

TERRORISM: INSURANCE

Sri Lanka in the Shadow of Terrorism

Since 1983, civil war and terrorism have, in the eyes of the international media at least, provided an ever present backdrop to Sri Lankan affairs.

By Ian Watt

The reality of course is that, for the most part, every day life for the average Sinhalese citizen and business carries on as normal. Until October 2006, more recent terrorist activity by the Liberation Tigers of Tamil Eelam (known as LTTE or Tamil Tigers) had been concentrated in the north and north east of the country. However, with the suicide bomb attack on the naval base at Galle 110 kilometers south of Colombo on 16 October 2006, which killed nearly 100 people, the conflict has once again assumed nationwide significance.

Now is, therefore, a timely opportunity for insurers, reinsurers, brokers, businesses and everyone else involved in the risk transfer process with interests in Sri Lanka, to take stock and perhaps reassess the level of insurance cover and contingency measures to meet the terrorist threat for the future.

For many businesses in Sri Lanka, the only terrorism cover they have may be that provided by the government. Risk managers, brokers and others contemplating their need for, and scope of terrorism cover, will wish to give thought to the following:

- All property should be insured for the value of reinstatement when work may be completed in the event of an attack at any time during the period of cover. For example, subject to the policy terms, completion of repairs could take place months after the period of

cover has expired, and sums insured should take this eventuality into account.

- Business interruption cover should be subject to an indemnity period of at least 18 months.
- The sum insured on business interruption cover should reflect a period of indemnity based upon a loss occurring on the last day of the policy term. This will call for budget forecasts of 24 to 30 months ahead of inception or renewal.

Terrorism cover usually follows the underlying policy, but it is important to ensure that a clear protocol exists between the terrorism reinsurer and the direct insurer.

Business experience

Our experience in dealing with major claims from terrorist attacks in Colombo during the 1980s and 1990s, as well as elsewhere in the United Kingdom and Middle East, tells us that firms which experience abnormally heavy workloads in the wake of such an event often lack systems that enable them efficiently to capture the data for presentation of their claim, let alone continue their business.

With large company claims, the ongoing business interruption exposure demands a high priority. The implementation of a tried and tested business continuity plan for swift resumption of normal business operations is essential. Offices and communication systems may be totally devastated and take months to repair. Businesses may be forced to move their operations into temporary accommodation, perhaps even resorting to nearby hotels while they seek office space.

In the wake of terrorist attack, access to central business areas may be tightly restricted where, for instance, a security cordon has been

imposed in an attempt to avoid further harm. The fear of further attacks does nothing to assist the return to normality.

Unlike many natural catastrophes, the 2004 tsunami being an obvious exception, terrorist attacks generally involve little or no warning and place people at greater risk of death or injury. Attacks often involve delayed devices such as mines or devices that are planted and triggered remotely. However, they can also involve voluntary agents, for example suicide bombers, or involuntary agents, perhaps acting under duress.

Risk management

The real threat is, perhaps, the coercion of innocents, often with threats to family members. It is, therefore, desirable that companies properly identify those members of staff who might be vulnerable, however remotely, and where practical to put in place mechanisms by which an employee can indicate problems, perhaps through the development of secret words or phrases. Monitoring systems also need to be established to detect any abnormal activity by staff or visitors.

We recommend scrutiny of day to day procedures, and the adoption of measures to prevent routines that might be exploited, particularly in security processes.

Security starts at the top; it is for management to take the lead in the development and deployment of security procedures. Multiple perimeters combined with a challenging security team and heightened employee awareness provide good starting points.

On a practical level, where a background threat of terrorism exists, there are a number of measures that can be put in place to avoid or minimise injury or damage in the event of attack, including:

- Development of routines; for example, telling staff not to go to windows to look out, reviewing escape routes and creating a signal procedure.
- The application of film to glazed windows.
- Provision of comprehensive first aid kits appropriate for extensive injury; for example, cling film for burns, eye baths and field dressings.
- Improved level and quality of first aid training, especially in the treatment of blast injuries, such as burns and splinters.
- Development and use of regular fire and emergency drills. The feasibility of actually escape following a bomb (which might make the building unstable) must be tested. Escape needs to be reflex.
- Arrangement and clear identification of muster sites that are both safe and accessible, considering the risk of secondary attack.

It is an unfortunate fact that, whatever contingency measures are put in place, preparation for the chaos, injury and loss of life, and extensive damage to property that a terrorist attack causes always seems inadequate. Inevitably, resources will be stretched and this adds a new dimension to the problems faced by management, risk managers, insurers and adjusters. When devastation is widespread and extensive, a wide range of skills have to be brought to bear upon the many and various issues that can arise within a single business.

For example, a Tamil Tiger bomb attack on the Central Bank in Colombo in the 1990s resulted in extensive material damage to many buildings, including a building complex, its basic structure, the building's systems, suspended ceilings, glazing, internal partitions and curtain walling. In at least one other affected building, a fire following the main explosion caused considerably more extensive damage than that caused by the blast. The structural skeleton of the building was severely weakened in places where the concrete cover to reinforcing bars had

been completely destroyed. The full extent of damage and its implications could not be determined until detailed structural testing had been carried out, giving rise to further delays.

Office and IT systems were destroyed, together with the data they contained. Reconstitution of these records was vital, therefore, both to enable resumption of business, and so that the business interruption losses could be determined and verified.

In all cases, building repairs are likely to be undertaken mostly by local contracting firms and supply orders placed with manufacturers or importers. Local authority involvement with building repairs is inevitable and knowledge of the appropriate official channels and the correct procedures can significantly save on time and cost. It should be borne in mind, however, that equipment supply is global and, human nature being what it is, suppliers will often prefer to replace rather than repair, even where repairs may be viable.

Summary

To summarise the main points:

- Review insurance cover and sums insured
- Develop a business continuity plan
- Implement physical security measures to reduce exposure to attack
- Adopt precautionary measures to mitigate the effects of an attack
- Prepare and train staff in immediate response and first aid

Although this article has been written in the context of terrorism, there are aspects that apply equally to any catastrophic situation.

Ian Watt is a chartered loss adjuster. He is a director of Concordia Consultancy's Middle East company whose experience in Sri Lanka dates back to 1983.

www.concordiaconsultancy.com.