Cyber

6 STEPS TO A BETTER CYBER INSURANCE POLICY

HYLANT

hylant.com

OBTAINING CYBER INSURANCE *HAS BECOME COMPETITIVE.*

The average cost per data breach in 2021 rose to $4.24 million, up 10% from the previous year.*

Unsurprisingly, the cost to obtain cyber insurance is also rising. In addition, underwriters are asking more questions before deciding whether to provide coverage, to whom, and with what restrictions.

Finance, IT and risk management professionals should prepare for these conversations to obtain the best coverage, pricing, terms and conditions in this competitive landscape.

Follow these six steps to prepare.

**Cost of a Data Breach Report 2021*, IBM Security/Ponemon Institute, July 2021

STEP 1:
SHOW THAT YOUR NETWORK IS SECURE.

Networks can be complex creatures with all sorts of vulnerabilities. The right network security may be your first line of defense, but only if you're aware when a threat actor tries to get through.

Most small and mid-sized businesses don't have the luxury of full-time information security teams, so how are you staying on top of the activity and traffic in and out of your network?

Want to impress the underwriters? Talk about the EDR (endpoint detection and response) and IDS (intrusion detection systems) tools you've deployed and how your managed security provider watches them. Don't have those things? You'd better add them before you apply for coverage.

6 Cyber Controls
Every Business Should Implement

1. Multifactor Authentication
2. Endpoint Detection & Response
3. Patching
4. Email Filtering
5. Data Backups
6. Web Security

STEP 2:
PROVE THAT YOU CONTROL ACCESS.

When Patricia in Poughkeepsie logs into your network, how can you be confident it's really her behind the keyboard? Once she logs in, how do you ensure she doesn't have the ability to get to parts of the system where she has no business being? And if she switches activities, are you completely sure it's still her and not Polina in Petrozavodsk?

In an era when everyone's working from their breakfast nooks or walk-in closets, access management is crucial. **Insurers will expect you to use multifactor authentication, but they'll want to know when and how often you double-check identities.** They'll want to see how you keep that shipping clerk from Schenectady out of the CFO's spreadsheets.

Insurers may not require biometric screening, but **they will want to see proof you're taking access control as seriously as you should.**

STEP 3:
KNOW HOW QUICKLY YOUR SYSTEM CAN RECOVER.

Ransomware has become a cat-and-mouse game. The bad guys lock up data, you're smart enough to have backed it up. So they figure out how to lock up everything on your network. You create an off-site backup. So they bide their time, learn your routine, and quietly infect the files you're going to put in that off-site backup before they strike.

> **Cyber insurers want to know how fast you can bounce back** when that happens:

- What's your plan if ransomware hits you tomorrow morning?
- Will you be out of business for a month, or have you created smart contingencies?
- Have you actually restored a backup, or are you just praying your process will work?

> **They'll also want to know if your planned response will wipe out forensic evidence that might help identify the source of the attack** or prevent it from succeeding at other companies.

> **Most of all, are carrier resources for all of these things and more built into your coverage?**

STEP 4:

PROVE THAT YOU TRAIN YOUR EMPLOYEES.

Your amazingly well-constructed security plan became toast when Doug fell for that phishing email. Underwriters know there's no such thing as total security, because there's always a Doug.

Insurers want to see how you're transforming employees from your weakest link into key elements of your defense. They want to be confident every team member understands their responsibility and how they execute that responsibility on every system and platform.

Helpful hint: **when employee cybersecurity training is structured around rewarding the right kinds of behavior, it's far more effective** than when it's all about punishment.

STEP 5:

HAVE A PLAN FOR RESPONDING TO CYBER INCIDENTS. TEST IT REGULARLY.

Expect underwriters to ask whether your company has an incident response plan. But they won't just check the box and stop there. They'll also ask:

- Have you tested your incident response plan?
- Does your plan include everyone it should?
- Do the people listed on your plan know they're part of the plan?

If you haven't tested your plan in the last three months, do it now. A tabletop exercise is a great way to determine whether your plan includes everyone it should or if there are significant gaps. It's better to find and fix those flaws before you face a critical incident.

And no, you can't anticipate every conceivable type of incident. But if you **have the right people and the right process in place,** you'll be ready for whatever gets thrown at you.

STEP 6:

DEMONSTRATE HOW YOU VET YOUR THIRD-PARTY VENDORS.

When it comes to the cloud and other third-party vendors, it's good to trust, but you'd better verify.

Your third-party vendors provide many advantages, but they also create risk exposures for your company. Cyber insurers want to know how well you understand that, along with how you confirm your vendors' promises aren't just persuasive marketing.

It's more than just due diligence. It's how you think about vendors, what systems you allow them to access, what you can reasonably expect from them in a crisis, where you'll turn if they can't help when you need them most, and how often you make sure they're continuing to hold up their end of the contract.

Most of all, never lose sight of the fact "the cloud" is just someone else's computer.

HAVE QUESTIONS ABOUT *TAKING THESE STEPS?*

Anyone can bring you a quote for cyber insurance coverage, but Hylant brings a strategic partnership and the specialized knowledge you need to manage your cyber risks.

Our expertise and familiarity with the cyber insurance market means **we know what questions underwriters are asking ... and why they want to know.** So before we prepare an application for coverage, we ask our clients those same questions and help them take the necessary steps so that they can provide the right answers for a successful outcome.

It's okay if you can't answer those questions right now. **With Hylant's help, you'll be ready to answer with confidence when the time comes**.

Learn how we can help you by reaching out to Hylant at **https://www.hylant.com/contact/**.

Helping you understand your cyber risks is our job. We guide you through all aspects of one of the fastest-growing risk categories affecting organizations worldwide. Ready to get started?