*Barclay Damon Liv*e Presents *Cyber Sip™*

Season 3, Episode 1: “Five Cyber Action Items for 2024”

Speaker: Kevin Szczepanski

Kevin Szczepanski: Hey, welcome back, everyone. It's Season 3, Episode 1 of *Cyber Sip* powered by *Barclay Damon Live*. I am your host, Kevin Szczepanski. And I've got to tell you, before we get started, we're in Season 3, and I wasn't sure there would ever be a Season 1. It was back in 2021. I was going through a bit of a personal time and throwing myself into creating and developing and launching a podcast was probably a good idea, but I really wasn't sure that I could do it back then.

Kevin: And thanks to the support of the *Barclay Damon Liv*e team and some of our friends outside *Barclay Damon Live*, we are now the award-winning *Cyber Sip* podcast, so we're very humbled to have received the Silver Award from the Academy of Interactive and Visual Arts, and this is a pretty cool organization. The award winners last year include companies like Amazon, IBM, Meta, Netflix, and the Walt Disney Company. So it's an organization that recognizes innovation and excellence in digital media, and we're really proud to have received our first W3 award from the Academy of Interactive and Visual Arts. And I am just the guy that sits on the screen, that you hear over the streaming service. There are a lot of people that I want to just quickly introduce to you and thank, beginning with our managing partner, Connie Cahill. Connie, you have been a tremendous support behind the scenes. I really appreciate it. Our director of marketing, Maureen Fyke, who imbued me with the sobriety of running a podcast many years ago and made sure that I understood how difficult it would be. I still didn't understand how difficult it would be, but I understood it better having had Maureen on the team and so many others to thank. Our senior marketing manager, Irene Meyer, our digital marketing manager, Lexi Belardinelli, and our multi-media specialist—and really the editor of the podcast…she's the one that makes me look good—and that's Kyla Handley. And I also want to thank one other person who is not on the inside here at *Barclay Damon Live*, and that is Al Cutri. Al was our first podcast editor, and he was one of the first people I really sat down and had a heart to heart with when I talked about whether this podcast made sense, and he spent a little time with me and we talked about it for a little bit, and he really gave me the courage and the strength I needed to take that final step.

Kevin: You know, when they say that the journey of a thousand miles begins with a single step, or you have to have the courage to step over the precipice and hope that there's something there to break your fall. That's what Al did for me. And he's been like a brother ever since. And I appreciate you, man. Thank you so much. And thanks to all of our *Barclay Damon Live* team.

Kevin: So with that said, I want to transition to the topic for Episode 1 of Season 3, and that is five cyber action items for 2024. Now, if you saw some of my digital content on LinkedIn, you've gotten a preview of these five action items, but I want to talk about them in a little more detail today because I think they're very important. I think some of them we all should be doing already. Some of them we may not need to do right away. But these are the action items that we see in our experience organizations fall down if they don't follow. So I want to talk them through with you. And by the way, before we get started, if you like anything you hear or see, please like, comment, and share.

Kevin: That is what tells our services—Apple, Spotify, and YouTube—that more people than you should see and hear our podcast. So we appreciate that. All right, cyber action item one. This is something that you should already be doing. And if you're not, you should really drill down soon as possible here in 2024, and that is a *cyber risk assessment*. So let's start by putting the cart before the horse. Suppose you're sitting there now and you're thinking, well, what do I need to do to improve my cyber hygiene? What are the steps I need to take? I hear I should do multifactor or two-factor authentication. I should have smart passwords, I should encrypt my data in transit and at rest. And if I do these and a few other things, I'm going to be safe, right? Not necessarily. In fact, in almost all cases you won't be. And that is because picking the security controls that you want to implement before you do a careful risk assessment of your organization's information security is literally putting the cart before the horse. So here's the horse: risk assessment.

Kevin: This is where you are going to point to identify your key applications and systems. We're going to identify, we're going to estimate, and prioritize the risks to those systems and the risks that they pose to your organizational operations. So you have assets, customers, consumers, your reputation, and even your relationship with other organizations. You may have vendors or you may be a vendor to another organization. And the purpose of this assessment is to identify the potential risks, the potential problems, that you could encounter. Maybe it's a business email compromise. Maybe it is a ransomware attack that will shut you down for an undefined period of time until you can figure out a way to restore your data. Maybe it's a data breach. Could be another cyber incident as well. But there are invariably risks that different components of your network and systems will face, and you need to identify them. You need to think about what will happen if those risks come to pass again. Am I going to be down? Am I going to suffer a loss of business? Am I going to suffer a loss of reputation or goodwill?

Kevin: And then the next step is to identify the mitigation strategies that you will implement to manage those risks. What is that? Those are the information security controls, the physical and legal safeguards that you need to implement to manage that risk. And that's where multifactor authentication, endpoint detection and response, encryption, a whole host of other potential safeguards come into play. And what you really want to do is not just divine these safeguards out of thin air. You want to tie the safeguards you're going to implement back to a recognized standard like NIST or ISO. And you also want, if you're a regulated entity, to tie those mitigation strategies back to the statutes or regulations that govern you. So, if you're a publicly traded company, those are the new SEC requirements everybody's hearing about. If you're a covered entity under New York's Department of Financial Services Amended Cybersecurity Regulation, there are requirements in that new regulation that you need to comply with. And it may be the FTC safeguards rule. The key is whatever you're bound by, you need to consult and you need to fashion your physical, electronic, and digital safeguards around those requirements.

Kevin: That way, you ensure that you have most effectively managed your system. And by the way, if something were to go wrong—and it inevitably does; it's not a question of “whether,” it's increasingly a question of *when*—you are going to be able to answer the difficult questions you might face from your business partners or a regulator, who will ask you how did this happen? What did you do to prevent it? How did you respond? And as they're measuring the strength of your preparation and response, your risk assessment that you did months or even a year ago is going to hold you steady and strong. So number one on our list of cyber action items for 2024 is a risk assessment.

Kevin: All right. So you've done this risk assessment. What's item two? The next item is an incident response plan. Now, I know that many of you know what an incident response plan is. Many of you have one in place, but many of us don't. And at this point in 2024, we're really past the point where we need to implement a written incident response plan. What is this? This is a written plan that tells you who to call, what to do, and in what order when you experience a cyber incident, like a ransomware attack. And we've addressed incident response in other episodes of *Cyber Sip*, so I'm not going to drill down on that too deeply right now—but you want to have all of your stakeholders from your IT department to your CISO, if you have a chief information security officer, your general counsel, your C-suite executives, your outside forensic firm, and first and foremost, your outside counsel, that's going to be your first call so that you can protect yourself and your communications to the fullest extent possible. You want to have this roadmap, this playbook of who you're going to call and what you're going to do, so that when the inevitable incident happens, you don't have to think about what to do first. You've already planned it. So that is cyber action item two for 2024.

Kevin: Let's move to cyber action item three, and that is tabletop exercise. You need exercise. And I'm not talking about the physical kind, I'm talking about exercise to your information security structure. And what do I mean by this? Well, I mean, we've all heard the adage “practice before you play,” right? No one sends professional athletes out onto the field without a week's worth of practice. In fact, we all know that if you haven’t practiced, you're probably not going to play because you're not *able* to play. You haven't prepared, you don't know the game plan, you're not physically ready. It's the same thing when it comes to cyber readiness and what's the cure for that? Tabletop exercises? So what are we going to do? We have our incident response plan. We want to practice or drill that plan, so that when the inevitable incident happens, we've done this before. And because it's an exercise, it's not a real event, you can fail, you can make mistakes. In fact, you almost want to, because in failing and making those mistakes, you identify the weaknesses in your incident response structure, and you can fix them. You can improve them before an actual ransomware attack or other cyber incident happens.

Kevin: So how do these work? You can certainly do it internally, but I would recommend bringing in an outside service provider who's experienced in offering tabletop exercises. It's basically a team leader. You and your stakeholders are all going to be in the room. Your in-house counsel, your outside counsel, your forensic team, your IT department, your C-suite executives, and you're going to role-play an actual cyber incident. And the service provider—that the person who's running the tabletop exercise—is going to walk you through that breach response, that ransomware response. And in doing so, you're going to get better and stronger and really prepare in a way that your competitors have not, for how to actually answer an attack or breach or other cyber incident. Yes, it's an additional cost. But again, do you really want to be in a position if you suffer a breach, you have to report that to affected individuals. You have to report that to your regulator. Do you really want to be in a position where you have to answer “no” to the question whether you did *anything* to prepare in advance, anything to drill in advance your response to that attack or breach or other cyber incident? You don't. So number three on our list of cyber action items for 2024 is tabletop exercise.

Kevin: Turning to number four, the fourth cyber action item for 2024 is *policy review*. Now, there are literally a plethora of policies and procedures that your organization could enact. I'm not going to touch on all of them. We should save that for another episode. I want to hit the highlights here. But the key takeaway is there are basic cyber policies and procedures that you want to have in place. And if you’re regulated either by federal law or by state law, you may be legally required to have these policies and procedures in place. So what are we talking about? In alphabetical order: a business continuity and disaster recovery plan. You want to have a written playbook in place that tells you what's going to happen if something happens to your systems and you are unable to access them or your data. And you want to have a plan in place for how you're going to recover from that disaster when it happens. Second, a cybersecurity policy. You want to have written policies and procedures designed to protect your information systems and the nonpublic data, PII. Personally Identifiable Information/PHI, Protected Health Information, are two examples that nonpublic information that you are legally required to safeguard. That's what a cybersecurity plan is. You want to have one of those in place as well.

Kevin: And finally, I'll pull one out of the many categories of potential policies and procedures. You want to have a privacy policy in place. We've seen over the last year or two what I like to call a true paradigm shift. When we started many years ago in the field of cybersecurity, the focus was on security. What do we do to protect an organization from an attack? What do we do to enable that organization to recover quickly and efficiently when it suffers that attack? Well, today that's still important. But there is an increasingly important and I would say more important… goal in place, and that is privacy. Privacy has overtaken security in today's world of cyber hygiene. And what does that mean for us? That means that if you have the data, protected data of individual customers, consumers, even employees, you have a duty to safeguard that data. And if you don't, bad things can happen. You can, you might have to report a data breach, you might face a regulatory investigation. And increasingly what we're seeing is when those data breaches are reported to regulators, the plaintiff's bar is monitoring those reports on a daily basis. And if you're one of the companies that has to make one of those reports, you may find yourself a defendant in a data breach class action. So privacy policy is very important. But undergirding a privacy policy is disclosing to those protected individuals what data you have, how you're using that data and how you're protecting that data. So that's item four on our cyber action items for 2024.

Kevin: Let's talk about item five. And this is one that you may not have heard of before, but if you are regulated entity and you are required to have a CISO, or a chief information security officer, you might have heard of this. And that is a virtual CISO. Before you know what a virtual CISO does, let me talk a little bit about what a CISO is. This is a qualified person in your organization who is responsible for overseeing your cybersecurity program and enforcing your cybersecurity policies. Increasingly, a CISO is responsible for managing your organization's cybersecurity budget, making sure that there are adequate resources in place to pay for the safeguards that you have to have in order to protect your systems and data. And even more important is the CISO’s role in governance, because more and more, particularly if you're regulated by federal and state law, a CISO is the point person that is going to converse with and report the state of your organization's cybersecurity to your board and to your C-suite officers.

Kevin: Now, that sounds important, or I hope it does, but not every organization can afford the cost of having, …of paying a salary, expenses, benefits to a brand-new employee. CISOs are invaluable and they can be expensive—and for good reason. You want a CISO. So but you may not have the resources enter the virtual CISO. So this is a product that you can purchase from qualified organizations. And what they do is they will have a response, essentially a response team that's available to you. They can perform discrete tasks. You may have a particular update or particular evolution in your information security apparatus that you want to undertake, and the virtual CISO can help that. Or you may want to have a virtual CISO to do what a real live human CSO does, which is manage your cybersecurity program. It's a tremendous service. It's a lot less expensive than having an actual CISO on board. So if you're one of those organizations that knows you need a CISO but can't quite budget for a real live CISO just now, consider a virtual CISO many organizations are doing this. I think it's a tremendous idea and I think the choice between no CISO and a virtual CISO is an easy one.

Kevin: All right, so those are the five cyber action items for 2024 I wanted to talk to you about. Again, if you enjoyed these tips, please like, comment, and share. And I want to close just by telling you about some of the things I'm really excited about for *Cyber Sip* season three. We are going to be talking about AI when we talk a lot about it. I've been out giving presentations on AI and I can tell you a lot of people are anxious about it. A lot of organizations are using it. Very few organizations are actually focusing on legal compliance, which is how do we embed our duty to comply with the law governing data privacy and security into our AI programs. So that's going to be a topic we're going to talk about.

Kevin: We're going to have a very special guest come back to talk to us about cybersecurity for kids and why it is so important to create a culture of cybersecurity in our schools. There are a lot of things that you look back and you say, boy, I wish they’d taught me about this in school. I wish they’d taught me how to manage money. I wish they’d taught me the importance of 401k investment. And I think cybersecurity is going to be one of those special items too. And I think rather than look back with regret, we should be focusing now on teaching our kids how to be safe out there. The Internet, streaming services, and in that murky world of TikTok and other social media.

Kevin: So, those are just a few of the topics we are going to cover in season three of *Cyber Sip*. I hope you're looking forward to it as much as I am. I hope you enjoy today's episode on five cyber action Items for 2024. If you have any questions, let us know. And we're back soon with another episode.

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.

*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.*

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.*