ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Terrorism and Australian business

by Peter Jennings

02 An ASPI Strategic Insight December 2003

Summary

If terrorists choose to launch an attack in Australia or against our interests overseas, then it is likely that Australian businesses could be targeted. Yet there is much that business can do to become more resilient against the threat of terrorism and to help government defeat terror groups. This paper outlines several steps businesses should take to harden their operations against terrorism. An important part of this process is closer cooperation between government and business. Indeed the best way to defeat terrorism will involve government and business borrowing some of each other's styles of operating: Governments must learn to be more open and flexible, while business must develop greater skills in strategic analysis and war gaming.

A continuing threat ...

Terrorism will remain a powerful threat to Australian interests for the foreseeable future, perhaps a decade or more. This dramatically changes our national security environment and will increasingly force a re-think about the best way to protect our interests. We cannot assume that terror attacks against Australians might only happen overseas. Through his public remarks Osama bin Laden has specifically identified Australia as a terrorist target. We must work on the assumption that terror groups will launch attacks in Australia if and when they can. The direct effect of terror attacks are, of course, horrendous, but there can also be serious ripple effects to local business operations even when the attack itself is in a distant location.

If terrorists strike us directly, it is likely that their targets will be Australian citizens and businesses rather than better protected government institutions or the police or military. In the United States it is estimated that eighty per cent of terrorist attacks in the last three decades have been directed at business. Firms may be targeted because they represent national and economic values that terrorists oppose. Modern business operations are also vastly more international and interconnected than in past decades.

A sustained terrorist challenge is moreover, very different from the threats and risks that governments and business typically manage. In dealing with traditional state-based threats, government security and intelligence agencies are built around a sharp distinction between domestic and international concerns, with limited cross over. For example policing and military functions have a different legal and constitutional basis. They rarely operate in each other's domain. Intelligence information is tightly held within government agencies. As far as possible business and the wider community are (rightly) kept at arm's length from operational concerns.

> **"We must work on the assumption that terror groups will launch attacks in Australia if and when they can."**

For its part the business community has not traditionally seen national security as a core interest. Potential risks to business operations are usually defined around a narrower set of concerns about employee safety, plant security, the integrity of IT and financial systems and so on.

Modern terrorism attacks these standard approaches by refusing to recognise national or organisational boundaries. The challenge for business is to work out how it can assure the safety of its people and infrastructure while continuing to operate in a vastly more difficult environment. That means paying much closer attention to threats outside the traditional realm of business risk management. So companies need to think about security more like governments do. The challenge for government is to work out how to defeat a non-state threat that constantly changes shape while seeking vulnerable targets. That means developing greater organisational flexibility and faster reaction times. So governments need to think about security more like modern business thinks about its operations.

"The challenge for business is to work out how it can assure the safety of its people and infrastructure while continuing to operate in a vastly more difficult environment."

The business cost of terrorism

The human cost of terrorism is, of course, measured in the lives lost and maimed by attacks that are deliberately designed to inflict maximum damage. The business and economic costs flowing from these attacks is also profoundly damaging. The International Monetary Fund estimate of the economic costs of the World Trade Centre attack is that it reduced US gross domestic product by 0.75 percent or US$75 billion in 2002. Estimates of insurance losses from September 11 range from US$30 to $58 billion. In Indonesia, a 2.2 percent fall in tourist arrivals in 2002—in part reflecting the Bali bombings—led financial market analysts to predict a one-percent reduction in national gross domestic product.

Then there is the impact an attack can have on broader consumer and investor confidence. One of the remarkable things about the World Trade Centre attacks was how quickly international markets recovered. The bond market resumed trading two days after the attack and Wall Street less than a week later. The inter-bank payments system slowed but did not break. Yet according to the Boston Consulting Group total global wealth traded in the financial markets fell by four percent in 2001—driven down by a combination of terrorism, the dot com bubble and the Enron collapse.

What of the business impact of possible future attacks? Booz Allen Hamilton conducted a simulated study of an attack using three radiological bombs delivered in a shipping container to US ports. In the war game the effect of shutting US ports down for nine days created a container backlog that took three months to clear. The cost to the US economy was estimated at US$58 billion.

Although the global shipping industry invested some US$1.3 billion this year and is spending US$730 million annually on better security systems it is estimated that only two percent of the world's shipping containers are physically inspected. This is hardly surprising when there are 232 million container movements a year.

What is clear from these figures is that the potential knock-on effect of terrorism is huge. This is particularly so in industries such as airlines, accommodation and restaurants, postal services and insurance. But the effect is more widely spread because of the high level of interconnectedness between all elements of global business today. For example, the Ford Motor Company was not a direct target on September 11, but it lost US$30 million through of supply chain disruptions when the US-Canada border was shut after the attack.

There are also some positives. For example enhancements to port security will speed processing of cargo and containers. But the very success of the global economy has made business more vulnerable to terrorist attack. Complex global supply chains, just-in-time manufacturing, distributed operations and information technology connectivity all mean that even locally focussed companies are exposed to the disruptive effects of terrorist attack in ways that are very difficult to predict.

The Australian footprint overseas

Australians and Australian business have been at the forefront of globalisation and this is reflected in the size and range of our presence overseas. Just under one million Australians live and work overseas in almost 150 different countries. That is around 4.3 percent of our total population compared to the US, which has an estimated seven million expatriates, or 2.5 percent of its population. Additionally, there are the 3.5 million trips Australians make overseas each year, around half a million of these for business.

In 2001–02, over 32,000 Australian companies exported their goods and services, and over 55,000 companies imported material. One Australian job in five depends on exporting. Exports as a proportion of gross domestic product has been steadily rising over the years—from 15 percent of GDP in 1960 to 20 percent in 2003.

"Business planning assumptions need to be tested from time to time against worst case scenarios for security"

What these figures show is that Australia's business interests and population movements are truly global. We are deeply integrated into the world economy and have a physical presence that far extends beyond our immediate region. The growth of these overseas interests has been a major economic success story of the last few decades. However it also means that Australian business is broadly exposed to the direct and indirect consequences of future terrorist acts. Whether the danger is to our people—as happened in New York, Bali and now Istanbul—or to our economic interests, Australian business now faces a heightened risk from international terrorism.

'Hardening' business against terrorism

What can business do to harden its operations against the direct and indirect effects of terror? Because the threat seems remote and the avenues of attack too unpredictable, some businesses may think there is little point trying to protect their operations against terrorism beyond the normal risk management agenda. A July 2003 survey of major US firms found that only four percent had increased spending on security measures since September 11, 2001. Australian business is unlikely to have done better than their US counterparts.

There are three reasons why this 'head in the sand' approach is no longer sufficient. First, it underestimates the ripple effects an attack can have within and across industry sectors—it is not safe to bank on being isolated. Second, there are practical things companies can do to protect their operations against the results of terrorism. Third, companies that harden their operations will build a competitive advantage over firms that do nothing.

Here, I suggest eight steps in a strategy that companies can use to harden their operations. This approach will help companies better anticipate sources of terrorist risk to their operations and to develop plans that maintain or quickly resume business operations after an attack.

1. Broaden risk assessments

Terrorism dramatically expands the range of external events that firms must factor into their planning. Businesses must understand how strategic and political events could impact on their operations. Where companies have overseas presences it is important to develop a good knowledge of local political and social concerns and to identify critical points where these issues touch company concerns.

Companies should invest more effort into analysing trends in regional security and terrorism and these assessments need to be more consciously brought into a firm's strategic planning cycle. Business planning assumptions need to be tested from time to time against worst case scenarios for security, in order to see how well the plan stands up against a major negative development. This can help companies develop a list of indicators that give early warning about possible negative trends or events.

Companies also need to understand the decision-making dynamics and policy priorities of the Australian Government in relation to counter-terrorism and what this means for the firm's activities.

Strategic analysis of this type is difficult and imprecise work, not readily quantifiable and hard to use as a basis for making clear policy decisions. It is also the stock in trade of the analytical work done for governments by intelligence agencies and areas concerned with defence and security. The Federal Government could help the business sector build more of this analysis into their planning by releasing more of its own analytical assessments and by advising on the processes and methods used to produce this type of material. Canberra has already gone some way down this track, at least in terms of speeding up on the release of information relating to terrorism. More needs to be done to actively bring business into this process.

"Because the challenge of terrorism is largely a new threat to Australian business, boards and top executive management need to personally lead planning to harden their operations"

2. Involve the board & top management

A McKinsey survey found in 2002 that 36 percent of US company directors did not feel they fully understood the risks their company faced, 24 percent said that their board had inadequate processes for handling risk and 19 percent said their board had no risk management processes at all. In an age of increasing risk this is a bleak picture.

Because the challenge of terrorism is largely a new threat to Australian business, boards and top executive management need to personally lead planning to harden their operations. In large firms, risk management can be devolved to operating areas where line managers are closest to potential sources of business risk. That remains an important task, but it is not necessarily enough to protect against the effects of terrorism, particularly the indirect effects of an attack that might be remote from a company's immediate operating concerns.

Businesses need to be satisfied at the most senior levels that they have a solid understanding of how their activities could be damaged by terrorist action. Boards should take an appropriately strategic view, ensuring that company strategies make sense in the light of current geopolitical circumstances. Senior management needs to put a high priority on developing a counter-terror plan throughout their organisations and linking it to traditional risk management and mitigation tasks. The work of risk managers needs to be regularly reviewed at board and CEO level. A major part of the task should be to make sure that the company's approach is broad enough to capture a full range of issues that might point to a possible business threats.

3. Review areas of organisational vulnerability

A company may be many thousands of kilometres away from the point of a terror attack but still find that its operations are disrupted because of the impact on suppliers, or transport routes, or vital IT and financial systems. In a globalised business environment companies must build an understanding of how their operations—and their supplier's operations—are vulnerable to these ripple effects.

It may not be wise for example to rely on a sole supplier for a critical component unless a firm can rapidly find a new source in the event that the flow of parts is disrupted. In the aftermath of September 11, 2001, many US firms reviewed stock holding policies in the light of disruptions to suppliers. Although maintaining larger stocks will cost more, it can be a vital way of maintaining business continuity after a shock.

Companies should consider whether a senior management team ought to be given responsibility to review sources of vulnerability. Here a useful lesson can be taken from the military approach of using 'red teams' in exercises to test the adequacy of doctrine. In business operations red teams may find possible faults which line managers overlook because the latter focus on making the system work rather than looking for problems.

Blackhawk helicopters © Defence Dept

"One of the best ways businesses can test their resilience is to put senior management through decision-making simulations of how they would respond to a terror attack"

4. War game responses to terror attacks

Australians are becoming used to seeing members of the Defence Forces and other government agencies engaging in counter-terrorism exercises. This has long been a method for military forces to test and develop their fighting skills. Other government agencies in Australia are increasingly using gaming techniques—also known as path gaming or scenario gaming—to help identify new threats and responses in many areas of public policy.

One of the best ways businesses can test their resilience is to put senior management through decision-making simulations of how they would respond to a terror attack. There are established techniques and processes that can be used to structure such games. Management teams can role-play the behaviour of different participants through a terrorism scenario. These exercises can highlight weaknesses—and potential responses—which were simply not apparent to management before the game. They can test business plans to see how well they work under different scenarios, or they can exercise a firm's risk mitigation and business continuity plans to see how well they would operate in reality.

The consulting firm Booz Allen Hamilton has gamed a number of terrorism scenarios, including an attack on US ports and responses to terrorists using pneumonic plague bacteria. Exercises of this nature can yield major improvements in how businesses should structure their responses.

Although participating in strategic decision-making exercises of this kind may at first blush seem like a distraction from the business of real management, they should be treated as a vital part of building greater business resilience against terrorism. Gaming is one of the best means to equip businesses with the necessary crisis management skills—far better to learn these skills in a simulation than in a real crisis. But beyond the immediate needs of crisis management, gaming can also bring a new perspective to a firm's strategy by suggesting ways it might be strengthened to handle unexpected events.

5. Share knowledge with other businesses

The major western governments are struggling to gather all the intelligence information they need to successfully defeat terrorism. Given that reality, Australian businesses will also find it

difficult to identify all the things they must know and do to protect their operations. Information sharing between businesses is one way to help overcome this dilemma. This recommendation may run against a natural business concern to protect commercial information. But the nature of the threat is such that there is an overriding common interest to defeat terrorism and to maintain a stable environment for all businesses.

Businesses within and across industry sectors should share information on the best ways to implement counter-terror plans; share their assessments about potential threats; discuss what strategies have worked and failed in their companies and refine future plans. No single business or government agency has a monopoly of wisdom on how to deal with a threat as unconventional as terrorism. There is significant business and national value to be gained by creating the means for companies to share their views on this problem.

"Up to now Australia's peak business associations have spent little time focussing on the impact of terrorism. They can, however, play a very useful and increasingly necessary leadership role"

6. Involve the major business peak bodies

Peak bodies such as the Business Council of Australia, the Australian Chamber of Commerce and Industry, the Committee for the Economic Development of Australia, the Australian Industry Group and the Australian Business Foundation, among others, have a significant role to play here too. They could develop some basic guidance for business on how to plan against terrorism. They could facilitate the pooling and sharing of business knowledge and best practice and they can act as a bridge between business and government at senior levels.

Up to now Australia's peak business associations have spent little time focussing on the impact of terrorism. They can, however, play a very useful and increasingly necessary leadership role to bring more structure, clarity and attention to this issue within the private sector.

7. Build links with government and non-business groups

To develop an understanding of the terrorist threat, businesses will need to build closer links with government agencies and non-business groups. In part this means simply that business must keep itself informed about information that only governments are likely to have. Travel advice issued by the Department of Foreign Affairs and Trade should be taken seriously, as should statements from senior government figures advising on threat levels based on intelligence information. The Attorney General's Department is developing a network for sharing critical information with the private sector designed to protect vital infrastructure. Progress in this area has been slow, but it nevertheless represents an important opportunity for business to engage with government on terrorism.

Beyond simple information gathering, business needs to engage with government and other non-business entities to get a more diverse set of views about the terrorist threat and how best to counter it. To use a current military buzz-word, terrorism is an 'asymmetric' threat—it seeks to defeat conventional approaches by attacking from the side. Conventional business risk management approaches may not be the solution, so business needs to adopt new and less conventional ways to deal with the threat. Different strategic planning approaches and perspectives are important here. Business needs to broaden the range of people and institutions it deals with to make sure it is testing its own approaches with the best alternate thinking available.

8. Communicate specialised knowledge to authorities

A final but very significant step in hardening business operations is to make sure that companies communicate information to government, which might be relevant to defeating terrorism. Just as business can be a terrorist target because of its exposed position, so too is it possible that firms with distributed networks and

engaged with local communities may identify information that could be highly valuable to counter-terrorist operations.

The demands of information gathering to defeat terrorism is often a slow process, requiring meticulous cross-referencing of small pieces of data to build up a bigger picture. Potentially the private sector has an important role to play here, by adding to the mosaic of information that ultimately leads to identifying terrorists and preventing their attacks.

Linking government and business—a proposal

My argument here has been that the business community can do much to protect its operations against terrorism and also make a broader national contribution to defeat this threat. The challenge that terrorism raises for our society—and for liberal democracies more generally—is one that cannot be left to governments alone to solve. If there is a solution to terrorism, it is likely to come out of a closer working relationship between government and business.

"The challenge that terrorism raises for our society—and for liberal democracies more generally—is one that cannot be left to governments alone to solve"

There has already been progress in this field. A 'Business-Government task force on critical infrastructure' was formed in late 2001 and officials and business figures met in 2002 to decide on strategies to help protect privately owned Australian infrastructure. Useful work has been done, but there is a need for a broader approach on terrorism managed at a higher level both within government and the business community.

My proposal here is that peak business bodies should decide to make countering terrorism a major focus of their policy work in 2004. The business community needs to engage with this issue and it needs to clarify its thinking about what should be done with government to develop a rigorous counter-terror strategy. Defeating terrorism will involve government and business working much more closely together than they have in the past or, indeed, are really comfortable with doing right now. A creative alliance against terror between business and government must find new ways of identifying and mitigating risk, faster and more comprehensive information sharing and new strategies to manage crises when they develop.

Once the business peak bodies have identified a clearer sense of what they can do about terrorism, and also what they want from government by way of information, assistance and support, then it would be necessary to approach government to start a ministerial-level dialogue on the subject.

One model would be to hold a 'Business-Ministerial advisory forum on counter-terrorism', to be chaired either by the Prime Minister or the Attorney General. This advisory forum could meet, say, on a twice-yearly basis. It would act as a clearing-house for ideas, a vehicle to drive policy development at a faster and more senior level and a way of ordering the many separate counter-terror activities which are currently being pursued in different areas of the government system.

A Business-Ministerial advisory forum would provide the right level of focus for government and private sector leadership. By bringing together two normally quite differently-focussed groups the forum could help to generate some lateral thinking on a problem that will only be solved by non-conventional approaches.

Lastly, a ministerial level forum with business gives this issue the prominence and priority it deserves both within government and the private sector.

Make no mistake about it, the terrorist risk to Australian business will remain higher for the foreseeable future. To date the business community has not put enough effort into working out how to respond to this danger. But it is not sufficient just to hope that Government will provide all the answers. Countering terrorism calls for a genuine partnership of effort between governments, business and the wider public. The immediate task for the business community is to work out a broadly agreed strategy for responding to terrorism. This will add substance and momentum to business cooperation with government and significantly strengthen Australia's overall counter-terror strategy.

Further reading

Sven Behrendt & Parag Khanna, "Geopolitics and the Global Corporation" *Strategy & Business*. Fall 2003.

Kevin S. Buehler & Gunnar Pritsch, "Running with Risk" *The McKinsey Quarterly*." No 4, 2003.

"Capitalism and its troubles: A survey of international finance" *The Economist*. 18 May 2002.

Department of Foreign Affairs and Trade, *Global Issues Brief: The Economic Costs of Terrorism*. Economic Analytical Unit. Report No 1/2003. April 7, 2003.

"Doing Business in a Dangerous World", *Harvard Business Review*. April 2002.

"Economic Consequences of Terrorism", *OECD Economic Outlook No 71*. 19 June 2002.

"Homeland insecurities" *The Economist*. 21 August 2003.

"Peril on the Sea" *The Economist*. 4 October 2003.

Randall Rothenberg, (Ed) *Enterprise Resilience: Risk and Security in the Networked World* (Booz Allen Hamilton Inc, 2003)

'Trusted Information Sharing Network for Critical Infrastructure Protection', maintained by the Attorney General's Department at http://www.cript.gov.au.

About the Author

Peter Jennings is the Director of Programs for ASPI. He is responsible for the Institute's research and publications programs on defence and international security issues. Peter was most recently the Senior Adviser for Strategic Policy in the Cabinet Policy Unit of the Prime Minister's Office. He has held a number of Senior Executive Service level positions in the Defence Department, including heading the Strategic Policy Branch and being deputy head of the Defence Imagery and Geospatial Organisation. Peter was a Sloan Fellow at the London Business School in 2000–01.

About ASPI Strategic Insights

ASPI Strategic Insights are published online and are intended to provide expert perspectives on specific current issues. They reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

About ASPI

ASPI's aim is to promote Australia's security by contributing fresh ideas to strategic decision-making, and by helping to inform public discussion of strategic and defence issues. ASPI was established in August 2001 and is funded by the Australian Government as an independent, non-partisan policy institute.

Cover banner image © Australian Picture Library

ASPI ■ Level 2 Arts House 40 Macquarie Street Barton ACT 2600 ■ T +61 2 6270 5100 ■ F +61 2 6273 9566 ■ www.aspi.org.au