# INSURING AGAINST TERROR: SOME COMMON COVERAGE BLIND SPOTS

Date: 4 December 2017

**UK Insurance Coverage Alert**

By: Sarah Turpin, Alexander J. Bradley-Sitch

In her speech at Mansion House in July earlier this year, Metropolitan Police Commissioner Cressida Dick said that the occurrence of terror attacks in the United Kingdom is a case of "when not if". She was speaking in response to a series of high-profile acts of terrorism which had taken place in the first half of 2017, which, combined, resulted in the deaths of 36 people.

It is therefore timely that Pool Re, the UK Government-backed terrorism reinsurer, has published its third Terrorism Threat and Mitigation Report. The Report analyses trends in global terrorism and identifies prevailing difficulties in the terrorism-related insurance market.

The Pool Re Report notes that current levels of terrorism in the UK are unprecedented with four attacks in a 17 week window earlier in 2017. The methods deployed by terror groups continue to evolve and respond to counter-terrorism efforts but the "fundamental principles" remain the same: to kill and cause damage for publicity so as to cause terror. In this regard, the effects of terrorism are widely felt. As well as causing significant causalities, recent terror incidents have had a notable impact on businesses and the wider economy.

Terror-related losses are risks which businesses can protect themselves against with appropriate insurance. Often companies do not have sufficient insurance in place, if they have any at all. According to the Pool Re report, take up of terrorism insurance is relatively low, particularly among SMEs, of which as few as ten per cent have purchased coverage.

Where insurance is obtained, it is not always comprehensive or protective against modern threats. A common assumption among policyholders is that their commercial property insurance will provide coverage for terror-related risks. Generally, commercial property insurance can exclude or restrict recovery for terror-related losses, and cover for such risks is frequently sold as a discrete, specialised product.

Another potential obstacle to recovery is that some policies require physical property damage as a trigger to the insurer's liability. As demonstrated by this year's attacks at London Bridge in June, and at La Rambla in Barcelona this August, losses flowing from actual property damage are often minimal. Instead, financial losses are often sustained as a result of "considerable business interruption and denial of access caused by extensive cordons, with the possibility of further loss to the economy and business from a reduction in future visitor numbers". In response to this, "denial of access" cover is more frequently included in business interruption and property policies but Pool Re notes that there remains a coverage gap. Policyholders should be alert to what kind of

triggers or onerous conditions their terrorism cover may have and, with that in mind, they should consider whether they are sufficiently protected.

The risks which a business should consider seeking coverage for will depend on a number of factors. Policyholders should consider undertaking a thorough risk assessment to determine what their vulnerabilities are likely to be. Some sectors face greater risks than others, and the types of risks and loss to which they are vulnerable will be highly sector and location specific.

By way of example, the aviation sector continues to be a prime target for terror groups, as the Pool Re report points out. Airlines are already bound by regulations regarding the type and scope of coverage they must have to operate. Besides carriers, other businesses which depend on the aviation sector are potentially vulnerable. Organisations which operate in or around airports (or whose business depends on the sector running smoothly) will want to ensure they are prepared for every eventuality.

Regardless of industry or sector, a terrorism risk assessment is likely to highlight any particular vulnerabilities. In conjunction with an insurance policy wording review, coverage gaps can be addressed and potential economic risks minimised.

In terms of location-specific risks, it remains the case that cities are more likely to be targeted by terrorists than remote or rural areas because of the density of potential targets, and the publicity they garner. Businesses should be conscious of any nearby symbolic or high-profile landmarks which attract crowds as well as major infrastructure and governmental buildings, all of which are more likely to be targeted. It is critical to consider how businesses could be affected if, for example, a police cordon is set up or travel restrictions imposed in the area surrounding their place of operations.

In more recent developments, Pool Re notes that cyber threats are becoming more common, and increasingly high profile. Such tactics are being used both by terror groups and state actors to disrupt business and infrastructure, and to enable and encourage terror globally. The market for cyber risk insurance coverage is still developing. Nevertheless it is becoming an essential aspect of many commercial insurance programmes. The Pool Re report states that "cyber attacks were estimated to cost businesses as much as $450 billion a year globally", and there are few, if any, sectors which are not vulnerable in some way.

The types of larger-scale cyber attacks which attract the most media attention are - for now - more likely to be caused by state actors than terror groups. One such example was the WannaCry attack on the NHS in May 2017, which Pool Re report explains was "likely to have been state sponsored and not terrorism". Terror groups, by contrast, currently prefer "enabling" tactics (disseminating information for the purposes of recruiting members and instructing them in committing acts of terrorism) to "disruptive" tactics (the stealing of money or data; dissemination of malware; or disruption of services and networks).

Whether cyber tactics are deployed by lone activists, established terror groups or hostile states, the consequences for affected businesses can be disastrous. Ultimately, cyber attacks can lead to: loss of confidential data or valuable intellectual property; interruption of business functions; reputational harm and

reduced customer confidence; and regulatory sanctions and fines. Indeed, with the entry into force of the General Data Protection Regulation in May 2018, the potential costs to businesses with inadequate protections are even more significant (breaches can lead to fines being imposed of as much as the higher of 4 per cent of global annual turnover, or €20 million).

Looking to the longer term, the Pool Re report highlights the fact that terror groups do not currently deploy "destructive" cyber tactics with any sophistication or regularity. Destructive cyber attacks are intended to cause physical damage or disable physical infrastructure, for example by hijacking control of power grids. The evolving nature of cyber terrorism means organisations should be prepared for this risk to grow. Reflecting this, from 1 April 2018, Pool Re will be able, for the first time, to grant cover "for physical damage caused by terrorists using a cyber-trigger to cause a fire or explosion".

For many businesses, the risks presented by terrorism may never materialise but, if they do, the consequences can be far-reaching. For peace of mind, it is important for each business to ensure that it has assessed its vulnerabilities and obtained the right insurance cover, tailored to meet the specific risks and vulnerabilities of the particular organisation.

You can view the full Pool Re Terrorism Threat and Mitigation Report here: https://www.poolre.co.uk/terrorism-threat-mitigation-report-january-july-2017/.

For more information about any of the topics discussed in this alert, or to learn more about the insurance coverage services which K&L Gates can provide, please contact one of the lawyers listed below.

## KEY CONTACTS

**SARAH TURPIN**
PARTNER

LONDON
+44.20.7360.8285
SARAH.TURPIN@KLGATES.COM



 