A Henderson Brothers, Inc. White Paper

Important Potential Changes Coming to your Cyber Liability Insurance Coverage Form.

Like 2020, the year 2021 was tumultuous for many reasons. Developments in cyber security and the market for cyber liability insurance were no different. In response to these conditions, significant changes to available coverage for cyber liability insurance may lie ahead. Several carriers have already submitted new forms and rates for 2022. Other carriers may follow suit, and we will likely also see newly crafted policy terms and endorsements for specific exposures. To be sure, the market for cyber liability insurance will be vastly different than what we knew in 2021 and prior policy years.

HENDERSON BROTHERS®

What are the driving forces for these changes?

Carriers and reinsurers consider exposures that are rapidly changing for cyber security risks. New types of attacks, vulnerabilities, and safeguards against the same are constantly evolving. Furthermore, the shear scale of security incidents presents more challenging issues. Entire supply chain and infrastructure disruptions are more prominent cyber risks than in the past. Software update susceptibilities create exponential risk, and, to top it all off, even the smaller scale, phishing and similar targeted attacks are becoming more sophisticated—see e.g. zero-click exploits. Carriers and reinsurers are faced with evaluating the high and low ends of these causes of loss in conjunction with fluctuating demand and risk tolerances from policyholders to obtain the coverage. This is a tension that results in coverage forms, endorsements, and exclusions being more specific, specialized, and, in certain situations, limited.

Claims costs are also contributing to changes in coverage, premium fluctuations, and retention amounts. Forensics, legal, technology/hardware replacement, and other expenses associated with responding to cyber claims are increasing. Moreover, the total size of a claim or expected costs to respond to a claim would historically be related to the number of sensitive data files and end points an organization had in its custody. The number of records the policyholders listed on their respective applications served as a way to normalize and formulate what the severity of claims would be across an entire risk pool. While an organization's number of records and end points is still important, it is less reflective of claims likelihood and claims cost in the forward-looking market. All of these factors are causing carriers and reinsurers to tighten their underwriting requirements, recede on prior coverage grants, offer less attractive pricing, and develop a new compendium of application questions and supplemental applications to drive accountability, thoughtfulness for a policyholder's cyber security hygiene, and, of course, consider for direct underwriting purposes.

What are the general trends to monitor for potential coverage changes?

While these variables abound, there are some noticeable coverage trends to monitor. Most carriers and reinsurers are pursuing various pricing strategies (with sub-limits), exclusions, or other limitations to insulate against catastrophic events. Carriers already included War, Terrorism, or other similar exclusions in most cyber liability policies. Coupled with those same concepts, a general trend now is for carriers to implement scaled-back provisions for exploits executed on a national or global front, infrastructure attacks generally, and known vulnerabilities that are left unremedied. Some carriers, in certain markets or industries, may even seek to laser-out particular exploits and/or vulnerabilities that the carrier identifies in the application and underwriting process. These definition changes for broad events like War and Terrorism along with the potential for the exclusion of specific exploits or policyholder-specific issues will likely continue to constrict how rich cyber coverage will be at both ends of the spectrum.

Related to the practice of lasering or making specific exclusions, carriers are also trending toward full bars against offering coverage in the first place when certain underwriting conditions are not met. Many carriers in the market now and moving forward are commenting that cyber coverage will not be offered if a prospective policyholder does not implement multi-factor authentication (MFA) or firewall protocols. At minimum, this practice will distort the capacity of the entire market for cyber liability and put additional pressure on pricing, coverage limitations, and application scrutiny.

The third general trend is the introduction of coinsurance, especially for coverage responding to ransomware events. Higher retentions/deductibles and lower sub-limits were already becoming more prevalent in 2020 and 2021. Beginning in 2022, there is the possibility that coinsurance for cyber losses (where the policyholder remains responsible for a percentage of the loss in excess and after paying the deductible or SIR) becomes a fixture for cyber policies.

All told, the general concepts of limiting policy terms, shrinking market- or individual-level capacity, and increased cost-sharing are developing into common and non-negotiable offerings for some carriers in the cyber market. It is possible some carriers may decline to follow these trends in an attempt to attract more policyholders. This remains to be seen. However, all policyholders will likely be exposed to these trends facing the market in 2022, and therefore, will need to be particularly mindful, and discuss with their insurance broker, when comparing various options for obtaining a cyber liability policy.

What are some specific examples of potential changes coming to your cyber liability insurance coverage form?

Coverage grants are changing generally. All carriers and reinsurers are attempting to better align their respective insuring agreements with the realities of today's technology-driven economy. There are, however, several specific examples of changes to policy forms that may be on the horizon and/or are already in motion with certain carriers. Some of those are described as follows:

1. A new/updated exclusion where the carrier will not provide coverage if the policyholder does not timely update its software, apply patches, or follow the manufacturer/developer's instructions in using the software. This type of exclusion may read similar to:

Intended Use/Neglected Software Exclusion:

A Cyber Incident may not be covered when the insured suffers a Loss from a known exploitation or vulnerability in the applicable software, and the insured did not update the software appropriately, perform the manufacturer's instructed patch, or otherwise did not comply with the manufacturer's support protocols (or did not comply with NIST standards).

The inference drawn from the presence of this type of exclusion is directly related to the Solar Winds incident from early 2021. The design here is to incentivize policyholders to run updates, apply patches, and conduct regular maintenance for their software and applications. If the policyholder does not, and this type of exclusion is present, there may not be coverage available for the policyholder in the event of a claim.

2. Classification or stratification into two different categories of losses. This policy language change is usually definitional. Every cyber liability policy identifies its coverage for a Cyber Incident, Security Incident, or Breach. One specific trend for this definition as we look to 2022 is for that applicable definition to be bifurcated. One sub-part will be divided to deal with large-scale, pervasive events. These are typically the variety of attacks we all read about in the press. The second sub-part is relegated to more specific impact or localized events—oftentimes, only affecting the policyholder itself. These separate definitions then lead to different coverage grants and applicable limits. A policyholder in 2022 may find its coverage for a pervasive or interdependent incident is less than its coverage for its own, isolated incident.

Widespread or Global Security Incident:

A Cyber Incident may not be covered or may be subject to a specific limit or sub-limit when a single act or interdependent series of acts occurs outside of the insured's organization but otherwise still causes a Loss to the insured or insured's Computer System.

This is not an uncommon practice for carriers and reinsurers. Coverage forms for other lines of business have evolved over the years to deal with widespread natural disasters. Coverage for floods, hurricanes, and other cat claims (catastrophic) usually differs greatly from other policies. It appears that the market for cyber liability in 2022 and forward may also be moving in that direction. Taken as a whole, the definitional changes for War, Terrorism, and the two potential types of security incidents will make/is making the landscape for obtaining a cyber liability policy very different. Perhaps this may signal the advent of new standalone cyber policies for certain types of risks. This remains to be scene, and thus, it is all the more important to understand the potential new definitions for what constitutes a security incident, per the terms of your proposed policy, for 2022 and beyond.

3. A recognition of the interdependent software ecosystem as well as recognition that it is sometimes difficult to determine the origin of an incident. Last, but not least, there may be specific changes in 2022 for how a Computer System, Network, or Shared Environment affects your coverage. Policies in the past would generally defined a Computer System to be the network solely within the policyholder's domain. If an incident occurred outside of your System, but ultimately impacted and disrupted your organization's operations, you may not have had a Security Incident on your Computer System for which there would be coverage. In a benefit to policyholders and an acknowledgement to the reality of how many organizations use interdependent technologies, there is the potential for a broader definition included in cyber policies moving forward. This language may appear as:

Shared Computer System:

A Shared Computer System means a Computer System for the insured, if the Shared Computer System is operated for the benefit of the insured under a written contract for [certain services] [e.g. data storage, software-as-a-service, data processing].

What the presence of this language would mean is that a policyholder would be in a better position to obtain coverage, even if the origin of the event did not happen on the policyholder's network. Most organizations do not have the leverage or control to dictate the security practices of their respective software vendors, application providers, or other technology partners. The specific trend of the broadening of the definition of a Shared Computer System or Computer System would help to grant coverage where previously there may have been none.

Conclusion

The market and coverage forms for cyber liability insurance are evolving. Some of this is predictable based on the exploits and outside forces. Some of these changes are unexpected and need to be carefully identified and vetted as a policyholder evaluates prospective coverage. 2022 is a pivotal year for how organizations will invest in their cyber security, insurance and risk management programs, and partnerships with third-parties. The potential changes identified in this article will impact all of those areas. As a result, it is a critical time to discuss with your insurance broker what your options may be to respond to these changes. If appropriate, please feel free to contact the Cyber Liability Insurance Practice Group at Henderson Brothers today.