



Barclay Damon Live Presents: The Cyber Sip Podcast
Episode 5: "Five Things You Should Know About Cyber Insurance"
Speaker: Kevin Szczepanski, Barclay Damon

[Kevin Szczepanski]: Hey, everyone, this is a Barclay Damon Live! broadcast of the Cyber Sip, practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[KS]: Welcome back, everyone. Today I'd like to talk to you about five things you should know about cyber insurance. First and foremost, cyber insurance is really an invaluable risk management tool. The average cost of a data breach continues to rise, and some reports indicate that it's well into the seven figures. So if you experience a breach of your data or your system, you want to make sure that you have insurance in place to help you pay for the lawyer that will quarterback your response, the forensic investigator who will determine what happened, what caused the breach, what data was accessed or removed from your system, and you'll definitely want to have insurance in place to cover the costs you may incur to provide notice to any individuals affected by the breach. If you have claims against you as a result of cyber events, you'll also be entitled to a lawyer who'll defend you and you'll have coverage for any judgments or settlements you have to pay. All of that very good reason to have a cyber insurance policy in place.

So, it's an invaluable risk management tool. Every organization should have it. That said, there are some caveats that we should talk about, which leads to the second thing you should know about cyber insurance: And that is that today the market is hardening. What does it mean to say that the market is hardening? Generally speaking, it means that premiums are on the rise and coverage is on the decline. What does that mean for us as a practical matter? It means that cyber insurance is going to be harder and harder to come by. If you don't yet have a policy, it will be harder for you to get one. If you do have a policy, you'll face a more rigorous renewal process ... which leads to the third thing you should know about cyber insurance.

The application process is increasingly rigorous. Insurance companies want to know generally about the physical, electronic, and administrative safeguards that you have in place to protect your data, your systems, and your customers. So you're going to be asked detailed questions about what kind of data do you have? Do you store, for example, PHI, or protected health information? Do you store PII, or personally identifiable information? Most organizations do. Yours likely does as well. You'll also be asked about the physical, electronic, and administrative safeguards you have in place to protect your data, your systems, and your customers.

Now we could do a full podcast on appropriate electronic safeguards, and we will in a future episode. But for now, your carrier is going to ask you questions about whether, for example, you use multifactor authentication, whether you require employees to have smart passwords, whether you restrict data to solely those employees who need to use it. Whether you have log collection and management procedures. Your carrier, in short, is going to want to know the scope of your cybersecurity safeguards and the extent of your coverage, and the premium you pay will depend in part on your answers to those questions. Your carrier will also ask you about whether you have written policies and procedures



in place for information security and data protection. And the carrier will ask you whether you would train your employees on those procedures. You might also be asked about whether you conduct regular vulnerability scans or penetration testing. Carriers are looking to see not only that you have the procedures in place, but that you're training your employees on them and you're regularly monitoring your compliance with your own internal safeguards.

So, you've gone through the application process and now you have a cyber insurance policy. That leads us to the fourth thing you should know, and that is, every cyber insurance policy is different. Unlike commercial general liability policies, employment practices liability policies, or even, DNO policies, whose forms have been around for many years and in some cases, decades, cyber insurance forms are not standardized; every carrier has different policy language, so it can be a challenge to compare one policy to another. But it's critically important to do that to make sure that you purchase the policy that best fits your organization, your needs, and your risks.

That's one good reason to make sure that when you're doing the comparison, you have an experienced insurance professional there to guide you.

And that leads us to the fifth thing you should know about cyber insurance, and that is there are potential coverage gaps. Let's talk about one that's become increasingly prevalent in this era of remote workforces, and that is the definition of "computer network," or "system."

Every policy will have a definition for network or system that includes employer-issued devices, phones, laptops, related devices that employees use to do their work. But in the era of remote workforces, oftentimes employees are working at home, and we're using our own laptops, our own phones. If the definition of "computer network" or "system" in your cyber policy does not include employee-owned devices and a cyber incident can be traced back to one of those employee-owned devices, you might not have coverage.

Now the good news is you can eliminate some of these coverage gaps up front. Let's take our example of the policy definition of "computer network or system." You can eliminate the gap for employee-owned devices, either by purchasing a policy that includes employee-owned devices right in the definition itself, or by working with your broker to endorse a policy to expand that definition to suit your needs.

So those are five things you need to know about cyber insurance. But of course, they're not the only five things you need to know in a future episode, we'll be back with a very special guest to talk more about cyber insurance. For now, that's all from the Cyber Sip podcast. We'll be back again soon.

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

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

