RISK & INSURANCE
Affiliated with THE INSTITUTES
Sponsored Content by Nationwide

Cyber Markets Might Be Stabilizing, but Pre-breach Services Are Essential in Keeping Your Firm Safe

Pre-breach services can help insurers prevent and prepare for cyberattacks.

By: Nationwide® | October 2022

It's been a rough few years for cyber insurance. COVID caused disruptions in 2020 and 2021, bringing dramatic rate increases as insurers tried to correct the market after a spike in severe ransomware attacks.

"It went from a soft market to a hard market overnight," said Todd Szalkowski, Associate Vice President, Cyber and Professional Liability, Nationwide. "Ransomware claims were going through the roof, BI claims were going up and carriers decided to make some market corrections."

These trends have made cyber risk top-of-mind for insureds and for good reason: In 2020, average ransomware remediation costs reached $1.85 million, Cyber Security Media reported. Then 2021 came, and the average ransomware demand — not including eventual remediation costs — for cases handled by the cybersecurity firm Palo Alto Networks rose by 144% to $2.2 million, an increase of 144% when compared to demand costs from the previous year. Remediation costs are higher than demand costs because they include the demand and additional things like business interruption and recovery costs.

"If companies have a ransomware event or a business interruption event and they can't produce the goods or services that they need, that'll have a significant impact on their revenues," Szalkowski said.

Even if rate increases aren't as severe this year, insureds will need to continue prioritizing cybersecurity efforts if they want to remain an attractive risk for carriers. Partnering with an insurer that offers pre-breach services can help companies keep their cybersecurity systems up-to-date and ready for an attack.

"2020 and 2021 was a time where there was significant change in the market," Szalkowski said. "Pre-breach services definitely help change the risk profile of an insured, because if you know that they've gone through

these steps, you know that they are taking the right steps to make things stronger and making them more capable in the event of an incident."

Why Current Market Trends Demand Pre-Breach Services

Todd Szalkowski, Associate Vice President, Cyber and Professional Liability, Nationwide

Thankfully, the cyber market seems to be stabilizing this year. Szalkowski believes rate increases may not be as dramatic and restrictions may not be as severe as companies improve their risk profiles and new entrants offer up additional capacity in the market.

"The market right now is kind of in flux," Szalkowski said. "There's new capacity. There is the softening of some of the restrictions that were put in place to correct a lot of these books that were driven by ransomware claims."

As the market continues to ebb, insureds will want to take advantage of an opportunity to strengthen their cyber defenses. A strong insurance partner can help guide them through the process by offering a variety of pre-breach services to their clients.

"The pre-breach services offered to our insureds are a value add in the policy," Szalkowski said. "It improves their risk profile."

The Benefits of Pre-Breach Services

Pre-breach services offer insureds a wide range of benefits. Encompassing everything from network vulnerability scans and employee cybersecurity training to disaster recovery plan prep, these services help companies ensure they have the strongest cyber defenses and are prepared if a breach occurs.

"They're services that we offer that shore up any gaps in an insured's network or their operations," Szalkowski said.

These services target key vulnerabilities companies may face. Employee trainings, for instance, reduce risk by producing cybersecurity-savvy workforces that know how to work safely using VPNs, multifactor authentication, secure password protocols and other key defenses. They can also help workers spot phishing attacks, which hackers often use to try to gain access to a network.

"Pre-breach services have the ability to help prevent an attack by making the company more proactive. These services, for example, can conduct a scan of the business' network to see if there's any areas that could use additional resources. These services can also provide sample wording on policy language," Szalkowski said.

"If a company doesn't have a disaster recovery plan, these services will help them build one up internally. It

offers employee training to help them get their employees up to date on best practices and to ensure they understand the risks associated with the information that they have access to."

Outside support from a pre-breach services partner can be key in the event of an attack. As Szalkowski explained: "If you have a ransomware event, your network goes down, you might not be able to email your boss so you have to have a secondary line of communication. Pre-breach services can help ensure that's in place."

These services can go a long way in helping companies enhance their risk profiles and appeal to underwriters. In a tough market, they aren't just an added benefit. They're a critical risk management tool.

"If your risk is subpar, then you're either going to pay higher premiums for that coverage or no one's going to want to insure you," Szalkowski said. "Pre-breach services can help shore up your defenses."

Partnering with a Trusted Cyber Insurance Carrier

Nationwide's pre-breach services can help insureds feel confident that they are prepared in the event of an attempted cyberattack.

The firm's Enterprise Cyber Insurance product goes above and beyond the benefits of a typical insurance policy. The service-based solution is designed to support internal cyber risk management efforts and provide support in the event of a breach.

"Everyone's going to have an incident. There's no avoiding it," Szalkowski said. "So making sure that insureds are prepared, that they have controls in place that actually stop the incident either before it occurs or has them ready when it does occur, and that they can handle it properly and mitigate any type of further damage is ideal."

Before an attack occurs, Nationwide's pre-breach services can help companies assess their networks and implement any needed protocols. Its experts will help your firm build up its cyber defenses.

"Our services help insureds be more well-rounded in terms of their risk profile and their network security and privacy controls," Szalkowski said.

Nationwide is a committed partner. If an attack occurs, the company is there to help insureds make things whole again and to provide support to help their cybersecurity defenses come back stronger than ever. Nationwide can also help firms find dedicated cyber attorneys to help guide them through the process of proper attack response.

"If an attack occurs, we will be working with them to make their network and their policies stronger," Szalkowski said.

To learn more, visit: https://mls.nationwideexcessandsurplus.com/fs/products/cyber-and-professional-liability/.

About Nationwide
AM Best Rated A+ XV | S&P A+ | Fortune 100 Company

&BrandStudio

This article was produced by the R&I Brand Studio, a unit of the advertising department of Risk & Insurance, in collaboration with Nationwide. The editorial staff of Risk & Insurance had no role in its preparation.