Episode 61: “Cybersecurity Basics for Employers,” With Kevin Szczepanski

Speakers: Ari Kwiatkowski and Kevin Szczepanski, Barclay Damon

[Ari Kwiatkowski]: Hi, everyone, this is a *Barclay Damon Live* broadcast where we discuss all things L&E, labor and employment. I’m Ari. Let’s dig in.

[Ari]: Hi, everyone. Welcome to episode 61 of the *Barclay Damon Live: Labor and Employment* podcast. This is “Cyber Security Basics for Employers,” and I’m really excited today because this is a main crossover event for the *Barclay Damon Live* platform. I’m thrilled to welcome Barclay Damon partner Kevin Szczepanski to the podcast. Kevin is also the host of our sister podcast *Cyber Sip*, which tells you what you need to know in the cybersecurity realm. So Kevin, welcome.

[Kevin Szczepanski]: Thank you. It’s great to be here. I’m so glad we finally put this together.

[Ari]: I know. I wish we were in the same room, but it’s okay. Well, we’ll get through it whilst across the hall.

[Kevin]: I’m in the new podcast studio, which yes, has acquired a collection of HP boxes, but I’m excited to be here.

[Ari]: Yes. Well, the new podcast studio is undergoing some renovations, to our listeners, but stay tuned for our future fancy studio. So, Kevin, I ...you know this, our listeners know this. I always ask my guests to share a fun fact about themselves. Just so everyone knows, I gave Kevin the option to opt out of that because hosting Cyber Sip is of course inherently very interesting. But Kevin is going to share a little bit more about himself or hit us with a fun or interesting fact about his personal or professional life, and I’m not sure what it is, so I’ll turn it over to you, Kevin.

[Kevin]: Okay, so two fun facts. I love wine and traveling to wine country on the West Coast.

[Ari]: Who doesn’t?

[Kevin]: And the even funner and weirder fact about me is that I am a big fan of dirt car racing and follow religiously something called the Super DIRTcar Series, which is largely laid out in New York State. But in some other states up north and in the south in the winter. So that dates back to the early ’80s when I was very young, my dad used to take me to these races in Canada and I’m still going today.

[Ari]: That is interesting. I don’t actually know what dirt car racing is. I feel like I’m going to need to give that a Google after our episode.

[Kevin]: I’ll...

[Ari]: ...or we’ll have to talk about it over a glass of rosé. So I’m really excited. As I mentioned a few minutes ago, to our listeners, you know, Kevin is a very experienced litigator, trial attorney, appellate attorney. When I first started at the firm way back when, we had the pleasure of working together, and Kevin is also the chair of our... co-chair of our Data Security & Technology Practice Area at Barclay Damon. So he is the perfect person to kind of give us a briefer on what you need to know as employers about cybersecurity. Kevin, I think this is great because you're going to demystify this for us a little bit. Obviously, we've all heard a ton about cybersecurity really come to the forefront the last couple of years, so I'm thrilled you're here.

[Kevin]: Oh, thank you. I'm glad to be here.

[Ari]: So Kevin, I think you and I talked about this a little bit offline. And I think one of the things that we wanted to touch on is, you know, business owners, employers, really, we are the weakest link, right? I mean, if there's going to be a cyber security attack, chances are there was something that probably could have been done to prevent it. Can you talk a little bit about, you know, employee training, things like that, ways that employers and businesses can prevent these types of attacks? Or maybe just your best tips for that?

[Kevin]: Yeah, well, let's start with that... and the weakest link idea that we talked about offline is actually does not come from the old TV show. It comes from the episode of Cyber Sip that we just recorded with Arun Vishwanath, who's a cybersecurity expert. And basically we were talking with him about is: it's all well and good to have the most robust security controls you can have to protect your system. But what we're finding is that the threat actors have said to themselves, well, why should I try to break in to an organization's computer network or system if I can trick my way in by fooling a busy employee who may not be as trained or paying as close attention as he or she should. So I thought, it's important to start with this point. We are, sadly, as employees, the weakest link and so what does that mean? It means that, I think, one of the most important things an organization can do is make sure that its employees are adequately trained regularly. That means at least once and preferably four times a year on how to spot phishing attacks, and what's a phishing attack just very briefly—they can be targeted. They can happen by email, by phone, by text. And these are essentially targeted attacks in which a threat actor will try to take advantage of some faux urgency, the need to deal with money, the need to avoid a harmful effect.

[Ari]: "I need you to buy me 10 gift cards from the Apple store."

[Kevin]: Yes, this happened to me! And it's a way of tricking you into giving up your security credentials. And it happens all the time. And it's really something that we can prevent with strong employee training programs.

[Ari]: Make sense. And I think our firm even does, you know, these kind of, I don't want to call them "test attacks," but they basically are right? Sending out emails that look suspicious but also could pass as non-suspicious. And, you know, I guess kind of after the fact, taking a hard look at how many people clicked on it and why and pointing out the things that make it illegitimate, I guess so it sounds like those could be helpful.

[Kevin]: They're super helpful and there's an art to them in the way that the tests are designed. And then what you do with the test results. How do you communicate with the person who fails the test? What additional training do you implement for those who need it? Very important.

[Ari]: So, Kevin, I know you talked about employee training and things like that. I'm assuming along with that there are some recommended policies and procedures? So I was wondering if you could kind of give our listeners a rundown of certain types of policies that they may want to have in place to prevent these kinds of attacks.

[Kevin]: Yes. So let's run them down and we can come back and talk about some of them.

[Ari]: Sure.

[Kevin]: So I think at this point, we know every organization should have a written information security plan, an acceptable use policy, an access control policy, an ADA website accessibility policy, a privacy policy, an incident response plan, and something we're doing based on information we've learned over the past few months is an artificial intelligence, or A.I., policy.

[Ari]: Okay, so obviously a lot a lot to unpack there. I'm thinking that we should start with what I assume would be kind of the Holy Grail, which is the information security plan. Can you talk a little bit about what that is and what that should entail?

[Kevin]: Yeah. So let's take a step back. Why do you need an information security plan? This is the Holy Grail. Basically, what you are going to do is review all of the business processes of your company, decide what laws and regulations apply to your use of customer data, employee data, consumer data. Identify the potential gaps that you have in your information security, and then lay out a series of controls and policies meant to close those gaps and ensure your compliance with the applicable federal and state laws.

[Ari]: Okay. And what... with respect to the information security plan, Kevin, what employees or who should be aware of that plan? Is that something that everyone should know the details of? Is it upper management? Is it HR? Or is it just...this...should everyone in your organization should know what this is?

[Kevin]: You know, it's funny you say that; this stat is a little bit old, but I remember reading a story a couple of years ago and they surveyed an organization. They surveyed a series of organizations, and they first asked the organization, do you have a WISP or a written information security plan? And two-thirds of the organizations said yes. Now, presumably it would be higher because they're required in many industries. But then they went and surveyed the employees and asked the employees, have you ever seen your organization's written information security plan? And two-thirds of the employees said, no, they hadn't. And the takeaway from that is you can have the strongest policies and procedures in your organization, but if your employees don't know what they are or they don't know what they're supposed to do, those policies are not going to be effective. So the long answer to your question is yes, your employees should know and should understand that information security policy and they should be trained on that policy so that they understand the physical, electronic, and legal safeguards that are in place to protect the corporation's sensitive information, but also the protected information that we hold so dear as employees and customers and consumers.

[Ari]: Right. Advice that really translates to any employment-related policy.

[Kevin]: It really does. So as to anything we're talking about, I was thinking about this earlier and what I would say is if you're hearing anything on this episode and you're thinking, "I don't know what that is" or "I haven't looked at that policy in a while," it's something you should probably focus on because... even if you have a policy, if it hasn't been dusted off and revised on a regular basis over time, that's something that could be an issue, if you do suffer a cybersecurity incident; you have to report that incident to federal or state regulators and they start asking you questions about these critical policies and procedures.

[Ari]: Right, right. So, Kevin, I think I'll let you choose what policy would you like to tackle next or what would you recommend to our listeners in terms of policies that can help prevent cybersecurity incidents?

[Kevin]: Let's take three and focus on those as quickly and concisely as we can.

[Ari]: Sure.

[Kevin]: First is the access control policy. Why is this important? Basically, it's a means of determining that or confirming that the right people in your organization have access to the data and that people that don't need access to the data, don't. And that's important twofold. First, to guard against insider threats. So the fewer people that have access to the critical data in your organization, the safer you are. And the second is to protect yourself from external threats. So if someone's hacking into the organization, and they've gotten my login credentials, if I don't have access to the firm's accounting information or other business sensitive information, I'm not going to be a vector for them to access it. So there are different ways to do that. I think... the again, the short the quick point I would make is if you don't have an access control policy, you want to implement that through your governing board. It can be done in different ways based on who the individual is. You know, you know that these three individuals need access to your accounting data, but no one else does. Could be based on what role that person plays in the organization. So everyone in the accounting department has access to accounting data, but people in the HR department don't.

[Ari]: Right.

[Kevin]: Or it could also be based on other controls. They're called attribute-based controls. So there might be limited access based on the time of day or the geography, the geographical source. So if somebody is trying to access your accounting information or your network at 3 a.m. from a place in North Korea, you know that that's probably not safe, particularly if you're an organization in upstate New York. So the second policy that we want to talk about is privacy policy. And these are critically important. There are upwards of 12 states now that have enacted privacy acts. They are robust. They are easy ways to get in trouble if your organization isn't on top of it...

[Ari]: Yeah, I've heard a lot about this over the last few months, I would say.

[Kevin]: Yeah. Texas is the latest state. California's Consumer Privacy Act was recently amended. California is the original admission states. You know, the requirements in California apply effectively across the country. So if you're doing business in any one of these states, if you are marketing products or services to consumers in any one of these states and you know, depending on the other restrictions, you could be responsible for complying with one of these 12 state's laws. And essentially they require disclosure to the customer or consumer what your privacy policy is, what data do you collect? How do you use it? They afford the customer/consumer the right to opt out, and they require the customer a consumer's consent. So again, if you are doing business at all outside the confines of a single state, you need to take a careful look at where your products and services are going, as you could very well have to comply with the privacy laws of multiple states.

[Ari]: Yeah, that's so important, especially because so many of our clients and listeners have multi-state operations.

[Kevin]: Yeah. Yeah. So third policy that I thought we'd highlight is what we call an IRP or an incident response plan. And this...

[Ari]: This sounds important.

[Kevin]: Oh, yeah. So do you want to know in advance who the important stakeholders are inside and outside your organization and how they're going to work together if you suffer a data breach or other cyber incident. And many people ask, well, what's most important? Well, I think what's most important is that you recognize that it's not just an IT issue, it is an organizational issue. So the decision makers in your C-suite, your general counsel, your chief privacy officer, if you have one, those people, those individuals all need to be involved and you need to know who you're going to call first. And, you know, when it comes to an incident response plan, probably the first person outside your organization that you're going to call is your lawyer, your privacy lawyer, so that that lawyer can serve as the quarterback of your incident or breach response. And I think the second two people you're going to call are your insurance company and your forensic professionals. And your lawyer is going to help you walk through that process and handle those communications. And a lot of people ask, well, why? Why is it important to have the lawyer quarterbacking those operations? And I think here we just want to underscore, Ari, that, you know, obviously communications that a client has with a lawyer are confidential. They may be protected by a privilege or other protection and by making sure that your incident response plan, your breach response runs through your outside counsel, you are maximizing the protection that will be afforded to whatever communications you may have. It's not foolproof. It's not a guarantee that those communications will be protected. But, to the fullest extent possible, if you're involving your outside counsel, they will be as protected as possible.

[Ari]: Yeah, I think that's really good advice. Kevin. And one of you mentioned, you know, calling your insurance agent. I thought maybe you could touch on that for us because I think it's becoming a lot more common in most businesses I think are... have cybersecurity insurance for front of mind. But could you speak a little bit to that? If it's something that it's a separate policy, is it included in your normal CGL policy or. I think that would be valuable information for our listeners.

[Kevin]: Yeah, No, that's an important point. You're right. It's a separate policy. It's typically not included with any of your other coverages. So if you're looking to your CGL policy or your property policy or your do-you-know policy for cyber insurance, you will either not find it there at all or you'll find very limited protection. And the reason is that cyber exposures are so unique that your insurance company is going to want to underwrite that separately. They're going to want to take a look under the hood at your organization. And they're going to want to make sure that you have the basic controls in place before they sell you cyber insurance coverage. So it's a separate policy. Now, there's some good news here, which is if you...for those organizations that don't have cyber insurance, there are some sources that you can go to that will help you prepare for the purchase of the coverage. One is your insurance broker and you want to talk to your broker first to make sure that the broker has experience in the cyber market. Many do. It's a hot topic, some do not, and they should tell you that they don't. And refer you to a specialty broker and another person you can talk to, of course, is your insurance agent or your insurance company itself, because insurance companies are at the forefront of security controls and cyber protection, they're going to be able to tell you what you need to have in place in order to purchase insurance so that if you don't have those things in place, you can go ahead and build them into your system so that in three months or six months, you'll be able to purchase insurance that you might not otherwise have qualified for.

[Ari]: Yeah, I think that's good to know, because I think, you know, especially in the labor and employment space, you and I have talked about this, Kevin, it seems that, you know, EPLI or EPL coverage is becoming more common. I think it's important for business owners, employers to know that this coverage is also available.

[Kevin]: Yeah, I think if we were just doing a quick and dirty summary, you want to have... you want to have commercial property insurance, you want to have CGL insurance, you want to have EPL insurance and you want to have cyber insurance. There may be other coverages that are built into those forms. But if you have those four in place, you're probably in good shape.

[Ari]: Right? So I think this is a good segue way to talk about risk assessment since we've had a discussion about insurance, Kevin. And, you know, I think that there are some things that you wanted to touch on or we wanted to touch on in terms of what is the best way to assess a risk of a cyber event and basically what should business owners be looking out for?

[Kevin]: Yeah, so this is probably one of the most critical and least known of the steps that every organization should take. And people talk about, well, what security controls do I have? What if I have multifactor authentication? What if I have passwords that can't be easily guessed? Right? And the answer is increasingly "no." Those things are good. Those things are important. But really, your cyber readiness begins with a risk assessment. It's important to talk about it at one point, and I want to share is that if we don't have the risk assessment, if you haven't done one if you don't update them—there are state and federal laws that require those in the financial industry. For example, you've got to do an annual risk assessment. If you do, you will have strengthened your organization. You'll have complied with the law. If you don’t and you suffer a data breach or other cyber incident. One of the things the regulators are going to come to you in any investigation with is have you done a risk assessment? We’ve seen organizations get fined if they don’t. So I don’t want to get sidetracked. But what is a risk assessment? At the highest level you’re going to... you or even better, an outside third-party auditor take a look at the sum total of your computer network and systems. It’s going to do an inventory of those, the networking systems, inventory of all the data that you have. The second step is you can once you have that inventory, you’re going to identify the key business processes or aspects of your business that rely on the network, those systems, and that data. Third, you’re going to identify any potential information security gaps. In other words, are there some things that you are not doing that you should be doing to protect that network and that data and you’re going to eventually review and implement security controls to protect those systems, protect that data, and then it becomes a little bit more complicated, but in a good way, because you’re not just going to be going online and saying, oh, I know I need MFA because I saw this podcast, or I know that I need smart passwords because I read it in a magazine. You’re going to want to map out those security controls to some applicable federal, state, or regulatory guidelines. So if it’s business in the financial industry, it might be Gramm-Leach-Bliley on the federal level or it might be the Cyber Security Rule promulgated by the New York Department of Financial Services. If you’re selling goods or services, it might be the FTC safeguards rules. So want to make sure that when you’re shoring up your information security controls, your mapping or tying those controls to a recognized standard. NIST is another one: National Institute of Standards and Technology, this is an invaluable governmental resource that initially promulgated and regularly updates the security controls that organizations should have in certain industries. So all of that is part of a strong risk assessment. And, Ari, I mean, I suppose that every organization could try to do that on its own. But if it is in any way possible to set aside resources to do it, I would strongly recommend considering going to an outside forensic firm to have them come in and work with your own IT and information security professionals. In some...under some laws, in some industries that’s required. You must have an outside information security audit. But even if you don’t, it’s never a bad idea to get the perspective of an independent professional. And that’s very often what we recommend.

[Ari]: Sure. Sure. Thanks, Kevin, that is so helpful in terms of the risk assessment. And, you know, I think having... pointing out that maybe having a third party, if you have the resources to do it, I think it’s also a helpful tip. Speaking of helpful tips, we’ve all heard, you know, practice makes perfect, but I think in the cyber space when you’re dealing with cyber events and you’re looking at incident response plans, that is probably the case. So can you talk a little bit about that? I think as we’ve talked about, it’s a quote, tabletop exercise, but can you tell our listeners what you recommend in that respect?

[Kevin]: Yes. And I’ll plug the Cyber Sip podcast.

[Ari]: Please do.

[Kevin]: We just did an episode on tabletop exercises. Who needs practice? Everybody needs practice, right? So you have this incident response plan. You’ve written down the steps that you’re going to take if you suffer a data breach or another cyber incident. But unless you practice that plan, you’re not really going to know if it’s good enough or where the potential gaps might be. So what we increasingly recommend is something called a tabletop exercise. And there are many ways of conceiving these and designing them. But basically you have an outside expert come in, everybody sits around the table, could be the boardroom and all your stakeholders from your CEO, your HR, your IT, information security, legal counsel, you are going to essentially role-play a breach. Lot of people choose to role play a ransomware attack. So you suffered a ransomware attack. The threat actor has locked you out of your data and is demanding a ransom in exchange for returning a decryption key to you, so you can access your data again. The goal of the tabletop exercise is to help you to execute, in real time, each of the steps of your incident response plan, just to see how your organization handles it, it will identify any gaps in communication. It will determine, for example, if you’ve got the right players at the table at the right time, if you have the right security controls in place. And at the end of the exercise, everybody sort of debriefs and says, okay, what went right, what went wrong, and what do we need to do to make sure that we're ready when we suffer a real breach? Because really, you know, it's just a question of when. It's really not a question of whether. And, you know, Ari, I always think about this. And what we tell our clients is that there are two good reasons to do a tabletop or really any other any other prophylactic measure. First, it's the right thing to do. You really do want to have the best incident response plan in place. You want to have the right security controls in place because that may not prevent a breach of your network or data, but it will make it less likely and it will make it easier for you to respond. The second reason to do it is very practical. Let's say you've suffered a breach and you have to report that breach to affected customers, states attorneys general... You're going to be asked questions. You may be facing regulatory investigation. You may be facing a data breach class action. We're seeing more and more of those. So your ability to come back and say, well, yes, we suffered the breach, but here are all the steps we took along the way to prepare ourselves. It makes it more likely that you can satisfy a regulator or a court that you really have done everything you could. And yes, you couldn't prevent this particular breach, but you are less, at the very least, you're less responsible than an organization that didn't take all of these important steps.

[Ari]: Yes, I think that is...that's the payoff, right? Any time we're counseling clients on how to prepare for any type of incident or conflict in the workplace, preparation is key right. So I think it sounds like that really translates to a cybersecurity world as well.

[Kevin]: Yeah, it absolutely does. And you guys do such a great job of working with your clients and conducting trainings, preventive trainings.

[Ari]: Right.

[Kevin]: I think that.

[Ari]: This is similar, I guess, in that respect. Yeah.

[Kevin]: Yeah, yeah. We really we try to...it's fun. My background as a trial and appellate lawyer. So it's kind of fun to handle compliance and preventive maintenance to try to eliminate or at least reduce the risk that you're going to end up in court answering for, you know, a criminal invading your network.

[Ari]: Right. So, Kevin, I think this is a good place for us to stop today. Thank you so much. I think this has been a great overview. Before we break, though, I wanted to ask you if there's any other words of advice that maybe you didn't touch on or anything you think it's important for our listeners to know before we sign off?

[Kevin]: Yeah, two quick ones that just popped. Okay. They didn't. I actually wrote them down. I forgot to mention. Okay, so number one, if you're dealing with biometric data, you're doing business in a state like Illinois that has a Biometric Information Privacy Act. Be very, very careful. Those acts are very strict. They're essentially strict liability. So if something happens and you're liable, you could be liable for $1,000 for each customer or consumer for each incident. That can obviously add up very quickly. So watch potential exposure under biometric information privacy acts. And the other thing I would mention is if it ever was this way, it isn't anymore. Cybersecurity is not an IT problem. It is an organizational risk. And particularly if you are a regulated organization or financial company, you are regulated by FTC, state or federal, doesn't matter. You have to make sure that your corporate governance is structured in such a way that it oversees and supervises the cybersecurity of your organization. Because increasingly, federal and state governments are holding those in the C-suite responsible for cyber failures. So be careful about that, too. More to come on that, particularly in New York this year when the Department of Financial Services issues a new cybersecurity rule.

[Ari]: Great. Well, thank you so much, Kevin. To our listeners, if you want to know any more about the topics that we talked about, please feel free to contact Kevin or me. And I really encourage you to take a listen to Cyber Sip if you're not already subscribed because it is so informative. Every episode is...I find myself learning something new and Kevin has a lot of thought leaders in the industry as guests on the podcast. So it's really the forefront. You're at the forefront of gaining information as it becomes available. So Kevin, thank you so much.

[Kevin]: Thank you. And by the way, I love, "Can I ask that?" I think I watch that every time it comes out and I feel like I can get through an interview now. Because I know what not to say.

[Ari]: Thank you to our listeners. Kevin is referring to a series that I published by LinkedIn account. It's called "Can I Ask that?" Every week or two I go through a question that you can or cannot ask and a job posting, job interview, job application. So if you want to hear more about that. We did a podcast episode on it last year and check out my LinkedIn. So Kevin, thanks again. We'll talk soon.

[Kevin]: Thanks, Ari. Talk to you soon.

[Ari]: The *Labor & Employment Podcast* is available on barclaydamon.com, YouTube, and all your favorite podcast streaming platforms. Like, follow, share, and continue to listen. Thanks.

Disclaimers:

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

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.*

Thanks for listening.