February 2014

Broad Interpretations of Terrorism Exclusions Are Incompatible with Cyber Insurance

The scale of some recent cyber events has been extraordinary. Target reports that 70 million people (almost 25 percent of the US population) were affected by the recent breach. *CNN* recently reported that in South Korea, there was a breach reportedly affecting 40 percent of its citizens. The staggering size of these events is leading companies to seek protection through both technology and financial products, such as insurance. Insurers typically attempt to avoid this sort of staggering exposure with terrorism exclusions, and one should therefore expect aggressive insurers to rely upon such exclusions to avoid their coverage obligations.

After 9/11, insurers added terrorism exclusions to their policies, providing coverage for losses arising out of terrorism only if special coverage was acquired. When a business is informed of a terrorism exclusion, it often reasonably understands the exclusion to bar coverage for violent events such as was witnessed in 2001. And indeed terrorism is defined to include acts that "involve violent acts or acts dangerous to human life," *see,* e.g.*,* 18 U.S. Code § 2331. With some notable exceptions, such as interference with computerized safety devices, cybersecurity events should not fall within this definition. Stolen information, for example, is not generally "violent … or … dangerous to human life."

Unfortunately, although labelled terrorism exclusions, some insurers use language that might be interpreted to exclude a broader range of activity. For instance, a common London policy defines terrorism to include:

> Acts, including but not limited to the use of force or violence and/or the threat thereof, of any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organization(s) committed for political, religious, ideological or similar purposes including the intention to influence any government and/or put the public, or any section of the public, in fear.

An insurer seeking to limit its obligation could argue that the definition does not include a requirement that the loss be caused by the use of force or violence, but only that it be performed on behalf of a group committed to some ideological purpose, and that any act, including the theft of personally identifiable information ("PII"), committed by the members of such a group would be barred by the exclusion. Thus, an insurer might contend that acts committed by loosely-affiliated activists or government-sponsored cyber terrorists would not be covered. Given that the definition is supposed to be one of "terrorism," the argument should be rejected by courts. But how this issue is resolved could have a serious impact on the sort of coverage acquired. For instance, in 2011 hacktivists stole 100 million records, as reported by *ZDNet*. If the activities of ideological groups are not covered, there would be a serious gap in the protection of cyber insurance.

Such language is not limited to European insurers. One US insurer's policy, for example, excludes coverage for losses:

> Arising out of war, invasion, acts of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power, confiscation, nationalization, requisition, or destruction of, or damage to, property by or under the order of any government, public or local authority; provided that this exclusion will not apply to any "act of terrorism" as defined in the Terrorism Risk Insurance Act as amended.

An insurer advocate, seeking to restrict coverage, might contend that the exclusion should be parsed to exclude any loss arising out of "damage to, property by or under the order of any government," and contend that cyber risks relating to the activities of government agencies are excluded, whether or not there is a risk of or an act of violence.

If a court were to accept that interpretation, coverage would be severely limited given the staggering rate and size of cyber events attributable to governments. For instance, the Verizon 2013 report on cybersecurity events claimed that cyber attacks by "[s]tate affiliated groups r[o]se to the number two spot…"

In sum, insurers are marketing cyber insurance as a mechanism for transferring cyber risk. With reports of cybersecurity events growing each day, there is an ever-increasing desire for such protection. Companies need, however, to scrutinize the particulars of the policies sold, lest they find themselves in a legal battle with their insurers over the nature of the covered risk, rather than receiving the coverage they sought to acquire.

Contact

Lon A. Berk
lberk@hunton.com