Decode terrorism risk.

Careful how you code: Cyberterrorism coverage under TRIA and stand-alone cyber policies

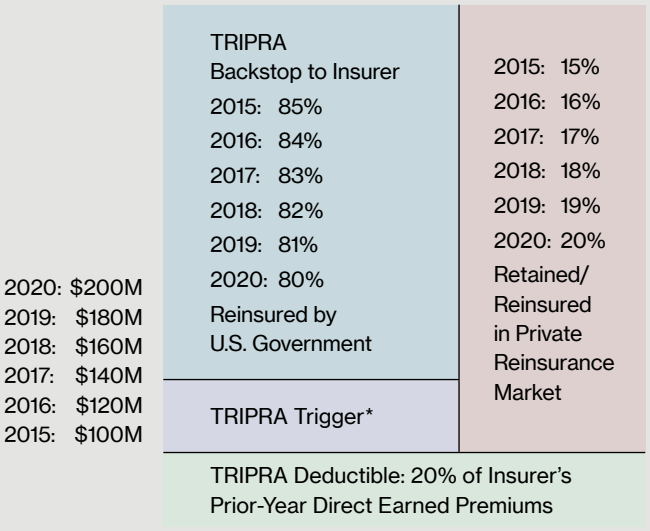
by Jason Krauss

On December 27, 2016, the U.S. Department of the Treasury issued a "Notice of Guidance" confirming that stand-alone cyber policies reported under the Cyber Liability NAIC code (17.0028) are included within the definition of "property and casualty insurance" and fall under the purview of the Terrorism Risk Insurance Act of 2002 (TRIA).

As background, TRIA is a federal law created after the 9/11 attacks to provide a federal "backstop" for insurance claims related to certified acts of terrorism. The goal was threefold: to ensure the affordability of commercial property and casualty insurance for terrorism risk, build insurance capacity to absorb future terrorism losses, and have the insurance industry and federal government share in losses according to a specific formula. President Obama signed the Terrorism Risk Insurance Program Reauthorization Act of 2015 on January 12, 2015 and the program was extended through December 31, 2020. The structure of the program is shown in *Figure 1.*

It was only in January of 2016 that state regulators first introduced "Cyber Liability" as a new subline of insurance under "Other Liability" for reporting purposes and defined it as *"stand-alone comprehensive coverage for ability arising out of claims related to unauthorized access to or use of personally identifiable or sensitive information due to events including but not limited to viruses, malicious attacks or system errors or omissions. This coverage could also include expense coverage for business interruption, breach management and/or mitigation services."**

Figure 1. **Terrorism Risk Insurance Program Reauthorization Act of 2015**



*Once TRIPRA Trigger is breached, TRIPRA coverage is provided from 1st dollar

Note: TRIPRA Trigger and Coinsurance levels increase annually at January 1st

*NAIC 2016 P/C Product Coding Matrix, p. 10. "Sub-TOI" refers to Sub-Type of Insurance.

Willis Towers Watson

Insurance reported as "Other Liability" is subject to TRIA with the exception of Professional Errors and Omissions Liability Insurance, as doctors, accountants and other professional firms successfully argued that TRIA's protections were not necessary for professional liability policies given the nature of the losses covered under these policies. But this exception led to an unintended consequence: namely, that coding stand-alone cyber policies as professional liability policies resulted in their exemption from the TRIA safety net.

During a meeting this past March, Treasury senior insurance regulatory policy analysts confirmed that TRIA would indeed be applicable to all coverages provided under a stand-alone cyber form or any other coverage form providing some type of cyber coverage, as long as the carrier utilizes Cyber Liability NAIC code 17.0028.

However, even with the recent guidance, there remained some uncertainty as to whether *all* losses covered under a traditional stand-alone cyber policy would be entitled to the government's TRIA backstop. A traditional stand-alone cyber policy has numerous insuring agreements and provides coverage for both first party losses, such as those stemming from a network interruption, as well as for losses resulting from third party security or privacy claims. During a meeting this past March, Treasury senior insurance regulatory policy analysts confirmed that TRIA would indeed be applicable to all coverages provided under a stand-alone cyber form or any other coverage form providing some type of cyber coverage, as long as the carrier utilizes Cyber Liability NAIC code 17.0028. This clarification from the Treasury is important, as it brings cyber coverage back under the veil of protection provided by TRIA, as long as that coverage is properly coded. It may also benefit the cyberinsurance market as a whole by making more capacity available, by providing carriers and captive insurers a level of comfort knowing that 83% of losses (reduced to 80% by 2020) stemming from certified acts of terrorism will be absorbed by TRIA once those losses exceed $140 million (increased to $200 million by 2020).

Certifying an event

It is important to understand that TRIA only provides coverage for a *certified* act of terrorism; a high bar that has not been met to date despite several events. In fact, for an event to be certified:

- The event must be certified by the Secretary of the Treasury, Attorney General, and the Secretary of Homeland Security;
- The event must be determined to be an actual act of terrorism;
- The event must be violent or dangerous to human life, property or infrastructure; and
- The event must:
  - result in damage within the United States; and
  - be committed by an individual or individuals as part of an effort to coerce the U.S. civilian population, or to influence the policy or affect the conduct of the U.S. government by coercion.

Further, an event cannot be certified if it does not cause property and casualty losses exceeding $5 million in the aggregate or if the act is committed as an act of war declared by Congress. As an example, the Boston Marathon bombing was not certified, in part because insured losses fell short of the $5 million certification threshold.

Covering non-certified acts of terrorism

This leads us to the very important question of what non-certified acts of terrorism would be covered under most traditional stand-alone cyber policies. Broad war exclusions are very common, but courts have traditionally interpreted such "war" and "warlike actions" as events involving two sovereigns or quasi-sovereign governmental entities. This interpretation would mean that a terrorist attack against civilians by an operative of a political organization or guerilla group would not be characterized as war or warlike operations, and a traditional war-risk exclusion would not generally bar coverage.* Policyholders should ensure that the war exclusion contains a cyberterrorism "carveback," or more preferably, an explicit *grant* of coverage for cyberterrorism. Recently, a state terrorist group hacked into a U.S. company's networks and released names, addresses and financial information of government employees and military personal.

*Pan American World Airways, Inc. v. Aetna Casualty & Surety Co.

Additionally, a security researcher recently took control of and manipulated traffic systems by exploiting vulnerabilities in traffic control devices. As such, special attention should be given to the policy's definition of cyberterrorism so that it is broad enough to include coverage for these scenarios that, while unlikely to be certified, still have the potential to present significant exposure.

An example of a broad cyberterrorism definition follows:

"Cyberterrorism" means the premeditated use of disruptive activities against any computer system or network by an individual or group of individuals, or the explicit threat by an individual or group of individuals to use such activities, with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives. "Cyberterrorism" does not include any such activities that are part of or in support of any military action or war.

"Cyberterrorism" also includes any such activity or threat by (or supported by) a sovereign nation unless such activity or threat is part of or in support of a war or other non-cyber military action.

Ensuring proper coding and broad coverage

In sum, it is imperative that clients are afforded the broad backstop protections provided by TRIA for cyber losses arising out of certified acts of terrorism. Recent Treasury clarifications seem to indicate that this can simply be accomplished by ensuring that any type of policy providing cyber coverage is coded properly. Because it is far more likely for an act of terrorism to be *non*-certified, it is equally important to ensure that the "front-stop" cyberterrorism coverage afforded via cyber-insurance policies is broad enough to provide coverage for losses arising out of both certified and non-certified acts of terrorism.

Contact

Jason Krauss
212.915.8374
Jason.Krauss@willistowerswatson.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

WTW-GL-17-PUB-8053a1b

willistowerswatson.com

Willis Towers Watson