



## The cost of a terrorist attack to your business

### Why all businesses should care about terrorism

Wouldn't it be wonderful if you could pick up a report which defined the costs for business of a terrorist attack in Australia? Ideally, the report would state the probability of each form of attack and the financial implications. Then the terrorism risk would become just like the risk of fire, floods and office thefts – a predictable and known risk that could be managed.

Unfortunately, there isn't such a report. The problem is that there are no useful statistics about the frequency and cost of terrorist attacks. The international statistics are too limited, and extrapolating them to cities in Australia is meaningless.

Because the cost of an attack can't be quantified, about the only organisations that have seriously addressed the terrorism risk are owners of critical infrastructure, like telecommunications, water and energy, or those which are high profile such as iconic buildings and internationally recognised corporations. These businesses can do this because they have resources and government support to monitor the ever-evolving threat environment, build relationships with police and intelligence agencies, attend meetings on industry vulnerabilities, undertake complex risk assessments, produce comprehensive risk registers, evaluate mitigation options, and undertake exercises with the police and emergency services.

The vast majority of Australian businesses do not have the resources, expertise, contacts and government support to do this. Nor would the police, emergency services and government departments have the ability to deal with the demand for assistance and cooperation if all Australian businesses requested it.

But this doesn't mean that the majority of Australian businesses should continue to ignore the threat of terrorism.

For just as there is a likelihood that a business will suffer a fire, there is also a probability they will be affected by a terrorist attack in some way at some time. And just as businesses minimise the risk of a fire through various measures, businesses need to minimise the consequences a terrorist attack would have on their operations.

---

*...this does not mean that every business should consider itself a prime terrorist target and install blast film on windows or create standoff distances*

---

However, this does not mean that every business should consider itself a prime terrorist target and install blast film on windows or create standoff distances to prevent vehicle bombs being parked close by. What it means is that businesses need to acknowledge that if there is an attack in Australia, they will be affected to some degree no matter where they are or what they produce.

The cost to a business will vary from minimal to catastrophic depending on the following four factors:

1. their location in one of the 3 damage footprints
2. the government's emergency response and reconstruction efforts
3. the public's response to the attack
4. their business' sector

#### **About the author**

Athol Yates is the Director of the Australian Homeland Security Research Centre which is a private sector think-tank on domestic security.

A version of this article was published in the March/April edition of the *Security Solutions* magazine.

## The damage footprint

Every Australian business will be located in one of three damage footprints that result from a terrorist attack. In each, the cost to business will be different.

The footprints are:

1. direct
2. collateral
3. oblique

### 1. Direct damage footprint

This footprint covers the area where the terrorist weapon has a direct and immediate effect. If it is an explosive device, it is the zone in which the blast overpressures, flying debris and building collapse cause blast casualties and physical asset damage. Most terrorist weapons, such as arson, firearms and explosives, will have a relatively small direct damage footprint which could affect several hundred businesses. Dozens more will have some assets, such as their vehicles or staff who are transiting through the area or visiting clients, caught up in the incident. [There are obviously attacks where the direct damage

footprint will extend over a huge area, affecting tens of thousands of businesses. For example, a dirty bomb which consists of radioactive material being dispersed by explosives.]

Following an incident, people will be evacuated from surrounding buildings, the area searched for secondary weapons, and then sealed off as a crime scene. Then the painstakingly slow detailed forensics work starts. Its aims are two-fold – to locate elements of the weapon such as timing mechanisms, fuses and explosive traces, and to recover human remains. Tons of material will be removed to a secure site for screening, including vehicles caught up in the blast if it is believed they may provide evidence. Impounded vehicles will normally not be returned for several weeks. During this time, businesses in the direct damage footprint will not be able to operate.

As the investigation continues, company representatives may be escorted back into the area to collect essential items, such as backup tapes, but this will only occur if their premises are safe and evidence will not be disturbed.

After the forensic examination of the area has been completed, reconstruction will start. This could involve decontamination of an area, cleaning up tons of broken glass, emptying the rotting produce from thawed refrigerated cabinets, and restoring damaged electricity, telecommunication, gas, and traffic systems.

Below are the main costs that businesses will experience if they are situated in the direct damage footprint:

- physical and mental injuries to staff
- counselling of staff
- staff resignations due to perceived inadequate company security preparations/response and danger of working in the area
- loss of trade due to the closure of the area during the investigation and reconstruction phases
- loss of trade after the area is re-opened due to a perception that the area is unsafe
- loss of customer and business records, including billing information
- destruction of premises, equipment and stock
- loss of vehicles and other assets which are impounded



The Australian Homeland Security Research Centre undertakes independent, evidence-based analysis of domestic security issues.

*National Security Practice Notes* is a publication series that covers topical issues which are of critical importance to building national and domestic security capability.

*National Security Practice Notes* is part of the research program of the Australian Homeland Security Research Centre.

The Centre's 2006 research priorities include:

- Performance measures for domestic security policy
- The appropriate sharing of security costs and benefits between business and society
- National security capability development
- The role of the private sector security in national security

Athol Yates  
Australian Homeland Security Research Centre  
Tel 02 6161 5143, Fax 02 6161 5144  
PO Box 295, Curtin ACT 2605  
Australian Institute of International Affairs Building  
Level 2, 32 Thesiger Court, Deakin ACT 2600  
info@homelandsecurity.org.au  
www.homelandsecurity.org.au

Copyright 2006. All rights reserved.

## 2. Collateral damage footprint

The collateral damage footprint covers the area where businesses experience significant collateral damage, due to either having clients, suppliers or inputs located in the direct damage footprint, or being near this footprint. For example, a business in the collateral footprint may have to stop work on a project because its accounting firm was in the direct damage footprint. While most of the businesses in the collateral footprint are physically close to the scene of the attack, there will be a significant number that will be kilometres and possibly thousands of kilometres away, which are affected because of their relationship with a business in the direct damage footprint.

Below are the main costs that businesses will experience if they are situated in the collateral damage footprint:

- suspension and possible cancellation of work for clients whose offices or businesses are in the direct damage footprint
- suspension of production because suppliers in the direct damage footprint are not operating
- loss of trade as clients consider the business's location is unsafe because it is so close to the attack site
- resignation of staff as they consider the area unsafe
- delays in business travel due to traffic disruptions caused by the attack and reconstruction efforts.

## 3. Oblique damage footprint

This footprint covers the rest of Australia, and all businesses not in the first two footprints. This is because an attack will affect consumer and business confidence, which will in turn alter demand for various goods and services. For example, a blast in Sydney may affect hotels in Townsville as Australia will lose its international reputation as a safe travel destination, meaning a decline in foreign tourists. It may also affect merino farmers in South Australia as it may lead to a decline in discretionary expenditure on high priced carpets due to uncertainty about the future state of the economy.

Thus, for businesses situated in the oblique damage footprint, the main costs they will experience are attack-induced changes in demand for goods and services.

## Which footprint will your business be in?

Statistically, you have a minute chance of being in the direct or collateral damage footprints. For example, if a suicide bomber detonates themselves in a metropolitan area and it damages 300 businesses directly, the chance of any one individual business being caught in it is 0.02%.

---

*The cost for business of a terrorist act will also be directly related to the government's emergency response and reconstruction efforts.*

---

Once it was assumed that only businesses near high profile targets, such as the Premier's Office or the State Crisis Centre, were only at risk. However as the aims of a terrorist attack are to kill and generate fear, just because you are located in a suburban area, shopping centre or regional centre, doesn't mean that your business couldn't be in the epicentre of an attack.

## The government's emergency response and reconstruction efforts

The cost for business of a terrorist act will also be directly related to the government's emergency response and reconstruction efforts. This issue will be of critical importance to those caught up in the direct damage footprint and to a lesser degree, to those in the collateral damage footprint.

The response and reconstruction period can be thought of as the time starting from the attack and ending with the area being sufficiently cleaned up to allow most businesses to resume operations. It includes the critical minutes and hours following the attack in which casualties need to be transferred to hospitals, the days required to collect forensic information, and the days and weeks needed to stabilise any damaged buildings, clean up the destruction, and restore essential infrastructure.

Given the high quality of Australian first responders' training, the immediate response is likely to be very good for most incidents. The critical factor for businesses will be how long it takes to release the crime scene to begin reconstruction. As Australia has limited experience with terrorism on Australian soil, the crime scene exclusion may remain in place for up to two weeks. If this was at a critical hub, such as

Melbourne's Flinders Street, then the impact for those in the entire city would be considerable.

### The public's response to the attack

A huge variable in determining the cost for business of a terrorist attack will be the public's response. This is because an attack will make people unsure about their future safety and job security, which will lower consumer and business confidence, and thus reduce the level of consumption and capital investment.

The decline in confidence may be as short as a matter of weeks, as seen after the July 2005 London bombings, or continue on for several years, as seen after the Bali 2002 bombings. In the case of the London bombings, the reduction to the UK's gross domestic product appears to have been negligible, but in Bali, the region's economy took a hit of several percent.

While it is impossible to predict the public's response to an attack in Australia, it is likely that the public's confidence in the economy would rebound quickly. This is because of two reasons.

Firstly, the government's response to an incident will most likely be well managed, boosting confidence in the government's ability to minimise economic damage. Australia's emergency response and coordination mechanisms are extremely good, having been tested in large-scale, multi-jurisdiction and multi-scenario exercises like Mercury 05 (November 2005) and used in practice responding to the Bali 2002 and Bali 2005 attacks.

Secondly, Australians have been conditioned to expect an attack and an actual strike will not surprise many. This is because the public has taken on board the government messages that an attack is a possibility and not every attack can be stopped. In addition, the media covers every major terrorist attack around the world and this in-depth coverage has reinforced the notion that it is only a matter of time before the last partner in the 'coalition of the willing' will experience an attack on its soil.

The prediction that confidence will bounce back quickly is only valid if the attack comes in the form expected and the government's response is adequate. If, however, the attack is radically different from what is expected, such as the use of biological weapons,

or if the response is handled badly, as it was in Spain following the Madrid attacks when the government tried to make political capital from the attack, then the public's response could be very different.

If public confidence drops considerably, then the cost to business in declining sales will be huge.

### The impact on the business' sector

The cost of a terrorist attack will not be uniformly spread across all sectors. Some will suffer more than others, and a few will actually experience increased demand. For example, in the weeks after the July 2005 London attack, business and private travel generally declined throughout the country with the notable exception of bicycle suppliers, which experienced a boom as bikes were perceived to be safer than travelling on the tube.

---

*If public confidence drops considerably, then the cost to business in declining sales will be huge.*

---

In general, the following sectors are likely to suffer a decline in business following an attack:

- **tourism businesses.** This is because Australia will not be seen as such a safe destination, resulting in a decline in international arrivals. Also, as Australians will be more insecure, they will want to stay closer to home, resulting in a decline in domestic tourism. Retail premises which depend on tourism, such as airport clothing stores and city supermarkets, will also suffer.
- **businesses that depend on discretionary expenditure.** This is because if there is a loss of consumer confidence, discretionary expenditure such as luxury cars, household appliances, fast food and fashion, is the area to first experience a decline.
- **enterprises which bring people together, such as public transport, theatres, sporting events and casinos.** This is because people will be less willing to gather in large numbers which may be perceived as more of a terrorist target.
- **property owners.** Demand for the type of properties most affected by the incident will decline as people will be reluctant to invest in these. For example, if an attack collapses a high density, multi-storey apartment, then this market would be expected to decline. In the case of the

New York real estate market, some apartment values fell up to 30% following the September 11 attack although they had rebounded to the previous levels three years later. Similarly, if the attack is in a shopping mall, then retailers may follow their shoppers to strip shops if these are seen as safer.

Sectors which will most likely see an increase in demand will be:

- security and safety suppliers, which provide goods and services that create a more secure environment at home, at work and while shopping. Examples are access control, closed circuit TV, guarding, and fencing.
- home-goods suppliers, which focus on renovation and home entertainment. This is because people will seek solace in the one environment they have full control over – their home.
- personal wellbeing goods and services. These include trauma counselling, spiritual development, aromatherapy, pharmaceutical and health-related goods and services.
- semi-rural properties. A terrorist strike in a city area will accelerate the existing trend of Australians moving to the coast and mountains, away from what is perceived as unsafe urban areas.
- services which reduce the need to travel, such as online transactions and video-conferences.

## Should my business do anything about terrorism?

The answer to the question 'should my business do anything about terrorism' is definitely yes.

This is because in the event of an attack, all Australian businesses will bear some costs. For businesses where the risks are high, a full risk assessment may be appropriate, along with hardening their assets, establishing a backup site and removing nearby bins. However, for the vast majority of businesses, more appropriate measures are the four activities discussed below. While there are a host of other activities that could also be taken, the ones below are the minimum that every business should undertake.

Firstly, managers need to examine what the impact of a terrorist attack would be on their business. Questions which must to be answered include:

- what will happen if we don't have access to our premises for several weeks?
- what will happen if we lose certain staff for an extended period?
- what will happen if we lose access to an area where our key suppliers or customers are located?
- what will be the public's response to an incident if it happens nearby?
- what will happen to our sector if there is an attack?

Secondly, an internal emergency plan should be developed which addresses the immediate crisis period following an attack. It needs to define when to evacuate the premises and when to shelter-in-place in the building, how to contact staff and their families, and how to work effectively with the emergency services. A key part of the success of any plan is to exercise it regularly so that staff know what to do and improvements can continually be identified.

---

*...businesses need to introduce no-regret, multi-purpose security measures.*

---

Thirdly, a business continuity plan (BCP) should be prepared or updated. The BCP must not focus solely on terrorism but consider other causes of interruptions such as power loss, sabotage, floods, fire and IT system destruction. The plan should focus on re-establishing the most critical functions first to ensure the business can survive by generating income sufficient to pay for its liabilities. To do this, an understanding of the critical business processes is required, plus the identification of their essential inputs such as staff, suppliers and procedures. The plan needs to identify these processes, identify the makeup of the crisis management team, and define recovery alternatives. These plans can be as simple as a few pages of notes with contact lists held off-site or a web-enabled planning and implementation tool used by all the organisation's various business units.

Fourthly, businesses need to introduce no-regret, multi-purpose security measures. No-regret measures are called this as businesses will not regret putting them in place even if they are never needed. This is because they either don't cost anything or are very low cost. Multi-purpose security measures are those which not only protect staff, customers and

assets from terrorists but also from other threats such as disgruntled staff, fires, floods and thefts. The advantage of implementing no-regret, multi-purpose security measures, rather than expensive counter-terrorism specific measures, is that they are easy to justify due to their potential to save the business money by reducing workplace violence claims, theft of company property, OH&S claims and insurance premiums. Another benefit of making the workplace more safe and security is that it becomes more attractive to both customers and staff.

There are many no-regret, multi-purpose security measures and using the Crime Prevention Through Environment Design nomenclature, they include

1. increasing passive surveillance of public areas around the building by having desks facing outwards, and placing coffee bars in public spaces
2. increasing visibility around buildings by pruning back bushes which obstruct clear fields of view, ensuring existing lighting comes on when it gets dark and bulbs are immediately replaced when they blow
3. increasing territoriality by creating ownership of areas. This is done by creating clearly defined public and private areas, so that people who should not be in a restricted area are immediately obvious.
4. improving access control for people entering and leaving. Entry control can be enhanced by installing access control systems and requiring the wearing of passes to get into certain areas. Exit control can be enhanced by putting up signs to allow for rapid evacuation.

## Conclusion

The cost of a terrorist attack in Australia is unknown but what is known is that all Australian businesses will suffer some costs. The consequences may be little more than a minor disruption or it could be as large as a catastrophic interruption causing the company to collapse. Despite not being able to quantify the costs of an attack, at the very least all Australian businesses should undertake three tasks – examine the business impacts of a terrorist attack, update both internal emergency and business continuity plans, and implement no-regret, multi-purpose security measures.