Shopping for cyber insurance? Six questions to ask before you call the insurer

Josh Cigna
April 13, 2022 7 minute read

The cyberthreat landscape has always been worrisome, but today there are many more CISOs noticing new gray hairs in the mirror given an anticipated uptick in cyber attacks from nation states and other bad actors. Ransomware attacks and other forms of account compromise continue to grace the news every month with malicious actors – state-sponsored or otherwise – having the potential to cost companies millions (or even billions) in downtime and lost opportunity. There are also serious reputational risks for vendors who might see customers flock to a competitor after a publicized attack.

These attacks have broken the old cyber insurance risk models because it's become too easy for an attacker to steal credentials and work from the inside. They use relatively simple technology, but can cause serious damage through days of downtime – even more than a classic breach or reputation damage. These developments have far-reaching implications across the entire insurance industry, from the insurers, to the brokers, to the insured themselves.

Due to a heightened risk profile caused by recent events, cyber insurance premiums have skyrocketed, going up by 150-300% in some cases. So it's no surprise that this increased-threat environment has inspired a quick uptick in cyber insurance interest as firms either consider signing up for the first time or seek to increase liability coverage.

The cyber insurance industry is still developing in response to all the new threats coming from novel sources, but the basic tenet of insurance still holds: Those companies at the highest risk will pay the highest premiums – or might not qualify at all.

Asking the right questions

What can you do as your "homework" before you approach cyber insurance providers? How do you put yourself in the best position to negotiate reasonable premiums on a policy that will pay out if the worst happens? Try running down this question checklist first:

1. Will we pass the minimum security requirements of the insurer?

Most quotes for cyber insurance will come with a cyber risk vulnerability report. It will be billed as a report beneficial to assessing your own risk, but of course it's in the insurer's interest to find any glaring weak links in your armor. While minimum requirements will vary, they will likely closely mirror the Biden executive order mandates. Those requirements, which call for implementation of phishing-resistant MFA authentication, will become the de facto standard because any company doing business with the government will need to comply as soon as possible.

You can be sure that simple password authentication isn't going to be enough to meet cyber insurers' minimum requirements, because the risk is too high for them. So before asking for a cyber insurance quote, it makes sense to grade yourself against the Biden standards first.

In the past, a simple signed attestation from the CISO that minimum standards were in place was sufficient – but now for high-liability or high-risk policies some firms may need proper due diligence to go any further.

2. How fast can you roll out more robust authentication?

If cyber insurance is something you need now you may not have the time to wait for a full cycle of security upgrades. It's worth asking what security practices, hardware-based authentication or increased employee training can you do today to make your profile more attractive to cyber insurers.

3. Has the pandemic weakened your overall security profile because more people are logging in from home?

Many companies pre-pandemic focused security efforts with the office sites as boundaries. But so many remote workers now either permanently remote or hybrid means that tightening the ship's cracks has gotten a lot more complicated. There is more risk because there are a larger number of attack vectors, and cyber insurers are acutely aware of this. It is not enough to just focus on firewalls, web proxies and data protection – today robust MFA for those who are logging in remotely has to be part of the picture.

As we like to say at Yubico, "Hackers aren't breaking in, they're logging on." Stolen credentials are at the root of 80% of security breaches. Raising the security bar for user authentication beyond passwords is an imperative.

4. Will a policy actually pay out when something bad happens?

This is a legal question, and still developing, but keeping up with court cases that lay down precedent on these issues is key. It's no secret that insurance companies stay in business by NOT paying out when they don't have to or keeping their payouts low. Therefore document all downtime and losses carefully from Day 1 of a breach or other incident. Some good news is a recent ruling on a $1.4 billion attack on Merck that came from Russia. Even though the attack was pointed at Ukraine in 2017 (a grim reminder of the physical invasion to come), the court ruled that it was not an "act of war or terrorism," and therefore a payout could not be excluded.

Insurance companies will try to limit their losses by breaking up covered items into categories. For example, losses due to downtime, hardware and systems replacement, ransomware payout, and identity protection for affected customers may have been covered in a single bundle before, but today they are likely to be itemized. That makes policies more complex, requiring brokers to shop around for reinsurers to spread the risk.

5. Have we done a full cybersecurity review recently? If not, how do we do it?

Risk assessment should be on a standard schedule, and it should include both internal and external threats. It can start with a comprehensive review of user access, IAMs you are currently using and what kind of anti-phishing user education you have employed or plan to employ. A review should look closely at privileged users – critical staff and admins – but it should not exclude any users. The safest end goal will be to at least start on a path toward strong MFA authentication for all users.

NIST's Risk Management Framework is a good place to start a discussion about what your internal review should look like, and what kind of data you want to get out of it. If you bring solid information from the review to conversations with insurance brokers, it will put you in a stronger bargaining position when you negotiate premiums.

6. Is your policy prescriptive enough, i.e., specific about what is covered and what will be paid out?

Boilerplate policies are never good because each firm will have specific threat vectors and most likely scenarios for how an attack would happen. Make sure there are enough specific references to your organization's vulnerabilities and that you're satisfied with how third-party liability is considered. In general, the more specific you can get on what falls under covered attacks, the better. Note: This is when having a proper legal advisor preferably with cyber insurance experience would help, what we say here shouldn't be taken as legal advice to follow.

These six questions are only a starting point for cyber insurance research, but it's a good foundation as you consider how to get the best deal on premiums and the most comprehensive protection for the years ahead.

——

Learn more about cyber insurance requirements and why security keys meet the requirements for strong, phishing-resistant authentication here: www.yubico.com/solutions/cyber-insurance/