Barclay Damon Live Presents *Cyber Sip™*
Season 5, Episode 8: "Have You Done Your Cyber Risk Assessment?"

Host: Kevin Szczepanski, Barclay Damon

[Kevin Sczcepanski]: Here's a quiet problem inside a lot of organizations: they invest in cybersecurity tools. They've got the MFA, they've got the EDR, and that alphabet soup of good stuff. And they adopt their policies, the written information security plan, the incident response plan, and they train their employees once a year, maybe more, with devices like Adobe4 or other training on how to recognize spear phishing. But they've never conducted a formal risk assessment. And that misses the mark because in many cases, that means they're already out of compliance with the law. Why? Because for many industries, a cybersecurity risk assessment is not optional. It's not just a nice thing to do. For many organizations, it's required by law. So today I thought we would walk through the prospect of risk assessments in a very practical way and cover three things. First, where does the legal requirement come from? Second, what does a defensible risk assessment actually look like? And third, how do we use it to strengthen your organization's security posture. All right. So let's start with the law. If you are subject to any of these laws—and we're not going to deal with them in detail today, we can do that on another episode or we can talk about that offline—but if you're subject to any of these laws, you must do a cyber risk assessment first. The FTC safeguards rule. You might not know this, but that rule applies to any organization that handles consumer financial information. So if you do that, you have to do a risk assessment. Second, the Gramm-Leach-Bliley Act, which applies to financial institutions. So if you're a financial institution, you need to do a risk assessment. Third, HIPAA. If you handle protected health information or PHI the HIPAA security rule, requires an accurate, thorough assessment of risks to electronic PHI. Fourth, the New York DFS, that's the Department of Financial Services cybersecurity regulation. If you're what's called a covered entity in New York, and you might be, you're required to perform an annual risk assessment and update that assessment annually. So let's sum up on the law. Whether it's the FTC safeguards rule, Gramm-Leach-Bliley, HIPAA or a law similar to the New York State Department of Financial Services cybersecurity regulation, you have a legal obligation to do a risk assessment, not just something to get around to when you can, but something that you need to do now. And if you've done it, and it's been longer than a year, you need to update that risk assessment. So with that in mind, let's talk a little bit about what a risk assessment does.

[Kevin]: So at its core a risk assessment is going to answer these questions. What data do you have? Where is it stored? Who can access it? What could go wrong if the wrong person accesses it? How serious would that be? And what safeguards do you have in place to manage all the risks that you identify? So we're talking about data. Let's go to the data and start there. What do you actually protect it. What data do you have—and where does it live? Is it in your own computer system? Is it in the cloud? Is it with a vendor? I've seen organizations discover during this step alone that sensitive data is stored in a legacy system that you no longer use, and you haven't looked at in years or it's sitting with a vendor, a trusted vendor, a vendor you need, but a vendor that does not have the same cyber safeguards that your organization has. This can lead to problems.

[Kevin]: And good news. Identifying those problems is just one of the things that a risk assessment does for you. So now let's talk about risks. You know what data you have. You know where it is. Now you want to identify the risks to that data. And it's not just external threats from hackers. We're talking about internal

weaknesses, like employee access. Maybe every employee has access to data that he or she doesn't need to do the job that they need to do. Maybe you have some misconfigured systems. Maybe there's some vendor exposure. You've got that vendor we just talked about that you need and you want to work with, but that vendor does not have the same safeguards that you have. So the important thing to keep in mind here is that risk is not just about bad actors. It's about weak controls, outdated systems, and policies and procedures that you either don't have, or you haven't dusted off and updated in a long time. So we talked about data and risks. Next step is to talk about safeguards. So you're going to evaluate that. Your administrative safeguards. What are those? Policies procedures; your technical safeguards. Are you going to have multi-factor authentication endpoint detection, smart passwords, a VPN for remote access. Those are just a few of the many technical safeguards you have in place. And physical safeguards as well. What do we mean by that? Well, you want to make sure that your organization's servers are secure in a safe place where not just anyone can access them. You want to make sure that your computers are locked down so that when you leave your office, some stranger can't come in and sit down at your desk and start doing nefarious things.

[Kevin]: It may even include a clean desk policy, but whatever it is, you've got to focus on all three: administrative, technical, and physical safeguards. Now I want to pause here and talk to you about something very important in the context of safeguards, because many organizations will place this step, this safeguard step into the hands of a technical vendor or an in-house IT team. And it's important to have a capable, dedicated IT team. And you want—if you don't have that expertise in-house—you want to have an expert professional IT vendor. All good. But here's the concern I have. You cannot rely on an IT vendor alone to conduct a risk assessment for you. The reason is that the assessment process is a mix of technical and legal steps. So you need to have someone familiar with both to help you. Keep that in mind as you consider your risk assessment. Let's move on from safeguards to prioritizing because not every issue is equal. A missing patch, which is very important. Or the absence of multi-factor authentication on remote access is very different from the failure to update your information security policy for three extra months. So what you want to do when you prioritize is work with both your technical professionals and your legal professionals so you're doing the most important thing first. You're laying the most important bricks first because that's the foundation you're building. Next step is documentation. You want to document everything because from a compliance standpoint, if it's not in writing, it doesn't exist. And when you're documenting, you want to be very careful. Consider retaining a legal professional to help you with the documentation so that to the fullest extent possible, your documentation is legally protected.

[Kevin]: The final step I want to talk to you about is action. This is the part where most organizations fall down. They identify their data and the risks. They map out safeguards, they get it in writing, and then it goes into a drawer somewhere. But here's the thing: a risk assessment is not the end product that you can stick in the file and forget about. You don't set it and forget it. The risk assessment is your starting point, because you're going to take the findings that you have from your risk assessment and turn them into a plan.

[Kevin]: Think about quarterbacking a game. What action do we need to take? Who's taking the lead, and what are the timelines? What are the deadlines that we need to hit to make sure that we put this risk assessment into practice? So for example, if your remote access lacks MFA, you implement MFA. If your vendor poses some risk because, for example, its safeguards aren't where you want them to be or it doesn't have cyber insurance, then you need to build a vendor review process to sit down with your vendor, talk about these issues, and make sure that you get as close as possible to what you need. Information security, indemnification, cyber insurance—they're all important, and you have to have that conversation. Finally, if employees have needless access, so you've got too many employees that can see too many things that they do not need to do their work, you tighten your access controls.

[Kevin]: So let's boil this down to these questions. Do you have a risk assessment? Has it been updated recently? And if it's been more than a year, it's time to open it up and update it. Does it identify the key cyber risks to your organization? And have you actually acted on that risk assessment? Because if the answer to any of those questions is no, you know what you have to do. Got to do a risk assessment. Go to update your risk

assessment. So let me sum up this way: most organizations don't struggle with cybersecurity because they ignore it. They struggle with cybersecurity because they skip over the step that tells them exactly where the trouble is. That's where the risk assessment comes in.

[Kevin]: And by skipping that assessment process, they put themselves in a little bit of legal peril. Like we said at the start, it's not just a good thing, a nice thing to do. It is legally required depending on where your organization sits, it could be the FTC safeguards rule. It could be Gramm-Leach-Bliley or HIPAA for health care providers, or even something like the New York State Department of Financial Services cybersecurity rule, or your state's equivalent. Whatever it is, we've got to solve this problem. So how do we do it? Start with a risk assessment. And if you do, you'll be well on your way to following the law, protecting your data, and reducing the risk of a data breach, a lawsuit, or one of those other cyber events that keep us all up at night. That's all for this episode of *Cyber Sip*. Thank you so much for joining us. Please like, comment, and share. If you have any questions or thoughts for me, please hit me up in the comments. And again, thanks. We're back soon with another episode.

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