AUSTRALIAN NATIONAL AUDIT OFFICE

14th Annual Global Working Group Meeting of Auditors-General

Country Paper - Australia

Cyber Security

Tokyo, Japan
11th April 2013

Ian McPhee, PSM
Auditor-General for Australia

With thanks to William Na, David Gray, and Lesa Craswell of my Office for their assistance in the preparation of this paper

Australian National Audit Office

Introduction

The internet provides government and business alike with opportunities to operate more efficiently. Its exponential growth and penetration has fundamentally changed the way we work and interact socially, and will continue to do so. Almost everything is now connected online and accessible via the internet.[1] For example, around 80% of Australian tax payers have their annual tax returns lodged electronically with the Australian Taxation Office; and virtually all import and export duties are being processed by the Australian Customs and Border Protection Services online electronically. Worldwide, it is an ongoing trend to increasingly integrate electricity, power, transport, and communications into the internet.[2]

ICT, or information communication technology, underpins this phenomenon and continues to develop at a historically unprecedented rate. Technologies development can lead to new opportunities and benefits due to increased connectivity, but can also create new exposures or accentuate old vulnerabilities, such as organised cyber crimes, state sanctioned or industry based cyber espionage and cyber terror, theft of consumers' identities and private information, just to name a few.

The Australian Government has acknowledged that being safer and more secure online is a shared responsibility. Emerging cyber threats require engagement from the entire Australian community – from government and law enforcement to the ICT industry and private sector and most importantly, members of the public – to create a safer cyber environment. A partnership approach to cyber security across all Australian governments (federal, state and local), the private sector and the broader Australian community is essential.

Opportunities, threats, risks and cyber security

As mentioned above, the new opportunities brought by the increased reliance on internet connected devices and services come with additional risks. As technologies evolve, the threat landscape also rapidly changes and risks commonly increase.

It is rare that a day goes by without a media report of malicious conduct, intrusions or crimes occurring in cyber space. Both Government and the private sector are the targets of cyber attacks. As publicly acknowledged by the Australian Security Intelligence Organisation (ASIO), cyber based electronic intelligence gathering is being used by both state-sponsored and non-state actors against Australia on a large scale to extract confidential information from governments, the private sector and ordinary individuals, with more than 65% of intrusions observed being economically motivated. Electronic intelligence gathering is used to steal intellectual property, commercially advantageous information, weapons designs, and defence secrets.[3]

In 2012, 5.4 million Australians fell victim to cyber crime with an estimated cost to the economy of $1.65 billion. According to figures released by Australian Government intelligence agency the Defence Signals Directorate, in the period January to November 2012, there have been over 1300 cyber security incidents against government entities, in which over 470 incidents warranted a response from the agency. Further, the Director General of the Australian Security Intelligence

[1] Minister of Defence, Stephen Smith, MP, *Speech to the DSD Cyber Security Conference, 2012*.
[2] Joye, C. *It's Global Cyber War Out There*, published in the Australian Financial Review, 2 January 2013.
[3] Ibid.

Organisation is quoted as saying, 'a single malicious algorithm might be able to turn off the lights, stop airplanes flying, or disrupt national financial transaction networks or the electricity grid.'[4]

Credible research undertaken by IBM and Gartner pointed out that people with malicious motives are increasingly using advanced technologies and conducting targeted cyber attacks. The fundamental concern is that the threats facing business and government are increasing at a rate faster than the deployment of defences in response. This gap needs to be bridged with a holistic approach that is integrated with long-term strategic business goals supported by appropriate legislation and awareness on the part of government. It is one thing to have a physical computer in an office to secure, but it is quite another to try to effectively secure a multitude of devices that rely on Internet connectivity to provide information processing and communication services.

Cyber security is an extension of the computer security we knew before the proliferation of the Internet and online services. The Australian Government defines cyber security as: 'measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.'[5]

Nowadays, cyber security is integrated with other business operations and becomes ever more strategic as enterprises move from physical to cyber space and more business is conducted in cyber space. This has necessitated organisations to completely rethink their approach to information security in this 'cyber age'. Senior executives need to be aware of the risks and incorporate cyber security measures while formulating their business strategies.

Focus of this paper

This paper briefly outlines the Australian Government response to cyber security from the perspective of utilising Internet technology in government administration. It also canvasses some of the lessons learned by government agencies when dealing with the elements of cyber security and by the ANAO encountering such issues while examining various government programs.

The paper concludes with a summary of the challenges for the ANAO when auditing selected government programs and administrations that are potentially impacted by cyber security.

Government initiatives in response to cyber security challenges

The Australian Government has an objective to protect government and Australian citizens from undue risks while utilising information and communication technology (ICT) for business or personal purpose. The Government takes cyber security seriously. In the *Strong and Secure: A Strategy for Australia's National Security*, launched by the Prime Minister in January 2013, the Government has put 'integrated cyber policy and operations' as one of three key priorities within this Strategy for the next five years.[6] The Government announced it has committed substantial funding and additional effort, including $1.46 billion out to 2020 to have appropriate arrangements in place to deal with cyber security threats against government, industry and citizens.

---

[4] Op cit, Joye, C.
[5] *Australian Government Cyber Security Strategy*, Attorney General's Department, 2009
[6] *Strong and Secure: A Strategy for Australia's National Security*, Department of Prime Minister and Cabinet website. http://www.dpmc.gov.au/national_security/docs/national_security_strategy.pdf

To assist in coordinating the Government's cyber policy agenda, the Department of Prime Minister and Cabinet assumed the responsibility for cyber security policy in December 2011. The department has created two roles – a National Security Chief Information Officer (NSCIO) and a Cyber Policy Coordinator (CPC) – to provide strategic direction and coordination for information sharing and on matters of cyber policy and strategies across the entire cyber 'spectrum'.

Further, as a key component of the Prime Minister's *Strong and Secure* policy announcement in January 2013, the Australian Government committed to establish a new Australian Cyber Security Centre (ACSC) within the Department of Prime Minster and Cabinet to provide leadership and coordination. The ACSC will be the hub of the government's cyber security efforts. Industry and state and territory partners will also have the opportunity to collaborate with the Government through the ACSC.

From a law enforcement point of view, the Australian Government has enacted legislation to combat cyber crimes. This legislation includes the *Cybercrime Act 2001*, the *Communications Legislation Amendment (Crime or Terrorism Related Internet Content) Act 2007*, and the *Cybercrime Legislation Amendment Act 2012*[7], which created a range of new computer offences and electronic communication offences (including hacking, denial of service attacks and virus propagation). These laws aim to combat and deter crimes that arise in cyber space. Additionally, the Government also enacted the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which is aimed at strengthening the protection of citizens' privacy in cyber space.

Government cyber security strategies, framework and policies

The objectives of the Australian Government's cyber security strategy are to ensure Australian citizens, businesses and government agencies are aware of cyber risks, make their information and communications technologies secure and resilient, and take steps to protect the integrity of their information, operation and administration.

Recognising that malicious cyber activity is a growing threat to Australia's national security and economic prosperity, the Government released the *Strong and Secure: A Strategy for Australia's National Security* as mentioned above. As stated in that document, the Government decided to focus on delivering integrated cyber policy and operations to deal with these developments in the context of its broader digital agenda and work closely with industry, the community and international partners.

At a government policy level, the Attorney-General's Department has issued the Protective Security Policy Framework (PSPF) that provides high level mandatory requirements applicable to all Australian Government agencies to protect the Australian people, information and assets, at home and overseas.[8] As a central document, the PSPF links Government security directives with agency specific policies and procedures and places an emphasis on the need for agencies to develop an appropriate security culture to securely meet their business needs to ensures the operational environment necessary for the confident and secure conduct of Government business.

[7] ComLaw, Australian Government website
[8] Australian Government Protective Security Policy, the Attorney-General's Department website. http://www.protectivesecurity.gov.au/pspf/Pages/default.aspx

A series of underpinning standards and guidelines have been developed to assist government agencies to improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest. The PSPF emphasises that the head of each agency is ultimately accountable for the agency's cyber security.

Government cyber security defence mechanism

At an operational level, the Australian Government has established some key entities to deliver cyber security capability with a common strategic purpose.

The Defence Signals Directorate (DSD) provides the Australian Government with advice and assistance to federal and state authorities on matters relating to the security and integrity of information. DSD produces the Information Security Manual (ISM) which is the standard governing the security of government ICT and which complements the PSPF.[9] The purpose of ISM is to assist Australian Government agencies in applying a risk-based approach to protect their information and ICT systems. The security controls defined in the ISM are designed to mitigate the most significant threats. The ISM has a wide application that also covers state and territory government agencies that implement the PSPF and organisations that have been authorised to access to sensitive or classified information held by the Government.

Based on its expertise, DSD has also developed detailed strategies, including its flagship document – the top 35 cyber security strategies, for advising agencies how to mitigate targeted cyber intrusions. DSD found that by implementing the following four of the top 35 strategies, organisations would have been able to prevent 85 per cent of targeted cyber intrusions:

- application whitelisting[10],
- patch applications[11],
- patch operating system, and
- minimise administrative privileges.[12]

A special unit called Cyber Security Operations Centre (CSOC), housed with DSD, was formed in January 2011. CSOC is charged with responsibility to provide government with a better understanding of sophisticated cyber threats against Australian interests, and coordinate and assist operational responses to cyber events of national importance across government and systems of national importance.

In January 2010 the Australian Government also created CERT Australia, or Computer Emergency Response Team. As the initial point of contact for cyber security incidents impacting upon Australian networks, CERT Australia works with the private sector to safeguard the critical infrastructure and ICT systems that are important to Australia's national interest from cyber based threats and vulnerabilities.

---

[9] *Information Security Manual*, DSD website. http://www.dsd.gov.au/infosec/ism/index.htm

[10] Application whitelisting is a security control to list permitted/trusted computer programs, thus preventing the execution of malicious softwares.

[11] Patch applications is to apply changes to correct known security vulnerabilities in software.

[12] *35 Strategies to Mitigate Targeted Cyber Intrusions*, DSD website publication, October 2012. http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm

As mentioned before, the establishment of Australian Cyber Security Centre will bring together government bodies currently engaged in cyber security response including CSOC and CERT, and the operational capabilities from other major intelligence and law enforcement agencies to work together. The goal is to strengthen Australia's ability to protect the nation's most valuable networks and systems against cyber attacks.

To combat the ever growing online identity thefts and frauds, the Attorney-General's Department has announced that it will extend access to the Government's Document Verification Service (DVS) to private industries, such as financial and telecommunication sectors, that are required by legislation to verify customers' evidence of identification documents.

With more than 80% of Australian citizens now having connections to the Internet, the Australian Government is fully aware this has a social impact. Internet users, particularly children and young people, are not immune to the risks and threats from cyber space. In order to protect Australian citizens from online risks, in May 2008 the Australian Government committed $125.8 million over four years to a comprehensive cyber-safety plan designed to combat these risks, including funding for cyber-safety education and awareness raising activities, content blocking and law enforcement.

The ANAO's audit coverage

Audit coverage for cyber security assurance

Cyber security is intertwined with many areas of government administration and invariably has a significant impact on them. For example, many government agencies utilise internet enabled utilities for revenue collection and payment processing, others use the Internet for services and program deliveries, reaching out to citizens, community groups and industries for consultation in supporting policy formulation.

The Australian National Audit Office (ANAO) has recognised the significance of cyber security and its impact on government administration. Through conducting annual audits of financial statements and selected administration areas for performance audits, the ANAO assesses key aspects of agencies' cyber security arrangements as part of the overall audit coverage. In line with the whole of government approach, the ANAO relies on the Australian Government Information Security Manual as authoritative criteria to assess the government agencies' cyber security control effectiveness.

In accordance with auditing standards, during the annual financial statement audits, the ANAO conducts IT general controls (ITGC) assessment of government agencies' overall ICT environments. ITGC assessment includes review of controls over IT security, which covers elements in ICT infrastructure, information and business processes that pertain to cyber security issues. The assessment results indicate whether the control measurements over confidentiality, integrity and availability of data for the purpose of preparing the agencies' financial statements, and the overall management of the IT function, are effective in government agencies.

The extent of assurance obtained is directed to our financial statement audit responsibilities and is not intended to cover all facets of agencies' operations.

In our performance audit role, the ANAO has recently completed several audits where cyber security has significant presence in the audit topics, including:

- The Protection and Security of Electronic Information Held by Australian Government Agencies[13];
- Management of Portable Storage Devices[14];
- Management of e-Passport[15]; and
- Processing and Risk Assessing Incoming International Air Passengers.[16]

These audits cover a range of cyber security issues, including the processing and maintenance of citizens' personal information and bio-metric data, intelligence information pertaining to national security, and technical controls specific for certain computer devices.

Additionally, the ANAO has identified two specific topics in the performance audit programs as potential future audits – 'Cyber Security' and 'Cyber-Safety Plan'. A Cyber Security audit would focus on examining the lead agency's effectiveness of coordination and leadership in the implementation of the Government's cyber security policy. An audit of the Cyber-Safety Plan would examine the administration of the cyber-safety education and awareness program and the extent to which it is achieving established objectives.

Given the increasing risks of cyber threats and their potential impact, it is likely that issues related to cyber security will feature increasingly in our performance audit program.

Recent audit findings and lessons learned

During 2011-12, the ANAO found that government agencies are generally operating in accordance with government protective security requirements in protecting and securing their ICT environment and the electronic information residing in it. The senior executives in agencies are responsible for overseeing cyber security and generally treat it with high priority. The agencies have established information security frameworks; assigned information security officers and developed information security awareness and training programs; implemented controls that safeguard information, protect network infrastructure and prevent intrusion and unauthorised access to information and ICT assets.

However, the capabilities and maturities for managing cyber security vary across different government agencies and the functional areas within the same agency. Our audits have revealed that, in isolated areas, there is scope for improvement. For example, in some agencies, intrusion detection and prevention mechanisms were not implemented in the agencies' internal computer networks; controls relating to the safe use of mobile computing and storage devices were absent;

[13] ANAO Audit Report No.33 2010-11. http://www.anao.gov.au/Publications/Audit-Reports/2010-2011/The-Protection-and-Security-of-Electronic-Information-Held-by-Australian-Government-Agencies
[14] ANAO Audit Report No.18 2011–12. http://www.anao.gov.au/Publications/Audit-Reports/2011-2012/Information-and-Communications-Technology-Security-Management-of-Portable-Storage-Devices
[15] ANAO Audit Report No.33 2011–12. http://www.anao.gov.au/Publications/Audit-Reports/2011-2012/Management-of-ePassports
[16] ANAO Audit Report No.50 2011–12. http://www.anao.gov.au/Publications/Audit-Reports/2011-2012/Processing-and-Risk-Assessing-Incoming-International-Air-Passengers

and controls over logical access, in particular privileged account access for some agencies' key ICT systems were ineffective.

The ANAO highlights the areas of security weaknesses identified through our audits and makes recommendations for control improvement. In general terms, our audits recommendations are in line with the DSD promoted controls and measurements. We should also bear in mind the importance of having the right people in key administrator roles.

These issues emphasise just how critical it is for governments to establish a government-wide framework and set the tone for how government agencies are expected to manage the risks to the delivery of government programs arising from cyber threats.

An important lesson learned in respect of managing cyber security is that senior executive commitment and support, and a mature security culture in agencies are imperative. Continuous review and evaluation of the existing security programs and keeping a forward looking approach in tackling the emerging trends in ICT also underpin the effectiveness and longevity of the agencies' cyber security measurements.

Another important lesson is that the implementation of controls that reduce ICT environment vulnerabilities and prevent cyber attacks and intrusions are the key to the overall success of a cyber security program. Preventive controls are more effective and economic to implement and operate than detective and corrective actions.

Additionally, the ANAO observed that in a climate of budget constraints, there is a risk of insufficient allocation of resources to areas that do not appear to directly contribute to core government activities, such as implementing controls over cyber security. Agencies need to manage the competing demand very carefully. Insufficient resource allocation for security increases the risks pertaining to information processing integrity, confidentiality and availability, which can impact on government program delivery and administration.

Future challenges

The amount of information maintained by government is continuously growing and access to this information is increasingly relying on ICT. There is no argument that the benefits offered by ICT for an ever-expanding range of affiliations outweigh the costs in terms of access, efficiency and effectiveness. Nevertheless, the complexity of ICT infrastructure, the diversity of technologies and the evolving nature of technologies and their vulnerabilities present challenges for government administration.

Cyber security management is fundamentally about risk management. Agencies must incorporate cyber security programs with their overall risk management framework, develop and maintain the programs in the context of their business objectives, utilise existing risk management procedures and tools.

For agencies to successfully manage cyber security, first and foremost it requires commitment from the top including their senior executive team, and ensures the head of agency is ultimately accountable for the security outcome. It is equally important to establish effective security governance arrangements and an internal control framework, allocate sufficient resources,

implement effective security programs, educate people and make sure security becomes part of the agency culture and is everyone's responsibility.

Furthermore, the availability of a competent and resilient team of ICT professionals is essential for a successful implementation of government cyber security strategies and programs. Agencies need to maintain access to such skills while managing the impacts of budget constraints.

In addressing this issue, through the Australian Government Information Management Office (AGIMO), the Government has developed a whole-of-government ICT strategic workforce plan[17] to maintain, develop and make better use of the ICT workforce, including cyber security expertise, across all levels of the government.

The complex and fast evolving technology environment, together with a skills shortage also present challenges for the ANAO to successfully manage our audit risks. In responding to these challenges, the ANAO has adopted an integrated audit approach through utilising the specialised skills of the IT audit team to support both financial statements and performance audit activities. We also utilise expertise available within the government, such as DSD, by using highly skilled resources, and their advanced analytic capabilities and techniques when examining specific technical components in performance audits.

Conclusion

The increased reliance on using ICT for government programs and service delivery has resulted in increased cyber security risks. The CEO or the head of each agency must assume the ultimate accountability. In order to mitigate these risks, which are increasing in frequency and severity, an organisation must establish clear leadership and foster an organisational culture that facilitates cyber security.

Given the whole of government approach, which has established a government framework and set the tone for how government agencies are expected to manage the risks from cyber security, agencies are not alone in dealing with cyber security challenges. There are existing resources, such as those provided by AGIMO and DSD, to be shared and utilised. Government agencies need to adopt a holistic approach by incorporating cyber security with their strategic business planning, and continuously assess the effectiveness of security measures and controls to ensure that risks continue to be adequately addressed.

Additionally, as demonstrated in the ANAO's recent work, robust financial statements and performance auditing is a value-adding exercise for cyber security management in government agencies. By assessing the ICT systems control effectiveness against cyber threats and risks, and providing recommendations on improvement, the ANAO assists government agencies in responding to the cyber security challenges.

[17] *Whole-of-government ICT strategic workforce plan*, AGIMO website. http://www.apsc.gov.au/publications-and-media/current-publications/ict-workforce