COVINGTON

The Noise About "Silent Cyber" Insurance Coverage

January 14, 2020

Insurance Recovery

In the wake of destructive cyber incidents over the past few years, the insurance industry and its regulators have focused more attention on so-called "silent cyber" exposures in traditional property/casualty insurance policy forms and started taking steps to reduce or specifically address those exposures. We explain here what "silent cyber" means, and what the "silent cyber" initiative may mean to policyholders.

What Is "Silent Cyber?"

"Silent cyber" is the insurance industry's term for coverage for cyber-related risks that may be available in traditional property/casualty insurance policies, such as standard-form first-party property and business interruption policies or third-party general liability (GL) policies. The insurance industry often terms such cyber coverage "silent" or "non-affirmative" in cases where traditional policy forms adopt a "comprehensive" or "all risk" structure: i.e., all risks of the covered category of loss are deemed covered unless specifically excluded.

Whether or not such traditional forms specifically grant affirmative coverage for cyber perils, if they do not comprehensively exclude cyber perils or cyber risks, then they may rouse insurers' and insurance regulators' concerns about "silent cyber" coverage. For example, one insurer has cited particular concerns about "silent" cover for so-called cyber-physical risks such as "a hacker attack on a transit system," "a malware-infected, GPS-linked navigation system incorrectly guiding a ship," or "a hacker creating significant disruption by opening the floodgates at a hydroelectric dam, likely causing significant downstream flood damage." *Allianz Global Corporate & Specialty ("Allianz")*, Making Noise About "Silent" Cyber (2019).

In light of Allianz's specific examples of potential claim scenarios, as well as the "silent cyber" initiatives described below, the holders of property, general liability and marine insurance, among other traditional coverages, should carefully review their policies at renewal time, as they may reflect new terms purporting to redefine their coverage away from such risks.

"Silent Cyber" Initiatives by Insurers and Their Regulators

The heightened attention to "silent cyber" coverage came to the fore in 2015, when the UK's financial regulator, the Prudential Regulation Authority (PRA), began a review focusing on systemic implications of cyber risks, particularly "silent cyber" risks, for the insurance industry and the UK financial system. Other regulatory bodies followed suit, including the European

Insurance and Occupational Pensions Authority, which launched successive surveys of insurers' cyber exposures in 2017 and 2018. In January 2019, the PRA reiterated its concerns, telling insurers they needed to do more to quantify and manage their exposure to "silent cyber" coverage.

Meanwhile, insurers in the London market and their industry associations have started taking steps to eliminate or narrow their prospective coverage for "silent cyber" exposures, including as follows:

- In October 2018, Allianz announced that it would introduce revised forms in some markets by January 2019, with the aim of adopting them in all jurisdictions by January 1, 2020. According to Allianz's publications, the updated wordings would cover physical damage and bodily injury from cyber events in regular property or liability policies, but cyber-related "pure financial losses" without physical harm would only be covered in dedicated cyber insurance policies. Whether that insurer's new wordings can draw a workable distinction between physical and financial losses is a matter deserving serious consideration by any policyholders to which they are proposed at renewal.
- In June 2019, the International Underwriting Association of London, a body that represents major insurers in the London companies (i.e. non-Lloyd's) market released two cyber exclusion clauses that underwriters can add to shield themselves against cyber-related loss or liability. Many policyholders may regard these exclusionary clauses (IUA 09-081 and IUA 09-082) as vague and thus susceptible of overly broad interpretation by insurers: they purport to exclude any loss arising from the use or operation of or lack of access to a computer system, network or data, including any "threat," "hoax," "error," or "omission or accident" relating thereto. The two model clauses differ only in whether they exclude losses that result "indirectly or directly," or just "directly," from the cyber event. Given the common exclusions in cyber forms for risks such as physical injury or damage, policyholders should carefully review and harmonize their lines of coverage at renewal, to preclude insurers from arguing that a newly-introduced IUA exclusion is so broad as to open a new gap between traditional and cyber coverages. Policyholders will also want to ensure that they have not potentially lost a non-cyber aspect of their traditional coverage if an IUA exclusion is introduced.
- In July 2019, Lloyd's told its member-syndicate underwriters that they must be clear on whether their products cover or exclude a cyberattack. Many policyholders, however, have challenged the premise that "silent cyber" coverage is unclear, because the comprehensive, "all-risk" scope of the coverage they purchased is unambiguous. In any event, this Lloyd's statement may be read as an implicit concession that prior Lloyd's policies were at least ambiguous in the scope of their cyber coverage—an ambiguity that U.S. courts would resolve in favor of coverage under established rules of contract interpretation.

Insurers in other markets in Europe and the United States are taking similar steps. For example, in September 2019 AIG announced that it will either affirmatively cover or affirmatively exclude cyber-physical exposures in virtually all its property/casualty insurance policies by January 2020.

What the "Silent Cyber" Initiatives Mean for Policyholders

In light of the evolving landscape for cyber coverage, policyholders will need to deploy even greater vigilance and expertise than usual at policy renewal time to ensure adequate protection from cyber-related risks. Steps policyholders should consider, guided by counsel as appropriate, include the following:

- Review your traditional lines of coverage at renewal for new exclusions or restrictions relating to cyber-related risks: could they impede recovery or spawn coverage disputes for a future cyber loss?
- Examine your dedicated cyber coverage to determine how it interacts with other coverages: does it cover all the first- and third-party cyber exposures newly excluded in the other lines of coverage, or have coverage gaps potentially opened up?
- To the extent practicable, resist or limit the addition of new cyber exclusions in traditional property/casualty policies. If your current insurer will insist on affirmative cyber exclusions, consider moving your business to one that won't.
- Alternatively, consider new products designed to fill cyber-related gaps (so-called "affirmative cover"): for example, broader cyber insurance forms that expressly cover liability for physical bodily injury and property damage arising from cyber perils, a risk that standard cyber policy forms have typically excluded in the past.
- Consider other available risk management mechanisms, including protections in vendor contracts and use of captives for certain types of risk.
- In the event of a major cyber incident, look across your insurance portfolio to identify all policies that might still provide cyber coverage, whether "silently" or not—including general liability (GL), directors and officers (D&O), errors and omissions (E&O), property, crime, and kidnap and ransom (K&R) policies. Provide notice and otherwise preserve the insured's potential coverage rights under those policies, to maximize protection for the multiple types of loss that may flow from that incident.
- Finally, if an insurer is disputing coverage for a cyber-related claim under a prior policy, but has added an express cyber exclusion to its later-issued policies, consider whether that wording change is effective evidence that the prior policy at issue provided "silent cyber" cover for the loss.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Insurance Recovery practice:

John Buchanan	+1 202 662 5366	jbuchanan@cov.com
Marialuisa Gallozzi	+1 202 662 5344	mgallozzi@cov.com
Scott Levitt	+1 202 662 5661	slevitt@cov.com
Richard Mattick	+44 20 7067 2023	rmattick@cov.com
René Siemens	+1 424 332 4751	rsiemens@cov.com
Bert Wells	+1 212 841 1074	bwells@cov.com

our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.