How-to

Getty Images

SECURITY > STRATEGY

How to Choose the Optimum Cyber Insurance Coverage

As costs of cyberattacks go up, organizations are more and more buying cyber insurance to cover some of those costs. But how much should you get and what should it cover – if you need any at all?

Karen D. Schwartz | May 23, 2021

When the city of Baltimore experienced a ransomware attack in 2019, it sustained some serious damage. Hackers demanded that the city pay the equivalent of about $76,000 to regain control of its systems. By the end of the ordeal, the attack cost

That high cost was in part due to the fact that the city had no cyber Because of the incident, city officials decided to buy $20 million worth of cyber insurance, with a premium of $800,000 and a $1 million deductible.

More and more organizations today are opting to get cyber insurance coverage. According to one report, the global cyber insurance market is expected to rise to $28.6 billion by 2026, up from $4.85 billion in 2018. Much of that is due to the rise in cyber incidents, which Allianz Global Corporate & Specialty finds is the top business risk globally.

Most cyber insurance policies will cover expenses related to getting the business back to the level it was before a loss. It covers ransomware attacks and other types of malware, network security and policy, business interruption and even actions by rogue employees. At the same time, it's important to note that it doesn't cover everything.

"Cyber insurance can reduce your risks, but it doesn't transfer your risk," said John Pescatore, director of emerging security trends at SANS Institute. "It can reduce your costs, but it doesn't cap your risk."

So do you need cyber insurance coverage? That's a trickier question than it might seem on the surface. There are so many variables involved. Do you need it at all? If you do get it, how much should you get? What should it cover?

You might not have a choice. If your business partners with other businesses, your partners might require you to carry cyber insurance.

If you work with third-party providers, considering cyber insurance can make sense. As digital transformation takes hold, more businesses are outsourcing critical applications and data to third parties. In most cases, these

Even if you have the latest security solutions in place, cyb can still be a viable option. "I work with some very sophisticated CISOs who spend millions on security each year, and they still recognize that it doesn't necessarily make them bulletproof," said John Loftus, co-cyber product leader at Alliant Insurance Services. "They might take a higher deductible, but they are still buying the coverage for catastrophic exposures, especially those associated with the human elements of cyber risk, including rogue behavior and human error."

Size matters. While larger businesses probably need most of the bells and whistles, the issue is more complicated for smaller organizations. It's less likely that smaller companies have enough resources or customers to experience a $300 million cyber event, for example, so these companies can probably get away with a smaller policy. And if smaller organizations do opt for cyber insurance, they are more likely to get away with standard coverages, while larger organizations with more to lose are more likely to go all in.

Do the math. Take the example of the Baltimore attack. If the city had the same incident today with the same damage, would the policy pay for itself? Pescatore estimates that it may have paid off the $8 million, but the city would still be on the hook for the $800,000 premium and $1 million deductible, bringing the payback down to $6 million. And once the city makes a claim, its premium is likely to rise. It's worth running the numbers, he said.

Evaluating policies also can help save money. For example, one policy might require a $10,000 deductible but waive that deductible if your company uses multifactor authentication or if you agree to use its people for restoration afterward. Some are beginning to limit ransomware coverage, particularly with larger risks. Some policies are even stipulating that they will only pay up to $300,000 for ransomware on a million-dollar policy, and they want to charge you more money to up that amount, noted Jeffrey Smith, founder of Cyber Risk

complicated. That's why Smith recommends that companies find an experienced broker who specializes in their vertical market. For example, if you healthcare provider, it's best to find a broker who works with cyber insurance policies for healthcare providers. Doing so will help companies identify and evaluate key operational risks and advise them on the best cyber insurance companies, coverage levels and important clauses.

Insist on strong first-party business interruption coverage. First-party cyber insurance coverage typically covers the expenses a business can incur after a cyberattack, as opposed to third-party coverage, which is designed for organizations responsible for the systems that may have allowed a cyberattack or data breach to occur. This coverage is critical for all companies.

Keep the idea of paying the ransom on the table. It's distasteful, but it can sometimes make sense. "With the way the threat landscape is trending today, it's important to have a well-negotiated coverage component for cyber extortion that would enable you to potentially pay a ransom," Loftus said. "It's not a foregone conclusion that anyone would do that, but if you are really over a barrel and people's lives are at stake, you want the ability to facilitate that transaction, and you want to be able to bring in outside security experts to negotiate with the adversary."

Don't forget about coverage for regulatory exposure. Data privacy is a bigger deal than ever, especially in light of regulations from the U.S. Securities and Exchange Commission, the Federal Trade Commission, and the Department of Health and Human Services, as well as various states (the California Consumer Protection Act) and countries (the EU's General Data Protection Regulation). Today, regulators can come after companies if they suspect they failed to protect confidential information, have wrongfully collected or retained information, or misused customer information. This is something that should be carefully negotiated into the policy, because there is going to be more activity surrounding

pace with the evolving threat landscape. Because of this, it is far from being commoditized. In other words, all cyber insurance policies today a most can be negotiated. “Because it’s a maturing market, you probably have more flexibility to negotiate today than you will in 10 years,” Loftus said.

0 COMMENTS

RECOMMENDED READING

Moving Your Organization's SecOps Beyond the Pandemic
JUL 20, 2021

What You Need to Know About Ransomware Insurance
JUL 13, 2021

Red Hat Report: IT Sensitive to Kubernetes Security Issues
JUL 07, 2021

Threat Hunting Basics: What You Need To Know
JUN 09, 2021