every organization should have so that we're all prepared adequately for the inevitable breach?

[Nick]: Yes. So generally they follow a category of data security policies or written information security plans. You see those used interchangeably with things you want to consider, you know, will be part of those plans or several separate policies however you decide to do it. You're going to want to talk about password policy, right? What your password should look like, how many characters and you have protocols for coming up with your passwords and how often you should change the email use policy. We've talked about, of course, access policy. We touched on those as well. You should have access. And how do we get that access? Update policies. You know how often you're going to update your systems and your software protocol, you're going to follow that.

[Kevin]: So that's a similar update is similar or analogous to a patch... or patch could be one form of an update?

[Nick]: Yeah. Yeah, patch policy. I've got an interchangeably patch policy update policy. There are you know, again, depending on how you handle your data and whether these would be part of your data stream, all your actual technologies in place, right. What your firewalls look like, what your encryption policies are, multifactor authentication, all those things could be put into these policies. And then on the back end, you should have a separate data breach response plan. And that's going to kind of spell out who's involved internally, externally, when there is some sort of issue. And then you know. Yeah the preferred way to do it, as you have right there in your policy list of people who are going to be called to have insurance down there as well. Your insurance policy, your carrier information. Who do you know your policy says you have to call when you have an incident? So. All those things. Again, you're if you're

dealing with these things beforehand, before you have an incident. Writing up the policies, considering the risk assessment, that could be in a policy. We're going to do an annual risk assessment have that right in the policy. You know what time of year you're going to do it, keep track of action items that need to be addressed and then in those policies. And hopefully, again, it's all about reducing the risk. And there's no one size fits all for the policies either, but by having a discussion about a policy and doing them the chance that something happens. But you're really.

[Kevin]: Right. No, we have no one size fits all. I think it's so critically important what you say. I mean, not only are some organizations required, to have these written policies in place because the regulations that govern the industry require it. But even if that weren't the case, I think they're just two really important practical reasons for it. To me, one is you don't want to be thinking about this for the first time when you actually have to respond to a breach. If you put that time into prepare, you're going to be able to execute your response much more efficiently, effectively, and successfully. And the second thing I want to hear your thoughts on this that I always tell our clients is that you want to do the right thing because it's the right thing to do and it's going to help you respond. You also want to do the right thing because you want to be able to say that you did, down the road because very often, not all the time, but we have seen situations where a regulator will come calling and will want to know from the client what they did or didn't do, what the thought process was. And if your answers to questions like do you have a written incident response plan, did you if you have a written information security plan? If your answers to these questions, or too many of them are "no," what does that mean?

[Nick]: That's bad news for you because as you said, you know, Kevin, there's still just a myriad of laws out there that... there is no one overriding law that says every business has to do this. New York does have a fairly new law called the SHIELD Act, which starts...started to address that. Most businesses fall within the SHIELD Act, and there are a few things that everybody is supposed to do. I think that's a topic for another day. But, if you do have a breach and you do have to provide notice and part of providing notice could involve notifying regulators or attorney general or some other state attorney general. They come and they what happened? What did you know, what are you what protections did you have in place at the time? And. Yeah. If you're saying. Well, you know, we, we had an IT guy who, you know, we had passwords, but that was it. You know, they're going to look at that in this day and age and say, we didn't do nearly enough. Everybody knows. See, that is protecting other people's data is important. And, you know, if you're not considering... haven't done some of these things. And haven't considered it. They're not going to come in and say, you know. Your business small or medium sized business should have been doing what Microsoft is doing. But they want to see are you are you acting reasonably for your business, for the data you have? And if you can answer those questions reasonably well, you considering the highest levels...there are other big things. As you know, the regulators, we don't want to see that. We want to see the top down. Not just that it was delegated to the IT people. IT people as much as possible... They want to see corporate level ...

[Kevin]: C-suite. Board of directors..

[Nick]: Whoever is taking this issue seriously. If you go back to the regulator and say, we did take this very seriously, we've done all these things. They're going to look at you a lot more favorably than somebody who well, we got hit by this thing and we didn't have protections in place. And now we're dealing with an angry regulator who's out there to protect other people's data. And we're going to be looking at it, wanting to impose hefty fines and can go make you do those things anyway, the regulators are very big on, okay, if you want to resolve this with us at all, you're you pay us money. You're going to do all these things. We're going to make you do them now.

[Kevin]: We've seen those situations for sure. So. All right, Nick, we've been talking about four keys to preparing for a data breach. We are near the end of our time. I wanted to talk with you about breach response and some of the things that we have learned, particularly in the last 18 months or so. Would you come back and talk about that with us another time?

[Nick]: Absolutely.

[Kevin]: All right. Thank you. We'll do a separate podcast on that. But Nick, thanks so much for joining. Glad we got to sit down and talk. And we'll do a lot more of this together.

[Nick]: Thank you.

[Kevin]: And thanks to all of you. If you enjoyed this podcast, like, comment, share. We always welcome your feedback and we're back soon the episode of Cyber Sip.

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

Disclaimers:

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

Barclay Damon Live podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of Barclay Damon Live programming is the audio file.