Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 19: "Breach Response: What We've Learned, With Nick DiCesare"

Speakers: Kevin Szczepanski and Nick DiCesare, Barclay Damon

[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.

[Kevin]: Welcome back, everyone. I'm Kevin Szczepanski. And today we're back with Nick DiCesare and we're going to talk about the waves of a data breach. As you may remember, Nick is the founding member and co-leader of the Barclay Damon cyber security team, and he works tirelessly counseling clients on best practices to maintain not only electronically stored information, but he also works with clients as the breach coach or quarterback when the inevitable breach happens. And that's what we're going to focus on today. Nick, welcome back to Cyber Sip™.

[Nick DiCesare]: Thanks, Kevin.

[Kevin]: So, I wish I could claim credit for the "waves of the data breach" thing, but that's not mine. That's yours. So we're going to talk about the three principal waves that every organization encounters when they do find themselves dealing with and responding to a data breach. But first, tell us a little bit about...how did you come up with that and why is the wave metaphor so fitting in your view?

[Nick]: So after doing the breach response coaching for a number of years, I think it's just the way it works. There's crests of a lot of activity, a lot going on. At the same time. It's very, very chaotic. And then there will be a lull. And then there is another, you know, just another swell of activity that happens and then another lull and then, you know, another swell. So that's just the way it occurred to me. And, you know, unfortunately, I think there is a somewhat of the connotation for me is, you know, the client getting slapped by a wave, a couple different points in time that can be difficult to deal with. That's where I came up with it. And I think it's fitting because it's, you know, every breach I've done, you know, the facts have been different. The customers or the clients have been different, the data, they have been different. But the kind of overall way that the breach response moves is almost always the same, and it's always these three major kind of events with activity going on the entire time. But it's like I said, it swells up, slows down, swells up, slows down, and there's waves. I got to deal each one as they come in.

[Kevin]: Right. And I think the other thing, too, to keep in mind for those organizations that have never been through it, is there are these periods of rests. And if you have the right partners, the right counsel, and forensic teams, these organizations that have been through it before, and that's all good. But the other thing to keep in mind is that you may, as an organization, learn about the incident or data breach in a very sudden manner, and at a very odd hour, the process of responding often takes time. It can sometimes be a matter of days, but sometimes, Nick, we've seen weeks and even months before the entire

process plays out from initial attack through decision—whether notice needs to be given to affected individuals and regulatory investigations commence.

[Nick]: Yeah. And a lot of that, you know, timing is going to depend on a lot of factors. It's going to depend on the type of attack, severity of the attack. It's going to depend on some of the stuff we've talked about in the past. Like, you know, how prepared were you for this in terms of your own policies, practices that you had in place? And knowing your data, which was a big thing we've talked about before. All those things are going to determine, you know, how long it takes between these waves and...you know, a big thing that a lot of our clients have trouble with is the need for some immediate...you know that there is often a need for an immediate response. The forensic people need to spend a lot of time in the system looking for their term of art is "artifacts." What happened? How did the bad guys get in? Where do they go in your system once they were in there? Is there evidence that they were accessing? Is there evidence that they took data out of your system? All that takes time. And then when you want to get to the next step doing notification, you finding that information on private package information for different individuals and determining, okay, what law applies to that individual. What are the rules for notifying those individuals which are different state by state. As much as everybody wants to push through as quickly as possible. And there are going to be these lulls where it has to be collected, work to be done. Everybody wants to get through it as quickly and efficiently as possible. And again, you know, last episode we talked about preparation. You know, in those preparation steps, it's going to be a lot smoother of a ride on these waves than if you haven't.

[Kevin]: I was just thinking the same thing. And for those of you that haven't seen it, check out the first episode Nick and I did together, "Four Keys to Preparing for Data Breach." And you'll know exactly what he means. So you alluded to some of the issues we're going to talk about now, but I really want to break it down, wave by wave, and just talk with you about the early waves of a data breach. And I think we're going to cover initial attack through regulatory investigation, maybe even some third-party claims. But let's start with the first one. Tell us about the first wave of a data breach. Let's assume a scenario that involves a ransomware attack, because I know that we want to talk about special issues with ransomware and email data later. So give us a scenario of a ransomware attack, and talk about the first wave of response.

[Nick]: Yeah, so and ransomware, I think we're going to talk about some special issues we've been seeing recently. But ransomware is, you know, by far the most common and we're seeing these days in the past two years, probably the number one issue that our clients are contacting us about when there is an incident. And typically it starts when somebody goes to log into the system, instead of getting their usual log-in window, they get a message saying, we have your data encrypted and if you want to get it back, you got to pay us $1,000,000 or something like that. And that's the start of the wave. Again, if you prepared well for that. Your next step is going to be contacting all of the stakeholders who can identify your breach response policy; that'll be internal people and external people, outside counsel. A forensic group...there may have insurance, might be contacting an insurance contact. And then all those people are going to get together and it's going to be "okay, let's talk about, let's identify the type of ransomware it is. Is there any identifier that lets the forensic people know what they're dealing with? In ransomware cases, you often bring in a ransomware specialist who will have a lot of data about ransomware variants, how those criminals respond, your chances of getting your data back, encryption code, all that kind of stuff is going to be considered in the initial discussion. How are we going to respond to this particular ransomware incident? Can we go without our data, getting the forensic people in immediately to try to identify people and figure out how they got into the system and figure out where it went into the system. They got to start getting as much data as they can and so they can start processing that. Your legal counsel is going to be looking at that situation, making sure that, you know, you're running the show and why your outside legal counsel to be in control of the breach response. Because I try to protect as much as possible under the attorney client privilege for...I'll get to those later waves, all that is going to be going on. And again, this is going to be a very hectic time

because you're going to want to try to get your system back, is going to impact your business? And you also have to start considering what are your legal obligations going to be. And, how are we going to deal with this ransom? What are...what does our back up situation look like? Are we able to get the business back up and running safely. And again, some of that will the people identifying those things. Did they get into our backup systems safely reinstall systems, without any threat of infection. And that, again, that ransomware expert might tell you how you, based on the ransomware variant, this is what these guys typically do. These are the files typically installing...that sort of thing so that you can try to endure the first wave. You know, big concerns, how to get them...Where are the...what data do they get, can we get our systems back online safely, our working minimum. We stop them from doing anything else beyond what you know, what they've already done and start upgrading the other data, any other data and make sure you're getting off something that is connected properly and safely. And a big thing is preserving data for people that are doing the investigation.

[Kevin]: Right. So I was I was thinking when you mentioned the calls, I'm going to date myself, but I immediately thought of Billy Dee Williams and "Ghostbusters." So who are you going to call? Your first call should be to your counsel because that's going to be your breach coach, the quarterback of your response. And it also ensures that to the maximum extent permitted by law, you will have the protection of the attorney client privilege. Your second call is going to be your lawyer's call to your forensic firm, and that's the firm that's going to go into....and we talked in our last episode about the metaphor of the home. Imagine your computer system as a home. That's the investigator that's going to go into your home, check the security system, figure out which door, which window the threat actor came in, which rooms in the house did they go to? What did they look at? What did they take? And if you do have cyber liability insurance, I think call number one is to your lawyer, call 1A is to your insurance company. You want to make sure that you provide that early notice. So we're at the end of the first wave then, Nick, and let's say that your forensic team and you may have a special ransomware team working as well...as an organization, you're kind of wondering you're trying to struggle to restore your data from backups. You may or may not have all the data you need. You're thinking about whether you need to pay a ransom, but you're also at the same time thinking of who, if anyone, you need or may need to provide notice of the incident to. So let's say at the end of that first wave, your forensic team comes to you and says, and I'll borrow one of our early analogies, you know, we know the analogy, the home. We know they didn't go to the living room, or the dining room, or the upstairs bedrooms. But we do know that they went into the kitchen, and we know that they looked in the cupboard. And that cupboard has your customers' financial information. And let's assume that's going to include some PII, that's going to include some protected information by law more than one state. And that is going to trigger you or at least potentially trigger your obligation to provide notice. So we're at the end of wave one. Talk to us now about wave two.

[Nick]: At this point, again, yeah, your forensic expert is going to have done their investigation. They'll come back and they'll say to two key words here, access and exfiltration. Access is just what it is. Somebody accessed your data. And the key being that the person who access it didn't have authority to do it. So it's unauthorized access. The other one, exfiltration, a fancy word for they took stuff. You know, the forensic expert will come back and say somebody who shouldn't have been looking in the cupboard, looked in the cupboard, and not only did they do that. They took some stuff from the cupboard. And now we have to start looking at our legal obligations. Where those legal obligations come from. Two main sources being the contract or law, statute. So, you know, the first thing we'll do is we'll ask our client, is the data yours or is the data somebody else's and it was on your system? Are you a vendor for somebody and you have this data that you were holding for them, using your business for that for that customer of yours, you know? And then we'll have to look and see, are there any special requirements under any contracts? On some contracts nowadays, and what we encourage our clients to look at these issues very closely or have notification requirements. You know, the law might say you have X amount of time to notify, but the contract might say something different. Now, we wanted a notification within two days, you know, 48 hours, 72 hours. So you're going to be looking at those contracts and

looking at notification obligations, potential indemnification obligations under those contracts. And figuring out, do we owe anything to this particular customer of ours. And then the second group you're going to be looking at are individuals, and it's your data. And you have individuals protecting information against the three big categories being Social Security numbers, driver's licenses, or other government ID numbers, or financial account information. And then you're going to look at where do those people reside, because data breach nonfiction laws are not based on where your business is located, it's based on where the impacted individual is located.

[Kevin]: Didn't we hear one of our friends told us recently, well, wait a second, I'm located in State A; these customers are in States B and C, so I'm not going to worry about them.

[Nick]: Yeah, unfortunately, that really is not the way government regulators will look at that situation. And if it comes out that you didn't provide notification to individuals whose data you had and you know, the law says you have to protect, you're going to be on the wrong side of a regulatory investigation and wave three is going to be a lot bigger and come crashing down on you a lot harder.

[Kevin]: Purposes of wave two though. I mean it's...it may be obvious to most. But just to underscore this, because I think you and I were talking yesterday, the day before, it was the first time I'd really heard this: be warned, if you have data for customers in 15 states, you are responsible for complying with the breach notification laws not only of the state in which you do business, but in the other 14 states in which your customers reside. Very important and many of the state laws overlap but there are some critical differences. So, Nick, really important to identify in this wave too, where your customers are because those are those are going to give you the statutory frameworks for your breach response.

[Nick]: Yeah, absolutely. So again, your data, you're looking at. What data did you have that's protected? Where are those people located? And then, you know, this is wave two, this is where the lawyers are going to be doing the majority of the work is looking at, okay, what do those states require? And again, all states now protect those three big categories. Different states might protect other categories. I think there are two states where just the name and a date of birth triggers a notification requirement. Some states now biometric. Biometric. So if for some reason our fingerprints or face scans and that sort of data, you know, that stuff might be protected differently under different laws. How you go about notification pretty similar under most state laws there can be differences there. Some will allow it by email, others ask the regular old-fashioned letters in the mail. Unless there are other special circumstance. What has to be in the notice is a little bit different. Some states require that you include information on how the person file a...their own claim with the state regulators. Some states require credit monitoring protection for a certain period of time. So that in this wave two be looking at all that, what states are involved, what people are involved, what data is involved, and from there, you know, who do we have to notify? What has to be in that notice? What else do we have to do to comply with any state notification laws? New York, for example, if it is over a certain number of people under ...over a certain number of New York residents involved, you have to notify a credit monitor. So all these different things we're going to be looking at stage two. Oftentimes at this stage, we're going to be involving another vendor who will help with notification, sending the actual notification letters or dealing with a large number of individuals, you know, a couple thousand people, 10,000, 20, 30, whatever the number is. You know, you bring in a vendor who does this for their business. Help you more efficiently get those out there rather than trying to get them out yourself, bring in vendors who will set up 800 hotlines, which kind of gets us to the next step, which usually part of this step is setting up that hotline; setting up credit protection services for people to sign up for it. And that's all part of the second wave, getting all that stuff in place. So you do the notification, these steps are in place. There may be some PR considerations at this point. It's going to be doing the notification we bring in. We help people with those considerations because obviously professionals have to deal with that as well. How are we going to know...what message are we going to put out of what occurred and how we respond to try to instill confidence back in our customers who trusted us with this data? And that's all

correct. The other big swell of activity, a lot of a lot of decisions to be made, a lot of time and effort's back now again after kind of this lull over the past year, figuring out.

[Kevin]: We're going to wade into wave three in a moment. But before we leave, wave two, Nick, and I know we've got some other ground to cover, but I would just want to ask you quickly, we often get questions from our clients in wave one, especially wave two about whether they should be contacting law enforcement. Let's talk a little bit about that. One of the more common question...should we call the FBI? Should we call federal law enforcement? Obviously, it's a case-by-case situation. There may be certain law enforcement officers that are required to be notified at various stages. Can you talk to us a little bit about that?

[Nick]: We typically encourage clients to notify law enforcement. It helps with a number of things; it helps with insurance requirements. Some insurers condition notifying law enforcement on paying a ransom. So clients who say, well, if we notify the FBI, we just put it in their hands. And that's not the case. If you make the report may or may not ever hear back from law enforcement in response to complaints about it. But again, it gives you the protection of you've done it. You're taking all the right steps; trying and do the right thing. There may be some benefit to it. In one case, we had, you know, the FBI happened to track down the bad guy's server that had some of our clients data on it, they were able to take down answer and tell our client, hey, we got this data. That was positive. Does that happen frequently? No. But again, law enforcement typically is not going to come in, they're not going to run your investigation. They may ask you some questions, what you're doing about it. They don't want to collect the data. There's been a big push recently, I think, from the president down. You know, they want to take away the appearance of the government being in an enemy of a data breach response. Because I think that the early thinking was that the governments are going to be mad at us and they're going to try to fine us and all that. And I think there's there is, you know, an active effort to move away from that sort of approach and have it be more of a partnership. Government wants the data. They want to know what's going on, and they want to partner more with the private sector so that it's not so much a scary experience, but, you know, a more collaborative effort. So I think our thinking is typically it doesn't hurt you to notify the FBI. There's you know, you don't have to make a call even to, you know, a local office. There is an online way for you to make that complaint on the website. Very easy, efficient, effective. We've used it. And, you know, local law enforcement typically not so much. They're not really equipped to deal with these sort of issues, but. You know, depending on the type of incident, maybe you file a report because it's going to protect you when you have to go deal with, you know, another customer or something on your own. But it'll depend, typically, though, I think our recommendation these days is at least at least make the report.

[Kevin]: Yeah, we've seen that issue come up, though. When you just mentioned with another vendor, we've seen that come up in the context of B2B, business to business, disputes in the cyber realm. So if you have a business that is ultimately going to be responsible, financially, or otherwise for a breach, that business may turn to you, and if you were at ground zero where the breach happened, they're going to want to know that you have reported the matter to law enforcement because they're going to want to maximize their protection. To this extent possible. We should come back and talk about this concept, and information sharing on another podcast is very important subject, which you alluded to the Biden administration. I think that's one of the things that everyone's really focused on now. It's a hot topic, but that'll be a teaser for another episode, because I do want to set up wave three now. So let's say, Nick, at the end of wave two, we've determined that an organization does in fact have a notice and reporting obligation. So it's going to have to provide notice to some affected individuals in...maybe in multiple states. And under those state's laws, it's also going to have to provide notice to the state's attorneys general. So let's assume we've done that. Talk to us now about wave three. What happens when this wave crests over your organization?

[Nick]: So typically the way this will occur is you'll receive a message from one of these attorney generals or

some other regulatory agency. If you're dealing with health care CMS is the federal agency that we'll be dealing with. If you report one of these breaches, you're going to receive a response from them. If you have submitted the report, which contains some detail. And then they're going to be asking, okay, well, you gave us this, but we want to know these other things.

[Kevin]: How does the regulatory agency within this context that CMS, how do they contact the organization? Is it a letter? Is it a phone call? How do you get that first notification?

[Nick]: So typically when we're submitting the initial reports we'll list ourselves as the contact point. So we'll either get a phone call or an email from one of the regulators saying, we've got your report. We have some follow-up questions. And it's either then a phone call, a follow-up phone call, or typically it'll be an email saying, we got your report. Here are other things we want to know about the organization, about the incident, and about the response. Typically, they're going to ask, you know, what were your policies and practices did you have in place? They may ask for copies of those that existed at the time of the incident. You know, ask, you know, for other details about, how the incident was discovered, how the response was conducted. They may ask for details about who is your forensic group? Who was the ransomware vendor involved with. Type of...you didn't tell them in your initial report what type of ransomware was involved. So that's the way, you know, the government inquiries will typically go and there'll be a request for information. You'll respond to that. And then again, typically is another phone call where they're asking you about all those details about the policies, okay, you have this in place, did you make any changes after the fact?

[Kevin]: Right.

[Nick]: What lessons did to take away? Did you implement any changes? They'll ask you, you know, if there had been any other responses from concerned individuals. Have you gotten any responses? Anybody started any law suits. That's sort of thing. And then it'll be, you know, one of two things will happen. They'll be satisfied that...these things happen, what you did as much as you could beforehand. You took all these preparatory steps we talked about in our last episode. And, you know, these things sometimes still happen. It's unfortunate, but we think you were, you know, above board in what you did and how you responded. And thanks. Or they're going to be upset because you didn't do something along the way they think you should have. And then there's going to be a discussion about what is going to be the remedy for that. And then that will involve looking at their statutory authority. Most of these regulators have some ability to impose fines and or require clients take certain steps to protect their data going forward. And so there will be discussion along those lines. What sort of fines are you looking at, what sort of remedial steps you have to take and that typically we're involved in trying to negotiate as we can see why, whatever they've done, it should be lessened.

[Kevin]: Right. And you know what popped into my head is you were saying that, Nick, I just wanted to follow up on it is. I feel like in today's climate there are some organizations out there that rightly or wrongly think, you know, I don't really have to worry about any of this because I have cyber liability insurance, so I have coverage and this is not going to be a problem. And what do we say, you say to an organization like that that is not trying to flout the law, but really believes that it doesn't have to worry about having all of these written plans and procedures in place. It doesn't have to worry so much about a cyber assessment because at the end of the day, insurance will cover whatever losses may come as a result of a ransomware attack.

[Nick]: I would say two things to that. First, I would defer to you on whether there could be some sort of exclusion under an insurance policy for not having certain protections for doing certain things. But from a you know, a bigger standpoint, you know, there's...if this comes out, you know, this is a public investigation, if there is some sort of public settlement, this...the New York attorney general loves to issue press releases when they fine somebody for this. Think about the damage it's going to do to your

business reputation. And that's huge. And, you know, there is that...it's an old stat these days from years and years ago that at some point there was a stat that, you know, good 60% of small to medium businesses that experienced significant data breach event that will go out of business because of that event. And that's not just. There's certainly hard costs that an insurance policy will cover. So that's the investigation, doing the notification, attorney's fees, and defending a lawsuit —those might be covered by your insurance policy. But if somebody has lost confidence in your business, is no longer going to do business with you. Well, that's a that's a big concern, that insurance isn't going to cover. And certainly you want to protect against that; you to be able to tell your customers, whether it's individuals or other businesses, that you deal with, that hey, we take our protection of your data seriously. We want you to keep your business with us and look at all the things we do to try to protect your data. So that's a huge consideration well beyond insurance.

[Kevin]: Yeah. I'll just jump in since you put the question to me. I'll tell you what I thought of three things. First, you can't decouple good cyber hygiene—the preparation that we talked about in our first episode together—from cyber insurance, because the market for cyber insurance is hardening. And increasingly, what we're finding is that organizations that don't make those preparations, that don't have the assessments, they don't know they're ...where their data is and where it's protected. And they don't have the other policies and procedures in place. They're not going to get cyber insurance, at least not right away. Secondly, as you say, there are some policy forms that will exclude coverage if you haven't maintained a safeguard that you indicated in your policy application you had. And third, even if the policy doesn't exclude coverage, it's going to be that much more difficult for you to get a renewal of your cyber insurance. If it turns out that the loss occurred as a result of your not having done something that you reasonably should have done. So that's a great point you make. And we should underscore that. We've got a little time left. And I do want to get to the last two topics that you wanted to talk about, which are special issues with ransomware and special issues with email. So let's break those down and first talk about ransomware. What special considerations and breach response does the ransomware attack present? And I know we've seen some of these in the last six months. So tell our listeners and viewers what they should be thinking about in the context of ransomware specifically.

[Nick]: The big thing for ransomware is, you know, it's a, what I would classify as a wave one issue, and that's backup systems. And two big issues we've seen in real-life cases recently are the backups...are they sufficiently isolated from the system so that if there is an attack or ransomware attack, those backup systems are still going to be viable? And one of the things our forensic experts will tell us is these newer variants of ransomware, when they when they get in your system, they're searching for backups so that they can infect the backups. Your typical ransomware attack is not to get into your system and immediately encrypt everything, lock you out.

[Kevin]: There in there.

[Nick]: They're in the system for hours or days, and you're going to search for as much as they can before they actually launch the ransomware. So, you know, our forensic people tell us that they're searching for those backups and they can find the backups. They're going to encrypt backups before they launch the attack on the main system so that by the time you're...you find that they're there and you're shutting them down, your backup is essentially useless as well. So that's item number one, is your backup system protected sufficiently from your main system so that it can't get into it? You still have this viable backup restore your system a lot quicker than if you don't.

[Kevin]: Yes.

[Nick]: And then item two about the backup systems is, are they being backed up frequently enough? I recently had a case where the backup was about two months old, and while it's great that they were

able to get the system restored and had some of that information, they actually lost two months' worth of business that had been gone. So making sure you're getting those updates ...those backup systems updated frequently enough and that they're protected are really key to being able to respond effectively to a ransomware. Take away: one of the big you know, one of the big factors that the ransomware actors are relying on. They want you. You need your data. You want this data. You have to pay us or you're not going to be able to do this. You have a backup system. Protected, isolated, and frequently backed up. You know, you're going to have a lot of pressure on you to even consider paying. You don't need to do pay that ransom for this reason anyway. You know, we can get our systems back up and running with current data.

[Kevin]: So here's a really simple example before we shift to the last point, because I know you wanted to talk about special issues with email data, but here's a real-life example with ransomware. So the ransom is $500,000 and your policy may or may not cover that. And we talked about potential coverage issues in a prior episode with Kelly Geary of Epic Insurance. But let's assume that your policy does cover...if you have reliable backups, they're segregated on the different system, the backup was frequent enough so that you've essentially lost a day or only a few days, maybe even a week...isn't the worst thing in the world. You're not going to have to pay that ransom. If, however, you don't have reliable backups, then you've got to confront the question of whether you want to pay the ransom, whether your policy covers payment of the ransom, whether you're legally permitted to pay the ransom because you could be the victim of a threat actor who is on the OFAC list or to whom you are otherwise prohibited from making a payment. So all of those issues can be eliminated if upfront, you know, you have reliable backups. So, Nick, in the time we have left, you talked about ransomware and the importance of backups. Let's talk about the special issues involving email data that come up in a ransomware attack.

[Nick]: Yeah. So this is a wave two issue, and it deals with identifying individuals whose information you have. And in our last episode, we talked a little bit about, you know, people transmitting protected information over email. And, you know, if you're doing that and if there is protected information in your email system, and you have a breach and that breach impacts mailboxes, oftentimes what we have to do is stage two, wave two of our response is now we're running searches through an entire email box to try to identify this potentially protected information. And if you start getting multiples of that, so if you one email box...that's maybe doable, it's going to take some time and effort. But if you start multiplying that you're dealing with 10 email boxes, 15 email boxes, 20, now you're dealing with a huge volumes of data. And, you know, we have to take a whole extra step of uploading all that data to a data review platform, even though you would run various search terms to try to pare that data down. Oftentimes, you're still looking at a very large volume of data that somebody is going to have to put their eyes on to say, okay, this is the actual, you know, PII versus all this is just stuff, you know, a false positive that the search picked up and that can really, you know, expand the expense and the time of that wave two notification process because. You know, you're looking at 200 gigabytes of data. You're talking about nearly a million plus files. And even if you're able to pare that down by 70%, that's still 300,000 documents that somebody is going to have to go. And, you know, that's either that the clients themselves, and taking resources away from, you know, every day running of their business or as an attorney or paying their attorneys time and again. It's all you know, you want to be able to do this efficiently, effectively. And that's why, you know, we constantly preach to your clients. If you have to take private data through email, make sure you're doing it in the safest way possible, securing that data with sending it via secure links or securing the files themselves by password-protecting them, making sure that, you know, if the data is transmitted by email, you get it out of email and make sure you're deleting it frequently. And if it's something you have to save, save it somewhere else to protect it, encrypted, whatever. But just make sure that you're not just having gobs of data, private data stored in email because you get to this stage on stage two. Reviewing emails, mailboxes. It's just that...it's a very expensive, time-consuming process and it's not something anybody wants to have.

[Kevin]: So we've been talking about the waves of a data breach today, Nick, but in our first episode together, we talked about the four keys to preparing for a data breach. And it sounds like if you follow those four keys, you take those steps, the waves of the cyber incident, the data breach are going to be a little more smooth and a little less costly than they might be if you hadn't undertaken all those protections.

[Nick]: Absolutely. I gather, you know, the wave analogy...

[Kevin]: I like it.

[Nick]: You know, is that...is it Lake Erie waves or is it Pacific Ocean waves? You know, and that's going to be key factor if you've prepared for it. If you've done things to reduce risk. Again, we're never ... no one will ever tell you in the cybersecurity world, you know, that you can eliminate all risk. You're aiming to reduce the risks as much as possible. And in reducing those risks, you make this breach response program much easier. Those waves are going to be much, much shallower. It's going to be a much smoother ride all the way through. And hopefully when you get to that third wave. Maybe there was no response at all from the regulators because you've done everything right and you're able to demonstrate it and get through it that much quicker and more efficiently, a lot easier in a very stressful situation, because no matter what, you know, a data breach is a very stressful situation.

[Kevin]: All right. Well, Nick, as we thank you so much for joining us on another episode of Cyber. You're going to have to come back soon and talk about some more of these topics in greater detail. But I really appreciate you coming on to talk about the waves in the data breach today. Thank you very much. Thanks to all of you. Like, comment, and share. We look forward to your thoughts. And we're back soon with another 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.