Published on *The National Law Review* https://www.natlawreview.com

Reasons for Communicating Clearly With Your Insurer Regarding the Scope of Coverage Before Purchasing Cyber Insurance

Article By:

Daniel I. Wolf

Purchasing cyber insurance is notoriously complex—standard form policies do not currently exist, many key terms setting the scope of coverage have not been analyzed by courts, and cyber risks are complicated and constantly evolving. Given these complexities, prospective policyholders should consider, before purchasing a cyber policy, communicating their expectations for coverage in clear and specific terms to their insurer. Such communications, which can be conducted through an insurance broker, can help a policyholder obtain policy terms that accurately reflect their desired coverage. Additionally, these communications create a written record of the contracting parties' understanding, which may prove useful should the insurer later contend that coverage is not available consistent with these discussions and the policyholder's expectations.

Singling out a key policy provision and examining the coverage issues that provision can present helps illustrate the potential value of such communication. Currently, the high-profile *Mondelez International, Inc. v. Zurich American Insurance Co.* litigation provides an excellent opportunity to examine the coverage issues that can arise from one such provision: the so-called "war exclusion." This exclusion, a variant of which is included in almost every insurance policy by insurers seeking to limit their exposure to potentially catastrophic losses that might result from war, may sound straightforward but can be difficult to apply, as the line between war and other conflicts is often fuzzy and fact-specific. *Compare In re Sept. 11 Litig.*, 931 F. Supp. 2d 496, 508 (S.D.N.Y. 2013), *aff'd*, 751 F.3d 86 (2d Cir. 2014) (concluding that the September 11, 2001 attack by Al Qaeda was an "act of war"), *with Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co.*, 505 F.2d 989, 1015 (2d Cir. 1974) (holding that the hijacking of an airplane by the Popular Front for the Liberation of Palestine was not the result of "war"). This is especially true in the cyber context, where understanding the precise nature and purpose of a cyber attack is often difficult. While the *Mondelez* case does not involve a dedicated cyber insurance policy—it concerns a property insurance policy that includes coverage for "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction"—it is still instructive because the insured seeks coverage for a cyber attack and the insurer disputes coverage based on the war exclusion, which almost all cyber insurance policies contain in some fashion.

The dispute in *Mondelez* arose when the policyholder suffered over one hundred million dollars in losses due to network disruptions caused by the NotPetya ransomware attack and sought coverage

under their property insurance policy for "physical loss or damage to electronic data, programs, or software . . . ." *See* Complaint, *Mondelez International, Inc. v. Zurich American Insurance Co.*, No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct., Oct. 10, 2018). In response, the insurer denied coverage based on the war exclusion that precluded coverage for "loss or damage directly or indirectly caused by or resulting from . . . hostile or warlike action in time of peace or war, including action in hindering, combatting or defending against an actual, impending or expected attack by any: (i) government or sovereign power (de jure or de facto); (ii) military, naval, or air force; or (iii) agent or authority of any party specified in i or ii above." In short, the policyholder believed it bought broad coverage for ransomware attacks, but now must litigate whether the NotPetya attack was a "warlike action" by a government "agent," under circumstances where numerous sources link the cyber attack to Russia and its armed forces (though Russia denies any involvement). While the *Mondelez* case is still in the early stages, and details of any communications among the parties regarding the wording and meaning of the war exclusion are not publicly known, the mere existence of this litigation highlights the challenges that can face a policyholder who learns only after a substantial loss that their insurer reads a key policy provision to preclude coverage that the policyholder expected to be available.

As noted above, communication prior to policy placement can be a valuable tool to secure clear wording for key policy provisions and potentially avoid this kind of situation. While this may seem obvious, such communication is often overlooked by policyholders more focused on other policy details like limits and premiums. A close review of the war exclusion helps illustrate the potential benefits of these communications. While the precise phrasing of the war exclusion at issue in *Mondelez* is more typical of property policies than cyber policies, war exclusions in many cyber policies arguably apply to conduct not only by state actors but also by quasi-state actors or groups with political motives. For this reason, policyholders may want to seek language specifying that the exclusion only applies to acts by a military force or a sovereign nation, as many cyber attacks are attributed to quasi-state actors or non-state groups with political ends, or are the subject of debated attribution. Similarly, some war exclusions apply not only to specified conflicts such as war, invasion, and mutiny, but also to more amorphous conduct like "warlike actions"—policyholders seeking greater certainty may wish to avoid such language. Further, as with any exclusion, avoiding overbroad introductory language (like that excluding any loss "in any way related to or arising out of" war) is generally in a policyholder's interest. And even if a war exclusion is broadly worded, some insurers will include a carve-back creating an exception for losses due to attacks on computer systems or breaches of network security, thus preserving cyber coverage even when the war exclusion might otherwise apply. Given the impact that small changes in wording can have on the scope of coverage, communicating clearly—with respect to the war exclusion or any other key policy provision—can play a crucial role in assuring that a policyholder secures wording that provides the coverage they desire. Of course, an insurer may respond to a policyholder by refusing to revise a policy term or insisting that a desired coverage is unavailable, in which case the policyholder has the benefit of understanding a policy's purported scope prior to purchase and the opportunity to investigate coverage from other insurers.

In addition, communication allows a policyholder to make a record of their expectations as to the scope of coverage, which may prove useful if an insurer later refuses to provide coverage consistent with the expectations that the policyholder conveyed. Many courts interpreting disputed policy language put substantial weight on an insured's reasonable expectations and often rely on communications between policyholders and insurers to support a policyholder's reading. *See, e.g.*, *Monsanto Co. v. Int'l Ins. Co. (EIL)*, 652 A.2d 36, 39 (Del. 1994); *Celley v. Mut. Benefit Health & Acc. Ass'n*, 324 A.2d 430, 435 (Pa. Super. 1974); *Ponder v. State Farm Mut. Auto. Ins. Co.*, 12 P.3d 960, 962 (N.M. 2000); *Michigan Mutual Liability Co. v. Hoover Bros., Inc.*, 237 N.E.2d 754, 756 (Ill.

App. 1968). As the recently-issued Restatement of The Law of Liability Insurance observes, where "extrinsic evidence shows that a reasonable person in the policyholder's position would give the term a different meaning" than the one advanced by the insurer, the policyholder's proposed meaning will often control. Another recent case addressing a war exclusion (completely outside the cyber context) demonstrates the role such communications may play in interpreting disputed policy provisions, as the court's analysis of the exclusion included a review of the communications during the underwriting process between the insured, the broker, and the insurer and an examination of what those communications indicated about the parties' intent for the exclusion's application. *Universal Cable Prods., LLC v. Atl. Specialty Ins. Co.*, 929 F.3d 1143 (9th Cir. 2019). While contested coverage provisions should generally be read in an insured's favor so long as that reading is reasonable—even in the absence of favorable underwriting communications—the cases above underscore the potential value in establishing during the underwriting process a record of the insured's expectations as to the scope of coverage (especially in an area such as cyber insurance, where guidance like prior court decisions is limited).

For these reasons, policyholders should consider clearly communicating their intentions to their insurer when purchasing cyber insurance—this may include communicating not just questions about the scope of coverage and requests for modifications to the policy, but also the concerns animating those questions and the goals behind those requested modifications. When having such communications with cyber insurers, policyholders will generally want to work closely with an insurance broker knowledgeable about cyber insurance, and may also want to consult experienced coverage counsel. Clear communication during the underwriting process can play an important role in helping policyholders obtain cyber coverage that will meet their expectations should they one day confront a cyber event.

National Law Review, Volumess X, Number 155