MARSH

INSIGHTS | APRIL 2018

2018 Terrorism Risk Insurance Report

SOLUTIONS…DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES

INSIGHTS | APRIL 2018

2018 Terrorism Risk Insurance Report

Although the number of incidents and casualties declined in 2017, terrorism remains a persistent and significant threat to businesses, governments, and individuals. Terrorist attacks rank among the top 10 risks for global businesses in terms of likelihood, according to the World Economic Forum's *Global Risks Report 2018*, produced in partnership with Marsh & McLennan Companies. Geopolitical concerns also rank high, with weapons of mass destruction identified as the top risk in terms of impact. And the past several years have demonstrated that these risks are rapidly evolving.

In our *2018 Terrorism Risk Insurance Report*, prepared by Marsh with support from Guy Carpenter, we explore the state of the terrorism insurance marketplace, presenting data on purchasing and pricing. And we review a number of mitigation strategies that are available to global businesses.

As terrorism risk evolves, businesses should:

- Continually review and reevaluate their risk financing programs to ensure they have adequate protection for property, business interruption, workers' compensation, general liability, and cyber losses.
- Effectively model their terrorism risk.
- Build and test robust crisis management and business continuity plans.

We hope you find this report to be useful as you take steps to manage your terrorism risk.

Tarique Nageer
Terrorism Placement Advisory Leader

CONTENTS

Executive Summary

ATTACK VECTORS CONTINUE TO EVOLVE

- Attacks by "lone wolves" and small groups against soft targets reflect a shift in the nature of terrorism risks.
- The use of vehicles as weapons has increased of late, notably in the US, UK, France, Germany, Spain, and Sweden.
- The threat of cyber-attacks continues to grow.

TERRORISM INSURANCE MARKETS LIKELY TO REMAIN STABLE

- Terrorism insurance capacity remains strong, but pricing could increase as global insurance costs generally increase following natural catastrophe losses in 2017. January 2018 year-over-year pricing changes for a majority of reinsurance program renewals that included terrorism coverage averaged flat to an increase of 10% on a risk-adjusted basis.
- 62% of US companies in 2017 purchased coverage embedded in property policies under the Terrorism Risk Insurance Program Reauthorization Act of 2015 (TRIPRA). Companies in the Northeast US were most likely to purchase terrorism insurance.
- Education entities, health care organizations, financial institutions, and real estate companies had the highest take-up rates by industry.
- As attack methods evolve, buyers are seeking to expand terrorism definitions in insurance coverage to include active assailant events.
- Outside of the US, capacity and competition is strong. Underwriters continue to offer innovative coverage solutions to meet insurance buyers' needs.

TERRORISM RISK AFFECTS OTHER INSURANCE AND RISK MANAGEMENT STRATEGIES

- Buyers are increasingly purchasing political violence coverage or broader political risk insurance in addition to standard terrorism insurance.
- Following high-profile cyber-attacks in 2017, multinational companies appear more interested in coverage for technology-driven business interruption and contingent business interruption.
- Workers' compensation insurers continue to consider employee concentration exposures in their pricing of terrorism risk.
- Insurers are developing specialty products that offer first- and third-party business interruption protection for businesses that suffer lost income or revenue without the need for a direct property damage trigger.
- The number of Marsh-managed captives actively underwriting one or more insurance programs that access TRIPRA increased 44% in 2017.

62%

of US companies purchased terrorism insurance in 2017.

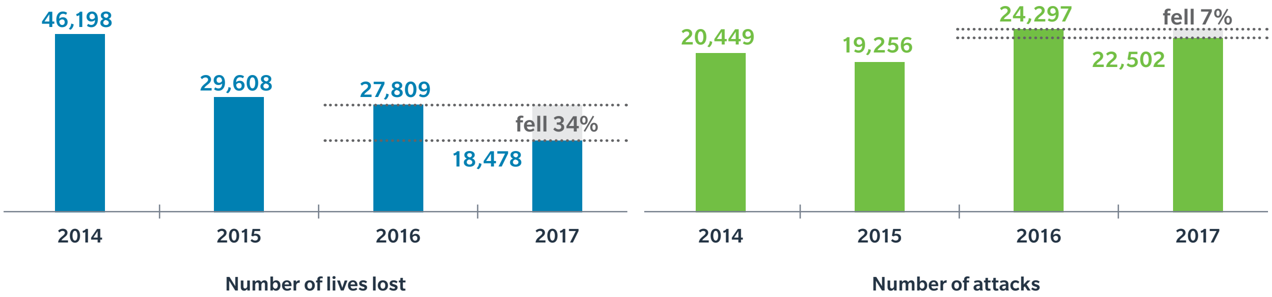
SOURCE: MARSH

Terrorism Threats and Impacts Shift

FIGURE 1

The number of lives lost to acts of terrorism, insurgency, and politically or ideologically motivated violence fell 34% in 2017

SOURCE: JANE'S TERRORISM AND INSURGENCY CENTRE BY IHS MARKIT



From 2014 through 2017, terrorists and other "non-state actors" globally killed more than 122,000 people (see Figure 1).[1] In 2016, insured losses from terrorism totaled $173 million.[2]

Although fewer people were killed in terrorist attacks in 2017 than in 2016, the means of attack and perpetrators have shifted. Past attacks were carried out primarily by specific groups against perceived high-value/high-profile targets. While that threat remains, many recent attacks have come against soft targets and been perpetrated by "lone wolves" and small groups with no direct connection to known terrorist organizations. Weapons of choice now include vehicles, knives, and other handheld devices:

- On May 22, 2017, a suicide bomber outside a concert in Manchester, UK, injured more than 500 people and killed 23.
- On August 17, 2017, an attacker drove a van into pedestrians in Barcelona, killing 13 and injuring over 100, after which he exited the vehicle and killed another person. Hours later, five men drove into a crowded area and attacked seven people with knives, killing one.
- On October 31, 2017, a man driving a rented truck struck and killed eight people and injured 11 along a bike path in New York.

Meanwhile, nation-state-backed actors launched destructive ransomware and wiper attacks in 2017 that caused severe disruptions and financial losses globally to government organizations, critical infrastructure entities, and businesses. Similarly destructive cyber-attacks could soon be carried out by technologically sophisticated terrorists.

The evolving nature of terrorist attacks affects organizations directly and indirectly:

- **Supply chain disruption:** In 2016, terrorist groups undertook 346 attacks on global supply chains, an increase of 16% from 2015.[3]
- **Security costs:** Greater security measures following attacks can bring a high cost. For example, stricter controls along France's borders following the November 2015 Paris attacks cost companies an additional $59 per delayed vehicle.[4]
- **Lost revenue:** Terrorist attacks in Western Europe in late 2015 and early 2016 cost European airlines $2.5 billion in lost revenue in 2016 as tourists stayed away following several high-profile incidents.[5]
- **Consumer confidence:** Although US consumer confidence increased in the third quarter of 2017, terrorism was cited as the top concern for 21% of consumers, trailing only the state of the economy (28%).[6]

1 Jane's Terrorism and Insurgence Centre by IHS Markit.

2 Swiss Re.

3 BSI Supply Chain Services and Solutions.

4 BSI Supply Chain Services and Solutions.

5 International Air Transport Association.

6 The Nielsen Company.

Terrorism Insurance Likely to Remain Stable in 2018

Overall property terrorism insurance capacity is abundant and, barring unforeseen changes, is likely to remain stable in 2018, backed by new entrants and a commitment by incumbents to underwrite the risk. Although attacks continue, insured losses have been limited in frequency and severity.

Following high global natural catastrophe losses and heavy attritional losses in 2017, some insurers are adjusting pricing, capacity, and terms and conditions in various areas of their business. However, barring unforeseen changes, terrorism insurance pricing generally will remain competitive in 2018.

Underwriters continue to scrutinize central business districts in Tier 1 cities, generally defined as those where the perceived risk of terrorism is higher and insurers have significant aggregations. Among other cities, these include New York, London, Frankfurt, Toronto, Brussels, Singapore, Bogota, Los Angeles, Chicago, Washington, San Francisco, Atlanta, and Houston. Pricing is generally higher in such areas, although individual circumstances will dictate results.

As insurers look for ways to differentiate their offerings, some are deploying terrorism insurance capacity closer to buyers' headquarters. For example, some London-based insurers are establishing footprints in the US and Asia or adding resources to existing ones, enabling them to be more responsive to insurance buyers' changing needs.

On the buyer side, more insureds are adding political violence coverage to standard terrorism insurance policies. The potential for cyber-based terrorist attacks has also raised interest in cyber-related business interruption coverage at owned and non-owned facilities. Seventy-five percent of senior executives recently surveyed by Marsh and Microsoft identified business interruption as the cyber loss scenario with the greatest potential to affect their organizations.

US FEDERAL BACKSTOP CONTINUES TO SUPPORT TERRORISM INSURANCE MARKETS

With $100 billion in capacity, the Terrorism Risk Insurance Program Reauthorization Act of 2015 (TRIPRA) provides the US with the world's largest public/private terrorism risk-sharing mechanism.

TRIPRA defines an "act of terrorism" as a violent act or an act that is dangerous to human life, property, or infrastructure that occurs on US territory (or on a US mission or air carrier or vessel outside of the US) and is committed by an individual or individuals as part of an effort to coerce the US civilian population or to influence the policy or affect the conduct of the US government by coercion.

For TRIPRA to apply, the following conditions must be met:

- Insured losses from the event exceed $5 million.
- An event is "certified" as an act of terrorism by the US government.
- The insurance industry "trigger" or overall loss level (currently at $160 million) is met.

Under TRIPRA, insurers are required to "make available" terrorism coverage for property, liability, workers' compensation, and ocean and inland marine risks. Since the original 2002 passage of the federal terrorism backstop, no event has been certified as an act of terrorism. However, TRIPRA has helped to keep the US terrorism insurance market stable since the terrorist attacks of 2001, contributing to low costs and wide availability for buyers. The current bill is due to expire on December 31, 2020.

FIGURE 2

Overall US terrorism insurance take-up rates remain near 60%

SOURCE: MARSH

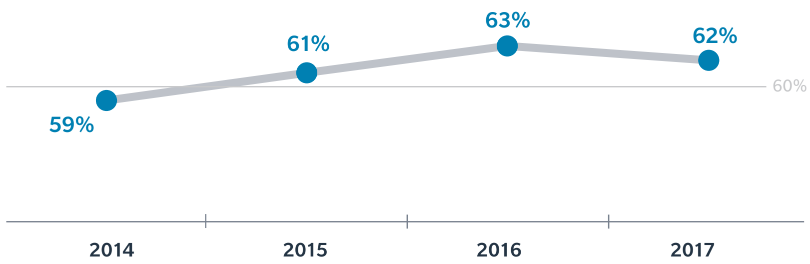


FIGURE 3

Smaller companies tend to have lower US terrorism insurance take-up rates

SOURCE: MARSH

Total Insured Value (TIV) Range	2017	Characteristics
Less than $100 million	53%	Often work with a single insurer and generally have a smaller spread of risks and lower overall premiums.
$100 million to $500 million	66%	Tend to have no more than three insurers involved in their insurance programs.
$500 million to $1 billion	67%	Typically work with several insurers and have layered programs.
More than $1 billion	67%	Typically work with several insurers and pay large premiums. Many use existing captives or establish new ones to access TRIPRA.

Both insurers and insureds have shown interest in coverage related to active shooter threats, in response to evolving attack methods. Hotels and casinos, sports arenas, restaurants, retailers, movie theaters, and others are looking to expand definitions of terrorism to include active shooter threats, which can result in bodily injury to employees and customers, property damage, direct or indirect business interruption, and reputational damage. Companies with significant exposure in developing markets are considering how to address these risks through a variety of coverages, including property terrorism, political violence, political risk, workers' compensation, and general liability. Many insurers appear receptive to broadening terrorism coverage to include such exposures.

US Terrorism Insurance Market Trends Stay Steady

Trends in the US terrorism market show relatively little year-over-year change. The take-up rate for TRIPRA coverage embedded in US property policies has generally remained close to 60% for the last several years (see Figure 2). Although there have been slight year-to-year variations, take-up rates by company size have generally been consistent since 2014 (see Figure 3).

Property terrorism insurance pricing typically shrinks as the size of the company increases (see Figure 4). The largest companies typically purchase higher limits of insurance and are likely to have a larger overall premium spend, which could result in lower allocated terrorism costs for this group. The cost of terrorism insurance as a percentage of overall property premiums (see Figure 5) was highest for companies with TIV of $500 million or more.

FIGURE 4

2017 median terrorism insurance pricing per million of TIV was generally lower for larger companies

SOURCE: MARSH

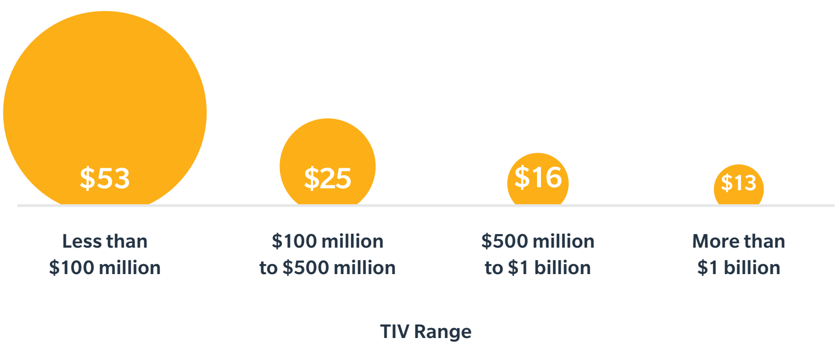
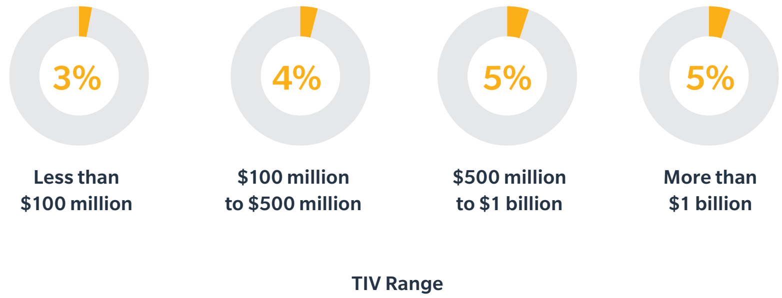


FIGURE 5

Larger companies generally allocated more of their property premiums to terrorism in 2017

SOURCE: MARSH



Approach to Terrorism Insurance Varies by Industry

The percentage of companies that purchased terrorism insurance in 2017 varied significantly by industry. A larger share of education and health care entities continue to purchases terrorism insurance, due in large part to differences in exposure concentrations (see Figure 6). Companies in some industries are more likely to locate in central business districts and major metropolitan areas and are perceived by underwriters to be at higher risk.

FIGURE 6

Concentration risk played a role in 2017 US terrorism insurance take-up rates by industry

SOURCE: MARSH

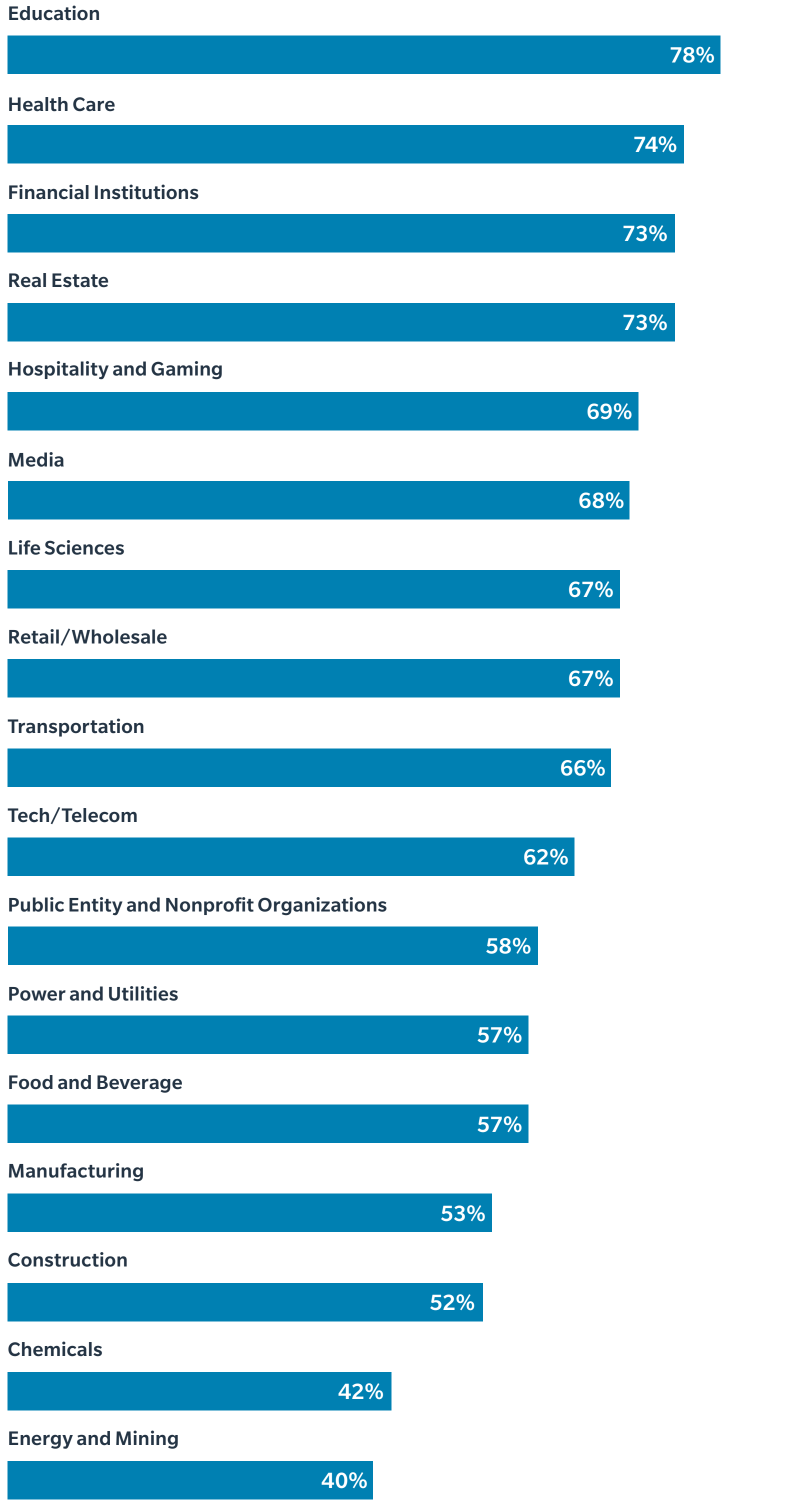


FIGURE 7

2017 median pricing per million was highest for public entity and nonprofit organizations

SOURCE: MARSH

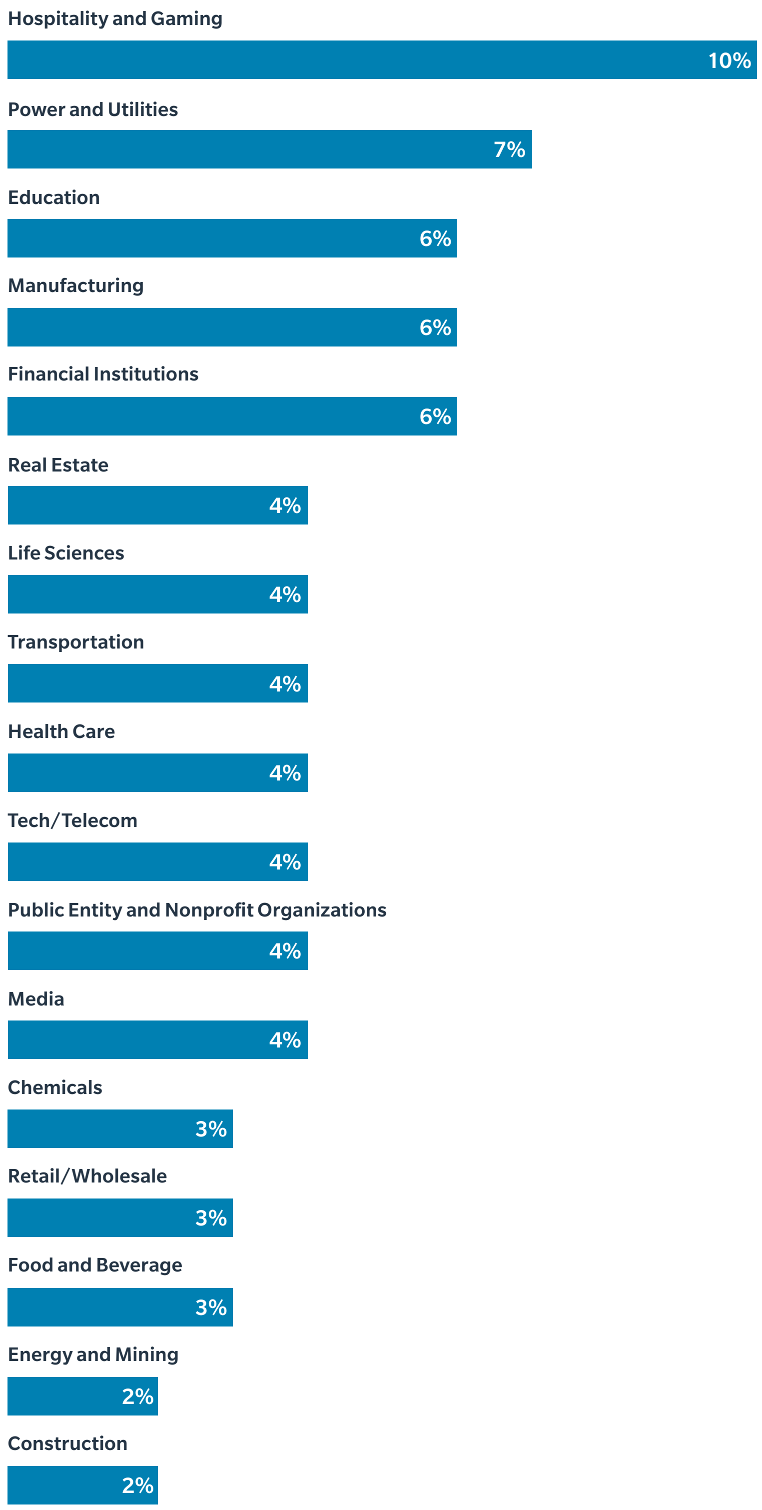
In 2017, pricing increased in five of the 17 industries surveyed by Marsh, with the sharpest increases being felt by hospitality and gaming companies and public entities and nonprofit organizations, which have been targets of terrorist acts in recent years (see Figure 7). Pricing declined in seven industries, most notably for energy and mining and construction companies, reflecting the generally positive conditions in the property insurance market prior to the 2017 Atlantic hurricane season.

Hospitality and gaming companies allocated the largest share, on average, of their property insurance programs to terrorism coverage (see Figure 8). These companies typically have large footprints in key business districts and in cities that are perceived as targets for acts of terrorism.

FIGURE 8

Hospitality and gaming companies allocated the largest share of 2017 property premium to terrorism coverage

SOURCE: MARSH



Northeast US Demand and Cost Increased in 2017

Companies based in the Northeastern United States continue to purchase property terrorism insurance at the highest rate (see Figure 9) among regions. Terrorism insurance was also most expensive in the Northeast US (see Figure 10), at a median cost of $30 per million. Both of these trends are largely due to the presence of several major metropolitan areas in the Northeast that are perceived as higher-value targets for terrorism, along with its population density. Rates were lowest in the Midwest, at a median cost of $18 per million. Because of the greater perceived threat of terrorism in the region, companies in the Northeast US also allocated the largest percentage of their overall property insurance premiums to terrorism coverage (see Figure 11).

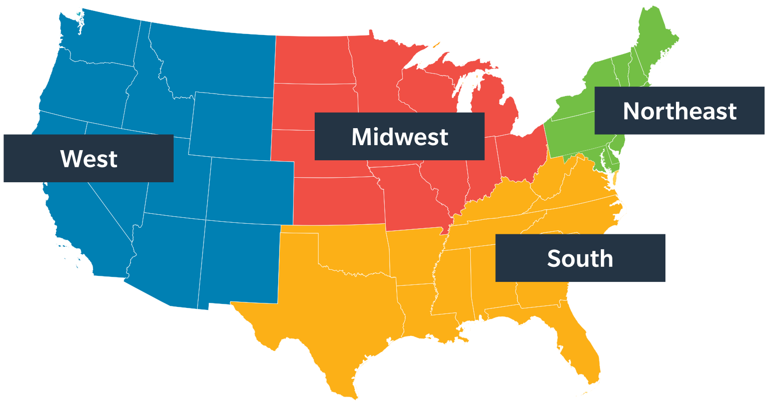


FIGURE 9

Population density contributed to high 2017 take-up rates in the Northeast US

SOURCE: MARSH

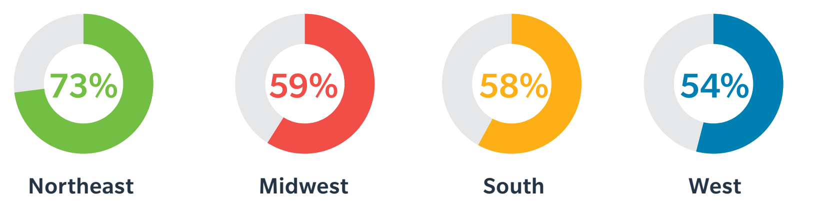


FIGURE 10

Companies in the Northeast US paid the highest median price per million for terrorism insurance in 2017

SOURCE: MARSH

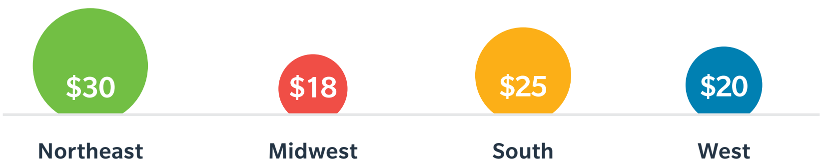
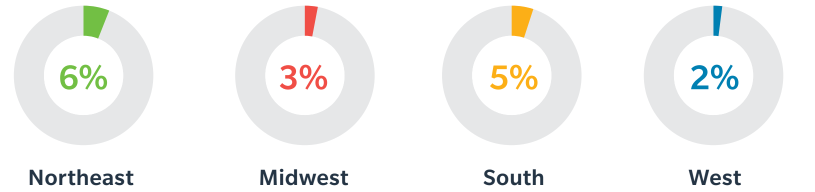


FIGURE 11

Companies in the Western US allocated the lowest percentage of 2017 property premium to terrorism

SOURCE: MARSH



IN FOCUS

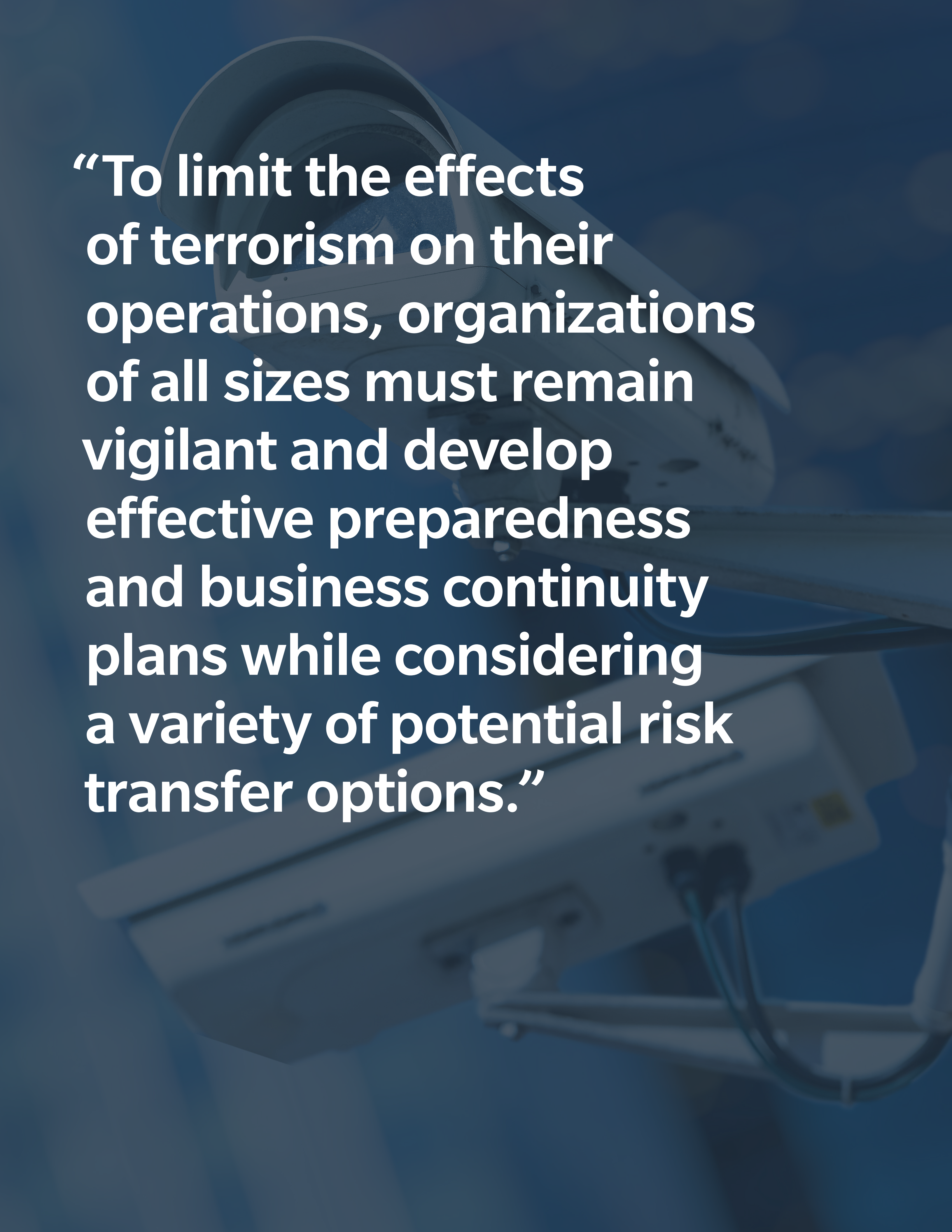
Standalone Terrorism Insurance Remains Competitive

Unlike TRIPRA coverage, which is normally made available within annual "all-risk" property policies, a standalone property terrorism insurance policy does not require the government to certify an act of terrorism in order for a claim to be paid. After September 11, 2001, but prior to enactment of the Terrorism Risk Insurance Act (TRIA) in 2002, the standalone market was the primary source of capacity for companies seeking to purchase property terrorism insurance as mainstream property insurers were generally unwilling or unable to offer coverage. After TRIA's passage, the standalone market continued to provide coverage, competing with "all-risk" property insurers that offered embedded TRIPRA coverage but offering coverage for both TRIPRA-certified and noncertified risks.

Companies may purchase standalone property terrorism insurance as an alternative to TRIPRA coverage or to augment it. Standalone pricing is competitive and is expected to remain so in 2018, barring a significant change in circumstances. Standalone policies can offer broad terms and conditions, including:

- A definition of "act of terrorism" as the use of force or violence — by any person or group, whether acting alone or on behalf of or in connection with any organization — for political, religious, or ideological purposes, including the intention to influence any government and/or to put the public in fear for such purposes.
- Tailored coverage for select locations, coverage outside of the US, and political violence coverage.
- Multiyear policy terms.
- Nuclear, biological, chemical, and radioactive (NBCR) coverage, although this may be limited in scope and costly.

Capacity has nearly tripled since 2005, to a current theoretical maximum of approximately $4.3 billion. Companies with exposures in locations where insurers do not have risk concentration concerns can readily secure up to $2.5 billion in standalone capacity per risk. For locations where insurers have aggregation concerns, typically Tier 1 cities in central business districts, estimated market capacity is approximately $1.5 billion.



"To limit the effects of terrorism on their operations, organizations of all sizes must remain vigilant and develop effective preparedness and business continuity plans while considering a variety of potential risk transfer options."

Global Terrorism Insurance Trends

In Latin America and the Caribbean, competition and capacity remain strong, driven by new market entrants, but pricing varies depending on economic and sociopolitical factors in specific countries and buyers' risk profiles. Miami is an important terrorism and political risk insurance hub for Latin America; in the last two years, several insurers have begun offering competitive standalone capacity from there.

Experienced underwriters in the region continue to demonstrate a willingness to expand the scope of available coverage to address evolving terrorism tactics. In Mexico, for example, it is now a standard practice to include organized crime coverage extensions — for acts committed by criminal groups tied to drug trafficking organizations — in terrorism and political violence placements. Meanwhile, in El Salvador, legislators have passed anti-gang reform measures intended to allow the country's law enforcement agencies to track gang violence as acts of terrorism, which could present an opportunity to develop bespoke insurance products for this risk.

In the UK and Continental Europe, terrorism pricing is driven in large part by insurers' aggregate accumulations, with the highest costs in major metropolitan areas. Insurers continue to innovate to meet buyers' evolving needs; for example, several insurers now offer active shooter/malicious attack coverage, introduced primarily following attacks in London and Barcelona. European insurers, however, have not introduced non-damage business interruption policies, despite growing demand for such coverage.

In Asia, insurers have differing views on how much risk they're willing to accept and are concerned about escalating tensions on the Korean peninsula. Insurers are also closely watching the volatile situation in the Philippines and remain cautious about insuring properties in the Mindanao region. Elsewhere, Singapore and Hong Kong continue to present accumulation concerns for insurers, while border tensions between Thailand and Malaysia remain high.

In the Middle East, capacity for standard risks remains strong, but is limited for war zones and higher risk regions, such as Yemen. Insurers have a strong appetite to write terrorism risks in the region and are offering general area damage and loss of attraction sublimits.

Public/Private Risk-Sharing Mechanisms

Property insurance policies can often be extended to include terrorism coverage in accordance with local terrorism pools (see Figure 12). Such coverage is typically triggered by a national government's declaration that a terrorist event has occurred. These pools are evolving to address potential loss scenarios for local buyers. For example, the UK government announced in March 2018 that it intends to amend the Reinsurance (Acts of Terrorism) Act 1993 to enable Pool Re to provide coverage for non-damage business interruption losses resulting from acts of terrorism. As of April 2018, Pool Re will also extend coverage to cyber-driven business interruption caused by acts of terrorism.

FIGURE 12

Public/Private Terrorism Risk-Sharing Mechanisms

SOURCE: MARSH, GUY CARPENTER, US GOVERNMENT ACCOUNTABILITY OFFICE, WORLD FORUM OF CATASTROPHE PROGRAMMES, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Country	Terrorism Pool or Reinsurance Mechanism	Year Est.	Policyholder Coverage
Australia	Australian Reinsurance Pool Corporation (ARPC)	2003	Elective
Austria	Österreichischer Versicherungspool zur Deckung von Terrorrisiken (The Austrian Terrorpool)	2002	Elective
Bahrain	Arab War Risks Insurance Syndicate (AWRIS)	1981	Elective
Belgium	Terrorism Reinsurance & Insurance Pool (TRIP)	2007	Elective For Large Property Risks
Denmark	Danish Terrorism Insurance Scheme	2010	Elective
Finland	Finnish Terrorism Pool	2008	Elective
France	Gestion de l'Assurance et de la Réassurance des risques Attentats et actes de Terrorisme (GAREAT)	2002	Mandatory
Germany	Extremus Versicherungs-AG	2002	Elective
Hong Kong - China	Motor Insurance Bureau (MIB)	2002	Elective
India	Indian Market Terrorism Risk Insurance Pool (IMTRIP)	2002	Elective
Indonesia	Indonesian Terrorism Insurance Pool (MARIEN)	2001	Elective
Israel	The Victims of Hostile Actions (Pensions) Law and The Property Tax and Compensation Fund Law	1970/ 1961	Mandatory
Namibia	Namibia Special Risk Insurance Association (NASRIA)	1987	Elective
Netherlands	Nederlandse Herverzekeringsmaatschappij voor Terrorismeschaden (NHT)	2003	Elective
Northern Ireland	Criminal Damage Compensation Scheme Northern Ireland	1972	Elective
Russia	Russian Anti-Terrorism Insurance Pool (RATIP)	2001	Elective
South Africa	South African Special Risk Insurance Association (SASRIA)	1979	Elective
Spain	Consorcio de Compensación de Seguros (CCS)	1941	Mandatory
Sri Lanka	Strike, Riot Civil Commotion and Terrorism Fund – Government	1987	Elective
Switzerland	Terrorism Reinsurance Facility	2003	Elective
Taiwan	Taiwan Terrorism Insurance Pool	2004	Elective
United Kingdom	Pool Reinsurance Company Limited (POOL RE)	1993	Elective
United States	Terrorism Risk Insurance Program Reauthorization Act of 2015 (TRIPRA)	2002	Elective

Reinsurance Market Conditions

Reinsurance capacity for terrorism risks continues to develop and grow. Many insurers continue to use the commercial reinsurance markets — at least in part — to buy down their TRIPRA deductibles and buy out their co-shares at acceptable prices, especially for conventional weapon attacks.

Since 2002, the federal terrorism risk insurance program has helped facilitate increased private market involvement, with commercial treaty and facultative reinsurance capacity increasing each year. TRIPRA's January 2015 temporary renewal lapse compelled a number of insurers to scrutinize their data quality, analyze their exposed probable maximum losses, and seek additional reinsurance protection by initiating and/or increasing their trading relationships with markets that offered terrorism capacity and solutions.

The inclusion of terrorism reinsurance coverage in many natural hazard property and workers' compensation catastrophe covers has resulted in traditional and alternative markets supporting existing relationships and diversification efforts.

Despite some January 2018 market hardening in pricing for catastrophe coverages, year-over-year pricing changes for a majority of reinsurance program renewals that included terrorism coverage averaged flat to up 10% on a risk-adjusted basis.

Insurers and Rating Agencies

In 2018, TRIPRA's minimum industry trigger increased to $160 million, contributing to continued rating agency concerns. In late 2017, A.M. Best updated its terrorism methodology and fully integrated the peril into its stochastic Best's Capital Adequacy Ratio (BCAR) model.

Insurers that participate in the federal backstop are required to retain a portion of their terrorism risk on their balance sheets — a figure that increases annually. Rating agencies continue to warn insurers that their ratings could suffer because of an overreliance on TRIPRA.

Insurers and reinsurers generally consider their terrorism risks to fall into two categories: conventional exposures and nuclear, biological, chemical, and radioactive (NBCR) exposures. The amount of capacity available for potential NBCR losses is notably lower than is available for conventional losses. This is especially true for locations in Tier 1 cities and central business districts.

Private market reinsurance capacity is not sufficient to provide the same level of capacity as offered by TRIPRA, making the federal terrorism backstop essential. With TRIPRA remaining in force through 2020, insurer retentions increasing, and the government's potential exposure over time reduced, the reinsurance market is expected to continue to grow, develop, and provide incremental capacity for cedents' net retained exposures to terrorism risks.

TRIPRA's 2015 renewal increased industry triggers and coinsurance obligations. Insurers — particularly smaller mutual and regional insurers — must continue to address solvency concerns from rating agencies, with some insurers seeing higher premium costs as they take steps to ensure that they maintain sufficient policyholder surplus. This could also result in higher premium costs for primary insurance buyers.

Rating agency portfolio reviews have identified potential losses associated with specific aggregations that exposed gaps in coverage beyond what standard reinsurance protections and TRIPRA recoveries provide. Insurers with these rating agency-related accumulations — and other notable terrorism accumulations — continue to access specialty, treaty, and facultative reinsurers for specific locations or aggregations that produced loss scenarios in excess of certain policyholder surplus thresholds.

Reliance on TRIPRA

In 2017, more than 800 insurers wrote $215 billion in TRIPRA eligible premium, with a combined policyholder surplus of $683 billion. Considering the current 20% deductible requirement and policyholder surplus as a filter, Guy Carpenter's analysis concludes that small to midsize insurers are substantially more vulnerable to the annual increases in the TRIPRA industry trigger and their overall net retentions as a percentage of policyholder surplus (see Figure 13). Insurers with less than $300 million in surplus will likely need to incorporate additional private reinsurance market capacity to protect capital and satisfy rating agencies and regulators as the industry trigger increases to $200 million in 2020.

FIGURE 13

TRIPRA Statistics by Policyholder Surplus

SOURCE: GUY CARPENTER

Policyholder Surplus	**Less than $50 million**	**$50 million to $100 million**	**$100 million to $300 million**	**$300 million to $500 million**	**$500 million to $1 billion**	**$1 billion to $5 billion**	**Greater than $5 billion**
Company Count	439	82	128	35	45	53	26
Average Year-End 2018 TRIPRA Direct Earned Premium	$9,567,000	$34,972,000	$88,579,000	$187,267,000	$359,918,000	$915,809,000	$4,560,434,000
Average TRIPRA Deductible	$1,913,000	$6,994,000	$17,716,000	$37,453,000	$71,984,000	$183,162,000	$912,087,000
Average Deductible as a Percentage of Policyholder Surplus	16.09%	10.35%	10.10%	9.59%	9.80%	9.88%	7.34%
Average $160 Million Terror Loss as a Percentage of Policyholder Surplus	3551.9%	241.2%	96.2%	41.2%	23.2%	9.6%	1.7%
Average $200 Million Terror Loss as a Percentage of Policyholder Surplus	5448.3%	301.6%	120.2%	51.5%	29.0%	12.0%	2.2%

US Reinsurance Capacity

In 2017, according to Guy Carpenter, the combined property and workers' compensation private conventional-only terrorism reinsurance capacity was estimated to be $2.5 billion per cedent program. Reinsurance capacity for coverage that includes NBCR, especially in Tier 1 cities and central business districts, has become increasingly challenging to secure over the past two years due to the accumulated aggregate constraints of some markets and is estimated to range between $500 million and $1 billion per program. These estimates represent theoretical maximums per program and assume the federal terrorism insurance backstop through TRIPRA will continue.

Just as primary insurance underwriters consider account specifics in their decisions to deploy capital, available reinsurance capacity depends on individual insurers' portfolio characteristics. Insurers with significant property and workers' compensation accumulations in Tier 1 cities should expect to have less access to reinsurance capital than those portfolios with exposure in Tier 2 and Tier 3 cities and regions.

Furthermore, should TRIPRA expire or renew at the end of 2020 with substantial increases imposed to insurer net retentions, multiple carriers would likely enter the private reinsurance market simultaneously. The impact this could have on aggregate US reinsurance sector capacity and market pricing is unknown.

According to a Guy Carpenter reinsurance capital study, dedicated global capital to the combined US insurance and reinsurance market is estimated to be approximately $700 billion. Despite this ample capacity, however, there is not sufficient capital available to provide comprehensive terrorism coverage, including for NBCR risks, throughout the US without the federal TRIPRA backstop. Catastrophe models that produce NBCR event scenarios estimate that losses from a large nuclear attack in Manhattan (at greater than $900 billion for property and workers' compensation) could likely exceed the total amount of dedicated US reinsurance market capital.

Terrorism Risk Affects Other Insurance and Risk Management Strategies

Concerns About Cyber Terrorism on the Rise

Traditionally, criminal organizations have carried out the majority of cyber-attacks, with most incidents failing to register on an enterprise risk scale in which businesses faced significant setbacks. In 2017, this dynamic changed with the WannaCry and NotPetya incidents. These two attacks affected organizations in more than 150 countries, prompted business interruption and other losses estimated at well over $300 million by some companies, brought reputational damage, and resulted in loss of customer data.

In December, the US government took a rare step and attributed the WannaCry attack to hackers backed by North Korea. WannaCry and NotPetya exposed a systemic risk and affected a broad cross-section of businesses without specific targeting, demonstrating the potential for escalation in the threat of cyber terrorism:

1. The landscape for points of attack is growing. Traditional physical processes carried out by industrial control systems — including critical infrastructure industries such as power utilities, water treatment services, and health and emergency systems — are coming online. Marsh sister company Oliver Wyman forecasts that 30 billion connected devices will be in use by 2030, creating more assets to be attacked and vulnerabilities to be exploited.

2. Cyber threats are becoming more sophisticated. The emergence of highly sophisticated hackers, often nation-state supported, coincides with the growing prevalence of sophisticated tools that are likely seeping into the broader environment through a thriving black market.

3. The consequences are high. Companies are now deeply dependent on their systems and data, and interference with those assets can materially affect market capitalization and endanger executive leadership, reputations, sales, and profits. Failures in cybersecurity have the potential to destabilize an enterprise overnight.

Another recent cyber-attack, against a petrochemical facility in the Middle East, suggests that actors backed by nation-states may now also be targeting industrial safety and control systems, with the potential to inflict physical damage and/or bodily injury.

A hostile government that is determined to compromise key corporate systems and networks will likely prevail. Businesses have little control over the expansion of cyber threats, but they can take steps to strengthen their cyber resilience, including scenario-based testing, quantifying the potential financial impact of an attack, and reviewing options for transferring the financial risk from cyber-attacks via insurance.

Over time, cyber insurance policies have evolved to cover the failure of technology and the resulting interruption or loss of revenue in addition to traditionally important privacy risks. In addition, in 2016, the US Treasury Department issued guidance clarifying that cyber insurance policies are included under TRIPRA, providing a critical federal backstop for covered cyber-terrorism losses. As experts struggle to differentiate espionage, cyber vandalism, cyber terrorism, and cyber war, insurance markets are responding with cyber insurance policy wording that provides broader coverage. Moreover, insurers and buyers are increasingly recognizing the growing vulnerability of technology systems. As such, many cyber policies now contain business interruption and contingent business interruption provisions. In 2017, 70% of US cyber insurance buyers included business interruption in their cyber policies, according to Marsh data.

Political Violence and Political Risk Insurance Can Help Close Gaps

For multinational businesses, the current turbulence in the geopolitical landscape translates into a variety of political risks, prompting some to explore political violence insurance (PVI). While standalone property terrorism insurance provides coverage for the physical damage and business interruption that can result from acts that are motivated by politics, religion, or ideology, PVI provides coverage related to war, civil war, rebellion, insurrection, coup d'état, and other civil disturbances.

Purchasing terrorism and/or PVI coverage alone can potentially leave some buyers — especially those with assets in developing countries — with gaps in coverage, as potential risks can extend beyond the threat of violence. Global businesses may have the option to buy broader political risk insurance coverage, which can help avoid disputes between terrorism and PVI insurers and bridge gaps between the two policies. PVI coverage can be included in political risk insurance policies, which can cover a range of other perils related to government actions and instability, including expropriation of assets, forced abandonment, currency inconvertibility, nonpayment, contract frustration, and terrorism.

KIDNAP AND RANSOM INSURERS FACING CYBER CLAIMS

Although kidnappings and extortion plots globally are most often perpetrated by criminals, terrorist organizations also engage in such activity. In 2017, militants — including terrorists and other armed groups — carried out 47% of all kidnappings in the Middle East and North Africa, 23% in sub-Saharan Africa, and 17% in Asia Pacific.[7] Common perpetrators of politically motivated kidnappings include the Islamic State, Al-Qaida, and Abu Sayyaf, a Philippines-based separatist group.

Kidnap and ransom (K&R) insurance generally responds to the costs of kidnappings. A K&R policy is typically triggered upon an insured's receipt of an extortion demand and can reimburse an insured in the event it chooses to pay a ransom. K&R coverage can also reimburse for extra expenses, medical costs, rest and rehabilitation for affected employees, and legal fees and liability, including costs incurred in litigation brought by employees (for example, alleging that their employers did not provide adequate security).

Recently, K&R insurers have seen significant cyber losses stemming from ransomware attacks. Although ransomware demands are often small — under $1,000 — forensic accounting and reputation management costs can be much higher. K&R policies have expanded over time to cover cyber exposures, but the marketplace did not anticipate such a high volume of claims. The recent surge in ransomware losses has many K&R insurers seeking to restrict coverage for cyber losses.

Global businesses should consider purchasing K&R coverage in coordination with terrorism, political violence, political risk, and cyber insurance coverage decisions.

7 Control Risks.

PVI and political risk insurance policies should be coordinated with property and/or standalone terrorism policies and local insurance pools. To help design an effective insurance program regarding political violence and related risks, organizations should:

- Review asset locations.
- Understand policy terms, conditions, and limitations.
- Ensure purchased limits are adequate for multiple loss scenarios.
- Understand their property and employee exposures.

For more on political risk threats for multinational businesses, view Marsh's interactive Political Risk Map 2018.

Terrorism Insurance Requirements for Workers Vary by Region

As attacks by "lone wolves" and small groups become more commonplace, employers are increasingly concerned about terrorist incidents occurring in or near their workplaces.

UNITED STATES

In the US, employers are required, with rare exceptions, to purchase workers' compensation insurance. Unlike with other coverages, workers' compensation insurers cannot exclude terrorism-related losses. Although pricing and availability were affected in late 2014 by uncertainty over the fate of the federal backstop, market conditions have generally reverted to historical norms since TRIPRA's 2015 reauthorization.

Workers' compensation underwriters carefully manage their overall portfolio. Large employee concentration exposures and the associated loss potential are key factors in workers' compensation underwriting and pricing of terrorism risk.

The quality of the data provided to underwriters can make a significant difference in how insurers evaluate an organization's terrorism risk — and thus how that risk is priced. Detailed exposure data can help employers differentiate their risk profiles. It also enables insurers to understand employers' risk profiles in the context of their overall workers' compensation book and correlating risks, including property, personal lines, and life insurance.

Simple payroll data by location, however, is unlikely to suffice, and employers should provide such details as:

- The number of shifts per location and employees assigned to each.
- Detailed address information, including ZIP codes.
- Employee locations on campuses.
- The number of telecommuters.
- Details from swipe cards showing the actual or maximum number of employees present at each location or building on a given day.

Because it is compulsory, employers need to secure workers' compensation coverage through some combination of private market solutions, state funds, assigned risk pools, and qualified self-insurance. There is no standalone terrorism insurance market for workers' compensation, meaning the support of TRIPRA is essential for employers most in need of the coverage. Absent TRIPRA, demand for coverage could easily begin to outpace the supply of available capacity.

OUTSIDE OF THE US

Compensation systems and requirements regarding workplace injuries vary by country, and even within a country.

Generally, there are three types of insurance or government-provided benefits for employment-related injuries and illnesses: workers' compensation, employers liability, and personal accident.

Employers are often legally required to secure workers' compensation for some or all employees. In many countries, it is provided through government programs; in others, employers must secure it. Employers may also purchase discretionary coverages — such as employers liability and personal accident insurance — to expedite workers' recovery and to protect companies from lawsuits.

The provision of compensation for medical care and lost wages for terrorism-related injuries will depend on the system in place in the worker's country of hire and/or work. Expatriate employees present a unique situation: They may seek coverage in their home country, their country of work, both, or possibly neither. When and where specific programs will apply to an expat will depend on local laws and policy terms, and could depend on:

- The employee's nationality (country of origin).
- Where payroll is reported (country of hire).
- The length of the employee's work assignment.

Workers' compensation policies issued to the parent company or "local" operations in other countries alone may not address the exposures associated with multinational enterprises and a transient workforce. To help address potential gaps, foreign voluntary workers' compensation (FVWC) coverage in the US extends state-based coverage for employees working outside of their country of origin and provides coverage for foreign employees on assignment in the US. FVWC is customarily purchased by US-based multinationals and secured primarily within their workers' compensation policies, with additional coverage and limits provided by a controlled master program (CMP) and umbrella and excess liability insurance.

Employers liability coverage defends and indemnifies employers from lawsuits brought by workers for injuries arising out of the course of their employment within the policy territory. Similar to FVWC, it is provided in the US as part of workers' compensation insurance. Outside of the US, the coverage may be found as an endorsement on local workers' compensation or general liability policies or purchased on a standalone basis. Coverage under employers liability is customarily included in umbrella or excess liability policies.

Employers will often purchase **personal accident insurance** coverage to supplement local workers' compensation benefits or as an employee benefit program.

Coverage for injuries and illnesses due to acts of war or terrorism may differ depending on which insurance policies are in place, which are triggered and, for workers' compensation, whether the law extends coverage to such events.

For compulsory workers' compensation coverage, terrorism is typically provided due to the broad extent of coverage under the law or by specific laws. In Belgium, for example, a 2007 law mandates terrorism coverage for workers' compensation and other insurances, including strict liability for fire and explosion damage in public premises. Such coverage was triggered by the 2016 Brussels bombings, with claims accounting for over €100 million. Nearly 43% of claims under the country's Terrorism Risk & Insurance Pool were attributed to workers' compensation.

In other countries, government-provided benefits are broad and may not distinguish the cause of injury or illness in determining eligibility. For example, in South Africa, benefits under the Compensation for Occupational Injuries and Diseases Act are administered by the government, and injuries or illnesses due to terrorism are understood to be covered.

Terrorism coverage under compulsory workers' compensation is dependent on local laws. While such coverage appears to be common, multinational employers should investigate the situation in each jurisdiction.

For discretionary insurance, such as FVWC, employers liability, and personal accident policies, terrorism coverage is typically not required and may be excluded by default. Coverage for terrorism can typically be added by endorsement, usually for an additional premium. However, terrorism is generally not excluded for FVWC policies placed in the US. Multinationals based in the US should review their general liability CMP and other umbrella or excess liability policies for coverage.

As part of an effective terrorism risk management program, employers should consider local insurance regulations along with the size, concentration, and significance of their workplace injury exposure in the countries in which they operate.

Shifting Terror Tactics Highlight Third-Party Liability Concerns

Changes in attack methods have raised awareness of potential third-party liability for businesses stemming from acts of terrorism. Vehicle-based incidents in Barcelona, Berlin, London, New York, Nice, Stockholm, and elsewhere highlight the possibility that a business's vehicles could be used in an attack. The Manchester and Paris bombings demonstrated that sports and entertainment venues remain "soft" targets.

In the US, two federal laws can help to limit businesses' potential third-party liability:

Graves Amendment: Signed into law in 2002, 49 USC § 30106, also known as the Graves Amendment, eliminates vicarious liability for car rental companies and other companies "engaged in the trade business of renting or leasing motor vehicles." According to the law, these businesses will not be liable "for harm to persons or property that results or arises out of the use, operation, or possession of the vehicle during the period of the rental or lease," provided that they have not been negligent or committed criminal wrongdoing.

SAFETY Act: Many organizations have sought to limit their liability by seeking protection under the Support Anti-Terrorism by Fostering Effective Technology Act (SAFETY Act). Introduced as part of the Homeland Security Act of 2002, the SAFETY Act allows sports organizations to apply for tort protection from the US Department of Homeland Security (DHS) for the physical and cyber security systems and security protocols, procedures, and policies used to protect facilities and assets. Awardees may receive substantial tort protection, including exclusion of punitive damages, favorable forum selection, and capped liability.

More Captives Insuring Terrorism Risk

Captive insurers can generally offer broader coverage than is available through policies issued by commercial insurers. By using a captive to access TRIPRA coverage or to supplement coverage purchased from commercial insurers, organizations can cost-effectively manage their net retained terrorism risk. Nevertheless, although captives can offer coverage for terrorism, many do not — or do not do so optimally.

Captive owners often find that the total cost of implementing terrorism insurance programs compares favorably to the cost of buying from commercial insurers. And they sometimes find a captive is the only viable option, such as when seeking to secure significant limits for NBCR attacks. Although TRIPRA guidance states that the federal backstop provides reinsurance protection to insurers that experience NBCR losses, insurers are not required under the law to offer the coverage. The lack of a TRIPRA mandate for NBCR has resulted in coverage not being widely available in the traditional insurance marketplace. Captive insurers are able to offer this coverage and gain access to reinsurance protection afforded by TRIPRA.

Captives are also a viable means for some companies to insure cyber terrorism. In December 2016, the US Treasury Department ruled that subject insurers that write cyber policies are included under TRIPRA. Businesses often conclude that using a captive to write cyber terrorism risk is a cost-effective and relatively easy way to reduce net retained risk, especially for companies that already own captives.

From 2016 to 2017, the number of Marsh-managed captives actively underwriting one or more insurance programs that access TRIPRA increased 44%, from 115 to 166. Through a captive, organizations can customize coverage and avoid some of the common restrictions or exclusions in commercial insurance policies, including for:

- NBCR attacks.
- Contingent time-element losses.
- Cyber terrorism.

INTEREST INCREASES FOR NON-PHYSICAL DAMAGE BUSINESS INTERRUPTION

Following multiple high-profile terrorist attacks, mass shootings, and natural catastrophes in 2017, demand for non-physical damage business interruption (NDBI) coverage increased. Terrorist attacks in major cities in recent years along with the October 2017 mass shooting in Las Vegas contributed to a loss of revenue for hospitality and entertainment companies, airlines, and others tied to tourism. For example, following terrorist attacks in January and November 2015, visitors to the greater Paris region fell by 1.5 million, and tourism-related revenues fell €1.3 billion in 2016.[8]

NDBI policies can provide coverage for loss of revenue even without a physical damage coverage trigger, but often have limitations. Many NDBI policies will respond only if a triggering event is officially classified as a terrorist attack or a civil or military authority prevents or impairs access to an insured’s property.

Insurers have expanded their offerings in this area, developing specialty products that offer contingent business interruption protection to supplement traditional standalone property terrorism policies.

8 Paris Region Tourist Board.

Terrorism Risk Modeling Poses Challenges

Terrorism risk modeling methods have been continually updated since leading modeling companies AIR Worldwide (AIR) and Risk Management Solutions (RMS) released their first terrorism models in 2002. Quantifying the economic, insured, and human losses from terrorist attacks poses major challenges for insurers, reinsurers, and alternative capacity providers. There are three main techniques to model terrorism risk:

- Probabilistic modeling estimates losses based on a large number of events. Due to the difficulty in predicting the probability of terror events, there is considerable uncertainty associated with this approach.

- Exposure concentration analysis identifies and quantifies concentrations of exposures around potential targets. Target-based accumulation assessments use predetermined targets (typically with high economic, human, and/or symbolic value) and aggregate an insurer's exposures at various distances from targets.
- Deterministic modeling represents a compromise between the two models. By imposing an actual event's damage "footprint" at a specified target, a specific yet hypothetical scenario can be analyzed with some certainty.

Compared to the modeling of natural hazards such as hurricanes and earthquakes, terrorism risk modeling poses unique challenges. Insurers, reinsurers, and modeling companies constantly refine their models and underlying assumptions, thereby increasing their ability to manage terrorism risk quantitatively. Currently, deterministic, scenario-based testing is the most common tool used by insurers and reinsurers to assess their exposure to terrorism risks.

As terrorism risks and attack methods evolve, businesses also use risk models and other analytical tools to:

- Simulate customized attacks to determine the expected impact to overall portfolios or specific locations.
- Determine appropriate insurance deductibles and limits.
- Optimize risk finance strategies.
- Rate terrorism risk to negotiate insurance premiums.
- Understand potential impact on capital.
- Build efficient business continuity plans.
- Address terrorism risk aggregation.
- Prioritize risk mitigation strategies.
- Make informed decisions on implementing loss control measures.

Crisis and Response Management is Crucial

The threat of violence resulting in mass casualties, including from terrorist acts, underscores the need for businesses to develop, maintain, and exercise corporate and site-level crisis management plans that address communications, emergency response, and business continuity.

Organizations should develop and test an overall framework and crisis management team structure for management, response, and recovery at the senior executive level. Following an incident, organizations must move quickly and efficiently to understand the impacts to people, property, and operations and to make policy and strategy decisions to address and manage those impacts.

Following an attack, organizations should be prepared to:

- Contact employees, their families, customers, investors, and other stakeholders. During an incident, communications should reinforce the crisis management team's overall strategies and decisions.
- Ensure the safety of employees and others via evacuations or sheltering-in-place and protect physical assets and the environment.
- Provide physical, social, emotional, financial, and other support, such as counseling and other services.
- Keep the business running once life safety issues have been addressed. Plans should account for the management and logistical process for continuing or resuming critical processes and functions.
- Ensure that technology is running. In a technology-driven age, disaster recovery plans should address the availability and recovery of networks, applications, and data.

ADDRESSING BUSINESS INTERRUPTION RISK

A terrorist attack can cause significant business interruption losses. Among other actions, businesses can manage this risk by:

- Developing and testing business continuity plans.
- Testing scenarios that could have direct or indirect impacts on businesses.
- Coordinating business interruption insurance with coverage of political violence, terrorism, and other related risks.
- Being prepared to gather appropriate information to support a claim, including recording damage via photographs and video.
- Maintaining separate accounting codes to identify all costs associated with the potential damage.

Conclusion

The cost of a terrorist attack for a business can be high, but the nature of terrorism losses is changing. Incidents that create significant property damage have declined in frequency, while mass casualty events involving vehicles, handheld weapons, and small, improvised attacks now occur more often.

The terrorism insurance market continues to innovate to meet the evolving needs of buyers across several industries and appears well capitalized. But public-private solutions, such as the one provided through TRIPRA in the United States, remain essential to continued market stability and health. As policymakers evaluate potential options as TRIPRA's expiration at the end of 2020 approaches, we expect discussions to focus on the merits of the law as a means to expand the private insurance market role in managing conventional acts of terrorism while also providing a critical backstop for large-scale and unconventional attacks.

Organizations of all sizes must remain vigilant and develop effective preparedness and business continuity plans while considering a variety of potential risk transfer options to limit the effects of terrorism on their operations.

Appendix

Industry Categories

This report examined property terrorism insurance purchasing patterns for 17 industry sectors, selected based on such criteria as sample population size, perceived exposures, take-up rates, and premium rates. Other industry groups were part of the overall analysis, but not reported on individually. The industry groupings included, but were not limited to, the following:

- Chemicals: specialty chemicals, agrochemicals, distributors, industrial gases, and personal care and household companies.
- Construction: contractors, homebuilders, and general contractors.
- Education: colleges, universities, and school districts.
- Energy and mining: oil, gas, and pipelines, mining and primary metal industries.
- Financial institutions: banks, insurers, asset managers, and other securities firms.
- Food and beverage: manufacturers and distributors.
- Hospitality and gaming: hotels, casinos, sporting arenas, performing arts centers, and restaurants.
- Health care: hospitals and managed care facilities.
- Life sciences: research, manufacturers, biotechnology, and pharmaceuticals.
- Manufacturing: all manufacturers, excluding aviation.
- Media: print and electronic media.
- Public entity and nonprofit: city, county, and state entities and nonprofit organizations.
- Real estate: real estate and property management companies.
- Retail and wholesale: retail entities of all kinds.
- Technology/telecom: hardware and software manufacturers and distributors, telephone companies, and internet service providers.
- Transportation: trucking and bus companies.
- Power and utility: public and private gas, electric, and water utilities.

Methodology

The report analyses relied on aggregated data concerning Marsh clients that purchased property terrorism insurance across the US. Purchasing patterns were examined in the aggregate and were also based on client characteristics such as size, industry, and region.

The 2018 data came from property insurance placements incepting during calendar year 2017. The study population does not include placements in the US for foreign-based multinationals or for small-firm placements made through package policies.

The 2018 study was based on a sample of more than 2,000 companies with the following characteristics:

	1st Quartile	Median	3rd Quartile
Tiv	$56 million	$241 million	$1,078 million
Property Premium	$77,250	$235,000	$768,581
Terrorism Premium	$2,417	$6,518	$22,563

It is important to note:

- For some companies, insurers quoted only a nominal terrorism premium of $1. These $1 premiums were omitted from calculations of median terrorism premium rates.
- Companies were assigned to regions based on the locations of the Marsh offices that served them. Generally, this was the Marsh office most closely located to a company's headquarters. Many clients have multiple locations across the US and around the world, meaning the potential risk for a terrorist attack may not be fully represented by where a company is headquartered. That said, the decision as to whether to purchase terrorism insurance is typically made at headquarters.

Notes

Notes

ABOUT THIS REPORT

This report was produced by Marsh's Property Practice, with contributions from:

- Marsh's Casualty Practice.
- Marsh's Credit Specialties Practice.
- Marsh Captive Solutions.
- Marsh's FINPRO Practice.
- Marsh Digital, Data & Analytics.
- Marsh Multinational Client Service.
- Marsh Risk Consulting.
- Guy Carpenter.

ABOUT MARSH

A global leader in insurance broking and innovative risk management solutions, Marsh's 30,000 colleagues advise individual and commercial clients of all sizes in over 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy, and people. With annual revenue over US$14 billion and nearly 65,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading firms. In addition to Marsh, MMC is the parent company of Guy Carpenter, Mercer, and Oliver Wyman. Follow Marsh on Twitter @MarshGlobal; LinkedIn; Facebook; and YouTube, or subscribe to BRINK.

ABOUT GUY CARPENTER

Guy Carpenter & Company, LLC is a leading global risk and reinsurance specialist with more than 2,300 professionals in over 60 offices around the world. Guy Carpenter delivers a powerful combination of broking expertise, trusted strategic advisory services and industry-leading analytics to help clients adapt to emerging opportunities and achieve profitable growth. Guy Carpenter is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With nearly 65,000 colleagues and annual revenue over $14 billion, through its market-leading companies including Marsh, Mercer and Oliver Wyman, Marsh & McLennan helps clients navigate an increasingly dynamic and complex environment. For more information, visit www.guycarp.com. Follow Guy Carpenter on Twitter @GuyCarpenter.

For more information, please contact your Marsh or other Marsh & McLennan Companies representative or:

TARIQUE NAGEER
Terrorism Placement Advisory Leader
Marsh's Property Practice
tarique.i.nageer@marsh.com
+1 212 345 5073

MATTHEW MCCABE
Senior Vice President and Assistant General Counsel on Cyber Policy
Marsh's FINPRO Practice
matthew.p.mccabe@marsh.com
+1 212 345 9642

CHRIS A. VARIN
Managing Director
Marsh Captive Solutions
chris.a.varin@marsh.com
+1 802 864 8133

EMIL METROPOULOS
Workers' Compensation &
Terrorism Specialty Practice Leader
Guy Carpenter
emil.metropoulos@guycarp.com
+1 203 229 8817