Your Cyber Risks: An Underwriter's Perspective

The last 12 to 18 months in the cyber environment have been challenging at best. As remote work grew exponentially, so did the cyber risks involved in conducting business. In March 2021, a global commercial insurance provider was hit by a ransomware attack that shut down its systems and website. The price paid to hijackers: $40 million. Just two months later, Colonial Pipeline suffered a ransomware attack. Hackers were paid $5 million.

Cyberattacks are increasing in frequency and severity. And hackers do not discriminate — cybercrime impacts all industries and all types of companies, large and small. Ransoms are becoming more expensive, as are the remedial efforts once the ransom is paid and systems are returned to their owners.

That kind of cost has a ripple effect. As the volume of claims increases, so does the volume of applications for cyber liability insurance. Since late 2020, the number of applications for cyber has skyrocketed.

With such demand, carriers are increasing rates. Depending on the provider, rates have increased up to 50% or more. Along with that, carriers are also lowering coverage limits. Underwriting is becoming tighter, and more is expected of the policyholders.

WHAT CARRIERS WANT

NFP's cyber brokers are seeing more restrictions and more selectivity coming from insurance providers. The types of risks they are willing to write in the cyber space are now being scrutinized more carefully. Carriers are looking for controls — what cybersecurity measures are in place, and how diligent is the organization in their attempts to mitigate cyber exposures?

The answer to that question could be the difference between your organization obtaining affordable coverage or paying more due to higher risks. To make your application more appealing to underwriters, make sure to have these controls in place:

Multi-factor authentication (MFA): MFA is a security measure that requires users to prove their identities via more than one method. For example, a user puts in a password, but then must type in a code that is sent via text message. Most carriers require MFA protection.

Backup processes: Back up data to offline storage, and put controls in place that limit access. Your carrier is also looking at how you handle the data you are storing. Is it encrypted? Are you segregating sensitive data so that should a breach occur, thieves cannot access everything?

Incident response plan: Your response to a cyber breach should be mapped out and practiced prior to any event occurring. If you know what to do and when, it gives your carrier more confidence in your ability to contain the damage and recovery faster.

Training: No amount of preparation is effective without your employees' cooperation. Train employees on how to spot phishing emails, what to do when they suspect fraudulent activity and how to use MFA regularly. The more your employees are aware of cyber threats, the more protected your organization will be.

GETTING HELP

To help reduce your cyber liability, utilize the services your carrier provides. Many carriers offer proactive services that may include educational pieces, training, assistance with development of processes and response plans, and documentation protocols.

Also, make sure you are doing your best to make your application stand out. Underwriters look for complete submissions. Your application should be filled out as much as possible. Give more details rather than fewer. Show evidence of your cyber controls, your employee training and education, and what your current response plan is.

CYBER READY

As cyber risks grow in scope and cost, underwriters will continue to be under even more pressure to ensure their insureds are doing what they can to manage risk effectively. The more controls and training you put in place, the lower your exposures.

That translates to a better risk portfolio, which in turn can lead to carriers wanting to take on your business. The result: double protection, both from inside your organization and from a cyber policy that fits your needs.

For more information, please contact Melvin Martinez at melvin.martinez@nfp.com.