COVERAGE INSIGHTS

6 Considerations When Buying Cyber Insurance

KRG INSURANCE BROKERS
A division of RRJ Insurance Group Limited

In today's interconnected world, it seems that no organization is immune from experiencing a cyber attack. In fact, there is a saying in the cyber security community that there are two types of businesses: those that have been breached and know it and those that have been breached and just don't know it.

As more and more companies have experienced data breaches in recent years, the market for insurance has grown exponentially. However, unlike other forms of insurance, cyber insurance is not a one-size-fits-all approach.

Most cyber policies are offered a la carte, allowing policyholders to negotiate terms and conditions and purchase the coverage that fits their needs. To ensure your business has best-in-class cyber coverage, it is critical to assess your business and consider the specific risks you wish to insure.

The level of coverage your business needs can vary depending on your range of exposure, and it's important to work with a broker who can tailor a policy to match your business's requirements. This Coverage Insights details some common elements of cyber insurance policies that you need to consider when building the ideal coverage.

Limits and Sublimits

One of the most important aspects of building the perfect cyber insurance policy relates to choosing your policy's limits and sublimits.

The cost of a cyber attack can be millions of dollars. As such, policyholders will want to first ensure that their overall limits are in line with their level of risk. To do this, compare the anticipated costs associated with a data breach to the limits of liability available. Your insurance broker should be able to assist you in determining appropriate limits by utilizing industry benchmarking data and projected breach costs.

From there, it's critical to examine your sublimits. Sublimits are extra limitations in an insurance policy's coverage of certain losses. That is, they do not provide extra coverage, but set a maximum to cover a specific loss.

Many cyber insurance policies impose sublimits on specific areas of coverages, including crisis management expenses, notification costs and regulatory investigations. So, while your policy may provide you with $5 million of coverage, specific areas could feature considerably less protection.

The sublimits found in cyber policies are often inadequate, but they are easily negotiable. Just be sure that your organization secures sublimits that make sense in relation to your specific exposures. Finally, make sure that the policy's aggregate limit applicable to all coverages is not less than the total of all sublimits.

Retroactive Coverage

A standard cyber policy will place a limit on or deny coverage for breaches that occur prior to a specified

6 Considerations When Buying Cyber Insurance

date, even if the claim is made during the policy period. This is typically the date of the policy's inception, which means that organizations will not be protected from any breaches that occur before the policy period.

In many cases, breaches can go undiscovered for months or even years. To ensure that you are protected from unidentified cyber incidents, always ask for a retroactive date that is earlier than the policy's inception date.

The specific retroactive date you choose will depend largely on your business. Retroactive coverage is commonly available for periods of one, two, five or 10 years. Some insurers offer unlimited retroactive coverage. Businesses should always work with their insurance broker to discuss all options for retroactive coverage.

Exclusions

Like other types of insurance, cyber policies often contain a variety of exclusions that can limit overall coverage. When evaluating any new insurance policy, it is a good idea for policyholders to be aware of common exclusions and how they could impact coverage.

The following are common cyber liability insurance exclusions to be aware of:

- **Outdated software**—Old and outdated software pose serious cyber risks and other vulnerabilities. Because of this, insurers will not cover claims related to tools that are neglected and not receiving regular maintenance.

- **Unencrypted mobile devices and data**—While encryption doesn't necessarily mean your data is safe, many insurers see it as a benchmark of cyber security. Insurers may not cover unencrypted data and devices, so it's important to review your policy carefully. Encryption can be a difficult undertaking for many companies, and the proper controls will be needed if organizations are to avoid this exclusion.

- **Card issuer fines and penalties**—One of the biggest concerns when dealing with a data breach relates to potential fines and penalties that could be levied against an organization from card issuers (VISA, MasterCard, etc.). These fines can be expensive, sometimes reaching six figures. Some policies exclude coverage for these types of fines, which could result in severe financial loss for an organization.

Other common exclusions are for bodily injuries and acts of foreign governments. Be sure to clarify what is and is not covered by your cyber policy with your broker. Many insurance companies are willing to modify exclusions to fit a business's needs, so it pays to be open with your broker about which exclusions concern you and your business.

Panel Provisions

In today's interconnected environment, many businesses take a proactive approach to cyber risk. In fact, many organizations have hired experts and legal professionals to assist them with their cyber security needs.

This may create an issue as many insurance companies require policyholders to use preapproved investigators, consultants and legal professionals in the event of a cyber breach. Therefore, your business may not be allowed to use its preferred expert or professional with whom it has a pre-existing relationship with, simply because that expert or firm is not on the preapproved panel.

6 Considerations When Buying Cyber Insurance

It should be noted that organizations can typically negotiate the terms of their policy upfront to include preferred third parties. In many cases, your preferred technology consultants or lawyers will have to work with your insurers to get approved during the underwriting process. The time to learn about and resolve these potential issues is before the policy is confirmed.

Consent Provisions

In addition, cyber policies often contain consent provisions that require policyholders to obtain the insurer's consent before incurring certain expenses related to cyber claims. Commonly, these expenses are related to notifying customers of a data breach, conducting forensic investigations or defending against third-party claims.

If prior consent provisions are included in the policy and cannot be removed, policyholders should at least change them to ensure that the carrier's consent cannot be unreasonably withheld.

Vendor Acts and Omissions

Most organizations utilize third-party vendors to process or store a portion of their data. While these third parties make doing business easier, they also represent a potential exposure. As such, it is critical that your business's cyber liability policy covers claims that result from breaches caused by your vendors.

While many cyber policies protect against vicarious liability, it's not guaranteed. If such coverage is not initially offered by the insurance company, work with your broker to ensure it is included in the policy.

Are You Adequately Covered?

Cyber insurance is a relatively new form of coverage—one that will continue to evolve alongside emerging cyber threats. As such, cyber insurance requires organizations to be proactive in assessing their risks and ensuring that their insurance coverages are in line with their specific business practices and exposures.

For more information, contact KRG Insurance Brokers today.