Association for Information Systems
AIS Electronic Library (AISeL)

ACIS 2005 Proceedings

Australasian (ACIS)

December 2005

Protecting Government Information Post 9/11: An Evolving Role for Security Architectures

Nigel Martin
Australian National University

Protecting Government Information Post 9/11: An Evolving Role for Security Architectures

Nigel Martin

School of Business and Information Management
Faculty of Economics and Commerce
The Australian National University
Canberra, Australian Capital Territory, Australia
Email: nigel.martin@defence.gov.au

Abstract

This paper discusses the results of a research study in the use of architectures in government agencies. The paper uses archival and time line analysis to present the context for securing the vast stores of protected government information, including the actions taken by the Australian government leading into the terrorist attacks of 11 September 2001 (termed 9/11), and the government reactions post 9/11. The results show that at the strategic level, the Australian government commenced a process of examining information security vulnerabilities and establishing a security architecture only to terminate the initiative due to a lack of budgetary funding. Also, a qualitative research method was used to examine the security architecture implemented in a large government agency. Results from the agency case study demonstrate that security architectures form part of the fabric of the agency's business, not only in terms of information and communications technology infrastructure, but also staff behaviours and attitudes to securing information stores and exchanges.

Keywords

Security, architecture, government, information, standards.

INTRODUCTION

This study has been motivated by the researchers' interest in the collection, processing and securing of sensitive information within federal government agencies, and specifically what architectural measures are being implemented to protect this information. A review of internationally recognised information security standards and practices shows that codes of practice for information security management (ISO/IEC 17799**:**2000) and specifications for information security management systems (BS 7799-2**:**2002) have been developed, and are in widespread use. This investigation forms part of a larger doctoral study of government enterprise architectures and is aimed at all government employees and researchers. The structure of this paper is outlined as follows.

The first section provides a structured summary of the international information security management standards and details of specific case studies where organisations have implemented the ISO 17799 and BS 7799-2 standards. This paper will look to identify how the Australian federal government sought to implement the principles embedded in these information security standards in the years leading up to the tragic events of 9/11, and the strengthening of those implementation measures post 9/11. Also, the paper will present the standards-driven information security architecture implemented within the Centrelink social services agency.

The second section outlines the research question and model that have been developed for the study. The research question is focused on determining the requirement for protecting and securing information in the government environment, and the type of security framework available for deployment. The research context model was developed using the Zachman Enterprise Architecture Framework (Sowa and Zachman 1992) and includes the contextual conditions to whole-of-government information security, and the information security management frameworks that can be deployed by agencies for secure information exchange.

The third section outlines the research methodology used in the study. The first part of the study was undertaken using archival research and time line analysis techniques to identify the key information security actions and measures implemented by the Australian federal government prior to, and post, 9/11. The second part of the study used qualitative research techniques to develop a concentrated case study of the security architecture implementation at Centrelink. The research used unstructured interview commentaries (recorded in field note format) and agency documents in developing the case (Burgelman 1983, 1994; Eisenhardt 1989). The senior executive responsible for the information security architecture and the principal information technology security strategist provided detailed accounts of the agency's architecture implementation. Also, agency architecture documents were collected and their content analysed as part of the study.

The fourth section outlines the key results of the study as follows:

- The federal government's actions in the area of information security prior to, and post, 9/11.
- The outputs from the implementation of an information security architecture within Centrelink using an analytical framework comprised of standards and drivers, architecture components, architecture domains and views, and business attributes profiling for security.

The final section provides a summary of research findings, research limitations, contributions of the research, and directions for future research efforts in other organisations.

MOTIVATIONS AND INFORMATION SECURITY STANDARDS

The following sections discuss the primary motivations for the information security research. Information security standards, and some example cases of information security compliance in the United Kingdom government.

Motivations

On 11 September 2001, the terrorist attacks on the twin towers of the World Trade Centre in New York and the Department of Defence Pentagon building in Washington DC fundamentally transformed the landscape of information security and government information operations. In what was to become an almost surreal experience, some Australian defence analysts were monitoring the unfolding events on Cable Network News (CNN) transmissions, as information flooded in from across the globe. One of the key messages that resonated from 9/11, and the bombing of the Sari Club in Bali, Indonesia on 12 October 2002, was that Australia is vulnerable in terms of its critical core infrastructure, particularly in the areas of information and communications.

While acknowledging that others have identified the need to protect critical information infrastructure (Rathmell 1999, 2001; Jones 2002), information is one of the most important inputs to national security activities and actions, and provides the temporal connectivity between critical events and outcomes. A good example is the reaction of emergency services and law enforcement agencies when advised of the occurrence of a natural disaster or unlawful act (eg, bush fires, robberies). The information passed to these agencies act as the trigger for their action or response. Given the importance of information under these types of circumstances, it might be argued that governments should systematically protect and secure their information stores.

If we agree that government information stores are an important resource that should be protected, then the information should be secured at the whole-of-government and individual agency levels. These levels of security cover the strategic exchange of information between agencies and the security of information within each individual agency. It should be noted that the Australian government has already developed an Interoperability Framework that supports the principles of information sharing and exchange, including policies, standards and guidelines for information operations (Commonwealth of Australia 2003). The underlying motivation for this study is to examine the strategic policy developed, and procedural actions taken, by the federal government in relation to secure information exchange, and investigate the security architecture that has been implemented by one agency to protect their information stores.

Information Security Standards

The information security management standards that are applicable to this study are the ISO/IEC 17799:2000 that outlines the voluntary code of practice for information security management and the BS 7799-2:2002 that defines the specification for information security management systems. Both standards are seen as complementary with the BS 7799 standard instructing users on how to apply ISO/IEC 17799 and build, operate and improve information security management systems. It should be noted that an equivalent AS/NZS 7799-2:2003 standard has also been developed by the local Australian and New Zealand standards organisations.

ISO/IEC 17799:2000 defines 127 security controls under the ten major areas of security policy, security organisation, asset classification and control, personnel security, physical and environmental security, communications an operational management, access control, systems development and maintenance, business continuity management and compliance. The controls enable users to identify and deploy safeguards that are appropriate to their particular business or area of responsibility. This standard emphasises the importance of risk management (AS/NZS 4360:2004) and stresses that only the relevant security guidelines should be implemented. The standard covers all forms of information including voice, data and graphics, telephones, fax machines, electronic commerce and the Internet.

BS 7799-2:2002 specifies how the information security management systems should be built, operated, maintained and improved. The information security management systems provide the vehicle to measure, monitor and control security management from a top-down perspective. The standard also specifies the system compliance path that includes defining the security policy, planning the scope of the system, managing the risk, implementing and operating controls, managing resources, initiating system improvements, taking preventative and corrective actions, and undertaking management review and audit. Again, risk management is emphasised as a critical element of this standard's implementation.

Information Security Compliance – Case Studies from the UK Government Environment

Specific to this paper, two case studies from the United Kingdom (UK) government environment demonstrates the imperatives placed on government agencies and businesses to become BS 7799-2**:**2002 compliant. Summaries of the cases are outlined as follows:

The Radiocommunications Agency is an executive agency of the UK government's Department of Trade and Industry and is responsible for managing the non-military radio spectrum. Other agency functions include international representation, allocating spectrum, spectrum licensing, and assuring clean spectrum. The principal driver of agency information security was the mandate by the Head of the UK Civil Service in November 1999 that required all government organisations to be BS 7799 compliant by the end of 2003. The agency was the first government organisation to achieve BS 7799-2**:**2002 compliance, including agency-wide information security management procedures. BS 7799 compliance also improved security awareness across the agency, particularly within the senior management group (available from http://www.insight.co.uk/casestudies.htm).

The Stationery Office (formerly Her Majesty's Stationery Office, HMSO) is a privatised government business that is the definitive source of official and regulatory information, and has been managing and publishing UK government information since the 1700s. The security of sensitive client information was the main driver of the BS 7799 compliance initiative in 2003. The Stationery Office has achieved a BS 7799 compliant IT infrastructure with business continuity procedures that exceed the standard's minimum requirements. The office's Intranet solution has also improved security awareness across the organisation (available from http://www.insight.co.uk/casestudies.htm).

The two BS 7799 compliance cases depict the key business drivers, emphasise the corporate direction towards business continuity procedures, and reinforce the important benefit of enhanced agency-wide security awareness.

RESEARCH QUESTION AND MODEL

The following sections discuss the development of the Research Question and Model.

Research Question

The Research Question is concentrated on the development of security arrangements for government information and is posed as follows:

Has the Australian federal government sought to systematically protect and secure their information stores and exchanges, and if so, what type of security frameworks are available to agencies for securing their information?

The research question looks to determine what types of strategic activities and actions the government has taken in attempting to secure its information stores and exchanges, while also examining the implementation of a more tactical, agency-specific security architecture.

Research Model Development

The two-part research context model for this study has been developed using the Zachman Enterprise Architecture Framework (Sowa and Zachman 1992). The first part of the model is the strategic or whole-of-government information security environment, and is based on the scope or contextual layer of the Zachman framework (ie, government organisations, business events, business goals, important information, and locations). The second part of the model is the tactical or individual agency information security environment, and is based on the business, system, and technology model layers and the detailed representations (component) layer of the Zachman framework (ie, conceptual, logical, physical, and component elements of the security architecture). The agency information security architectures are considered to enable the secure storage, transmission and reception of government information. The research context model is depicted in **Figure 1**.

The model depicts the bounded whole-of-government information security environment that contains the government agencies (GA). Each government agency is considered to have developed and applied an information security architecture (ISA) that secures agency information stores and enables secure information exchanges between agencies (depicted by the broken line arrows). This study has carefully grounded its research context model in the published literature of Sowa and Zachman (1992).

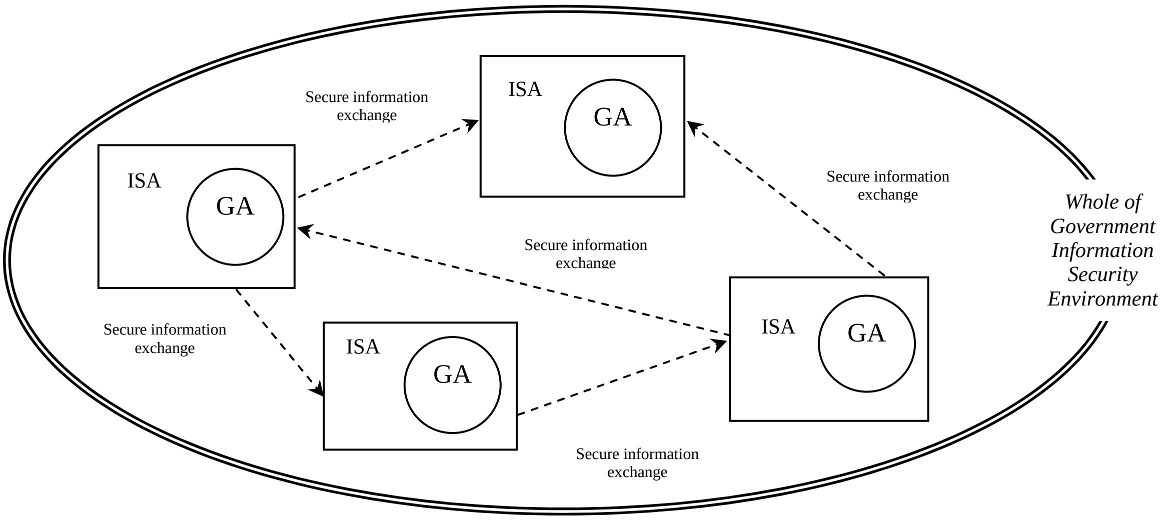

ISA
GA
ISA
GA
ISA
GA
ISA
GA
Secure information exchange
Secure information exchange
Secure information exchange
Secure information exchange
Secure information exchange
Whole of Government Information Security Environment

Figure 1: Research context model (based on Sowa and Zachman 1992)

RESEARCH METHOD

This study has used a two-part qualitative research method that includes the use of time line analysis, archival research and document discovery, unstructured interviews with key information security executives, and public presentations by agency executives. This method employed data collection from multiple sources, and used testing and triangulation of the collected data similar to the research programs executed by Burgelman (1983) in Eisenhardt (1989), and Burgelman (1994).

In the first part of the study, archival research and time line analysis was combined to provide a consolidated picture of the government information security environment. Archival documents and papers from the National Office for the Information Economy (now the Australian Government Information Management Office) and the Attorney General's Department were reviewed for specific actions and activities undertaken by the federal government in relation to the implementation of a strategic information security framework. A time line analysis was then overlayed on the discovered documents with particular emphasis placed on the periods leading into and out from 11 September 2001.

In the second part of the study, key executives in the area of information security at Centrelink were interviewed and provided their views on the development and on-going implementation of the agency information security architecture. The executive commentaries were recorded in field note format. Agency and independent public audit documents relating specifically to the information security architecture were collected and the relevant content analysed using text and headings searches and integrated with the executive viewpoints. Also, public presentations of Centrelink's enterprise and information security architectures were attended and presentation notes collected and compared with the other case information. Information for part two of the study was collected between March 2003 and October 2004.

STUDY PART ONE RESULTS

The following sections describe the key results from part one of the study.

Legal and Legislative Drivers

In 1988, the Australian federal government took its first steps towards securing citizens privacy and individual information in the broader (including online) environment when the Privacy Act (1988) was passed (Commonwealth of Australia 1988). This Act set legal markers for the interpretation, definitions and functional scope of information to be protected under the legislature. The Privacy Act also set out privacy codes, information privacy principles, national privacy principles, established the Federal Office of the Privacy Commissioner (including investigative and enforcement powers), and set the guidelines for public interest determinations.

The relevance of the Privacy Act (1988) to this study is grounded in the Information Privacy principles, where the fourth principle outlines the storage and security responsibilities of record-keepers, while other principles (six through eleven) set out the guidelines for access, disclosure and use of stored information. The implications for all government agencies (eg, Australian Taxation Office, Health Insurance Commission) that collect, use and manage client information is the requirement to provide safe and secure storage and protected transmission of client data between the required points of presence.

Information Security Guidelines and Government Directives

In addition to the legislative drivers, the Australian federal government also developed a number of guidelines and policies that have application to online and broader IT security. The federal government issued the Protective Security Manual (PSM) in early 2000, with the manual maintained by the Protective Security Coordination Centre in the Attorney General's Department. The PSM is the federal government's top-level framework for physical, information and personnel security, and was compiled using a broad-based consultation process (Commonwealth of Australia 2000b).

It should be recognised that federal government information requiring protection needs to be classified according to the schema contained in the PSM. The classification system used by the federal government comprises Top Secret, Secret, Confidential and Restricted for national security material and Highly Protected, Protected and '-In-Confidence' for sensitive material (Australian National Audit Office 1997). These national security classifications are long standing and consistent with other countries. This paper will deal with information in the sensitive material classification schema only.

A key part of the PSM is the Australian Communications Security Instructions (ACSI) 33. The ACSI 33 provides the framework for agencies to develop and implement effective Information Technology and website security processes and practices, with the Defence Signals Directorate (DSD) having overall responsibility for issuing and maintaining the instructions (Commonwealth of Australia 2004). DSD also has administrative responsibility for the government Gateway Certification Guide (GCG) and the mandatory procedures for portal certification. The GCG was developed to assure security at all points where the federal government connects to the Internet.

The federal government also requires agencies to use the Gatekeeper (Baltimore Technologies) accredited products and services when implementing online systems that use Public Key Infrastructure (PKI) (Commonwealth of Australia 2004). Security guidelines, products and services adopted by the federal government are consistent with the Organisation for Economic Co-operation and Development (OECD) Information Security Guidelines that were released in 1992 (OECD 1992) and re-released in 2002 (OECD 2002).

Information Security gathers momentum into 2000

While the Australian federal government had worked steadily to achieve greater levels of information security since the late 1980s, March 2000 saw further concentration on compliance with specific electronic security (eSecurity) measures. The federal government declared that all agencies *must adopt a minimum set of standard online requirements* that address the important security and privacy elements of existing legislature, and conformed with existing Commonwealth standards (Commonwealth of Australia 2000a). Specifically, government agency web sites were to comply with the Commonwealth Privacy Act 1988 (as modified by the Privacy Amendment Act 2000), government agencies were to develop an agency-wide information security policy and plan, and from 1 June 2000, all federal government agencies were to manage online systems and websites in accordance with ACSI 33.

The federal government also observed a need for all tiers of government to actively cooperate on eSecurity issues. In supporting this direction, inter-jurisdictional co-operation was to be pursued. It was intended that agreeing common standards with States and Territories on issues including privacy, security, meta-data tagging and access principles was a clear priority, and that the former National Office of the Information Economy (NOIE), now the Australian Government Information Management Office (AGIMO), would lead this consultation process. AGIMO was formed in April 2004, following the restructuring of NOIE and the returning of information economics functions to the Department of Communications, Information Technology and the Arts (Minister for Communications, Information Technology and the Arts 2004).

The multi-tiered government co-operation on information security was an extension of the Online Government Council (OGC) arrangements that were initiated in January 1997. The OGC is a forum of Federal, State and Territory Ministers and local government that agrees national strategic approaches to government use of information and communication services. The OGC is charged with *providing leadership to all areas of government, the private sector and the broader community, in promoting and encouraging cooperative approaches to electronic communications, as well as a customer-focused approach to electronic service delivery* (Online Government Council 1997).

The March 2000 electronic security measures mandated by government were tied to the Government's Online Strategy "Government Online" that was released on 6 April 2000 (Commonwealth of Australia 2000c). The strategy aimed to provide an implementation framework for the Prime Minister's 1997 'Investing for Growth' commitment to ensure all appropriate government services are available online by 2001 using a seamless eBusiness approach (Commonwealth of Australia 1997). The second strategic priority sought to ensure that 'security enablers' were implemented in the areas of authentication, privacy and security (eg, passing of the Electronic Transactions Act 1999).

Government information security momentum continued to build throughout 2000 and in November 2000, the federal government announced further measures directed at securing government information and data (Commonwealth of Australia 2000a):

- NOIE were tasked with a greater co-ordination and awareness promotion role in the online security domain, including closer working arrangements with the Attorney General's Department and DSD.

- Implementations of an enhanced, online incident reporting and response system, to be overseen by DSD and developed in consultation with appropriate agencies and stakeholders. The system is based on the DSD Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS).

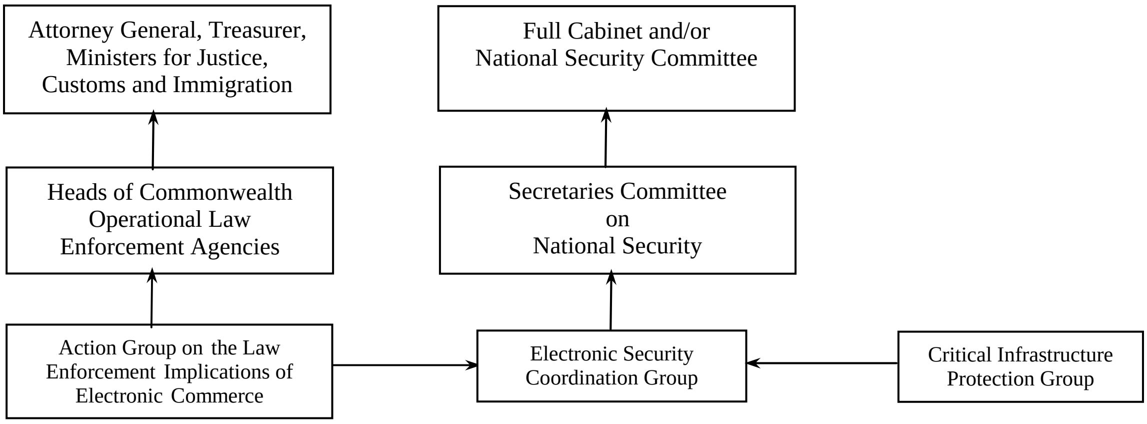
- Introduction of a protocol for the independent and external certification, auditing/testing and verification of agency online security.

- Assurance that non-government services providers or intermediaries who may deliver some Commonwealth online services (eg, utilise web-enabled customer databases) manage the provision of those services in accordance with PSM and ACSI 33.

In a move to positively enforce these measures, agency Chief Executive Officers (CEOs) were requested to warrant that their online assets were managed in accordance with security standards like the ACSI 33 and PSM. CEOs must also confirm that any non-government online service providers are operating within the PSM and ACSI 33 guidelines. These enhanced eSecurity measures were to take effect on 1 March 2001.

Accelerated Information Security Arrangements Post 9/11

The implementation of the November 2000 eSecurity measures were well underway when the events of 11 September 2001 transpired. Within two weeks of the attacks on US infrastructure, the Australian federal government launched new administrative and operational arrangements in strict accordance with the Protection of Australia's National Information Infrastructure and eSecurity Policy that was released on 27 September 2001 (Commonwealth of Australia 2001). These administrative and operational arrangements focused on the development of three major groups within a broader eSecurity co-ordination and reporting regime as depicted in **Figure 2** (Note, arrows indicate reporting channels and directions).


Attorney General, Treasurer, Ministers for Justice, Customs and Immigration

Full Cabinet and/or National Security Committee

Heads of Commonwealth Operational Law Enforcement Agencies

Secretaries Committee on National Security

Action Group on the Law Enforcement Implications of Electronic Commerce

Electronic Security Coordination Group

Critical Infrastructure Protection Group

Figure 2: Australian Government eSecurity Regime (Commonwealth of Australia 2001)

The Electronic Security Coordination Group (ESCG) is the primary eSecurity policy body that is chaired by AGIMO and includes membership from the Attorney General's department, DSD, various security agencies (eg, Australian Security Intelligence Organisation), and other federal government departments (eg, Department of Foreign Affairs and Trade). The ESCG has been tasked with raising the profile of eSecurity across the Australian community, developing information sharing arrangements with industry and government bodies, co-ordination of international eSecurity activities, and looking forward to the development of eSecurity skills and research priorities.

The Critical Infrastructure Protection Group (CIPG) is a sub-committee of the ESCG that is chaired by the Attorney General's department and has the primary role of identifying and providing advice on Australia's critical information infrastructure. The CIPG has overseen comprehensive threat and risk assessments on Australian telecommunications, electricity, banking and finance, and air traffic control infrastructure. The CIPG continues to work with infrastructure owners to mitigate those key vulnerabilities identified in the assessment process.

The Action Group on the Law Enforcement Implications of Electronic Commerce (AGEC) is the government's peak response body on the investigation and prosecution of criminal offences involving electronic communications. AGEC is chaired by the Director of the Australian Transaction Reports and Analysis Centre (AUSTRAC) and includes members from the Australian Competition and Consumer Commission, the Australian Centre for Police Research (ACPR), Australian Federal Police (AFP), various government agencies (eg, Australian Customs Service), the Federal Director of Public Prosecutions (DPP), and the National Crime Authority (NCA). The AGEC has an ongoing role in developing law enforcement strategies in areas such as access to email conversations, disclosure of intercepted information, computer intrusion warrants and co-operation between international authorities.

The key relationships between these eSecurity groups are outlined as follows:

- The AGEC reports directly to the Heads of Operational Law Enforcement Agencies, including government agency CEOs, police departments chiefs, that in turn reports to senior ministers in the key law enforcement portfolios. AGEC also provides the results of its studies and research to ESCG as a 'primary policy' input to electronic security coordination.

- The CIPG is a working sub-committee that continues to progress mitigation strategies on the infrastructure vulnerabilities identified in the threat and risk assessments discussed earlier. CIPG reports its progress to the ESCG as a 'policy implementation' input to electronic security coordination.

- The ESCG reports directly to the Secretaries Committee on National Security (CEOs of the Prime Minister's, Defence and Treasury Departments) who consider and pass important policy and coordination issues forward to the National Security Committee (NSC) or the Full Cabinet of government.

The relationships demonstrate cooperation and commitment to eSecurity at the three levels of government, and between a group of law enforcement agencies that have separate state, national or international responsibilities. These arrangements have been in place since 2001, and noting Australia's participation in coalition actions in Afghanistan and Iraq, provide a measure of confidence in the electronic security domain.

A Security Architecture for the Government Environment (SAGE)

In early 2004, the Australian federal government announced its intention to consider the development of a security architecture for the government environment or 'SAGE' (Australian Government Information Management Office 2004). The architecture could be best described as 'a set of security policies, standards and guidelines' that address how agencies should conduct their business in the exchange and use of information. This initiative follows from the Management Advisory Committee (made up of federal government agency CEOs) report *Australian Government Use of Information and Communications Technology: A New Governance and Investment Framework* that was released on 15 October 2002 and highlighted the importance of security, confidentiality, privacy and protection of information (Commonwealth of Australia 2002). Unfortunately, following further budget restrictions and the restructure of NOIE, the SAGE initiative was terminated in late 2004. A summary of the part one time line analysis is shown in **Figure 3**.

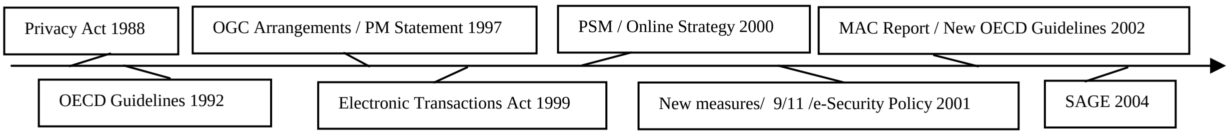

Privacy Act 1988
OECD Guidelines 1992
OGC Arrangements / PM Statement 1997
Electronic Transactions Act 1999
PSM / Online Strategy 2000
New measures/ 9/11 /e-Security Policy 2001
MAC Report / New OECD Guidelines 2002
SAGE 2004

Figure 3: Summary of Time Line Analysis (Part One Results)

STUDY PART TWO RESULTS

The following sections describe the key results from part two of the study.

The Centrelink Agency

Centrelink is one of the largest federal government agencies in Australia, employing over 27,000 full time equivalent staff to deliver over 140 different products and services valued at approximately $55 billion for 25 government agencies, while operating over 1,000 service points from a recurrent annual budget of $1.6 billion (see www.centrelink.gov.au). Centrelink operates a large Information and Technology (I&T) environment that includes mainframe computers, mid range electronic business networks, a large desktop computer fleet, twenty-nine call centres, and a diverse range of software products and solutions. Consistent with its implementation of the Zachman Enterprise Architecture Framework (Treadwell 2003), Centrelink has implemented the Systems and Business Security Architecture (SABSA) (Sherwood 2003) in its I&T environment.

Security Standards and Drivers

Centrelink identified the Privacy Act (1988), Social Security legislation, PSM and ACSI33, BS 7799-2**:**2002, and the agency eBusiness strategy as the primary standards and drivers in their information security stack (Coates 2004). As noted from the analysis in part one of the study, with the exception of the specific social security legislation, each standard and driver adopted by Centrelink is consistent with the broader information security environment established by the federal government. Centrelink stated that the information security stack drives the six SABSA architecture layers (ie, contextual, conceptual, logical, physical, component and operational) and the vertical column abstractions (interrogatives) in the areas of assets (what), strategic motivation (why), processes (how), stakeholders (who), location (where) and timing (when) (Coates 2004). By implementing SABSA, Centrelink focused on creating components that addressed the assets to be protected, the motivation for security architecture application, the required security functions, the organisational aspects of security, the locations where security actions were undertaken, and the temporal nature of security within the agency.

Security Architecture Components

Centrelink identified the three key components of their security architecture as the information security policy, procedures and products (Coates 2004). These components were consistent with the security architecture observed and reported to the federal parliament by the Australian National Audit Office (ANAO) in mid 2001. In particular, the ANAO found that Centrelink had established strict policies and procedures for controlling logical access to the use of computing resources supporting pensions and employment benefits, conducted regular monitoring of user access and changes to access rights, and exercised appropriate security incident handling procedures. The ANAO also found a number of integrated systems and software products that worked in combination to secure the I&T environment, including Access Control Facility 2 and SAMS/390 (mainframe security), and NetWare Directory Services and SAMS (local area network security) (Australian National Audit Office 2001).

Architecture Domains and Security

Centrelink's implementation of the Zachman Enterprise Architecture Framework saw the agency establish four major sub-architectures (ie, business, information, applications and infrastructure domains) (Crisp 2003). Centrelink stated that the security architecture intersected each of the sub-architectures. Specifically, the information security architecture embraced all parts of the organisation, including personnel and staffing (business), security software (applications), corporate information stores (information), and the network, platforms and facilities (infrastructure) (Coates 2004). This type of approach has built a strong and intimate connection between the four agency domains and the overall security function. At Centrelink, information security is a common theme that influences the complete organisation.

Business Attributes and Practices

Centrelink's implementation of SABSA has also seen the creation of the agency business attributes profile (Sherwood 2003). Centrelink analysts developed a profile of business attributes that included the user needs, management features, operational understanding, system characteristics, legal-regulatory environment, information technology strategy and business strategy (Coates 2004). The attributes profile was an integral part of the conceptual architecture layer and allowed performance metrics to be developed and measured for managerial reporting and control. At Centrelink, the attributes profile is analysed using a multi-pass business process that applies traffic light performance indicators. Agency business analysts generate enterprise views using no control, existing control and risk mitigation plan implementation scenarios. The results are colour coded using traffic light indicators and are presented for non-executive board and executive management team review and consideration. On the basis of these analyses, agency management decisions are taken and actions implemented (Coates 2004).

SUMMARY

In conducting this research it was considered important that the timeframes preceding and following 9/11 be examined in order to determine what strategic information security actions Australian governments were taking around the time of the terrorist attacks. The time line analysis showed that prior to 9/11, Australian governments had implemented strict requirements for information privacy under the Privacy Act (1988) and had directed that government online environments comply with stringent security guidelines (eg, PSM/ACSI 33). In the sixteen days following 9/11, the Australian federal government moved to strengthen the national information security framework and implemented a consolidated set of executive management teams, groups and committees to deal with information and electronic security at the strategic level. The research also showed that the federal government has given some consideration to implementing a whole of government security architecture for the protection of government information stores (subject to suitable funding arrangements).

The Centrelink case showed that public sector agencies could successfully implement security architectures provided they follow certain architectural guidelines. First, the architecture should be based on established security standards and sound business drivers. This approach should allow the security architecture components to be integrated with the various parts of the business and organisational structure. Second, agencies should develop policies, procedures and products that enable an integrated approach to agency-wide security. Deficiencies in any of these components will leave the agency vulnerable to security threats and risks. Third, the security architecture should be integrated with the complete agency enterprise architecture in order to build the security function into all business domains. This integration effort should allow information security to be firmly established in the complete organisation and form part of its work culture. Fourth, organisations should look to develop a business profile and understand how the business and security might be coordinated and meshed. Agency managers can use the business profile to exercise various security and risk management scenarios and make informed decisions. While other associated actions may also be required, following these four guidelines would give most organisations a useful start in developing a security architecture.

In summary, the findings of this study are consistent with contemporary empirical research from Meta Group in the area of information security. Meta Group found that organisations use their information security architecture to provide a framework of principles, procedures, and management products that enables security solutions, demonstrate a serious intent to secure information, manage risk, and assure regulatory and legal compliance, and provide a common vision for information security across the business (Scholtz 2004). While the research was limited in scope to the Australian government view and one large public sector agency, the results reaffirmed the on-going importance of information security at the strategic and tactical levels of government, particularly in the post 9/11 environment. The research also provides a good example of how information security can be implemented in a large and geographically dispersed public organisation. Future research studies might investigate the outcomes of information security architecture implementations, including the avoidance, handling or incurrence of critical incidents.

REFERENCES

AS/NZS 4360:2004. Risk Management.

Australian Government Information Management Office (2004). Australian Government Electronic Security Framework: A Security Architecture for the Australian Government Environment. Presentation to the Commonwealth Architecture Forum by Bricet Klören, 2 April 2004.

Australian National Audit Office (1997). Protective Security, Audit Report No. 21, Performance Audit Program 1996-1997.

Australian National Audit Office (2001). Information and Technology in Centrelink, Audit Report No. 39, Performance Audit Program 2000-2001.

BS 7799-2:2002. Specification for Information Security Management

Burgelman, R.A. (1983) A Process Model of Internal Corporate Venturing in the Diversified Major Firm. *Administrative Science Quarterly*, 28, June 1983, 223-244.

Burgelman, R.A. (1994) Fading Memories: A Process Theory of Strategic Business Exit in Dynamic Environments. *Administrative Science Quarterly*, Vol. 39 Issue 1, March 1994, 24-56.

Coates, B. (2004). Centrelink - Security Architecture Framework. Presentation to the Commonwealth Architecture Forum, 15 October 2004.

Commonwealth of Australia (1988). The Commonwealth Privacy Act, 1988.

Commonwealth of Australia (1997). Prime Minister’s Statement ‘Investing for Growth’, Department of Industry, Science and Resources, 1997.

Commonwealth of Australia (2000a). Commonwealth Information Security Guidelines, Government Online Measures, 2000.

Commonwealth of Australia (2000b). The Commonwealth Protective Security Manual, 2000.

Commonwealth of Australia (2000c). The Online Strategy for Government Agencies, 2000.

Commonwealth of Australia (2001). Protection of Australia’s National Information Infrastructure and eSecurity Policy – Administrative and Operational Arrangements, 2001.

Commonwealth of Australia (2002). Australian Government Use of Information and Communications Technology: A New Governance and Investment Framework, Management Advisory Committee, 2002.

Commonwealth of Australia (2003). Interoperability Technical Framework for the Australian Government, June 2003.

Commonwealth of Australia (2004). Commonwealth Information Security Guidelines (ACSI 33), Online Security for Government Agencies, 2004.

Crisp, S. (2003). Private email on Centrelink’s - Enterprise Architecture Framework, 23 March 2003.

Eisenhardt, K. (1989) Building Theories from Case Study Research, *Academy of Management Review*, 14, 532-550.

ISO/IEC 17799**:**2000. Code of practice for Information Security Management.

Jones, A. (2002) Protecting Critical National Infrastructure – Developing a Method for the Measurement of Threat Agents in an Information Environment. *Information Security Technical Report,* Vol 7, No 2, 22-36.

Minister for Communications, Information Technology and the Arts (2004). Media Release. Formation of AGIMO, 8 April 2004.

Online Government Council (1997). Communiqué, 7 March 1997. Retrieved on May 16, 2004 from http://www3.dcita.gov.au/ OC/mediarel/Comm01.htm).

Organisation for Economic Co-operation and Development (OECD) (1992). Guidelines for the Security of Information Systems.

Organisation for Economic Co-operation and Development (OECD) (2002). Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security.

Rathmell, A. (1999) International CIP Policy – Problems and Prospects. *Information Security Technical Report,* Vol 4, No 3, 28-42.

Rathmell, A. (2001) Protecting Critical Information Infrastructure. *Computers and Security* 20, 43-52.

Schotz, T. (2004) The Benefits of an Information Security Architecture. Retrieved on December 7, 2004 from http://eacommunity.com/ articles/openarticle.asp?ID=2069.

Sherwood, J. (2003) Enterprise Security Architecture. Sherwood Associates Limited White Paper, 31 January 2003.

Sowa, J.F. and Zachman J.A. (1992) Extending and formalising the framework for Information Systems Architecture. *IBM Systems Journal* **,** Vol 31, 590-616.

Treadwell, J. (2003). Centrelink Capabilities and Connections Presentation, NOIE Seminar Program, Enterprise Architecture: Integrating Business and Technology across the APS, March 2003.

ACKNOWLEDGEMENTS

The authors wish to thank the AGIMO and Centrelink organisations for their assistance with the research.

COPYRIGHT