



Terrorism Risk Insurance

2019 Report

Introduction

In 2001, the world was shocked by the terrorist attacks of 9/11. Neither the United States, nor the world at large, were prepared for the scale of the attack and the unprecedented destruction accompanying it. Not only did 9/11 mark a new historical era, but terrorism continues to shape much of the global conversation.

There were more than 135,500 terrorist attacks worldwide between 2006-2017.¹ In 2017 alone there were 10,900 attacks which claimed 18,488 victims.² While most of these attacks took place in the Middle East and none matched the devastation of 9/11, it's clear that global terrorism remains a persistent threat.

Aon has noted a shift in the ideologies underlying terrorism. New risks are posed by returning Islamic State fighters and in North America and Europe the rise of political extremism creates an emerging threat. Fortunately, the marketplace is responding to the needs of insurance buyers with solutions that are tailored to address evolving needs.³

In the United States, there remains a need for a financial backstop for catastrophic terrorist attacks. Adjusted for inflation, “insured losses across all insurance lines from the September 11 attacks exceeded \$45 billion.”⁴ The original federal Terrorism Risk Insurance Act (TRIA) and its subsequent reauthorizations provides the necessary buttress against such significant loss of property caused by acts of terrorism. The structure of the current law also protects taxpayers from paying for a terrorist attack that exceeds the cost of the 9/11 attack.

TRIA will expire on December 31, 2020. In this report, Aon lays out the case for a long-term extension of TRIA* coupled with a requirement to study in detail a growing threat vector that will influence future coverage: cyber terror.

Aaron Davis
Managing Director,
Commercial Risk Solutions

Edward Ryan
Senior Managing Director,
Reinsurance Solutions

Catherine Mulligan
Managing Director,
Cyber Reinsurance

Stephen Hackenburg
Chief Broking Officer,
Commercial Risk Solutions

*Please note that for the sake of clarity and unless otherwise noted, we use the acronym “TRIP” inclusively from this point forward when referring to either the initial Act (TRIA), the Program (TRIP) or any of the Reauthorizations (TRIPRA).

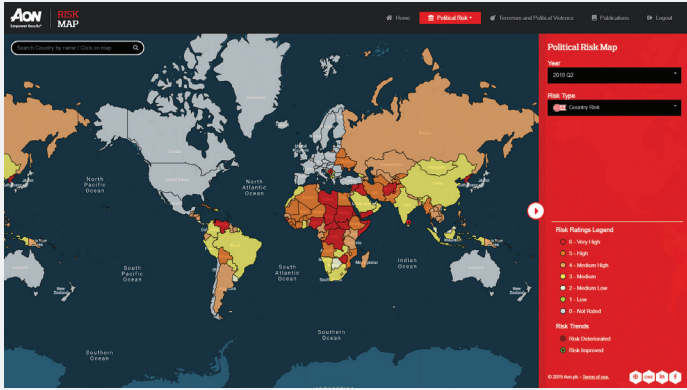
Present-Day Terrorism

The threat posed by terrorism remains potent and “extraordinarily high compared to historical trends.”⁵ According to the 2018 Global Terrorism Index, “Every region in the world recorded a higher average impact of terrorism in 2017 than in 2002. The increase in the impact of terrorism was greatest in the Middle East and North Africa, followed by sub-Saharan Africa.”⁶

According to Aon’s Terrorism and Political Violence Risk Map,⁷ we see continued political instability across virtually every region of the world. The resurgence of authoritarianism and nationalism has widened fault lines between allies and fueled geopolitical competition. It has also increased regime instability across much of the world as more governments adopt less inclusive policies and systems of governance.

The map also captures how the threat of terrorism is evolving across the globe. It depicts a reduction in the number of attacks motivated by Islamist extremism in North America and Europe, and an increase in the impact of attacks motivated by extreme right-wing views. It shows that terrorism fueled by “far left” ideology is on the rise again in Colombia, despite a much-lauded peace deal with FARC in 2016, and that the pace of attacks by jihadists in Indonesia rose by almost six-fold last year.

The most notorious terror group, the Islamic State (IS), is less capable of mounting and inspiring attacks in the West.⁸ There were less than half the number of IS-linked attacks in North America, Europe and Australia in 2018 (11) than there were in 2017 (26). After IS lost territory in Iraq and Syria in 2017, it shifted focus to other countries with fragile security environments, particularly Afghanistan, Nigeria and the Philippines. The group and its supporters mounted at least twice as many attacks in these three countries in 2018 compared with the year before.



Aon’s Risk Maps Online

Aon’s Risk Maps portal is freely accessible to all those interested in the issues of political risk, terrorism and political violence, as well as their potential impact on global operations. Type the URL below into your browser to access the interactive website.

<https://www.riskmaps.aon.co.uk/>

Far-right terrorism in North America & Europe⁹

Far-right terrorist attacks and plots have almost doubled in frequency since 2016. The Risk Advisory Group (www.riskadvisory.com) and Aon together recorded 27 attacks in 2018 compared with 14 attacks in 2016. This trend has remained evident in 2019 with the attack by a far-right extremist on two mosques in New Zealand that killed 50 people.

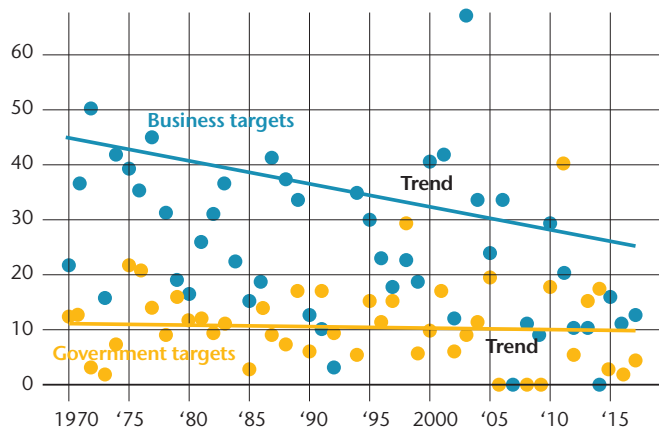
According to an assessment by Peter Bergen and David Sterman writing in *NewAmerica.org*, “jihadists are not the only threat to the United States. Far-right extremists have killed 73 people since 9/11 and have conducted six deadly attacks” since the beginning of 2017.¹⁰

Violent right-wing extremists broadly target ethnic, religious and LGBT+ minorities, as well as politicians and other public figures. These attacks are most frequently targeted at mosques, synagogues, refugee centers and other symbols of multiculturalism and immigration. The attacks in 2018 included the use of arson, knives, firearms and bombing.

The lack of organizational affiliation among far-right terrorists makes it more difficult for authorities to identify plots and intervene before an attack. Our data indicates a 70 percent completion rate for planned far-right attacks in 2018. By contrast, jihadists achieved an attack in just 28 percent of their plots.

“Lone wolf” attacks and the risk to business

Terrorism as a lethal political tool has evolved from efforts to pull off highly sophisticated attacks like 9/11 to much smaller operations conducted by so-called “lone wolves.” These individuals are often self-radicalized, free of organized command structures, unaffiliated with known terrorist groups and carry out attacks by themselves. Examples include the 2013 Boston Marathon bombings, the 2016 Orlando nightclub massacre, the 2017 New York City truck ramming and, in June 2019, the disruption of an alleged plot by a Syrian refugee to bomb an African-American church in Pittsburgh.



Source: FiveThirtyEight

Similar attacks have been carried out in U.S. workplaces, prompting increased concern from employers. Businesses are, in fact, more likely targets than political targets.¹¹ In the first half of 2019, five people were killed in a SunTrust Bank in Florida; 12 people were killed at a municipal office in Virginia; and five people were killed at an industrial warehouse in Illinois. All three incidents involved an active shooter.

While the workplace shootings seem to have been motivated by personal grievances, it's not much of a leap to imagine a scenario in which such attacks are driven by ideological motives. Indeed, the 2015 massacre of 14 people at a Department of Public Health event in California was one such incident.

NCBR threats

Potential attackers who possess nuclear, chemical, biological or radiological (NCBR) weapons and detonate one in a densely populated commercial urban center could render a large area uninhabitable, resulting in significant loss of life, property and revenue, potentially activating TRIP.

The risks of NCBR are specifically problematic for workers' compensation insurance. While property insurers must offer terrorism coverage, this provision may have the effect of pricing themselves of the market. Insurers who write workers' compensation business are obligated to provide statutory benefits to injured workers and may not exclude such risks from their policies. Without TRIP, the only risk mitigation technique available to insurers is to exit the business. Such a development would have a significant negative impact on businesses and the economy, and would shift risk to the states, which in critical high-risk states are the insurers of last resort. This also presents a particular solvency risk to smaller insurers and may force those insurers to exit from the market first.

Cyberterrorism

A threat vector deserving closer attention is cyber-terrorism. Cyberattacks have become a significant threat and have the potential to create loss on a massive scale. For instance, Yahoo, the Internet giant, suffered the largest breach in history when *all three billion* user accounts were compromised.¹²

U.S. healthcare providers, government services, entertainment companies, manufacturing (including supply chain) and financial institutions are all potential targets. Between 2015 and 2017, the U.S. was targeted by 303 known large-scale attacks, more than any other country.¹³

Cyberattacks are an means of achieving wide-spread destruction and perpetrators have increased the frequency and sophistication of their attacks.¹⁴ According to the 2019 Verizon Data Breach Investigations report, "threat actors attributed to state-affiliated groups or nation-states combine to make up 96% of breaches ... [and] phishing was present in 78% of Cyber-Espionage incidents."¹⁵

The systemic potential from cyber losses can be achieved via a narrow gap in an enterprise network, including unsecured Internet of Things (IoT) devices. Such interconnectivity provides a wide attack surface, enabling cyber attackers to target multiple companies or organizations in a single event. Moreover, the damage potential extends beyond financial loss from a data breach. Cyber-attacks have been the cause of significant physical damage, such as the December 2014 fire following a breach at a German steel mill¹⁶, and the protracted business interruption of supply chains following the *NotPetya* wiperware attack.

A nation state sponsored attack on a New York State dam¹⁷ in 2013, further illustrates the issue. An Aon study found that the more than 90,000 dams in the U.S. are particularly vulnerable to a cyberattack as more and more implement automated control systems to increase efficiency and safety. In the published report, we found:

- "Major impacts not only to dam operations but also to the resilience of local businesses and communities, with the highest economic loss estimated at USD 56 billion;
- "Silent cyber [non-affirmative] exposure to insurers, with total insured losses of up to USD 9.7 billion"; and
- "A significant protection gap that would hurt homeowners and businesses if such an event were to occur, with only 12 percent insured in one of the dam scenarios."

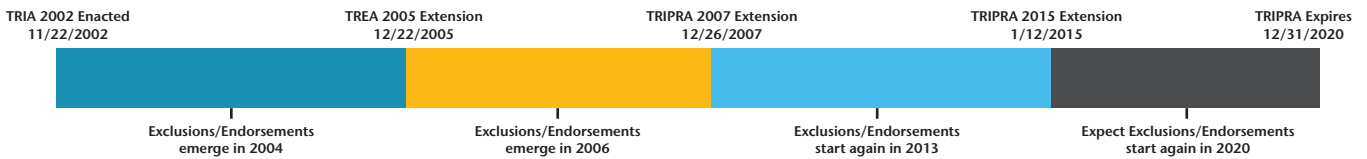
In this scenario, the majority of the loss is uninsured due to low take-up rates of flood insurance. This underscores how severe the consequences of such an attack could be if successfully executed by malicious actors.¹⁸

Finally, in a first-of-its-kind study, *Bromium* found in 2017 that the cyber-crime economy had grown to USD\$1.5 trillion annually in illicit profits. That number includes illegal online markets, theft of trade secrets or intellectual property, data trading and ransomware.¹⁹ These losses differ from other terrorism losses only in the means used to carry them out. For that reason—and given the continued growth in exposure—cyber is a logical subject for the TRIP program to address. We provide more of our thinking about an approach to cyber below in our recommendations.

The Terrorism Risk Insurance Program

The federal loss-sharing program known as the Terrorism Risk Insurance Program (TRIP) has had a stabilizing influence on the property insurance market since its original inception in 2002. The legislation gives insurers confidence to write policies and take on risk they might otherwise refuse which, in turn, allows clients to transfer risk at competitive pricing without fear of cost volatility or capacity shortages.

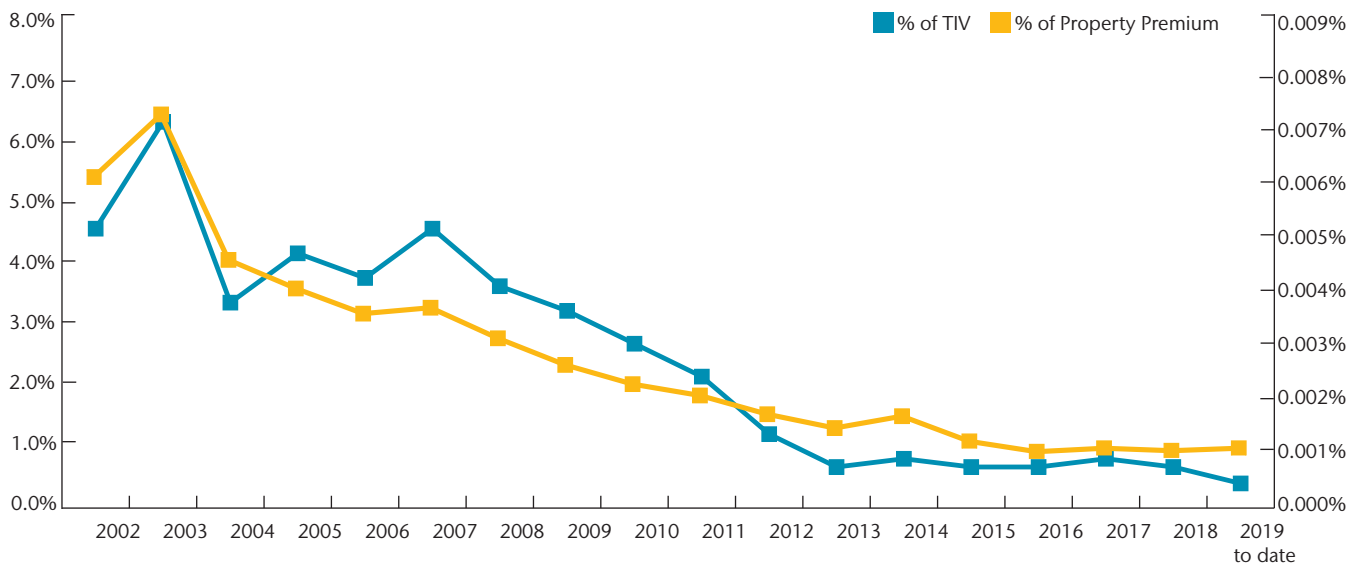
The TRIA Timeline



In its 2018 Report on the *Effectiveness of the Terrorism Risk Insurance Program*, the U.S. Department of the Treasury found that “[t]he Program has made terrorism risk insurance available and affordable in the United States, and the market for terrorism risk insurance has been relatively stable for the past decade. While the purchase of terrorism risk insurance is not mandated by the Program, a significant proportion of commercial policyholders nationwide have elected to obtain such insurance, and take-up may be even higher in metropolitan areas at greater risk of terrorism.”²⁰

Underscoring TRIP’s success is Aon’s Data & Analytics Group pricing data since TRIP’s inception for commercial, complex property accounts (one of the most stressed areas of capacity following the events of 9/11), which has seen property terrorism premiums decline by more than 80 percent since 2003, when the impact of the original Act’s passage began to take effect.

Medium Terrorism Premium as % Medium Property Premium & TIV



Source: Aon Data

Aon's View on the Future of TRIP

TRIP remains untested for actual losses. However, given its important role in the insurance industry and for policy-holders alike, we believe the expiration of TRIP would produce significant negative consequences, including a return to conditions similar to what led to the creation of TRIP in 2002. Following 9/11, “terrorism coverage became scarce as primary insurers filed requests with their state insurance departments for permission to explicitly exclude terrorism coverage from their commercial policies. By early 2002, 45 states had approved such exclusions for use in standard commercial policies. Reinsurers were also unwilling to reinsure policies in urban areas perceived to be vulnerable to attack.”²¹

We believe that if TRIP is not reauthorized, terrorism insurance pricing would likely spike as many insurance carriers exit the market. Risks that include high numbers of workers—and therefore a great concentration of exposure, particularly in large metropolitan areas—would lead to an unavailability of coverage. The shortage of capacity and increased pricing would affect embedded TRIP coverage, standalone terrorism insurance, workers compensation and TRIP captive placements.

Recommendations

The possibility of a future 9/11-style attack warrants further discussion on terrorism risk insurance. Because the threat of a large terrorism event still exists, **Aon recommends that the Terrorism Risk Insurance Act (TRIA) be reauthorized on time.** Specifically, we recommend the following actions:

1. **Extend TRIP 10 years prior to its expiration on 31 December 2020**
2. **Keep current deductible and co-participation features unchanged**
3. **Keep current trigger amounts unchanged**
4. **Keep Insurance Industry Retention for Mandatory Recoupment unchanged**
5. **Study cyberattacks and their potential impact on TRIP**

A fuller discussion of each recommendation follows.

Duration and Market Stability

TRIP was enacted in November 2002 and is due to expire on December 31, 2020, at which time it will have been in place for 18 years. The program will have been through three reauthorizations ranging in duration from two to seven years.

The lead-up to each extension created uncertainty in the insurance industry, which led to disruption in the market. The turmoil created by the renewal discussion (most notably in 2015) was equally difficult for policyholders who faced potential loss of coverage. Even though most expected TRIP to be renewed, insurers still spent significant time and effort to revise policy forms to include conditional terrorism exclusions on property insurance. Policyholders were faced with the possibility of no terrorism coverage. With respect to workers compensation, insurers took steps to manage their exposures which included non-renewals, short term policies, and premium changes.

Similarly, the 2020 deadline is causing concerns in the insurance industry due to uncertainty about whether TRIP will be extended or modified. Rating agencies routinely monitor TRIP and measure the benefit it has for companies with terrorism exposure.

Leading up to the expiration in 2014, A.M. Best conducted a review of carriers' terrorism exposure should TRIP not be in place. Thirty-four carriers were identified as having accumulations that called into question their rating with 31 of them being predominantly workers' compensation or commercial casualty writers. All carriers avoided a downgrade through data cleansing on workers' compensation policies and the purchase of additional reinsurance.

A.M. Best recently released commentary regarding the impact that changes to TRIP could have on certain companies and their expectations for managing the uncertainty going forward. To meet rating agencies' expectations, insurers with terrorism exposure will meet with A.M. Best to present risk mitigation practices and strategy in the event of changes or expiration in the current legislation.

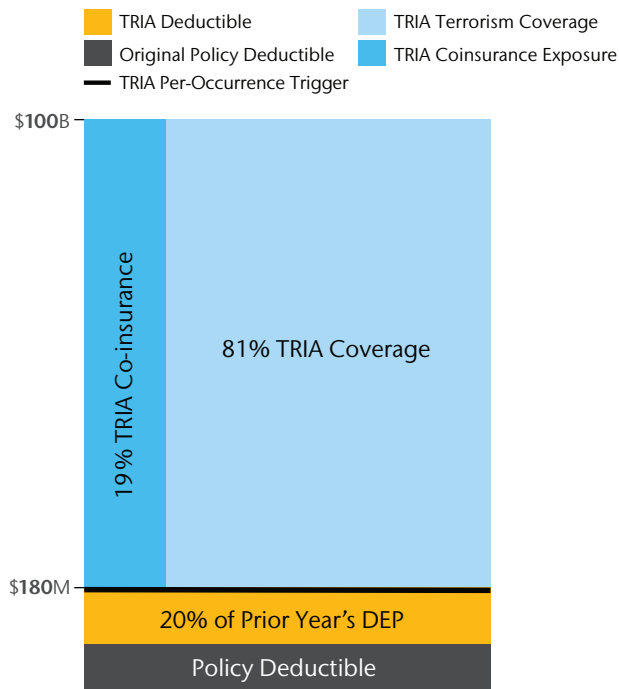
With the uncertainty concerning TRIP reauthorization, we expect carriers to implement conditional terrorism exclusions on property policies in 2020 (although competitive market pressure may make such an option unattractive for some clients). We also see the potential for the purchase of additional workers' compensation terrorism reinsurance. And, while capacity is currently plentiful, increased demand will result in increased pricing, especially the later into 2020 we get.

If TRIP is not extended, we expect that potential expiration and/or significant changes to TRIP will have an impact on the ratings within the insurance industry, but **an early and extended reauthorization will go a long way to keep the market stable and avoid increased costs.** A minimum extension of ten years would forestall the turmoil created in the run-up to renewal.

Modifications

The reauthorization of 2015 included two revisions to the Act:

1. The Program trigger raised from \$100m to \$200m in annual \$20m increments through 2020. It is currently at \$180m.
2. Insurers' co-participation in the loss excess their deductible increased from 15 to 20 percent in annual one percent increments through 2020. It is currently 19 percent.



- The 2015 reauthorization includes provision that insurers' co-participation increases 1% per year from 15% in 2015 to 20% in 2020.
- The Program Trigger, likewise, increases \$20m per year from \$100m in 2015 to \$200m in 2020.
- Prospects for reauthorization before year-end 2020 appear good with no obvious obstacles to passage
 - However, a contentious atmosphere in Washington, DC, particularly between the House and the Administration, could derail the reauthorization process

The latter feature ensures increased industry participation in loss and reduces federal involvement. Furthermore, though the insurer deductible remained unchanged at 20% of prior year's direct earned premium, the growth in the industry premium also helps reduce federal involvement. Since 2002, the total industry TRIP premium for U.S.-based insurers has increased 71 percent. Thus, on average, the insurance industry retention of loss has increased significantly, while lessening the likelihood of the backstop being triggered.

This increase in the overall amount of insurer deductible and the percentage of loss the industry retains above that deductible ensures the insurance industry has a meaningful role in the provision of terrorism coverage even with the existence of the backstop.

The metrics above suggest carriers have a significant retention under the backstop. **We recommend the deductible and co-participation features of the program remain unchanged.**

The increase in the program trigger creates an issue for smaller insurers. Given the increase, the possibility of no recovery under the backstop increases. If a small insurer or group of small insurers were to bear the entire loss without TRIP recovery, the impact could be devastating. For this reason and given the mandatory recoupment provision applicable for smaller losses, **we recommend no further change in the trigger.**

Insurance Industry Retention for Mandatory Recoupment

This is the insured loss threshold for requiring the recoupment of Federal Government Payments based upon mandatory post-event surcharges. In other words, it sets an index for requiring that any Federal Funds (i.e., taxpayer funds) be repaid based upon Insured Losses falling below the five-year figures listed below. Following year five of the program, when the retention amount equals USD\$37.5 billion, the aggregate retention shall be equal to a three-year average of the sum of insurer deductibles for all insurers participating in the program.

- 2015 – USD 29.5 billion
- 2016 – USD 31.5 billion
- 2017 – USD 33.5 billion
- 2018 – USD 37.5 billion
- 2019 and onward: a three-year average of the sum of insurer deductibles for all insurers participating in the program

Aon recommends no change to the Insurance Industry Retention for Mandatory Recoupment, noting that at a figure of USD\$37.5 billion, it would cover close to 85% of the inflation-adjusted insured losses suffered under 9/11 (USD\$45 billion of adjusted, insured loss).

Cyber threats

Cyberterrorism is a logical peril already covered by TRIP. Interconnected networks are susceptible to attack from threat actors who can exploit component security vulnerabilities, resulting in disruption to supply chains, wide-spread business interruption and the potential for physical damage and bodily injury.²² The proliferation of malware and other evolving hazards increases the potential magnitude of a major cyber-attack.

The Atlantic Council has said there is “strong correlation between malware propagation and geopolitics,”²³ and the potential ramifications can run wide and deep with astonishing speed.

For example, the 2017 *NotPetya* malware attack, which cost an estimated \$10 billion,²⁴ affected hospitals, power companies, and banks in a matter of minutes.²⁵ A successful attack against even a small percentage of companies in the U.S. would put pressure on the standard cyber (re)insurance market, which is already deeply concerned about the aggregation and accumulation potential from cyber exposures.

To offer a simple example of how this would work, imagine if an insurer wrote a cyber policy for each of 1,000 companies. Suppose that 90 percent of those companies (i.e. 900) were all using the same cloud service provider. If the cloud suffers a cyberattack and causes a business disruption for users of the services, all 900 companies might suffer loss, exposing the insurer to liability on a staggering scale.

Even if an insurer doesn’t write a policy specifically covering cyberattacks, they may still suffer loss in the same scenario if they haven’t specifically excluded or charged a premium to cover cyber. When a cyberattack causes downtime (e.g. *NotPetya*), it is considered a “business interruption” (BI) in insurance terms. A stand-alone cyber policy can include BI, but claims can also be submitted under standard property policies where BI traditionally sits. It is possible that (re)insurers may find themselves paying out for losses they didn’t fully plan for.

Regulators and rating agencies are beginning to ask insurers to fully assess the cyber exposure that may exist under all policies. The potential systemic exposure has led (re)insurance executives to publicly comment that cyber risk is ultimately too big for the traditional market to shoulder.²⁶ As malware proliferation and other hazards put pressure on traditional markets, reliance on a federal backstop could become more pronounced as (re)insurers seek to limit their liability.

We recommend a study of cyber exposure and its potential effects to understand its future impact on TRIP.

Conclusion

A renewed Terrorism Risk Insurance Program (TRIP) is an essential component in protecting our nation's business from the threat of terrorism. It lends confidence to insurers that they will have the backing of the federal government if another large-scale terrorist attack is conducted on U.S. soil, and it benefits policyholders who are assured of being able to recover their losses in the event of such an attack. It has spurred the decline of property terrorism premiums by more than 80 percent since its inception and it allows clients to transfer risk at competitive pricing.

While it has never been fully tested, the success of TRIP—and the specter of a continuously evolving terrorist threat matrix—should encourage our government to seriously consider other risks that are expressly covered by the program. Nuclear, biological, chemical or radiological (NBCR) weapons delivered by a single individual or group can cause enormous damage, as might the actions of right-wing extremism, and cyber-attacks are emerging as one of the greatest threats to our world. These new and developing risks represent the potential to dwarf the attacks of 9/11 in terms of insured loss of life and assets.

On the opposite side of the risk spectrum, insureds must consider if a particular event is not certified as “terrorism” and is therefore not covered by insurance. Clients will need to evaluate whether the scope includes “lone wolf” attackers whose low-tech approach may not generate the impact required to trigger policy changes (i.e., no damage to property), but may nonetheless find themselves under-insured following such attacks. To the extent TRIP's current coverage isn't as broad as the risks facing U.S.-based insureds, it has encouraged insurers to expand terrorism coverage to a broader range of risks that are not covered by TRIP.

We appreciate the opportunity to add our perspective to the conversation about TRIP. However the terror landscape develops, Aon believes that a federal program like TRIP will be necessary for the foreseeable future.

Endnotes

1. <https://www.statista.com/statistics/202864/number-of-terrorist-attacks-worldwide/>
2. Global Terrorism in 2017. National Consortium for the Study of Terrorism and Responses to Terrorism (START)
3. 2019 Aon Risk Maps
4. Memo: The Reauthorization of the Terrorism Risk Insurance Program
5. Global Terrorism in 2017. National Consortium for the Study of Terrorism and Responses to Terrorism (START)
6. <http://visionofhumanity.org/app/uploads/2018/12/Global-Terrorism-Index-2018-1.pdf>
(available from <http://economicsandpeace.org/reports/>)
7. Risk Maps 2019: Aon's Guide to Political Risk, Terrorism & Political Violence, p. 28
8. <https://theconversation.com/will-terrorism-continue-to-decline-in-2019-104466>
9. Risk Maps 2019: Aon's Guide to Political Risk, Terrorism & Political Violence. This section is based on pp. 31-32.
10. <https://www.newamerica.org/international-security/reports/jihadist-terrorism-17-years-after-911/>
11. <https://fivethirtyeight.com/features/how-to-make-sense-of-this-weeks-mail-bombs/>
12. The theft of names, dates of birth, email addresses, passwords, security questions and answers knocked an estimated \$350 million off Yahoo's eventual sale price to Verizon.
13. Internet Security Threat Report, Symantec, March 2018
14. Aon 2019 Cyber Security Risk report
15. <https://enterprise.verizon.com/resources/reports/dbir/2019/incident-classification-patterns-subsets/>
16. <https://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report>
17. <https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html>
18. <https://www.aon.com/reinsurance/gimo/20181025-gimo-cyber>
19. <https://www.bromium.com/press-release/hyper-connected-web-of-profit-emerges-as-global-cybercriminal-revenues-hit-1-5-trillion-annually/>
20. <https://www.irmi.com/term/insurance-definitions/terrorism-risk-insurance-act-of-2002>
21. <https://www.iii.org/article/background-on-terrorism-risk-and-insurance>
22. https://www.atlanticcouncil.org/images/publications/Supply_Chain_WEB.pdf
23. <https://www.cyberscoop.com/ukraine-election-2019-cybersecurity/>
24. Aon's estimates based on publicly available data
25. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>
26. <https://www.globalreinsurance.com/ils-is-needed-to-transfer-cyber-risk--aigs-duperreault/1428660.article>

Contacts

Aaron Davis

Managing Director
Commercial Risk Solutions
Aon
+1.212.441.1144
aaron.davis@aon.com

Edward Ryan

Senior Managing Director
Reinsurance Solutions
Aon
+1.973.966.3554
edward.ryan@aon.com

Catherine Mulligan

Managing Director
Cyber Reinsurance
Aon
+1.212.441.1018
catherine.mulligan@aon.com

Stephen Hackenburg

Chief Broking Officer
Commercial Risk Solutions
Aon
+1.212.441.2227
stephen.hackenburg@aon.com

Additional information on post-recovery resources, including updated service and claims information for clients, can be found at www.aon.com/disaster-response.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

© Aon plc 2019. All rights reserved.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

www.aon.com

GDM10819