



#### RISK & INNOVATION

### Rethinking Terrorism: How Preparedness Is Evolving

---

## OVERVIEW

Terrorism has been one of the most contentious and often-used words over the past decade and a half. It has massively shaped the contours of our world. But behind the word – loosely defined as the use of violence against innocents to enact political change – lies a complicated, evolving phenomenon. And as the goals and methodology of terrorism shift, new preparedness thinking is needed from those it impacts.

Following high-profile terrorist attacks across Europe, Asia, and the U.S., together with continued violence across the Middle East, the threat of terrorism to individuals, governments and organizations only seems to be growing. It is perceived as one of the largest issues facing the U.S., with a Gallup poll showing that 16 percent of citizens said that it was their number one concern.

---

## IN DEPTH

Protecting against terrorism isn't a simple task. While terrorist attacks can cause large amounts of suffering, it is difficult to predict where they will occur and what the scale of damage might be. This makes it hard for businesses to assess their levels of risk. For instance, 9/11 prompted the U.S. government to put in place the Terrorism Risk Insurance Act, which helps insurers meet the massive losses that major terrorist attacks can incur. The mid-1990's IRA bombs in London drove similar responses within the UK.

But recent attempts to better enable organizations to protect against and recover from this threat have been complicated by the continually shifting nature of modern terrorism. As Scott Bolton, Director Aon Crisis Management, explains, "While the insurance industry and governments have developed (re)insurance – that is, insurance for insurers – solutions to provide financial resilience to organisations after an attack, the focus has remained on the 'traditional' property damage and business interruption cover." With today's terrorist tactics, such an approach to risk mitigation – while still valuable – often doesn't go far enough to reduce risk and enable organizations and their staff to be more resilient.

While the goals of terrorists have usually been to inflict some suffering in the form of death and injury, their tactics have also typically sought to cause property and financial damage, as a way of putting pressure on governments without alienating potential supporters with excessive violence. In 1996, the IRA detonated a bomb in the centre of Manchester, after giving a warning 90 minutes in advance – a similar tactic to that used by other terrorist groups throughout Europe during the 70s and 80s. Leaving time for mass evacuation meant that there were generally limited human casualties, but significant property damage. The Manchester attack caused over £700 million in economic damage.

#### New Models Of Terrorism

However, the 9/11 attacks signalled that once again terrorist tactics were changing. "Instead of having a desire to limit casualties, because they didn't want to alienate people from their political cause, terrorists now have a desire to inflict as many casualties as possible, as a means of publicising and energising their cause," says Henry Wilkinson, Head of Intelligence and Analysis, The Risk Advisory Group.

This trend has only become more pronounced as the way terrorism is organized has changed. In particular, there has been a rise in so-called "lone wolf" attacks, which are often much harder for security services to detect and prevent.

Attacks by the likes of the IRA and al Qaeda were supported by sophisticated networks with access to weapons and funding, operating with defined political aims. This level of organization and coordination was absent in attacks like those in Nice and Orlando. These were carried out by individuals only nominally attached to wider networks, sometimes only via social media, and acting without centralized planning or control. “Their strategy is more erratic – and more difficult to anticipate,” says Wilkinson.

Wilkinson highlights how the constraints on lone attackers have affected their tactics: “their ability to acquire explosives, or construct their own improvised explosives, is relatively limited by their lack of technical know-how and their lack of materials, because often new monitoring controls that are in place that control these materials. This shifts the emphasis onto physical harm to people.” The stabbings at Ohio State University and the use of a truck in Nice, demonstrate attackers can continue to find ways of causing harm that work around practical limitations. These “low tech” attacks are less likely to deliver a significant level of property damage – you can’t bring down an office block with a knife, car, or automatic rifle. Yet they are often just as deadly – the Nice attack killed nearly as many as the Paris attacks, but was logistically a far simpler operation.

### Reducing The Impact Of Terrorism On Business

This changing threat landscape implies a corresponding change in the way businesses need to think about terrorism risk mitigation.

Traditionally, terrorism insurance focuses on property damage, and costs incurred during business interruption, in a similar way to how organizations might insure against natural disasters. But today, organizations and insurers alike need to consider new sources of potential damage. The 2013 attack on the Westgate shopping center in Nairobi left 67 dead and resulted in \$78m in damages – and a good deal of the latter was caused by the Kenyan military forces brought in as counter-terrorism. The possibility of damage resulting from the response of the police and security services needs to be factored in to modern terrorist insurance.

Changes in tactics towards those that maximise human casualties also means that businesses need to revise their emergency response protocols. “With earlier terrorist groups like the IRA in Britain, or ETA in Spain, warnings were sometimes given to minimize the death toll, allowing an evacuation – similar to a fire drill – as a sensible response to a terrorist threat,” says Bolton. “Today, with the potential for evacuation placing employees and customers in further danger from follow on attacks (as seen in the Brussels Airport attack), with attackers positioned to target those trying to escape or emergency services.”

Many of these broader potential impacts are not included within traditional terrorism insurance, and while there has been some early innovation it will likely take much more to reduce the potential scope of terrorism’s impact on both property and people with enhanced coverage. In tandem, exposed organizations and individuals need to understand how to deal with terrorism, and what protocols and strategies need to be adopted in the light of changing terrorist behaviour.

### Thinking About Terrorism Holistically

With an increasing emphasis on “soft” targets, like the offices of French satirical magazine Charlie Hebdo, The Bataclan concert hall, the Pulse nightclub in Orlando, a public park in Istanbul, or a coffee shop in Jakarta, while it is understandable that some may feel that nowhere is safe, sensible precautions can significantly improve the potential to avoid or at least better respond to an attack. However unpleasant the prospect, organizations need to think about how to plan for the eventuality of an attack.

“Terrorism should always be viewed as part of a comprehensive risk management program – insurance is only part of the solution,” says Bolton. “The industry, both brokers and underwriters are becoming more articulate about the threat in order to better tailor the multiple lines of insurance that may be needed to respond to the impacts of a terror attack” says Bolton.

This means thinking about insurance as part of a “comprehensive risk management program”. This could include:

- **People Safety:** With the current focus on mass casualties, organizations’ responses to terrorist attacks within the workplace need to focus on limiting terrorists’ ability to cause people harm. This will also require plans that are flexible and can accommodate the need to different responses depending on the attack (evacuation or shelter in place, run-hide-fight/tell, for example). Factoring the response times of Police presents the practical reality of planning to deal with a violent attacker; response time may be 10 minutes or more. “Many businesses in the U.S. have security protocols to deal with active shooter events. As terrorism takes on more of the characteristics of mass shootings, these protocols could provide a model for terrorism management,” says Wilkinson.
- **Preventative Measures:** Preventative security may need to deny access to a hostile individual within the service or tenant spaces of a building; much of security investment is to deter an attack. “The challenge is to match the security to the local business or cultural norm – what is acceptable in Johannesburg or Tel Aviv may not be practical in London or New York,” notes Bolton. This could take the form of anything from turnstiles to metal detectors, security cameras to armed security.
- **Understanding The Context:** Even if none of a company’s assets or personnel have been directly attacked, this does not mean that there will be no negative business impacts. In the wake of the 2015 Bataclan attacks in Paris, hotel bookings in the city (7 percent of whose economy is tied to the tourist industry) fell by 30 percent. It’s estimated that the attacks cost the French economy around \$2.1 billion in total in direct and indirect financial damage. Companies need to understand and make provisions for this attritional loss resulting from a continued period of anxiety or from a number of attacks.
- **Proper Insurance:** Pool Re, the terrorism insurer set up by the UK government following two decades of IRA bombing campaigns, estimates that fewer than 5 percent of British SMEs have terrorism insurance. In the 1996 Manchester bombing, Bolton notes, up to 80 percent of companies affected were out of business the following year, having been unable to shoulder the financial impact of the damages incurred. Working with professionals helps ensure that the potential impacts to people and assets are matched by insurance designed to respond.

### Reducing The Impact

Terrorism is complex, multi-faceted, and an evolving risk. And the realities of today are not necessarily the realities of the 90s. Terrorism is more unpredictable, less attached to organised groups with targets we could anticipate, and skewed towards human suffering over the destruction of physical assets. And organisations haven’t caught up yet.

Solutions need to come in the form of preventative measures, emergency procedures, and wider planning and risk assessment, as well as insurance solutions. Only then will organisations across the world be able to weather the ever-changing evolution of terrorism risk.

## TALKING POINTS

“While public apprehension is understandable, the response to every terrorist attack cannot be the creation of another security perimeter. Will a new security perimeter create new vulnerabilities? Will it merely shift the risk to other equally vulnerable places where people gather?” – Brian Michael Jenkins, Senior Advisor to the RAND President, RAND Corporation

“Some of the businesses that responded most effectively to recent unrest and terrorist events are those that have plans and practise them. I know several who, when events happened in North Africa, Paris or Belgium, because they had plans and had rehearsed them, knew what to do and their people also knew what to do.” – Julia Graham, Technical Director, Airmic

## FURTHER READING

- Terrorism Economic Impact And Wisdom As A Solution – The Middle East Observer, October 27, 2016
- Cost Of Terrorist Attacks Reaches \$90B A Year And Western Countries Are Being Hit Increasingly Hard – Forbes, November 18, 2016

- Defending Against The Lone Wolf – Insurance Business, November 10, 2016
- Ohio State Attack Suggests Terrorist Threat Evolving – WJLA, November 29, 2016
- Terrorism & Insurance: What Homeowner And Auto Policies Cover – Huffington Post, November 3, 2016

