KAUFMAN | DOLOWICH

Examining Silent Cyber Coverage in the Wake of Russia's Ukrainian Invasion, New York Law Journal, by Eric Stern, Esq.

As the risk of cyber-attacks grow, and procuring cyber-insurance has become more difficult, policyholders have tried to rely on non-cyber policies to cover their cyber-related losses. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) recently issued a warning of the risk of Russian cyber-attacks spilling over onto United States networks as part of the Russian invasion of Ukraine. This follows previous CISA warnings on the risks posed by Russian cyber-attacks for critical infrastructure. The European Central Bank (ECB) has similarly warned European financial institutions of the risk of Russian cyber-attacks and related market disruptions.

The risk of cyber-attacks forces businesses and insurers to examine their policies to determine the coverages that may apply to losses caused by a cyber-attack. The current elevated risk draws into focus the recent decision in Merck and International Indemnity v. ACE (et al.), in which the Superior Court of New Jersey examined coverage under an All-Risk for loss arising from the NotPetya malware, which was allegedly used by Russia in a cyber-attack on Ukraine and spilled over into the rest of the world. The Merck court found that the "Hostile/Warlike action" exclusion contained in the subject policy was inapplicable and could not be used to exclude coverage for the loss.

As will be discussed in greater detail here, although the Merck court found coverage for the policyholder for a cyber-attack under a non-cyber policy, the Merck decision should not be read to support reliance on "Silent Cyber" coverage to protect companies from elevated risk losses due to cyber-attacks.

A cyber-attack or data breach event typically involves a third-party attacking the computer systems of an individual or company for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing infrastructure, destroying the integrity of the data, and/or stealing controlled information. The productive time lost, and/or the theft or disruption of a company's controlled information, can cause a direct loss—through business interruption, lost records, reputational damage, and costs to correct and repair the damage done by intruders.

A cyber-attack may also subject victim companies to lawsuits from their customers as well as fines and investigations from state and federal regulatory agencies. Unfortunately, such attacks have become more widespread with each passing year. On June 27, 2017, a major global cyber-attack utilizing malware called NotPetya spread through France, Germany, Italy, Poland, the United Kingdom and the United States. The majority of infections targeted Ukraine, where more than 80 companies were initially attacked, including the National Bank of Ukraine. The U.S. government said the cyber-attacks were the work of the Russian military and were part of the "Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict." Multiple nations were critical of Russia for the NotPetya spread. Notwithstanding the foregoing, the Russian Federation denied involvement in the spread of the NotPetya malware.

One of the companies impacted by NotPetya was the pharmaceutical company, Merck. In response to loss suffered, Merck sought coverage under its All-Risk insurance policies. The issuing insurers denied coverage relying on the "Hostile/Warlike Action" exclusion contained in the All-Risk policies, arguing that NotPetya was an instrument of the Russian Federation and was deployed as part of a broader offensive campaign against Ukraine. It is important to note that, although the specific language is not quoted in the decision, according to the Merck court, the policies at issue contained "coverage for damage or loss resulting from destruction or corruption of data and software." The Merck court also noted that the "nature of the coverage" was not in dispute. The parties did not focus on whether there was coverage for loss from a cyber-attack under the subject policies. Rather, the Merck decision rested squarely on the applicability of the "Hostile/Warlike Action" exclusion.

The Merck court decided that the "reasonable expectations of the insured" prevented the use of the "Hostile/Warlike Action" exclusion. The court specifically reasoned that "no court has applied a war (or hostile acts) exclusion to anything remotely close to the facts" at issue and that the "Insurers did nothing to change the language of the exemption to reasonably put this insured on notice that it intended to exclude cyber-attacks." Accordingly, the court concluded that the policyholder could anticipate that the exclusion applied only to "traditional forms of warfare" and not to cyber-attacks.

Because the court found that the "Hostile/Warlike Action" exclusion did not apply, it did not broach the issue of whether NotPetya was, in fact, a hostile or warlike action from Russia or a proxy on its behalf. The court, in its decision, did not find whether NotPetya was attributable to the Russian Federation or whether it was implemented as part of ongoing hostilities with Ukraine.

Policyholders should not seek to rely on the Merck decision to avoid procurement of a cyber-specific policy in the hopes that they will be protected from loss from an attack by potential "Silent Cyber" coverage in their existing All-Risk policies. Silent Cyber is coverage for cyber-risks that is neither expressly covered nor excluded in a non-cyber policy. As the risk of cyber-attacks grow, and procuring cyber-insurance has become more difficult, policyholders have tried to rely on non-cyber policies to cover their cyber-related losses. Such reliance on a policy to provide coverage for a risk it did not anticipate can lead to disputes between the policyholder and its insurer when a cyber-attack ultimately occurs. These Silent Cyber coverage disputes have been before the courts for years leading to disparate outcomes based on, among other things, applicable state law, subject policy language, and the underlying facts of a claim.

As discussed in greater detail below, the Merck decision will not be broadly supportive for policyholders seeking to trigger coverage for cyber-losses on non-cyber policies. Initially, parties seeking coverage for cyber-related losses from non-cyber policies will typically need to overcome the insurer argument that cyber-coverage was not an intended part of the policy's coverage. For example, courts have precluded coverage for cyber-losses on property policies absent resultant physical loss. In Ward v. Employers, 7 Cal. Rptr. 3d 844 (Cal. Ct. App. 2003)., the court reasoned that the policy only covered physical damage to property, and that the loss was not physical because the lost information was not tangible. And again in Am. Online v. St. Paul Mercury Ins., 207 F. Supp. 2d 459 (E.D. Va. 2002), it was determined the policy did not cover loss because such lawsuits did not involve "physical damage" to "tangible property."

In the Merck decision, as noted above, the nature of the policy's coverage at issue was not in dispute. The court in Merck addressed a dispute about the applicability of an exclusion, not whether cyber-related loss was covered by the subject policy in the first instance. Accordingly, the initial hurdle in a Silent Cyber dispute was not before the Merck court in the recent decision. Furthermore, New York is striving to move insurers and policyholders away from reliance on Silent Cyber coverage. Last year, the New York Department of Financial Services (NYDFS) released Cyber Insurance Risk Framework (the "Framework"), which provides "best practices for managing cyber-insurance risk." Among other things, the Framework provides six categories of focus for cyber-risk, including a directive to "manage and eliminate exposure to 'silent' cyber insurance risk, which results from an insurer's obligation to cover loss from a cyber incident under a policy that does not explicitly mention cyber incidents."

Finally, the current combat involving Russia and Ukraine is substantially different than the hostility which existed in 2017, at the time of NotPetya. In 2017, unlike today, there was no traditional forms of physical warfare upon Ukraine by Russia. The Merck court specifically ruled that the policyholder could not reasonably expect the application of the "Hostile/Warlike Actions" exclusion absent "traditional forms of warfare."

In 2022, a cyber-attack executed along with ongoing traditional forms of warfare, may force a court to interpret such an exclusion and the policyholder's expectations regarding the exclusion, differently. Insureds who are concerned about coverage for data breaches and cyber-attacks would be well-advised to purchase cyber-specific policies, especially in light of the increased risk of cyber-attacks as predicted by CISA and the ECB. Despite the holding in Merck, an effort to seek coverage for a cyber-incident under a non-cyber policy, counting on Silent Cyber coverage for protection, puts too heavy a reliance on courts to find coverage where none exists through a disfavored method of interpretation.

Eric B. Stern is a partner at Kaufman Dolowich & Voluck and co-deputy chair of the firm's data privacy & cybersecurity practice group.