This is the published version:


Available from Deakin Research Online:

http://hdl.handle.net/10536/DRO/DU:30036276

Reproduced with the kind permissions of the copyright owner.

Copyright: 2011, Academic Publishing
Australian National Critical Infrastructure Protection: A Case Study

Matthew Warren and Shona Leitch
Deakin University, Australia
mwarren@deakin.edu.au
shona@deakin.edu.au

Abstract: Australia has developed sophisticated national security policies and physical security agencies to protect against current and future security threats associated with critical infrastructure protection and cyber warfare protection. This paper will discuss some of the common security risks that face Australia and how their government policies and strategies have been developed and changed over time, for example, the proposed Australian Homeland Security department. This paper will discuss the different steps that Australia has undertaken in relation to developing national policies to deal with critical infrastructure protection.

Keywords: critical infrastructure, Australia and policy

1. Introduction

Australia is a modern society and is highly dependent on key critical systems at the national and state level. These key systems have become more dominant as the Information Age has developed. These key systems are grouped together and described as critical infrastructure; this is infrastructure so vital that its incapacity or destruction would have a debilitating impact on defence and national security (Lewis, 2006). Many of these critical systems are based upon ICT (Information and Communication Technology) systems.

Australia takes ICT security very seriously, it has been estimated that Australian organisations spend between A$1.37 – A$1.74 billion per year on IT security, and the total financial losses due to computer-related security incidents in the 2006 financial year have been estimated to be between $595 and $649 million (Australian Institute of Criminology, 2009).

This paper will review the current strategies used by Australia over a decade and evaluate their differences and discuss the reasons for these differences. Future threats such as Cyber Warfare and the steps that are being proposed will be considered. This paper will highlight current Australian best practices in critical infrastructure and cyber warfare protection many of which may be applicable in a European context and provide an informative contrast.

2. The initial view of the Australian Federal Government

The initial focus of the Australian Federal Government policy was that critical infrastructure protection was a commercial consideration and related to Information Security (Busuttil and Warren, 2004). The Australian Federal Government has been aware of the problems that Australian corporations may have with dealing with these new security issues. The Australian Federal Government has responded by offering advice for corporations. The initial Australian Government advice (AGD, 1998) suggested ways in which organisations could reduce Critical Infrastructure Protection risks (Busuttil and Warren, 2004):

- Organisations should implement protective security such as passwords etc in accordance to a defined security standard such as AS/NZS 4444 (Now 17799) (Information Security Management);
- Organisations should formally accredit themselves against security standards such as AS/NZS 4444 (17799);
- Organisations should raise awareness of security issues such as password security, E-commerce risks among their staff;
- Organisations should train their staff in how to use computer security systems efficiently and effectively.

This advice was subsequently updated and in 2004 the Australian Government responded with new security advice (Australian Government, 2004):

- The Australian and New Zealand Standard for Risk Management AS/NZS 4360:1999 is the standard by which all critical infrastructure will be assessed to assist with the review of risk management plans for prevention (including security), preparedness, response and recovery (PPRR).
Matthew Warren and Shona Leitch

In 2004 the Australian Federal Government formally defined the following: "Critical infrastructure is defined as 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 Australia's ability to conduct national defence and ensure national security" (Australian Government, 2004). In essence this description describes organisations that exist at a government level or at a corporate level (Australian Government, 2004).

Historically, much of Australia’s infrastructure was originally owned and operated by the public sector at the federal, state and local government levels (Smith, 2004) however the majority of Australia’s critical infrastructure has now been privatised and is under private sector ownership. Consequently, protecting Australia’s critical infrastructure now requires a higher level of cooperation between all levels of government and the private sector owners. Hence, the federal government has developed a policy for critical infrastructure protection that focuses broadly on addressing the following strategies (Australian Government, 2004; AGD, 2004):

- Distinguishing critical infrastructures and ascertaining the risk areas;
- Aligning the strategies for reducing potential risk to critical infrastructure;
- Encouraging and developing effective partnerships with state and territory governments and the private sector;
- Advancing both domestic and international best practice for critical infrastructure protection.

As Warren and Leitch discussed (Warren and Leitch, 2010), the Australian Federal Government recognised the importance of crucial systems and the development of new industry support mechanisms, in particular Trusted Information Sharing Network (TISN).

The TISN is a forum in which the owners and operators of critical infrastructure work together by sharing information on security issues which affect critical infrastructure (TISN, 2007). TISN requires the active participation of Critical infrastructure Protection owners and operators of Critical infrastructure Protection, regulators, professional bodies and industry associations, in cooperation with all levels of government, and the public. To ensure this cooperation and coordination, all of these participants should commit to the following set of common fundamental principles of Critical infrastructure Protection (TISN, 2007). These principles are (TISN, 2007, Warren and Leitch, 2010):

- Critical infrastructure Protection is centred on the need to minimise risks to public health, safety and confidence, ensure economic security, maintain Australia’s international competitiveness and ensure the continuity of government and its services;
- The objectives of Critical infrastructure Protection are to identify critical infrastructure, analyse vulnerability and interdependence, and protect from, and prepare for, all hazards;
- As not all critical infrastructure can be protected from all threats, appropriate risk management techniques should be used to determine relative severity and duration, the level of protective security, set priorities for the allocation of resources and the application of the best mitigation strategies for business continuity;
- The responsibility for managing risk within physical facilities, supply chains, information technologies and communication networks primarily rests with the owners and operators;
- Critical infrastructure Protection needs to be undertaken from an ‘all hazards approach’ with full consideration of interdependencies between businesses, sectors, jurisdictions and government agencies;
- Critical infrastructure Protection requires a consistent, cooperative partnership between the owners and operators of critical infrastructure and governments;
- The sharing of information relating to threats and vulnerabilities will assist governments, and owners and operators of critical infrastructure to better manage risk;
- Care should be taken when referring to national security threats to critical infrastructure, including terrorism, so as to avoid undue concern in the Australian domestic community, as well as potential tourists and investors overseas;
- Stronger research and analysis capabilities can ensure that risk mitigation strategies are tailored to Australia’s unique critical infrastructure circumstances.
Matthew Warren and Shona Leitch

3. Australia’s critical infrastructure – the alternative viewpoint

During the time that the Australian Federal Government defined National Policy for Critical Infrastructure Protection, the opposition Australian Labor Party defined their own very different policy and viewpoint. The following is a time sequence of their policy development:

2001 - Initial Policies

In October 2001, as a response to the act of terrorism in New York in September of the same year, the Australian Labor Party (ALP) which was the Australian opposition of the time led by Kim Beazley proposed a range of national security reforms. The reforms focussed on three main areas (ALP, 2001):

- Improving border security;
- Combating terrorism;
- Improving national security planning.

It was stated that these reforms were previously in the planning stages but the first announcement was made only two days after the attack on the World Trade Center. Australia’s border security was announced by them as a high priority with changes to the coast guard and aviation security regimes upmost. In terms of the aviation industry this included more counter-terrorism measures including the Federal Government taking over responsibility for all airport security checks, making sure there is a visible presence of officers at airports and introducing tighter controls on aviation security information by amending current laws and regulations (ALP, 2001).

Rather than just concentrating on the physical security controls which were very much in the forefront of the public’s mind in 2001, the ALP also proposed a range of changes and initiatives in regards to protecting Australia’s national infrastructure. This focused in on the establishment of a Defence Cyber-warfare Task Force which would use all the elements and agencies of the current defence force to counteract cyber security threats and cyber terrorism attacks.

This strategy proposed by the ALP revolved around the concept of “Homeland Security”, this was the first time this term was used in Australia and the notion of integrating security agencies, expanding the range of activities and including the national infrastructure (transport, electricity, water, communication systems etc) as the most important elements was a dramatic leap in the protection of Australia from cyber terrorist threats.

2003 – 2005 – A Period of Reflection

In 2003, the Australian Labor Party was still the countries opposition party. The department of Homeland Security was still being advocated by them, so much so that an opposition Security minister was created whose portfolio encompassed border protection, crime prevention, intelligence-gathering, investigation and prosecution (ALP, 2003) and they set up the Shadow Department of Homeland Security Portfolio.

In 2005 the notion of a Homeland Security department was still forefront in the ALP’s policies as a way to address the issues of national security and bring together all of Australia’s defence agencies (as was done during the 2000 Olympic Games held in Sydney, Australia). They believed that this level of integration and cohesion was the only way to truly protect Australia and its citizens from the continued threats and attacks. They outlined a number of cases which they felt supported this proposal (Beazley, 2005):

- The alleged involvement of Sydney Airport baggage handlers in an international drug trafficking syndicate. The Australian Federal Police claims baggage handlers were key players in a conspiracy to smuggle cocaine worth $15 million into Australia;
- Constant warnings from the Transport Workers’ Union, that the Federal government had been aware of potential security breaches at Australian airports for at least four years and the TWU’s call for improved security checks of short term employees and the immediate x-ray screening of all baggage and freight;
- Passengers’ baggage containing large amounts of narcotics being diverted to domestic carousels to avoid Customs inspections;

277
Matthew Warren and Shona Leitch

- 39 security screeners out of 500 employed at the airport have serious criminal convictions, with a further 39 convicted of minor matters;
- Engineers with unauthorised duplicate keys;
- Lack of customs checks on airline staff.

2007 – 2008 From Opposition to Government

The Australian Labor Party in 2007 had moved from being the opposition party to forming Government. One of their main policies leading into the Federal election was that they would continue with their long term plan of forming a Department of Homeland Security.

In 2008, the Prime Minister announced that he planned to cancel the long term plans of the ALP to create the new department on the basis that the integration of all the defence agencies would be too “cumbersome” (Franklin and Walters, 2008).

Seven years of planning and proposals had disappeared less than a year after an election due to the complexities of how administration would be dealt with and confusion over how the complex integration could be achieved (Nicholson, 2008).

The fact that the initial plans arose swiftly after the terrorist attacks in September 2001 may pose questions as to whether the plans were ill thought out and borne out of the need to react rather than a sensible, productive and workable policy.

4. Recent Australian Government strategy

The Australian Federal Government (2008) has identified new security challenges, it is increasingly evident that the sophistication of our modern community is a source of vulnerability in itself. For example, we are highly dependent on computer and information technology to drive critical industries such as aviation; electricity and water supply; banking and finance; and telecommunications networks. This dependency on information technology makes us potentially vulnerable to cyber attacks that may disrupt the information that increasingly lubricates our economy and system of government” (Rudd, 2008). This public acknowledgement by the Australian Prime Minister, Kevin Rudd, identifies the new security challenges facing critical infrastructure protection and highlighted the following security concerns (Rudd, 2008):

- Maintaining Australia’s territorial and border integrity;
- Promoting Australia’s political sovereignty;
- Preserving a cohesive and resilient society and strong economy;
- Protecting Australians and Australian interests both at home and abroad, and
- Promoting a stable, peaceful and prosperous international environment; particularly in the Asia-Pacific region, together with a global rules-based order which enhances Australia’s national interests.

In 2009 the Federal Australian Government has responded to the issues regarding cyber security and critical infrastructure by proposing a coherent and government led approach to critical infrastructure protection. The primary objectives identified focus on all areas of Australian society where there are security risks, e.g. that individuals should be aware and take steps to “protect their identities, privacy and finances online” (Australian Government, 2009) that businesses and the government operate “secure and resilient information and communication technologies” and trusted electronic operating environment that supports Australia’s national security and maximises the benefits of the digital economy (Australian Government, 2009). The Australian Federal Government also has developed a wide range of new strategic directions to focus Australia’s cyber security programs (Australian Government, 2009):

- Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest;
- Educate and empower all Australians with the information, confidence and practical tools to protect themselves online;
- Partner with business to promote security and resilience in infrastructures, networks, products and services;
Matthew Warren and Shona Leitch

- Model best practice in the protection of government ICT systems, including the systems of those transacting with government online;
- Promote a secure, resilient and trusted global electronic operating environment that supports Australia’s national interest;
- Maintain an effective legal framework and enforcement capabilities to target and prosecute cyber crime;
- Promote the development of a skilled cyber security workforce with access to research and development to develop innovative solutions.

As part of the new Australian Federal Government strategy, a new of number bodies have been developed with new capabilities. These include (Australian Government, 2009):

- CERT (Computer Emergency Response Team) Australia;
- This new Government body has moved to a national level to enable a “more integrated, holistic approach to cyber security across the Australian community”;
- Some of the previously formed cyber security activities that were undertaken by numerous different agencies such as the Australian Government’s Computer Emergency Readiness Team (GovCERT) have been combined together to form CERT in order to promote a greater (shared) understanding; provide targeted advice and give Australians a single point of contact.
- Cyber Security Operations Centre (CSOC).
- The core functions of the CSOC are focused mainly on government, infrastructure and critical private sector systems and aims to be a source for all issues related to awareness (especially the detection of sophisticated threats) and a facility to respond to cyber security risks and problems which are of national importance.

Another key aspect of CSOC is that it provides Australian Defences with a cyber warfare capability and provides a resource designed to service all government agencies (DSD, 2011).

The Australian Federal Government has started to refocus away from Critical Infrastructure Protection to Critical Infrastructure Resilience. The Australian Attorney General Robert McClelland announced that “The time has come for the protection mindset to be broadened – to embrace the broader concept of resilience”. The aim is to build a more resilient nation – one where all Australians are better able to adapt to change, where we have reduced exposure to risks, and where we are all better able to bounce back from disaster” (TISN, 2010).

The Australian Federal Government in 2010 launched the new Critical Infrastructure Resilience Strategy. The aim of this new strategy is the continued operation of critical infrastructure in the face of all hazards as this critical infrastructure supports Australia’s national defence and national security and underpins our economic prosperity and social wellbeing. More resilient critical infrastructure will also help to achieve the continued provision of essential services to the community (Australian Government, 2010). This new strategy also deals with new areas such as disaster protection and disaster resilience and this shift in policy is going to have a major impact upon Australia.

5. Discussion

The major issue facing Australia is the currently adopted distributed model of critical infrastructure protection and decision making and how that can effectively manage and secure Australia’s critical infrastructure. Whilst it is commendable that an Australian Federal Government has faced the issue of critical infrastructure and cyber threats, the fact that this approach attempts to cover the entirety of Australia may in itself be problematic. There has been some streamlining of operations by nationalising CERT, however there are still a number of separate agencies that are involved in this process; Attorney-General’s Department (AGD), the Australian Communications and Media Authority (ACMA), the Australian Federal Police (AFP), the Australian Security Intelligence Organisation’s (ASIO), the Defence Signals Directorate (DSD), the Department of Broadband, Communication and the Digital Economy (DBCDE), the Australian Government Information Management Office (AGIMO), the Joint Operating Arrangements (JOA) and the Cyber Security Policy and Coordination (CSPC) Committee. It is clear that there has been an overall Government shift to form two “umbrella” agencies (CERT and CSOC) to monitor, promote and control cyber threats however complexity will still arise as there are so many sub agencies that are involved in this process. In an area such as cyber security where speed is often of utmost importance to limit damage, the interaction of a large number of other agencies will surely slow
Matthew Warren and Shona Leitch

this process down. If an Cyber attack occurs in real time against Australia, would they be able to react and make decisions in real time, or would the distributed model actually impact the decision making process? Another unique issue that relates to Australia is the federated government system consisting of a federal government and a number of state governments. A key issue is that when an attack occurs against an infrastructure at a state level that the response time to escalate the decision making process to the Federal government may be slow. This time lag could cause serious consequences and limit the effectiveness of these agencies.

A new factor with the introduction of CSOC is the move away from civilian organisations protecting Australia’s critical infrastructure and cyber security risks and making defence organisations responsible for this role. This may heighten the chance of attacks against Australia’s critical infrastructure because it could be considered a military target. The major shift in Australian policy is the announcement in 2010 of the move away from Critical Infrastructure Protection to Critical Infrastructure Resilience and the inclusion of natural disaster into the policy. This will have a major impact upon Australia and the real implications are still yet to emerge especially with the recent natural disasters in Australia.

6. Conclusion

Australia over the last decade has taken major steps in the protection of its national critical infrastructure. The Australian model is a workable model that has helped to protect Australian critical infrastructure against physical and cyber risks. The issue is whether the distributed model will work in a real time situation and whether the time delays would impacts the decision making processes.

A new emerging issue is the focus upon Critical Infrastructure Resilience and the future impact that this may have.

References

Australian Government (2004). Protecting Australia Against Terrorism, Department of the Prime Minister and Cabinet, Barton, ACT.

280