Centre for International Corporate Governance Research

VICTORIA UNIVERSITY

Sponsor:

Victorian Department of the Premier and Cabinet

Beyond Fragmented Government: Governance in the Public Sector

15-17 August, 2005

Victoria University City Campus,

12th Floor, 300 Flinders Street. Melbourne, Australia
In a conference devoted to issues of governance, it might seem a bit odd to talk about issues of security policy and critical infrastructure protection. But this is very much in the context of what Peter Johnstone has also discussed at this conference: understanding the forces that are changing us and surrounding us, and the types of governance responses we need to put in place to respond to those forces.

**Security as governance**

It is important to recognize that one of the keys to good governance is identifying, assessing, monitoring and managing risk, which is what security is about as well. Security policy and governance are therefore intertwined.

After the IRA bombing of central Manchester in 1996 40% of the businesses which were affected by that bomb blast, did not re-open.¹ Our reaction to this frightening statistic must also be put in the context of what United States Homeland Security Secretary, Michael Chertoff said in April 2005, that the “risk management approach applies to infrastructure too....It means that not everything gets 100% protected”².

In this paper I will discuss critical infrastructure protection and consider some of the governance issues arising from the relationship between government and business. I will also suggest that the government responses to these

---


issues show a move beyond fragmented government.

**Critical infrastructure**

The agreed view of all Australian governments is that when we are talking about critical infrastructure we are talking about those:

physical facilities, supply chains, information technologies and communication networks, which, if destroyed, degraded or rendered unavailable for an extended period would significantly impact on the social or economic well-being of the nation or affect our defence or national security.

“Significantly impact” refers to “an event or incident that puts at risk public safety, confidence, threatens our economic security, harms our economic competitiveness or impedes the continuity of government and its services.”

Critical infrastructure also involves all the chains that link together, finance, transport and distribution, energy utilities, food health, communications, key government services and so on. And we also need to think about the interdependencies between all these elements. Some of the issues discussed in other papers, such as systems and convergent communication technologies, make this an even more important issue today.

Government and the owners and operators of critical infrastructure need to work together to identify these interdependencies and to put in place strategies to reduce risk where possible.

---

3 The definitions in the part of the paper are from the definition of critical infrastructure agreed by all Australian Governments which can be found in What is critical infrastructure? www.nationalsecurity.gov.au/agd

4 The definition also states “The continuity of supply of all critical infrastructure is dependent, to some extent, on the availability of other infrastructure and some sectors are mutually dependent on each other. The degree and complexity of interdependencies is increasing as Australia becomes more dependent, for instance, on shared information systems...”
Joined-up Government

The theme of this conference is about moving beyond fragmented government. The very fact that all Australian governments are identifying infrastructure that is critical to the nation or vital to a State shows the nature of the joined up work all governments are engaged in. One of the key lessons that emerged from the events of 11 September 2001 is the importance of coordination between agencies in all levels of government to ensure effective emergency management and law enforcement. In a speech shortly after those attacks, the Director of the FBI said, “No one agency or entity at any level, whether it be federal, state or local, has the length or breadth of talent and expertise. We must work together. Law-enforcement, quite simply, is only as good as its relationships.” And that phrase “only as good as its relationships” is a theme that could underlie a lot of the issues about joining up government and making whole of government approaches work.

The State of Victoria has had for many years structures and processes in place for what is called the “all agencies, all hazards” approach to major incidents. This means that there is one system in place to provide a whole of government response to all major incidents, whether they are natural disasters or terrorism. This was first tested in Victoria through the response to the outage at Longford where an industrial accident brought about major interruptions to the power supply. This approach has now been imported into the modern world of counter-terrorism. The National Counter Terrorism Plan extends that approach to the Commonwealth and other States as well. But we need to understand that well-functioning relationships between the policy areas, law-

---

enforcement, intelligence and emergency management agencies across all jurisdictions are key to making these structures and processes work. All Victorian agencies work hard to keep strong relationships with other Victorian agencies, with officials in other States and Territories, and with the Commonwealth.

Setting aside its cause (politically motivated violence) the result of a terrorist act is in many respects, just another emergency. An explosion of a gas main in a street results in response by police and emergency services and health professionals, whatever its cause. People may recall that in 2003, there was a massive power failure across northeastern United States. There was enormous relief that this was not in fact a terrorist event. However, the social and economic disruption remained. Similarly, in the United Kingdom, as many people have died in recent years from rail accidents as died from the bombs detonated on the London underground.

One of the things that business therefore needs to understand is that, in terms of response, many of the things they have in place for ‘normal’ emergencies are equally appropriate for a terrorist event. As Secretary Chertoff said earlier this year in the United States, “the market place itself creates a very strong incentive through business self-interest in enhancing security”\(^6\). A terrorist event is therefore a possibility that businesses must prepare for in the same way as they prepares for other emergencies.

In New York after 11 September, those businesses that had taken the threat of Y2K seriously and had created robust business continuity plans were generally able to survive and continue operating after the 11 September attacks. While the nature of the threat is different, terrorism may have effects

---

\(^6\) Secretary of Homeland Security Michael Chertoff at the US Chamber of Commerce, Washington DC, April 29 2005
similar to other potential disasters that a business may suffer. Businesses protect themselves from fraud, system failure and other disaster. Dealing with the consequences of terrorism should therefore also be the part of any risk management and business continuity plan. This does not depend on having detailed prescriptive government regulation about security. The role of government is, as Secretary Chertoff said, “collaborative, it tries to give guidance…it doesn’t dictate or try to micromanage”.

In Australia, business often gives mixed messages about its views on regulation. On the one hand, it does not want to be told what to do. On the other hand, it can seem it wants to be certain that if a business does XY and Z then it will have covered all the risk. Governments these days, however, favour light-handed regulation that stresses outcomes rather than detailed prescriptive regulation.

I recall working in the early 1990s on issues to do with mining regulations when some regulations actually contained enormous detail on, for instance, how to put up a ladder. These were replaced by fairly simple statements about providing a safe working environment. Likewise in the new security environment, governments do not provide detailed advice on how businesses should protect themselves. There is an ever growing number of consultants who are willing to do that. As one senior police officer put it, we do not put a police officer in everyone’s backyard, but if there is an intruder, the police will respond. To do otherwise, transfers all the risk to government and would absolve business from taking steps that it should be taking anyway. This was stated well in one of the foundation plans for homeland security in the United States which said that the “private sector should conduct risk assessments on their holdings and

invest in systems to protect key assets. The internalization of these costs is not only a matter of sound corporate governance and good corporate citizenship, but it is also an essential safeguard of economic assets for shareholders, employees, and the Nation.”

Should government intervene?
The market itself therefore imposes some discipline on business to address security issues because businesses that are not prepared for catastrophic events risk losing their business entirely. While the market creates a strong incentive, sometimes governments have to impose regulatory obligations. There is a general view that new regulation should be based on broad consideration of benefits, costs and risks. Regulation can create compliance costs, reduce productivity and constrain labour force participation.

Some businesses are concerned about the regulatory burden arising from the new security environment. But Government is also concerned about the consequences of unnecessary regulation. One question is why should governments impose regulations on those businesses that do not take care of themselves? Governments across Australia, and indeed much of the developed world, have tried to stay out of prescriptive measures. The UK Home Office Handbook, which is designed to help businesses affected by major terrorist bombings in urban areas to recover quickly, said this about itself:

> the Handbook cannot provide a blueprint for every kind of business. Indeed, there can be no such blueprint. The measures which any particular business will need to take in order to recover from the consequences of a large bomb explosion will depend on the nature and circumstances of

---

that business. Only a person with a sound understanding of the operation of that particular business is in a position to draw up its recovery plans.  

This is why in critical infrastructure protection the main role of government is to be a guide and not a regulator. For instance, the Council of Australian Governments has endorsed a set of national guidelines on infrastructure protection available to all businesses.

In some cases it is clear that governments have to intervene in a very prescriptive way, such as with the major airports, which have been regulated heavily for years. Security at ports now has a new regime in place through Commonwealth legislation, which in turn implements new international maritime standards promulgated by the International Maritime Organisation (IMO). Some of these new standards themselves are quite inflexible, but the Victorian Government and its ports have complied with all of them, because if countries that do not comply with these new IMO standards are unable to trade with the United States.

A contrast is the way in which governments in Australia are working together on issues of surface transport security through the new Inter-Governmental Agreement that was signed at the 3 June 2005 COAG. The IGA is designed to achieve national consistency in approach. However, as every city in Australia has a different public transport system because of geography, population, history and the way the cities have grown. Only Sydney and Melbourne have any significant underground rail; Melbourne has trams; Sydney has ferries. Significantly in Melbourne the major public transport systems are privately operated. So across Australia a single heavy handed national standard is neither practical nor desirable.

---

A specific approach has been developed in Victoria because so much infrastructure, including energy and public transport, is privately owned or operated. The new security environment meant that a new tool was needed to bridge the gap between the expectation that government would protect critical infrastructure and the fact most of it is in private hands. To do this Victoria passed Part 6 of the Terrorism (Community Protection) Act 2003, covering essential services infrastructure and risk management planning. Under one section of this Act the operator of a declared essential service must prepare a risk management plan to cover prevention, mitigation, recovery and continuity of service. As well, the operator must audit its plan once a year and has a duty to test the plan and participate in an exercise under the supervision of the Chief Commissioner of Police.

The reason for this legislation is that while government does not prescribe standards, the government does have a role in making sure private operators are fulfilling their obligations to the community of which they are a part. Of course, most owners and operators want to do this as part of their obligations to their shareholders. The Victorian legislation is an attempt to connect the obligations of government with those of business, and to put in place a regime that allows government to insist that businesses address key risk management issues. There is no such legislation in any other jurisdiction in Australia partly because Victoria has the most privatised sectors in regards to its infrastructure. For other States, the energy and the transport sectors are still in public hands. Those governments can intervene to insist upon plans and systems in a way that is very difficult to do within Victoria in the absence of legislation.

Business and government increasingly realise that in this new
era, issues of security are become part of mainstream thinking. They are not things that are just out there that somebody else has to deal with. They are part of this new world in which we live, and we have to take account of them.

The Director-General of the British Security Service said in an address to British industry in 2004 that in “the same way that health and safety and compliance have become part of the business agenda, so should a broad understanding of security, and considering it should be an integral and permanent part of…planning and Statements of Internal Control.” She also added, do not allow it just to be left to specialists.

Security is no longer an add-on in the world of governance. Every aspect of our society is challenged by the new security environment. What I have outlined are just some of the issues that are now becoming part of mainstream thinking. These issues have only been given high public prominence in the last four years. However, the security environment that has taken a generation to develop its current form will be with us for at least a generation to come. So, we all need to realise that there are now new, additional, set of measures against which governments and business must assess all their policies and actions.

---

10 Eliza Manningham-Buller, CBI annual Conference, 8 November 2004.
www.mi5.gov.uk