US TREASURY MAKES STANDALONE CYBER INSURANCE POLICIES MORE VALUABLE

By Kevin P. Kalinich, Esq.
Aon Global Cyber Insurance Practice Leader
January 3, 2017

The United States Department of the Treasury issued a "Notice of Guidance" December 27, 2016, which clarifies that stand-alone "Cyber Liability" insurance policies are included under the Terrorism Risk Insurance Act of 2002, as amended ("TRIA"). TRIA requires insurers to "make available" terrorism risk insurance for commercial property and casualty losses resulting from certified acts of terrorism (insured losses)[1], and provides for shared public and private compensation for such insured losses. Effective April 1, 2017, and consistent with TRIA and the TRIA program regulations, an insurer must provide disclosures and offers that comply with TRIA and the program regulations on any new or renewal policies reported as standalone Cyber Liability insurance.

BACKGROUND

Unable to accurately model or price terrorism exposures following the September 11, 2011, terrorist attacks on the World Trade Center, insurers and reinsurers largely withdrew from the terrorism insurance market. Many businesses were not able to purchase insurance protection against future terrorist attacks. Such situation was a serious threat to industries where lenders and investors required terrorism protection for their investments, such as construction, defense contractors, aviation, real estate, transportation, energy, financial institutions and utility sectors of the economy. Congress responded by enacting TRIA in November 2002 to provide a government reinsurance backstop in case of large-scale terrorist attacks ($140 million for 2017, which increases $20 million per year up to $200 million), requiring that business insurers offer terrorism coverage for certain types of insurance. Under TRIA, the federal government would help insurers cover losses in the event of a terrorist attack under certain conditions (including 2017's $31.5 billion insurance marketplace aggregate retention, which increases by $2 billion per year up to $37.5 billion), and would also impose assessments on the insurance industry to recover all or a portion of the federal payments.

Unfortunately, the TRIA federal "backstop" up to $100 billion for insurance claims related to acts of terrorism, did not specify whether "Cyber Liability" insurance was included as a covered line of property and casualty insurance – until now.

[1] As is the case with all other coverages subject to TRIA, policy losses that do not arise from an "act of terrorism" certified by the Secretary of the Treasury would not trigger the program backstop. For example, an act cannot be certified as an "act of terrorism" unless it is, among other things, "a violent act or an act that is dangerous to human life, property, or infrastructure. . . ." 31 CFR 50.4(b)(1)(ii). To the extent a cyber event did not satisfy this requirement, the backstop provisions of TRIA would not be implicated. Any specific determination in that regard could not be made in advance and would depend upon the circumstances and considerations presented in any particular case.

As organizations of all sizes, industries and geographies increasingly rely on technology and information assets, cyber terrorism has become a major concern for all companies. Prior to December 27, 2016, it was unclear whether TRIA included or excluded cyber terrorism. There is congressional commentary speculating TRIA would have back-stopped cyber insurance if there is a catastrophic cyber incident, but no conclusive position until the subject Notice of Guidance.

FINANCIAL STATEMENT IMPACT

Prior to the December 27, 2016, Notice of Guidance, many of the 67+ different primary cyber insurance base policies specifically exclude cyber terrorism in some manner. Fortunately, most carriers will remove or carve back the cyber terrorism exclusion to provide fairly broad coverage for cyber terrorism. However, the total limits available for cyber exposures for any one risk has generally been capped at approximately $300 million -- $500 million. The primary reason given by cyber insurance carriers for not providing greater limits is often the systemic aggregation risk (along with lack of actuarial loss data, dynamic nature of cyber exposures and lack of standardized cyber assessments, etc.). For instance, if most of the organizations in a sector, such as transportation or grid related entities, used the same enterprise resource planning software, SCADA systems, or outsourced IT providers, the aggregation risk could create catastrophic systemic losses from a cyber attack.[2] A recent study estimated that a major cyber attack on the US power grid[3] could result in $21.4 billion to $71 billion in claims paid by the insurance industry, with a much larger impact on the US economy.[4]

Not all cyber exposures are equal. The relative frequency and severity of cyber exposures should be considered in each situation.

Aon Cyber Enterprise Solution™ is a first-of-its-kind property/casualty and Internet of Things[5] insurance policy that offers comprehensive and integrated enterprise-wide coverage against cyber risk. Retroactive effective to January 1, 2016, such solution is eligible for the federal government backstop protection from catastrophic cyber risk. The current cyber insurance market addresses elements of network business interruption, cyber expense reimbursement and security/privacy liability. Aon Cyber Enterprise Solution™ broadens the scope of coverage to address emerging areas of cyber risk and regulation with a large retention, large limit approach. Depending upon the retention, terms and conditions, coverage highlights include:

- Comprehensive limit approach – up to USD 400 million in capacity per policy
- Aon proprietary language – single policy form
- Property damage arising out of a network security breach
- Products liability coverage to address Internet of Things exposures[6]

---

[2] Lights Out! Can Insurance Help?

[3] In "Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath," author Ted Koppel suggests that a catastrophic cyber attack on America's power grid is likely and that we're unprepared.

[4] Lloyd's and the University of Cambridge Centre for Risk Studies 2015 Report, "Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid."

[5] Internet of Things Exposures & Enterprise Risks

[6] Note that The Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, or "SAFETY Act," can provide liability protection to a wide range of technologies including cybersecurity products and services.

- Business interruption and extra expense coverage arising out of a systems failure
- Contingent network business interruption for IT vendors and the supply chain
- Cyber terrorism coverage, specifically eligible for TRIA backstop
- European Union General Data Protection Regulation (effective May 25, 2018) fines and penalties, where insurable
- Privacy/security liability and event expense coverage
- Media liability and technology errors and omissions by endorsement
- Potential captive utility
- Business interruption proof of loss calculation is included
- Coverage is primary over any valid and collectable insurance

LIMITATIONS & UNANSWERED QUESTIONS

The December 27, 2016, Notice of Guidance should further accelerate the rapid growth of standalone cyber insurance. However, there remain a few issues to resolve. For instance, many technology, media and professional services organizations rely on their "Technology Errors & Omissions," "Media" or "Professional Liability" insurance policies to address third party cyber exposures. Inexplicably, "Professional Errors and Omissions Liability Insurance" policies are specifically excluded from TRIA protection. Ironically, "Property and Casualty" policies that may not have intended to address cyber terrorism exposures are included under TRIA whereas professional liability policies that are intended to address cyber terrorism exposures are not eligible for TRIA protection. Other lines of insurance could remain in the grey area.

Some cyber policies require the insured to prove that the cyber incident was not cyber terrorism in order to not be excluded. How can an insured ***prove the motivations*** of a 13 year kid in his mom's basement vs. a competitor hack vs. a foreign national state action? Nearly impossible. From the insureds' perspective, it does not make much difference regarding the motivation of the hackers – the economic/financial loss = economic/financial loss. Most carriers differentiate removing the "Cyber-terrorism" exclusion from the "War" exclusion, which they will not remove. The key is to limit the "War" exclusion to a declaration of "War" by Congress. Furthermore, with the TRIA backstop now in place for Cyber Liability policies, insured's may be able to completely remove the "War" exclusion. The specific details of cyber insurance policy wording continue to evolve. In breadth and depth identification and quantification of each organization's unique cyber exposures and risk mitigation strategies, along with an analysis of existing and available insurance coverage is recommended.

Unless TRIA is extended, it is scheduled to expire December 31, 2020.