FINE PRINT

The Implications of Silent Cyber Coverage Restrictions

by Joshua Gold and Daniel J. Healy

This summer we learned that coordinated efforts were underway in London to tackle the thorny issue of coverage for cyber claims under insurance policies that are not specialty cyber insurance products. Specifically, at least one large industry segment of the global insurance marketplace urged its constituents to address cyber coverage by either excluding it altogether or expressly addressing the scope of cyber protection that would be provided under a "non-cyber" insurance policy. The problem was presented as the scourge of "silent cyber."

For policyholders, there is nothing unduly "silent" about claims within the coverage grant that are not explicitly excluded. The problem is where to look if the insurance industry solves its "silent cyber" problem by cutting back existing coverage in traditional policies.

Policyholders have due cause for suspecting that the notion of harnessing "silent cyber" is insurance industry code for cutting back on much needed insurance protection. For the past few decades, a movement has been afoot in the insurance industry to create new insurance product lines to respond to a growing list of designated risks that insurance companies do not want to cover under existing insurance products. The result has been a proliferation of specialty insurance products, including fiduciary liability policies, environmental policies, and, most recently, cyber policies. Risk managers who need seamless coverage are forced to piece together a coherent insurance program in an ever more segmented market.

Insurance industry attempts to limit or essentially eradicate "silent cyber" coverage will only be tolerable to policyholders if coverages ultimately excluded from non-cyber insurance products are balanced with coverage enhancements to cyber policies. For example, in an environment where senior managers of public companies are increasingly targeted by shareholder litigation as a consequence of a cybersecurity incident, where will the insurance protection be placed? Presently, policyholders can almost always count on their D&O coverage to respond to cyber-related litigation targeting directors and officers. While few if any D&O policies make specific reference to cyberrisks (i.e., they are "silent" on this front), the existence of coverage for cyber-related incidents leading to allegations of a D&O "wrongful act" should be axiomatic. This is no small issue: Many cyber insurance products contain exclusions seeking to bar insurance claims for securities suits. As such, the "silent" D&O insurance coverage for cyber-related lawsuits against senior management is, and remains, essential. If that coverage were to ever disappear, then corresponding cyber policy coverage for securities suits should be provided.

The implications for policyholders do not stop with D&O insurance protection. If insurance companies begin a concerted effort to remove "silent" coverage for cyber-related claims from policies protecting against bodily injury, property damage, first-party property, business interruption, maritime and marine cargo insurance claims, then that protection will need to be found under cyber policies that provide more robust coverage than is presently the norm.

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com

October 2019

In addition to exclusions for securities claims, many cyber policies contain exclusions for claims of bodily injury or property damage. Whether "silent" or not, first-party property insurance coverage remains essential because cyberattacks can paralyze hardware and computer operating systems (and mechanical operations that are computer reliant). Indeed, the majority of reported insurance coverage decisions addressing property coverage for harm to computer systems have found insurance coverage for policyholders' losses. On the liability side, it is simply a matter of time before cyber perils absolutely necessitate coverage for third-party claims of injury, death and destruction. CGL coverage, however, has been under siege for the last few years with various iterations of ISO exclusions injected into a growing number of policies.

Thus, generally speaking, policyholders have uneven general liability coverage for an array of cyber liability exposures. Some policyholders have bodily injury coverage, some also have property damage coverage, and just a few still possess advertising injury and personal injury coverage for cyber-related claims. If cyber-related claims for such losses and liabilities are not picked up by cyber policies, this scenario of potentially limited CGL coverage will increasingly expose policyholders to risks that are gaining (terrifying) momentum—especially with the advent of inadequately protected industrial controls and the internet of things.

Given the challenging landscape, policyholders will need to be vigilant as they seek to craft the best insurance program that they can given the array of insurance product offerings and the array of exclusions. The challenges are compounded by changes in both the underlying risk of all matters cyber and within the cyber insurance marketplace, with cyber policy terms changing regularly. Until the insurance marketplace develops a reliable cyber solution, policyholders should be wary of insurance company efforts at renewal to restrict or otherwise limit "silent" cyber protection in their other lines of insurance coverage. The current environment is too dangerous to bank on one insurance policy to provide all necessary protection. ■

Joshua Gold is a shareholder in Anderson Kill's New York office and chair of Anderson Kill's Cyber Insurance Recovery Group. He regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property/casualty insurance coverage issues. **Daniel J. Healy** is a partner in Anderson Kill's Washington D.C. office. He is the deputy co-chair of Anderson Kill's cyber insurance recovery practice group and a member of the firm's blockchain and virtual currency and regulated products groups.

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com