



thinkpiece

Promoting debate and fresh thinking in the financial services industry

Responding to the terrorist threat: Implications for UK businesses and insurance

Raffaello Pantucci

Summary

- As events in Mumbai in late 2008 have indicated, the terrorist threat to the UK as well as British interests abroad remains at a very high level. Virtually all aspects of the UK economy, but particularly high profile business and economic hubs such as the City of London, remain under threat of attack.
- While Al-Qaeda seems to have a preference for high profile, mass casualty attacks attracting maximum attention such as 9/11 and the Madrid bombings; recent attacks or foiled attempts have indicated that not all targets fall into this category.
- Although the threat is real and constant, it is not overwhelming and it is a risk that can be managed through preparedness and vigilance. Firms must understand the nature of the risks they face and take appropriate precautions to protect operations and staff. This article helps by setting out a 12-point action plan of specific measures, and signposts resources that offer further assistance.
- The insurance industry too can contribute to preparedness, both through the Pool Re system and by incentivising firms to take precautions through terrorism insurance cover.

Number 11 (January 2009)

The Chartered Insurance Institute is the world's largest professional body for insurance and financial services and is the leader in awarding qualifications to industry practitioners. Our thinkpieces are a key part of our ongoing commitment to promoting innovative thinking and debate within the insurance and financial sectors.

The views expressed within the article are those of the author and should not be interpreted as those of the Chartered Insurance Institute and its members. The author has asserted his right under the Copyright, Designs and Patents Act 1988 to be identified as the author and copyright owner of the text of this work, and has granted the CII worldwide perpetual licence to reproduce and distribute it in whole and in part. We welcome suggestions from potential contributors, but we are also seeking feedback from our readers. We urge you to get involved—especially as we intend some of our articles to be open to rebuttals for publication.



CII Group



CII Introduction: last month's Mumbai terrorist attacks were a reminder that the international terrorist threat remains real and varied. While the security services work to prevent further atrocities, the corporate world and the insurance industry can also help by demonstrating that business would go on should another attack occur. The CII itself is organising a workshop for its members in the London Market in February to review such threats, and other businesses as well should be take advantage of the advice resources available by the government. In this latest article, Raffaello Pantucci of the International Institute of Strategic Studies examines some realities around the terrorist threat and shows how the risks can be managed by firms and the insurance industry.

In early October 2008, the government released information to the media that it was planning to revamp its counter-terrorism strategy. Along with this information, journalists were given a briefing as to the state of the threat and were told that currently the threat assessment from terrorism in the UK was "at the severe end of severe."¹ In counter-terrorism parlance, "severe" means that "an attack is highly likely."² Yet, since the terrible events of July 2005, the UK has not experienced a successful terrorist attack, and such statements might be seen by some as alarmist.

However, as events in Mumbai last year show, British nationals remain threatened abroad, and according to the head of MI5, "the strategic intent of the Al Qaeda core in Pakistan is to mount attacks in the UK." This article starts by examining exactly how real the terrorist threat is including what it might look like. Then it considers what might be most at risk and the potential costs of an attack. Finally it explores what business can do to insulate itself against the threat and establish good business continuity planning.

What is the threat?

The IISS believes the threat to the UK, as well as British interests abroad, remains very real. In his first public speech, Jonathan Evans, the Director General of the UK Security Service (MI5), declared that the

¹ Richard Norton-Taylor, "Security Officials plan to combat of lone terrorist," *Guardian*, October 3, 2008 – but it should be highlighted that the same quote appeared in a number of different sources.

² The threat levels are set by the Joint Terrorism Analysis Centre (JTAC), for more information: www.mi5.gov.uk/output/Page63.html

security service had identified at least 2,000 individuals who they believe pose "a direct threat to national security and public safety." In addition, he speculated "that there are as many again that we don't yet know of" – meaning that MI5 believes there may be as many as 4,000 individuals of concern in the United Kingdom.³ These figures have been further broken down into 200 networks and 30 plots.

To understand what exactly confronts MI5, it is instructive to look to another of their reports, this one leaked to the media that surveyed some 300 case studies of individuals involved in terrorist activity in the UK. The report, produced by the Service's Behavioural Science Unit and entitled "Understanding Radicalisation and Violent Extremism in the UK," highlighted the fact that Britain's terrorist threat was made up of individuals who were for the most part "demographically unremarkable." While the majority are male, in their 20s, and of South Asian origin (either as first or second generation children of immigrant families), this is by no means a complete picture with individuals drawn into violent extremist activity from all ethnic backgrounds, older and younger, and both genders. Some of these individuals are loners, but this tends to be the exception rather than the norm, with many seemingly well-adjusted to a middle class lifestyle with families and jobs.⁴

The main conclusion to draw from the report is that there is no single profile for a British terrorist, nor is there a single pathway to radicalisation. The report identifies a number of "key vulnerabilities" but ultimately casts a very wide net in our society which MI5 narrows down to the fact that those who go on to get involved in terrorist activity tend to have come "into contact with existing extremists who recognized their vulnerabilities."⁵

Thus far, while some "lone wolf" terrorist plots have been uncovered, it predominantly seems as though many plots have an external connection of some kind. For example, the 7/7 bombings, the subsequent 21 July 2005 attempt, the so-called "fertilizer plot" group arrested in 2004,⁶ and the August 2006 Transatlantic Airlines plot group all appear to have connections to the Al Qaeda core in Pakistan.

³ Jonathan Evans, "Intelligence, counter-terrorism and trust," Address to the Society of Editors in Manchester, November 5, 2007, www.mi5.gov.uk/output/Page562.html

⁴ Alan Travis, "MI5 report challenges views on terrorism in Britain," *Guardian*, August 21, 2008

⁵ Alan Travis "The making of an extremist," *Guardian*, August 20, 2008

⁶ Dubbed *Operation Crevice* after its police codename, the plot implicated five men, mostly second generation Pakistani, of plotting to blow up a 600kg bomb made out of fertilizer in an unspecified location thought to be the Bluewater Shopping Centre or the Ministry of Sound nightclub.

What are the targets?

Al Qaeda has a preference for high profile, mass casualty attacks attracting maximum media attention. From a business perspective, this means you are most at risk if you operate in an iconic building or are operating in a foreign country and are a visible foreign brand. Aside from the infamous 9/11 attacks on the United States which specifically targeted its military (the Pentagon), and its wealth (the World Trade Center in New York), other examples include:

- 15 and 20 November 2003: four truck bombs later claimed by Al Qaeda were detonated in the Turkish city of Istanbul. Targets included synagogues, the British consulate and HSBC bank headquarters in the city. 30 were killed including consul general Roger Short, and 400 injured.
- August 2003: Al Qaeda affiliate Jemaah Islamiyah attacked the American-brand Marriot hotel chain in Jakarta with a suicide truck bomb 11 people were killed and an unknown number injured. Subsequent investigation uncovered that the plotters had contemplated targeting a local Citibank office as an alternate target.
- Late November 2008: a coordinated unit of 10 Pakistani-based terrorists on the Indian city of Mumbai targeted hotels and bars frequented by foreigners. During the course of the attack, reports emerged that the men were specifically targeting US, UK and Israeli nationals. 173 people were killed, including 30 foreigners, and at least 308 injured.

The most common target in Europe, however, would appear to be mass transportation systems, including:

- August 2004 *Operation Rhyme*: amongst targets, plotters were looking at the Heathrow Express and the London underground.
- 11 March 2004: attacks on Madrid's trains system, killing 191 and injuring 1,755.
- 7 July 2005: attacks on London's underground and bus network, killing 52 and injuring 700.
- 21 July: copycat attacks on London's buses and underground network – 4 bombs failed to go off
- August 2006 *Operation Overt*: an alleged plot to destroy eight airliners in transatlantic transit from the UK using liquid based bombs.
- 30 June 2007: Bilal Abdullah and Kafeel Ahmed drive an attempted car-bomb into Glasgow International airport. The day before they had left two car bombs outside a London nightclub.

Finally, the attack in May 2008 by mentally disabled Nicky Reilly, aka Mohammed Rasheed, who attempted to carry out a suicide attack on a Giraffe restaurant in Exeter shows the potentially extremely dispersed nature of the terrorist threat. Reilly's

device injured only him, but had it successfully exploded as intended, approximately 20 people could have been killed and dozens injured.

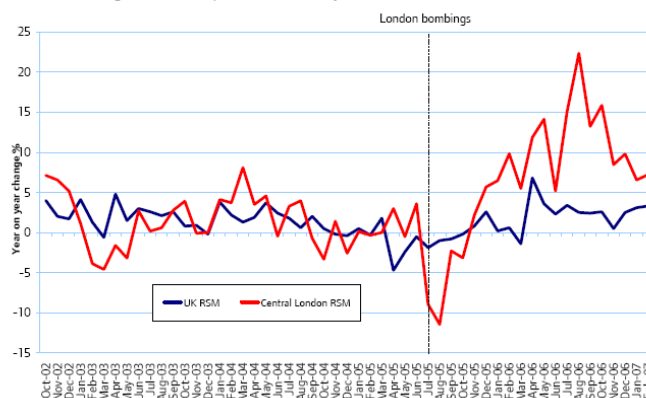
What is the cost?

It is very hard to put an absolute pound figure on the financial impact of terrorism. In three prominent cases, the 2001 attacks in America, the 2004 attacks in Madrid and the 2005 attacks in London, there is a clear dip in the financial markets in the immediate wake of the attacks, but these appeared to right themselves relatively soon afterwards. The story is slightly different if one looks to Bali, which was struck by a series of successive attacks on an annual basis over a period of years and saw a noticeable dip in tourism revenue over the same period – anecdotal evidence pointed to specific resorts suffering heavily in this regard.

“There was a clear dip in the financial markets in the immediate wake of the [New York, Madrid and London] attacks but these appeared to right themselves relatively soon afterwards.”

The retail sector can also be economically affected from a terrorist attack. The graphic below produced by the Greater London Authority (GLA) in 2007 shows the considerable short-term impact that the London bombings had on the city's retail sales.⁷

Annual % change, last data point is February 2007



Source: UK Retail Sales Monitor – BRC/KPMG, Central London Retail Sales Monitor – London Retail Consortium

Some further limited impact was felt in tourism numbers which apparently grew at a less elevated proportion than previous years, although others also blamed this on the depressed value of the dollar and high London prices. A report published in August 2005 by the London Chamber of Commerce and Industry entitled “The Economic Effects of Terrorism on London”⁸ seemed to show that a wide cross-

⁷ “London's Economic Outlook: Spring 2007,” GLA Economics

⁸ “The Economic Effects of Terrorism on London – Experiences of Firms in London's Business Community,”

section of London businesses had suffered little *long-term* ill effect. The most pronounced impact was an elevation of costs in the immediate aftermath of the attack as workers were unable to get to work or companies were obliged to pay for alternate modes of transportation for staff wary of using public transport – a fear that was accentuated by the almost identical attempt on 21 July. London transport reported a sudden 30% drop in passenger volume on the weekend after the attack, and a 5-15% drop in the subsequent week. On the other hand, companies offering courier services around the city noticed an up-turn in business.

“Before 9/11, the most expensive terrorist attack took place in April 1993 when the IRA bombed Bishopsgate in the City of London, resulting in an insured cost of \$907 million.”

All of these factors and trends are broadly reflective of the usual economic fall-out in the wake of such a terrorist attack. The bigger fear is that terrorists manage to achieve a spectacular on the scale of the 9/11 attacks, the November 2008 attacks on Mumbai India, or manage to detonate a chemical, biological, radiological, or nuclear (CBRN) weapon in a major city. Such attacks bring cities to a stand-still and in the case of a CBRN attack, might leave portions of a city uninhabitable for a period that could extend to years. In the case of the 9/11 attacks, the physical damage incurred to New York ended up either completely destroying or severely disrupting 14,500 businesses, with some financial firms based in the World Trade Centre complex having their operations almost completely wiped out. Before 9/11, the most expensive terrorist attack took place in April 1993 when the IRA bombed Bishopsgate in the City of London, resulting in an insured cost of \$907 million. Parts of the City were totally laid waste and Liverpool Street train station was put out of action for some time. While services were restored after a few days, in the instance of a successful CBRN attack on a major centre like the City of London, Canary Wharf or outside the UK, the period could be far longer and companies would potentially find themselves suddenly and abruptly unable to access their premises for an extended period of time.

Where are the possible costs to business generated by a terrorist attack?

The Centre for the Protection of National Infrastructure (CPNI) should be one of the first ports of call for any business leader seeking to understand how to effectively insulate against threats such as terrorism. They identify the following consequences as the first issues to bear in mind after a terrorist

attack. Understanding these will help assess what the actual cost of an attack is likely to be:⁹

- loss of staff through death or injury
- damage to your buildings
- loss of IT systems, records, communications and other facilities
- unavailability of staff because of disruption to transport or their unwillingness to travel
- adverse psychological effects on staff, including stress and demoralisation
- disruption to other organisations and businesses on which you may depend
- reputational risk for not taking precautions
- changes in the business demands placed on your organisation
- cost of business continuity

Furthermore, in the immediate wake of an attack, mobile telephone networks are almost invariably overwhelmed. In some cases, security services also tend to block mobile phones after an attack in an attempt to prevent them being used to detonate further planted devices. This can have a cost to companies attempting to operate. CPNI further identifies the following resources as essential to maintaining critical business functions, and must be factored in as they might generate further potential costs:

- sufficient people with the necessary expertise and motivation to lead and manage the organisation
- access to key records and IT systems
- reliable means of communication, especially with your staff
- the ability to carry on paying staff, to ensure their safety and to provide them with welfare and accommodation
- the ability to procure goods and services
- the ability to respond to media demands

What can be done?

This may seem contradictory within the context of this paper, but the key thing to bear in mind is that while the threat may be real and constant, it is nonetheless a risk that can be managed, rather than an *overwhelming* threat. A key aspect to effectively countering the threat is to demonstrate resilience – in other words, to have the ability to bounce back and continue life as normal in the wake of an attack.

London Chamber of Commerce and Industry, August 2005, www.londonchamber.co.uk/docimages/754.pdf

⁹ More on CPNI and its suggestions on how to effectively prepare can be found on their website: www.cpm.gov.uk/

At a more practical level, certain key actions should be taken now to ensure that your company is adequately prepared in the event of a terrorist attack. In most instances the measures suggested are basic security issues that are relevant more generally in any case:

1. Staff should be effectively screened, and managers should stay engaged with their staff.¹⁰
2. When building new properties, design security in – this does not mean unsightly concrete bollards everywhere, but some more subtle measures designed into structures which can considerably protect properties.
3. Make sure you have effective security measures to allow people into your property. If you share a property or have an underground car park, make sure that is also adequately secured.
4. Ensure you have a well developed and practiced Business Continuity Plan (BCP). While outside entities can be deployed to help construct it, the final product must be owned and understood by the company and rehearsed regularly.¹¹
5. Make sure you have spare points of contact and emergency lines of communication for staff.
6. Establish a safe room in your property that is away from windows (the majority of injuries in terrorist attacks occur from flying glass) that should be the first port of call for staff in the event of an attack. In a similar way to which properties carry out fire drills, companies should drill staff evacuation to this location.
7. Make sure you know who your neighbours are in surrounding buildings or properties. This may also help you establish whether a neighbour has a high profile and therefore risk potential on yourself. Establishing personal connections can also be useful in the event of an attack.
8. Be sure to know your complete supply chain – and make sure that you have alternatives so that you do not develop any chokepoints.
9. Similarly, make sure you know where your IT systems are located and make sure you have back-ups in alternate sites. Also, ensure your IT staff are aware and on the lookout for cyber-hijackings or other malicious online behaviour.
10. Have a reserve location established where you can set up operations in the event of an attack on your main property. Be aware that in the event of a Chemical, Biological, Radiological or Nuclear (CBRN) attack, your primary property

¹⁰ CPNI has written instructive reports to help managers, see: www.cpni.gov.uk/ProtectingYourAssets/personnelsecurity-268.aspx

¹¹ There are numerous online resources for developing BCPs, both in the public and private sector. One good place to start in the first instance is to find through your local police force your nearest Counter-Terrorism Security Adviser (CTSA) who will be able to start your thinking into this: www.nactso.gov.uk/

and much of the surrounding area may be inaccessible for months or even years.

11. More basic protection from CBRN includes ensuring that staff is able to completely shut off the ventilation system in your property.
12. For companies able to spend substantial amounts on such protections, breathing apparatus and mail screening is also a good idea, but more lo-tech approaches can be found to both problems – sort mail far from main body of staff and train people to use more mundane office equipment as protective breathing apparatus.

“For those travelling abroad, make sure you know any potential trouble in regions where you are going, and make sure some basic anti-kidnapping measures are taken.”

For those travelling abroad, make sure you know any potential trouble in regions where you are going, and make sure some basic anti-kidnapping measures are taken (such as varying routes and routines, and making sure people know where you are at all times). This lesson can be translated at home too in terms of making sure you have a good body of knowledge internally about the potential risks while staying abreast of new developments.

For the insurance industry specifically, this last detail is possibly the most important: making sure you are aware of the extent and degree of threat that is extant in any given market. There are plenty of open-source places good information can be found, as well as private firms, and government agencies that can provide up-to-date advice on the terrorist threat at home and abroad.

In terms of proactive behaviour, the insurance industry could further incentivise businesses to protect from terrorism by including some of the above-listed measures as prerequisites for terrorism insurance coverage.

Pool Re

The Pool Reinsurance Company Limited (Pool Re) was established in 1993 as a result of a series of major IRA attacks in the UK. Fear started to grow that insurance companies would not be willing to cover the growing costs and were shunning terrorism cover, and so the British government established Pool Re in conjunction with industry, which was to act as a final reinsurer with full government support. Initially established to insure commercial property firms against fire and explosion costs, in the wake of the 9/11 attacks on the US, terrorist ingenuity was taken into further account and possible use of CBRN, aircraft attacks and floods were woven in to its charter. Thus far, the government has not had to step in yet and it has managed all its payouts. Pool Re draws its funds from a premium paid by members (there are about

274 members), along with a surcharge on top of terrorism coverage offered by members to insureds. This is supplemented by investment income and ultimately the government.

“Promoting diversity in the workplace, as well as remaining sensitive to individuals’ needs and beliefs will also help advance the Government’s counter-radicalising agenda as well as promote corporate responsibility.”

In a written answer to a parliamentary question about Pool Re in the wake of the July 7, 2005 attacks on 19 January 2006, then-Chief Secretary for the Treasury Des Browne said:

- a. “Pool Re, and several of its members, are currently dealing with claims arising from the tube and bus bombings of 7 July 2005. However none of the claims has yet progressed to the point where Pool Re has been called upon to make actual payments. This is consistent with Pool Re’s claims payment patterns for previous terrorist events.
- b. Pool Re has paid out £609 million in respect of all incidents it has dealt with to date.
- c. Pool Re had reserves of £1.664 billion, as shown in its audited accounts at 31 December 2004. This figure has increased since that date.”

It is estimated that current Pool Re reserves are at approximately £2 billion. To find out more about the Pool Re market, please see: www.poolre.co.uk/.

Conclusions

In the longer term, it is clear that business will have a role in countering the Islamist terrorist threat. Demonstrating good corporate citizenship by supporting community activities is not a certain way to insulate from attack, but will undoubtedly help. Furthermore, fostering economic activity in

economically depressed parts of the nation will help further the government’s counter-radicalizing agenda as well as promote corporate responsibility. Promoting diversity in the workplace, as well as remaining sensitive to individuals’ needs and beliefs will also help advance this agenda.¹² If operating abroad, and in particular in an Islamic country, then these themes are even more relevant and any such actions may help deflate the Al Qaeda narrative somewhat.¹³

Prime Minister Gordon Brown has stated that the Islamist terrorist threat we face is a “generational struggle,” suggesting it will be with us for a while yet. In the face of this complex threat, there can be a tendency to simply throw up ones hands in despair, thusly handing the terrorists a premature victory. Careful and simple preparation, vigilance, and maintaining an awareness of the potential threat can instead go far to helping manage the risk.

If you have any questions or comments about this publication, please contact us on: ☎ 020 7417 4783 ✉ thinkpiece@cii.co.uk

¹² For businesses seeking more information on this, please visit the Department for Communities and Local Government (DCLG) website:

www.communities.gov.uk/communities/preventingextremism.

For more information on how to protect your physical building or train staff, please visit the National Counter Terrorism Security Office (NaCTSO) website: www.nactso.gov.uk

¹³ For more on the terrorist threat to UK business abroad, please visit the Security Information Service for Business Overseas (SISBO) website: www.sisbo.org.uk



Raffaello Pantucci is a research associate in the Transnational Threats and Political Risk Programme at the International Institute for Strategic Studies. His research at the IISS focuses on terrorism and radicalization, as well as helping business think through some of the risks associated with terrorism. He is a regular contributor to the media, as well as a variety of academic outlets. Prior to the IISS he worked for a number of years at the Center for Strategic and International Studies (CSIS) in Washington where he worked on European security and transatlantic relations more broadly.

The **Chartered Insurance Institute** is the world’s leading professional organisation for insurance and financial services with 93,000 members in 150 countries. Its mission is to protect the interests of the public through guiding the profession. This is achieved through maintaining the professional, ethical and technical standards of those working in insurance and financial services. For more in the **thinkpiece** series, please visit www.cii.co.uk/thinkpiece

The **International Institute for Strategic Studies (IISS)** is a leading global authority on political-military conflict, and is the primary source of accurate, objective information on international strategic issues for a range of customers including foreign affairs analysts, international business, and economists. The Institute owes no allegiance to any government, or to any political or other organisation. While based in London, the IISS has offices in Washington and Singapore, making it a truly global think tank. For more information, please visit: www.iiss.org.uk/