AUSTRALIA'S AGENDA FOR E-SECURITY EDUCATION AND RESEARCH

M.J. Warren
School of Information Technology, Deakin University,G eelong, Victoria, Australia, 3217

Abstract: The paper describes the development of a national E-security strategy for Australia. The paper discusses the rationale behind its development and the issues that relate to the policy and its possible implementation and its impact upon E-security teaching and E-security research. The paper also discusses how current situations are having an impact on the development of a national education and research initiative.

Key words: Australia, National Policy, E-security, Security education and Security research.

1. INTRODUCTION

The widespread use of computer systems has resulted in a new dependence upon computers and the data they contain. Computer systems now contain millions of records relating to commerce, healthcare, banking, defence and personal information. All this information is at risk of either being mis-used for fraudulent purposes or modified for malicious reasons. This description describes the situation in most Western countries including Australia. The problem that all developed countries face is how to define a policy for E-security at a national level. In order for this policy to be effective it must also cover key issues such as security education and security research.

This paper describes the steps that Australia has taken and some of the issues that Australia faces in development of a national policy.

In terms of the paper the term E-security will be used, this is the term used by the Australian federal government to represent what is known as IT Security, Information Security, etc.

C. Irvine et al. (eds.), *Security Education and Critical Infrastructures*

2. THE AUSTRALIAN SECURITY PROBLEM

A recent AusCERT Survey (Auscert, 2002) has focused upon the state of E-security within Australia, the following is a summary of the main results:

- 67% of all organizations surveyed have been attacked in 2002 - twice the 1999 level and 35 per cent of these organizations experienced six or more incidents;
- 98% of companies had experience either computer Security incidents / crime or other forms of computer abuse (such as network scanning, theft of laptops, employee abuse);
- Of Australian organisation who were victims of computer incidents, 65% of these attacks were from internally parties within the organisation and 89% came from external sources;
- 43% of Australian organizations were willing to hire ex-hackers to deal with security issues, three times more than in the US.

The survey showed that E-security and computer misuse are a major problem within Australia. The survey showed that external attacks were the source of the majority of attacks. An Australian Federal Government department NOIE (National Office of the Information Economy) sponsored project tried to determine the risks associated with the Information Economy. They determined that 43% of survey respondents were concerned with privacy issue and 42% of survey respondents were concerned about fraud (Allen Consultancy Group & NOIE, 2002).

These studies indicated that Australia has a major problem in regards to E-security and that people are concerned about the associated E-security risks. This also points to the importance of E-security education and E-security R&D in helping to reduce this problem.

3. DEVELOPMENT OF A NATIONAL POLICY

NOIE has been looking at the Australian E-security situation by undertaking a number of projects. The aim of the first project was to determine what the situation was within Australia in regards to E-security education. The project found that the main issues were (Aeuckens, 2001):

- Demand for people with E-security skills is expected to be strong over the few years;
- Recruitment of personnel with E-security skills is difficult compared to other IT&T skills.

This project also identified some key issues that related to Australian organisations and the impact of E-security, these key issues were (Aeuckens, 2001):

- *Demand is rising.* As E-security becomes an integral business issue, demand for skilled personnel is growing within Australia;
- *Recruitment of people with the right skill sets is difficult.* The greatest difficulty is in recruiting people with well-rounded security and risk management skills (likely to include technical and business skills);
- *E-Security is not just an issue for security personnel.* All IT personnel should have an awareness of E-security issues and its place in a business environment;
- *Limited Graduate programs.* Many organisations recruited new IT graduates. Graduates did not generally have any specific understanding of security, therefore it was necessary for them to undergo further training;
- *Education and training opportunities in E-security are not widely available.* The minimum qualification demanded by employers is generally at the Bachelor level but these lack security content.

A further NOIE investigation was into E-security research and its development within Australia. This NOIE project found it was essential to ensure the long-term future of Australia's E-security research for a number of reasons (King, 2001):

- Dependence on foreign E-security providers limits the input that Australia has into the type and character of products and services developed. Australia should not be reliant upon other countries dictating appropriate levels of security;
- A commercial imperative also exists. A secure and trusted electronic environment is a necessary condition enabling electronic commerce;
- The E-security industry is experiencing substantial growth. R&D is an important link in the innovation chain driving developments in this industry sector. The Government has an important role to play ensuring that Australia is a global supplier as well as a consumer of E-security products and services. Eventually, some kind of security technology, be it hardware or software, will be resident in every networked device. Maintaining a critical mass of E-security R&D in Australia is essential to achieving this aim;
- A robust E-security R&D environment can also play a key role in attracting skilled E-security workers to Australia, and keep homegrown talent from moving overseas;
- E-security R&D will assist in providing the Government with the tools to perform its role in law enforcement activities to protect information infrastructure and the public.

These projects showed the importance of E-security teaching and E-security R&D in an Australia context. The outcome of the NOIEs projects was the need to develop a National E-security strategy. The objectives and aims of the draft policy were defined as (Aeuckens, 2001):

- That Australian Defence Signals Directorate (DSD) to scope the feasibility of new schemes, e.g. a Scholarships for Service program to provide scholarships to students in exchange for a period of service with DSD upon graduation, etc;
- That NOIE canvass the interest of other major government IT employers in participating in a scholarships and/or internship/vacation employment program;
- That key academics and government and industry representatives work towards a security core body of knowledge reflecting the latest developments in security technologies and policies;
- That a comprehensive survey of industry and government be conducted to obtain views on a wide range of security skills-related issues in order to inform the design and implementation of future initiatives;
- That NOIE undertake further work to scope the establishment of a National E-security Education Centre (NESEC), in conjunction with universities (Australian and overseas), DSD and other government and industry representatives. NESEC would be a central repository of E-security course information, which institutions could build into their existing IT/Computer Science courses;
- The feasibility of an industry-backed E-security professional certification scheme should be further investigated, including the potential applicability of the internationally available schemes to Australian industry and government needs.

NOIE had defined within its National E-security strategy two major key areas that were important for the future of Australia, these were:

- E-security Teaching – ensuring that E-security skills are taught at Australian Universities to all students. Ensuring there is co-operation between Australian Universities and industry to teach and develop courses;
- E-security R&D – ensuring that E-security R&D is considered important area for Australia's future R&D national strategy.

Then events outside Australia caused a major impact, the bombing of the World Trade Center (September, 11th, 2001) and the Bali bombing (October, 12th, 2002) had a direct impact upon Australian national policy. In the Australian Federal budget (2001-02) the government announcement that A$400 million would be allocated over four years for defence purposes (Scott, 2001. This had an impact that budgets of other government departments were reduced.

In 2002 the structure and role of NOIE was changed, the area of IT industry policy and its development was removed from its portfolio, this has in impact upon the role of NOIE (Cant, 2002). Following the budget, the role of NOIE's strategy was refocused upon the following areas (Western Australia Government, 2002):

- developing strategic advice on the demand drivers for Broadband, and provide the secretariat for the Australian Broadband Advisory Group;
- mapping the long term strategic environment for the ICT industry, as a contribution to the ICT industry 'Framework for the Future' study;
- accelerating the uptake of E-business and E-procurement by small to medium business enterprises; and
- promoting E-security, facilitating implementation of a coordinated national E-security agenda.

An important policy refocus during this time was the fact that NOIE was more involved with "Protecting National Infrastructure: E-security". NOIE became more involved with a number of projects aimed at protecting Australian Critical Infrastructure such as e.g. National Security Australia, (http://nationalsecurity.ag.gov.au), and Business-Government Task Force on Critical Infrastructure (http://www.cript.gov.au/). This was a major shift away from general E-security and a move towards National Security Protection.

The author went to Canberra in 2002 to talk to key stake holders of NOIE to find out about the current state of the National E-security strategy. The outcomes of the meetings were:

- Key staff had left NOIE, this had a direct impact upon the project as there was no one left to 'champion' it;
- Budgets cuts and realignment of strategic aims had a major impact upon NOIE with a refocus of its goals and objectives.

The amended National E-security strategy was cut back to only **one area** of the initial National E-security strategy, which was:

- The feasibility of an industry-backed E-security professional certification scheme should be further investigated, including the potential applicability of the internationally available schemes to Australian industry and government needs.

Currently NOIE is working with AusCERT to develop a strategy for this objective. This means that all the key issues put forward by the National E-security strategy in relation to E-security teaching and E-security R&D have been abandoned including the need to develop an Australian common body of knowledge and surveys of industry to determine needed security skills with Australia.

4. CONCLUSION

The aims of the draft National E-security strategy was to define key areas for Australia's development, which were E-security teaching and E-security R&D. But because of world events the focus of NOIE and National E-security strategy has moved towards critical infrastructure protection. This change in strategic direction could cause long-term damage for Australia's development as E-security teaching and E-security R&D is abandoned.

REFERENCES

Aeuckens D (2001) E-Security Skills, Education and Training in Australia: A Policy Scoping Paper, NOIE Report. Canberra, Australia.

Allen Consultancy Group & NOIE (2002) Report: Australia Information Economy – the Big Picture, Sydney, Australia.

AusCert (2002) 2002 Australian Computer Crime and Security Survey, University of Queensland, Australia.

Cant, S (2002) Confusion reigns as NOIE role shifts, The Age, June 24th, Melbourne, Australia.

King G. (2001) Report on E-security R&D in Australia: an initial assessment, NOIE Report. Canberra, Australia.

NOIE (2001) Protection of Australia's National Information Infrastructure & E-security Policy (Administrative and Operational Arrangements), Canberra, Australia.

Scott B (2001) Media Release: Budget 2001-02 - Defence People Win, MIN 144/2001, Department of Defence, May, Canberra, Australia.

Western Australia Government (2002) NOIE focus on economic transformation, improving government information.

URL: http://www.ecommercecentre.online.wa.gov.au/government/noie.htm

Accessed 12/12/02