

Engaging National Security Policy into Business Strategy

Address to National Security Australia 2006

27 February 2006

There are many threats that business needs to account for these days. Few in business can be confident that their business models will survive the next decade. They are struggling to catapult themselves into the future and they are also trying to hold back the waves and manage the risks imposed by globalisation, technology and government regulation creep. Into this uncertain equation, has entered an additional and sinister threat: the rapidly morphing construct of national security.

From a business perspective, we have always had a key *stake* in Australia's national security, while governments have traditionally been the custodians of our nation's security. However, the new kinds of threats that we now face, and the nature of our modern society and economy, have dramatically changed the national security calculus. Circumstances now require that business partner closely with government in advancing and ensuring our national security.

The Changing Nature of the Threat

I'd like to just take a moment or two looking at the changing nature of the threat. The notion of "national security" now encompasses the broad issues of our national survival and wellbeing. It takes in both internal and external threats, it goes to all the risks that confront Australia.

They can be military threats, they can be the risk of a pandemic, they can be major social problems. Ai Group held a conference recently on avian flu. If that virus mutated into a form transmissible between humans it would be a major catastrophe on a global scale.

There has been much more focus on national security since the terrorist attacks of 11 September 2001. The whole concept has shifted since then. Our notion of national security used to be protecting Australia from invasion, an external threat, making sure that society was nicely balanced and harmonised. Terrorism was a tangible construct – the PLO or the Irish cause. While it was terrible, you knew who the enemy was and it was confined. As well, the world had become complacent about disease; our attention was more drawn to our success in eradicating diseases such as malaria and polio and success in treating threats such as HIV (although limited), than on new threats.

Now it's as much about internal threats as well as external threats, it's about terrorism more than national hostility; it's about the effectiveness of global

governance on issues like health as much as military preparedness. After September 11, Ai Group convened conferences on national security and it was rather confronting, because up until then only companies that really had to, such as defence oriented companies or others like Qantas, were thinking every day about this subject. It was a major wake-up call. Companies were scrambling because they had plans in the bottom draw, but they weren't really honed, and September 11, even if they weren't directly affected and few in fact were, exposed the softness of our underbelly.

The interesting thing is that those companies that were directly affected, coped better than might have been expected both in the short and medium term. This is because the nature of modern business with its dependence on IT and IP has heightened the focus on risk management. IT systems are routinely backed up, IP has to be protected, client privacy and interests have to be safeguarded, offices have to be secured, OH &S has to be elevated to the top of the Board agenda. This thinking has also contributed to confidence such that lost ground can be relatively quickly regained. For example, the subsequent recovery by markets to September 11 was quite rapid – the S&P 500 dropped around seven per cent in the week after the September 11 attacks but one year later it had risen 15 per cent.

In short, the advent of this new era of global threats coincided with a business community learning to factor in heightened risk and this has added to our national preparedness to an extent many are not aware of.

At the same time, there was and undoubtedly remains, a big gulf between what might be required and what is. Indeed, the increased, and very real, threat of a terrorist attack or pandemic on Australian interests means that business strategy must encompass security concerns to an extent that would not have been conceivable only five years ago.

However, seeking to guarantee absolute security from the broader range of threats that Australia now faces would be an illusory goal. What can be achieved is a practicable minimisation of threats and ensuring preparedness to deal effectively with their consequences. This will require close collaboration between governments and business.

It is a new and worrying threat environment, but one which must be placed in perspective. While the impact of terrorism on the community and business can be catastrophic in the short term, life - and business - can and do go on. This resilience can be illustrated by the response and rapid recovery of the financial sector to major terrorist attacks.

Business Working with Government

So how does business work with government in this new environment?

The Federal Government is doing a solid job on national security issues. It's been very supportive of our attempts to engage business on the issue and it's opened up the agencies to us, as with Dennis Richardson's presence (when he was the head of ASIO) at our conferences, and our dialogue with other agencies. It has established the Business-Government Advisory Group on National Security which brings together some core players in industry and government. Since September 11 the Federal Government has spent A\$4.4 billion on strengthening national security, with a further A\$825 million in the latest Budget.

The Government legislated in 2003 to nullify terrorism exclusion clauses in insurance contracts and provided a A\$9 billion indemnity to cover the potential cost of claims. At the state government level, we've had good dialogues with the police and other government agencies- it's the police a company will call first if there's a threat – and other state government agencies.

My participation in the Business-Government Advisory Group on National Security has given me an understanding of what the government is thinking and of what is required from business in this task.

Business has to be cautious, because we have to take a balanced approach to risk. If we factored in everything, the cost would be enormous and we would be building endless barriers within organisations. As well, we need to achieve some clarity about who is responsible for the risks. I will return to this issue a little later. If a terrorist attack happens, and an IP system is destroyed, governments should be able to expect that the individual company has backed up their system and covered that risk as it is consistent with prudent commercial planning. If the attack is caused by a failure of the customs or policing system or the employees can't find their way home from work, that should be the states responsibility. As in IT, there will be areas of alignment; however to mandate CCTV in all industrial premises for anti-terrorism purposes, where this goes beyond the commercial needs of the companies involved, is doing the states work. The responsibility and implicitly the costs should at least be shared.

So it's really a question of managing the issues astutely and achieving a proper sharing of the risk. If the government wants us to be involved in broader issues, we're happy to contribute, but this cooperation must take the form of a partnership, not a series of prescriptive, yet unfunded dictates which may be more appropriately dealt with through taxpayer-funded measures. Business must retain the freedom and flexibility to do what it does best, and where possible, the formulation of national security policy must take the business environment into consideration.

Ai Group has developed good relations with the Australian Federal Police and with ASIO. As I said, Dennis Richardson, the previous Director-General of ASIO, addressed our conferences and this was very important because many of our

members regarded ASIO as a somewhat shadowy spy organisation. Dennis turned up and spoke directly and constructively and got a dialogue underway, and the new head, Paul O'Sullivan, is keen to keep this going. ASIO will have access to a wider pool of information in assessing threats to the community, and business will benefit from timely and expert assessments of potential threats.

We and ASIO's Business Liaison Unit are currently examining ways in which we can work together to assist our members in accessing this important national resource. In practical terms, though, the first contact of any member concerned about an immediate threat would probably be with the police.

How Businesses are Responding

If we look at how business is responding to the new security environment that we face, then in its broadest terms, it has certainly added a new variable to the business equation. For the first time, many businesses have had to consider and make contingencies for the possibility of a terrorist attack on their employees, customers or assets. The depth and scope of security measures have increased significantly – and so have security industries and associated technologies.

However, some of the security requirements of modern business, such as improved surveillance systems, are already in place, as a response to fraud or other forms of crime.

Companies operating across national boundaries have had to review all their management strategies pretty vigorously; and in many cases have had to significantly upgrade security for overseas operations. It's added a whole new layer of costs to doing business.

This new environment has prompted companies to look more closely at their risk management strategies. While the costs in some cases have been substantial, we have reached a stage where these are now factored into the costs of doing business, and are likely to remain with us for the foreseeable future. While not insignificant, they have not proved insurmountable. However, as in all business costs, these vary from sector to sector and from country to country. Most people still want to have an open culture, but they're certainly more aware of security issues than in the past, and the need to minimise threats and mitigate potential injury.

There has been a greatly increased demand for products and services related to protective security, and companies are active in meeting this demand. It's very important that Australia has the capability to understand and develop this capability. If we have to rely on off-shore supply for critical products and capabilities it makes us much more vulnerable. The fact that we can produce anti-avian flu drugs like Tamiflu and Relenza is important. The national security issue has created opportunities for a number of companies. They're not huge

players, but they're making a good impact in their sectors. Some of the security requirements lend themselves to more solutions-based responses rather than volume-based production, and this can fit more effectively with Australian companies' operations and Australia's competitive advantages.

The Federal Government's major investment in defence is also providing many opportunities for our defence companies. It used to be rather old-fashioned to say we needed to retain a strategic manufacturing capability for defence. Nowadays it's not old-fashioned, and I think the government recognises it's important we have that capability to do a lot of things which do go to the heart of "national security" in its wider meaning.

Protection of Critical Infrastructure

Of course when we think of security issues, we often think firstly of protection of critical infrastructure as a key task. This has closely involved industry. The Federal Government has developed a database of national critical infrastructure assets covering such areas as transport, energy, health and communications, and of the 27 assets categorised as "nationally vital", 16 are privately owned. This raises many critical issues for the companies that own and operate these assets.

For example, there is the issue of security checks, which have to be handled rigorously but very professionally. Companies just have to be much more security conscious these days and they are; it's a very different world.

The critical infrastructure assets most at risk are various. There are icons such as the Sydney Opera House and Harbour Bridge. There are also transport hubs, land, sea or air – we saw what happened after the attack on the London Underground – energy generation and supply, telecommunications and broadcasting, supply chains for medical supplies and food, and information technology.

Australia's vast distances exacerbate these vulnerabilities: for example the total length of Australia's natural gas transmission pipeline system is over 20,000 km. Australia's motor vehicles use almost 30 million litres of fuel each year, fuel which needs to be transported, stored and distributed across the country.

The challenge of securing critical infrastructure is one that is shared by both the private and public sectors. Australian owners of critical infrastructure have been working closely with the Federal Government to reduce its vulnerability. The Business Government Advisory Group on National Security has been working with the Prime Minister and other relevant ministers to provide strategic guidance to this process. At the more detailed level, the Government has done much to coordinate the ongoing work of a number of Infrastructure Assurance Advisory

Groups, through which key companies and sector-specific industry associations are involved in the process of identifying and remedying vulnerabilities.

Some of the key features of the modern Australian industrial landscape, its involvement in global and domestic supply chains, and its utilisation of lean manufacturing principles, contributes to its potential vulnerability. Disruption to an individual business or operation can have a catastrophic follow-on impact to suppliers and customers.

Australia is also a major market for global tourism, which is very sensitive to terrorist attacks. One example of this is the drop in tourism to the United Kingdom in the wake of the terrorist attacks in London last year, where retail sales in London dropped nine per cent in the month of the attacks.

Companies need to determine what their liabilities would be if they were unable to supply their customers. They need to establish a very comprehensive risk management strategy which would involve the costs of addressing threats and whether government support is required.

Australian industry has come a long way with regard to security planning and risk management. For people in banking, in transport, in energy, it's a major focus, it's in their commercial interest, and it's in their board reports. At the top they're doing a lot but I think they could cooperate more. Commercial confidentiality is relevant, but perhaps they could do more in collaborating on good practice.

Dealing with the Consequences, and Recovery

Many other Australian companies should be doing more in the way of preparing for a serious disruption of their business, not necessarily just from terrorism, but from events such as pandemics and natural disasters.

Australian companies with overseas operations need to be cognisant of the need to ensure the safety of their staff, customers and assets, particularly as they may be operating in an environment where the threat of attack is greater and the local government's anti-terrorism measures may be less effective than the measures taken in Australia, or where the potential health and natural disaster risks are greater.

More investment needs to be made in disaster recovery plans. If we had an attack like London, what would happen? I don't think there's enough of a national focus on basics such as how people would get home. Does a company provide more resources to the known commercial challenges or more on possible threats related to security from terrorism or pandemics? The answer is that companies must do a proper risk assessment and do both, depending on the nature of the company. This planning should also involve consultation with the appropriate government emergency management authorities.

The failure of US emergency management systems last year to deal with the aftermath of Hurricane Katrina provides sobering example of the dire consequences of a glaring disconnect between policy formulation and policy implementation. Here was a natural disaster that had been anticipated for years, and the specific event was the subject of clear warnings for days, and yet the response was tardy and uncoordinated, exacerbating the human and financial toll. It may have also indicated a major structural flaw: the new omnibus Department of Homeland Security had all of its key resources directed at terrorism while other threats were relegated to second place. This suggests that rolling all threats into one can deliver poor results and resources can be allocated to the 'urgent as against the important'.

An emergency response system that had been built in the wake of the September 11 attacks by the world's most powerful country proved to be appallingly unresponsive to such a domestic calamity. If the community is to have confidence in Australia's ability to respond to a national emergency, coordination between government agencies and between levels of government in such a crisis must be honed to state of operational perfection. As well, we must not let our fixation with global threats cause our focus and our resources to be unable to be directed to the everyday threats to our national well being. Eg bush fires.

Allocation of Costs

As I alluded to earlier, the imposition of the costs on business for improving security is an area which we need to keep a close eye on with regard to regulation and costs. We need to make sure we don't add unnecessary pressures to businesses already facing a fiercely competitive international environment.

In all of these situations, cost alleviation will always be an important area where the sector concerned is providing benefits to the whole community. While the Federal Government has played a key role in coordinating the public-private effort on national security, it has also made the assumption that much of the cost of improving security can be shifted on to business.

There are a few exceptions in areas where there are overlaps with existing regulatory regimes, such as aviation safety. In the area of IT security, the Government contributes to the costs of assessments under the Computer Network Vulnerability Assessment programme. There hasn't been a big take up of this scheme, but it's a good example of where government and private sector interests are aligned. We will encourage Australian businesses to avail themselves of this important service.

By and large business has factored additional security costs into the costs of doing business, and has frequently passed them on to the consumer. There is an assumption that the users of products and services are the beneficiaries of improved security measures. I would argue that this is not always the case and ultimately the Australian community as a whole, or a sector of that community, is the ultimate beneficiary of specific measures.

Businesses, of course, have a responsibility to protect their employees and assets, necessitating a certain level of investment in security. The level of this investment will vary significantly from business to business and sector to sector.

However, a compelling case exists where additional levels of security are required of businesses by governments for the protection of the wider community, that the responsibility for funding this additional requirement should lie with government.

September 11 showed that individuals that did not expose themselves to the particular risk, such as flying, also suffered. This brings the application of so-called user-pays approaches for national security programs into question. Perhaps an analysis of a user-pays approach with regard to specific national-security related measures, such as the passenger movement charge.

There's also a limit to how much can be passed on to users and consumers in a fiercely competitive domestic environment. I think responsibility for some things must be shared by government – for example the repair or replacement of a major energy facility destroyed by terrorists.

In order to enhance private-public cooperation on national security, governments could examine innovative solutions, such as tax concessions for expenditure on security improvements, or widening the scope of government grants to include such kinds of expenditure.

In making national security policy, we should hasten slowly. It is important to ensure that comprehensive analysis and consultation takes place on major national security-related initiatives that could have broader impacts on society and the economy.

For example, with regard to the proposal to introduce an identity card, Australia should first ensure that there is a thorough assessment of the benefits and costs. It would cost a huge amount of money to implement and at this stage the case still needs to be made that such a card would provide value. A study undertaken last year by the London School of Economics estimated the likely cost of the 10-year rollout of the proposed identity card scheme in the UK at between 10.6 and 19.2 billion Pounds (A\$26.5 and A\$48 billion).

This figure did not include public or private sector integration costs, nor did it factor in possible cost overruns. The existence of an identity card scheme would certainly not have prevented the London attacks last year, which involved British citizens, and it's debatable whether such a scheme would have contributed to preventing some of the other major attacks that have occurred. One wonders whether, over there, it is not more about sending strong messages through the power of symbolic laws, than actually increasing national security.

Conclusion

So I would conclude by saying that business remains firmly committed to supporting the critical effort of safeguarding Australia's national security. We applaud the substantial efforts to date of Australian governments to work in partnership with the private sector to minimise the threats to our community, and to ensure that our ability to respond to the consequences of any emergency situation is optimised. We look forward to strengthening and growing this important relationship, and as in all partnerships, we need to keep a close eye on ensuring a proper balance between costs and responsibilities.
