



9 TIPS FOR BUYING CYBER INSURANCE

A GUIDE FOR ENTREPRENEURS TO MAKE MORE
EFFECTIVE DECISIONS ON CYBER INSURANCE/

GORDON B. COYLE, CPCU, ARM, AMIM, PWCA

MANAGING PRINCIPAL & CHIEF RISK ARCHITECT AT
THE COYLE GROUP

9 TIPS FOR BUYING CYBER INSURANCE

Assessing the Risks, Understanding Cyber Insurance, and Making a More Effective Buying Decision

There are several issues to consider when purchasing cyber insurance. In this short checklist we're going to go over the issues you should be thinking about not only to help reduce your costs, but to make sure you're getting the right protection.

First, let's lay out what cyber insurance is and what it's not.

I like to explain that Cyber Insurance is a combination of two buckets to help you weather a cyber related storm. The first bucket is expertise. Most cyber insurers have a 24/7 hotline staffed with experts to call when you suspect you've had a breach, hack or other cyber related event. This is going to give you the peace of mind knowing that regardless of the time of day you can speak to an expert to help curtail or stop the threat of an event from continuing and set you on the right track to recovery.

The second bucket is money. Cyber events are expensive to remediate, and most cyber policies will provide reimbursements for the cost of experts in tech, legal, forensics, investigations, public relations and other fields to help mitigate and remediate from the effects of an event; as well as pay for legal liabilities you may face from third parties.

Without both buckets, a company suffering a cyber event can face a possible bankruptcy due to the serious costs involved.

But one of the most important things to understand about cyber insurance is that it is a non-standardized form of insurance coverage. Almost every cyber policy on the market is different, so it takes a skilled expert to negotiate the best terms and conditions to fit your needs.

So where do you start?

1. **Work with an expert.**

Look, if you're a small company with less than 10 employees an "off-the-shelf" policy will probably work just fine and the insurance broker who handles your business insurance can likely help you with obtaining a cyber policy. For firms larger than that or in more complex industries (such as technology or financial services) you need to find an expert in the field of cyber to help you.

2. **Understand your needs.**

If you've purchased cyber insurance in the past and have a \$1,000,000 limit of liability policy, you should start with asking yourself how did you get there? Did the broker who got you that policy ask you questions specific to the number of "personal records" your company had in storage? Or, did they perform any sort of calculation and offer you alternative quotes with different limits of coverage?

If you don't have a policy, we recommend and will do this with you – go to the NetDiligence breach calculator. Here is one we often use:

<https://evolvemga.com/databreachcalculator/db-calc-standalone/data-breach-mini.html>

By inserting a few basic numbers you'll get a sense of what your potential risks are for cyber breach and with that can make a more informed buying decision. Our recommendation - don't get one quote – ask for limit options from the top insurer(s) your broker is recommending.

3. **Read your policy coverage terms and conditions**

If you have a policy, and if not, your proposal. Ask questions and if necessary, go through the policy or proposal with a highlighter and ask your broker for a better

understanding of what is and what's not covered. A BIG issue that is not addressed in many cyber policies is how cybercrime is addressed and what sub-limits apply. As I mentioned earlier, no two cyber policies are the same and many forms may be customized to fit your particular needs.

4. If you purchased cyber insurance several years ago....

Good for you. But the bad news is that your policy form may be outdated. Newer policy forms and entrants to the cyber field are providing broader more tailored solutions to cyber. If your policy form has not been updated, it may be ineffective to the latest threats.

5. The more defense you can build...

Into your cyber security systems and the less dependent you may be on cyber insurance in the future the better you will be. Like all insurable losses, it is much cheaper to prevent a claim than to have your insurer remediate that claim. And, the greater your defense, the more favorable your policy terms and premiums will be. Relative to this, ask for discounts. Your broker may not ask specifically in the initial underwriting phase of pricing your policy about system security or the level of cyber security training your employees get so it's important to disclose this upfront to get the best pricing and available policy discounts.

6. Look out for policy warranties.

A policy warranty in a cyber policy may indicate that you must authenticate every wire transfer before made. This isn't necessarily a deal breaker, but if this is not clearly communicated and put into your standard operating procedure you may at some point break your SOP, in a rush and issue a wire. If that wire was fraudulent it may not be

covered under the policy. Some underwriters do not put warranty teeth into their policies, but some do. Be aware of them.

7. Some policies come with pre-breach risk management services.

USE THEM. Often these services are free and may include building a risk aware culture in your firm, having an external firm penetration test the security of your network, tools to have strong passwords, testing phishing schemes, and more.

8. Obtain Coverage Retroactively

Cyber insurance is written on a claims-made policy form and if you're purchasing your first policy some insurers will provide what is known as "full-prior acts" coverage or put another way there is no retroactive date on the policy. What this does is give you the peace of mind that if a hacker has been lurking around in your network prior to your policy taking affect, and you didn't know about it, there would be coverage for claims which may arise from that breach.

Now, if you do know that you've got a cyber event problem and that motivates you to go out and buy insurance, that potential claim will not be covered, even if the insurer provides you "full prior acts".

Why? Because most applications will ask a warranty question like "does the applicant have any knowledge of any fact, circumstance, situation, event or act which could give rise to a claim if this policy is issued." Breaching that statement will void coverage. This is similar to what we call "burning barn" exclusion, insurance cannot be purchased for known issues that will result in a claim.

9. Coordinate cyber coverage with your other insurance policies.

This is particularly true of cybercrime coverages and your commercial crime policy. You'll want to avoid duplication without coordination to avoid "other insurance" clause issues which will force two insurers with similar coverages to fight over who is not paying the claim.

SUMMARY

As you can see there are a lot of moving parts with Cyber Insurance. On top of all that is presented here, there are also market conditions and forces which change over time. At the time of this writing, early 2021 the commercial insurance marketplace, including cyber has been experience a hardening trend. Meaning that prices are rising, and availability is somewhat restricted. Cyber has not been hit as hard as other lines of management and professional liability insurance (such as D&O, Employment Practice Liability or Professional Liability) but there is a return to more disciplined underwriting.

The more thorough and consciously you complete applications and provide supporting information to your broker, the better you will be in terms of achieving broad terms, conditions and competitive pricing. Now is not the time to provide scant details on system securities and protocols.

This is only a brief overview of the issues, for a more in-depth conversation regarding cyber insurance as well as other business insurance and risk issues, please contact us!

Gordon B. Coyle, CPCU, ARM, AMIM, PWCA
The Coyle Group
845-474-2924
gbcoble@thecoylegroup.com