



# War Risk Exclusions Threaten Cyber Coverage

by Joshua Gold

It has become common knowledge that some cybercriminals are affiliated with nation states, and may have state backing for the mayhem they have wrought—money stolen from international banking funds transfer systems, email caches hacked and exposed, reams of personal data published.

The suspected role of nation-state actors has raised the possibility that insurance companies may attempt to invoke war risk exclusions to escape paying cyber-related insurance claims. But even if a given war risk exclusion does have some technical applicability to a cyber claim where state involvement is suspected, would an insurance company actually attempt to invoke it to deny coverage?

Until recently, disputes over the application of a war exclusion have generally remained private and been resolved through negotiation. Last fall, however, a property insurance company invoked the war risk exclusion over a cyber loss claim, compelling the policyholder to sue for coverage.

In October 2018, snack company Mondelez International, owner of Nabisco and Cadbury, filed suit in Cook County, Illinois, against its insurer, Zurich American Insurance Company, challenging a cyber coverage claim denial. According to the Mondelez complaint, the 2017 NotPetya attack, which has been attributed to state-sponsored Russian hackers, rendered 1,700 company computer servers and approximately 24,000 laptops “permanently dysfunctional.” Mondelez sought coverage under an all-risk property policy that protected against property damage and business interruption losses and promised protection for computer-related harm. The policy also provided express coverage for cyber perils, including “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.”

Zurich denied the \$100 million claim, however, and invoked the property policy’s war exclusion, which barred coverage for “hostile or warlike action...by any...government or sovereign power...military, naval or air force,” or an agent or authority of the aforementioned entities. The suit has not yet been adjudicated.

Mondelez should have the stronger legal position in this dispute. Under an all-risk insurance policy, a policyholder has a very limited set of items upon which it carries the burden of proof. As a corollary, courts often reject an insurance company’s attempt to narrow the scope of the insuring agreements and broaden the scope of the insurance policy’s exclusions.

When war exclusions have been invoked in response to claims for losses caused by terrorism, courts have typically narrowed the application of those exclusions. Under both aviation and property insurance policies, courts have mainly deemed that the war risk exclusion applies more narrowly to fairly conventional notions of military force and armed conflict. As such, the law should favor Mondelez and other similarly situated policyholders in this area.

Nonetheless, the Mondelez case demonstrates the need to assess the potential scope of war exclusions in cyber policies and other lines of property and casualty insurance coverage.



Mondelez also serves as a reminder that property policies can cover cyber losses. Case law indicates that damage to computer networks, hardware and peripheral equipment can be covered “physical loss or damage.” For example, in *NMS Services Inc. v. The Hartford* in 2003, the court found that the deliberate erasure of computer files and databases by a former employee was “damage to its property, specifically, damage to the computers it owned.” Similarly, in the 2000 case *American Guarantee & Liability Insurance Company v. Ingram Micro Inc.*, it was determined that property insurance coverage was available for the loss of custom programming information stored in computers’ random access memory that was lost when the data center experienced a power outage. The 2006 decision in *Southeast Mental Health Center Inc. v. Pacific Insurance Co. Ltd.* held that the policyholder proved necessary direct physical loss where its pharmacy computer data was corrupted due to a power outage. In 2012’s *Landmark American Insurance Co. v. Gulf Coast Analytical Laboratories, Inc.*, the court found that electronic data is also susceptible to direct, physical loss or damage.

While the Mondelez case is being fought in the context of a property insurance policy, many cyber policies do contain war exclusions. Risk managers and brokers must consider what clarity and assurances can be obtained in the marketplace to minimize the risk that insurance companies will attempt to deny coverage for cyber claims where a state actor is allegedly involved in a hack, virus or other form of cyberattack.

Additionally, the Mondelez case illustrates that, when a serious cyber loss occurs, policyholders may have coverage under business insurance policies like their property and crime insurance policies. Policyholders should not solely focus on stand-alone cyber insurance products when they face losses or claims to the exclusion of other lines of potentially applicable coverage. ■

**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.