Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Exploring The Need For Standalone Cyberinsurance Products

By **Daniel Cotter**

Law360, New York (May 30, 2017, 3:50 PM EDT) --


Daniel Cotter

At the annual RIMS Conference in Philadelphia in late April 2017, JLT Re and JLT Specialty Limited released a report, "JLT Re Viewpoint: Unlocking the potential of the cyber market,"[1] in which they advocate for the increased use of standalone products in the cyberinsurance market. This article describes what a standalone cyberinsurance product is and then addresses some of the issues insurers and the insurance market should consider when drafting standalone insurance policies.

A Standalone Product

The current market for cyberinsurance is estimated at $2.5 to $3.5 billion in annual premiums, with that number expected to triple by 2020.[2] Insureds in the United States represent the vast majority of cybercoverage purchasers in the world.[3] One challenge in determining a more precise estimate is that many insurers include some form of cybercoverage in their traditional property and casualty ("P&C") products, and thus delineating the amount of premium attributable to that cyber coverage is at best difficult.

Another reason that some industry participants are pushing for a standalone product with perhaps new terms and conditions is to stay innovative and ahead of potential competition from third parties not in traditional insurance. The industry also faces pressure to create "attractive products" or risk competition from disrupters.[4]

A standalone insurance product is one that is designed to provide insurance protection for a "specific risk or cost"[5] and afford an insured coverage for a particular concern. The concept of standalone coverage has been around for some time, but developed quickly during the late 1990s, when many in the insurance industry (including the author of this column) were addressing a way to cover risks for Y2K that were excluded under traditional P&C policies.[6]

The Legal Issues Relating To Standalone Cyberproduct

Unintended Coverage

For insurers, one risk of cyber as a peril potentially covered by traditional policies is that insurers may have exposure to what JLT calls "a silent killer" — the potential for insurers to incur liability for cyberlosses that have not been explicitly excluded by endorsement.[7] In many cases, cyber was not

contemplated to be covered by policy language drafted many years ago, but courts may now rule that cyber is in fact covered by existing policy language. Given the ever-changing nature of technology and the increased sophistication of hackers, many exposures not contemplated to be covered and not priced into the traditional policies may nonetheless be found to be covered.

The industry has responded by drafting endorsements clarifying that cyber is not covered. For example, in 2016, Insurance Services Office Inc. ("ISO") issued endorsement CG 21 06 05 14, which provides the following exclusions:

- "Access Or Disclosure Of Confidential Or Personal Information And Data-related Liability" (added to "Coverage A- Bodily Injury and Data-related Liability"), and
- "Access Or Disclosure Of Confidential Or Personal Information" (added to "Coverage B- Personal and Advertising Injury Liability").[8]

However, there is no guarantee that these exclusions, if added to a policy, will prevent insurers from being exposed to this "silent killer." In addition, in many instances insurers are using partial exclusions and different language for different policy types.[9] As a result, an insured faced with large cyberlosses will likely sue its insurers seeking coverage under those policies.

An example of a potential "silent killer" in the area of cyberrisk is the identity of the cyberevent which will trigger coverage under a traditional commercial liability policy. Two courts (one federal and one state),[10] both considering typical general liability policy language addressing "publication" in the data breach context, came to differing conclusions on the issue of whether actual access of records must occur for publication to occur. A standalone policy could potentially alleviate such issues, provided that the language is tailored to consider the context of technology and cyber.

New Policy, New Language

A related legal issue that faces the insurance industry in developing standalone cyberpolicies is new and untested wording. Language in traditional P&C policies does not often change. Insurers cite difficulty in getting new policy wording approved by insurance regulators in all 50 states, as well as the litigation risk of having untried language challenged. Insurers generally understand the exposures and interpretations of existing language, with the exception perhaps of the "silent killer." A major challenge in creating a standalone policy for cyberrisk is that the industry must develop policy language different than the traditional policy wording contained in the policy from which cyberrisk is explicitly excluded. Insureds will challenge new wordings and litigation is likely.

Multiple Coverages in a Standalone Policy

If the intent of a standalone cyber insurance policy is to aggregate all cyber exposures in one policy, then this policy will, by necessity, cover multiple perils with first party coverages such as business interruption included alongside third party coverages. Insurers have to consider how such a policy can be drafted to afford coverage while not creating unintended exposures or resulting in situations where the policyholder has multiple policies responsive to a cyberbreach.

Conclusion

The continued growth of standalone cyberinsurance products offers a number of potential benefits to

insurers and insureds alike, including better understood needs for the insurance and better certainty about what is covered. At the same time, insurers must proceed cautiously so that in attempting to eliminate "silent killers," they do not inadvertently set in motion greater exposures and clashing coverages.

Daniel A. Cotter is a partner at Butler Rubin Saltarelli & Boyd LLP, where he chairs the insurance regulatory and transactions practice and is a member of the cyber and privacy practice. Cotter obtained his CIPP/US in 2016.

[1] Available at https://www.jltre.com/~/media/files/sites/jltre/insights/viewpoint/jlt_re_viewpoint_cyber_april_2017.pdf?la=en-gb.

[2] Heller, Mark, "Cyber Insurance Market to Triple by 2020," CFO.com, http://ww2.cfo.com/risk-management/2015/09/cyber-insurance-market-triple-2020/.

[3] See Souter, Gavin, "Global ransomware attack hits cyber insurers, but losses limited," Business Insurance, available at http://www.businessinsurance.com/article/20170515/NEWS06/912313427/Global-ransomware-WannaCry-attack-hits-cyber-insurers-losses-limited ("the United States is by far the biggest market for cyber insurance").

[4] JLT report.

[5] Hartman, Dennis, "What is Standalone Insurance?," Sapling, available at https://www.sapling.com/8597896/standalone-insurance.

[6] See, e.g., "Cyber insurance continues to evolve," available at http://www.agcs.allianz.com/insights/expert-risk-articles/cyber-insurance-continues-to-evolve/ ("Standalone cyber insurance can trace its roots to 'Y2K' and the infamous 'Millennium bug'. Concerns that programming issues associated with the Year 2000 date change would cause widespread computer system failure prompted many companies to first assess the potential for cyber risk to their businesses.")

[7] Unlocking the Potential, p. 12, available at https://www.jltre.com/~/media/files/sites/jltre/insights/viewpoint/jlt_re_viewpoint_cyber_april_2017.pdf?la=en-gb

[8] Available at http://www.independentagent.com/Education/VU/SiteAssets/Insurance/Commercial-Lines/CGL/Endorsements/WilsonDataBreach/CG21060514.pdf .

[9] See, e.g., Unlocking the Potential, p. 13/20, Table 1, available at https://www.jltre.com/~/media/files/sites/jltre/insights/viewpoint/jlt_re_viewpoint_cyber_april_2017.pdf?la=en-gb

[10] See Recall Total Information Management Inc. v. Federal Insurance Co., 83 A..3d 664 (Conn. App. 2014), aff'd , 115 A.3d 458 (Conn. 2015) and Travelers Indemnity Co. of America v. Portal Healthcare Solutions LLC, 35 F.Supp.3d 76 (E.D. Va. 2014), aff'd, No. 14-1944, 2016 WL 1399517 (4th Cir. Apr.11, 2016).
