NotPetya Was Not Cyber “War”

This summer marked the anniversary of the most costly cyber-attack in history. NotPetya wreaked havoc for some large companies, costing them billions of dollars in lost revenue, damaging computer systems, and requiring significant expense to restore global operations. In its wake, entire industries reassessed their practices for patching, business continuity, supply chain interruption, and more.

In the year since NotPetya, we have learned much about the attack, but many details remain elusive. One continuing discussion for the insurance industry, however, is whether NotPetya was “warlike” — and more specifically, whether the ubiquitous war exclusion found in cyber insurance policies could have prevented coverage. A recent Wall Street Journal article described this as “a multimillion-dollar question for companies that purchase cyber insurance.”

Conflating the war exclusion with a non-physical cyber event like NotPetya grows out of two factors: (1) NotPetya inflicted substantial economic damage on several companies, and (2) the US and UK governments attributed the NotPetya attack to the Russian military. These two factors alone, however, are not enough to escalate this non-physical cyber-attack to the category of war or “hostile and warlike” activity. These terms of art that have been considered by courts, and the resulting decisions, which are now part of the Law of Armed Conflict, make it clear that much more is required to reach the conclusion of “warlike” action.

First: What were the effects of the attack? For a cyber-attack to reach the level of warlike activity, its consequences must go beyond economic losses, even large ones. Years before NotPetya, when President Obama was asked to characterize a similar nation-state cyber-attack that inflicted no physical
damage but still proved “very costly” for a US company, the president aptly described the incident as “an act of cyber vandalism.” His comments were supported by a legal history of armed conflict in which warlike activity always entailed casualties or wreckage. For a cyber-attack to fall within the scope of the war exclusion, there should be a comparable outcome, tantamount to a military use of force.

Second: Who were the victims and where were they located? Did the victims serve a military purpose and did they reside near the actual conflict or “at places far removed from the locale or the subject of any warfare.” The most prominent victims of NotPetya operated far from any field of conflict and worked at purely civilian tasks like delivering packages, producing pharmaceuticals, and making disinfectants and cookies.

Third: What was the purpose of the attack? NotPetya was not a weapon that supported a military use of force. The attack struck just before Constitution Day, when Ukraine celebrates its independence. The resulting chaos caused by NotPetya bore greater resemblance to a propaganda effort rather than a military action intended for “coercion or conquest,” which the war exclusion was intended to address.

As cyber-attacks continue to grow in severity, insurers and insurance buyers will revisit the issue of whether the war exclusion should apply to a cyber incident. For those instances, reaching the threshold of “warlike” activity will require more than a nation-state acting with malicious intent. As shown by the recent indictments of foreign military intelligence officers for interfering with US elections, most nation-state hacking still falls into the category of criminal activity.

The debate over whether the war exclusion could have applied to NotPetya demonstrates that if insurers are going to continue including the war exclusion on cyber insurance policies, the wording should be reformed to make clear the circumstances required to trigger it. Absent that clarification, insurers and insurance buyers must default to the Law of Armed Conflict, including rulings that might be more than a century old, to discern between the categories of criminal activity and warlike actions. As for the latter, all precedent indicates that NotPetya simply didn’t reach that level.

For more information on this matter, contact your Marsh representative or:

THOMAS REAGAN
US Cyber Practice Leader
+1 212 345 9452
thomas.reagan@marsh.com

MATTHEW MCCABE
Assistant General Counsel for Cyber Policy
+1 212 345 9642
matthew.p.mccabe@marsh.com