1

Security and Integrity of Electronic Information

Introduction

1.1 The secure storage of information has always been a challenge for Commonwealth agencies. As the use of computers and electronic communication has expanded, this challenge has escalated and taken on new dimensions.

1.2 Computers and electronic communication allow business to be conducted more efficiently. Everyday activities such as information retrieval and processing can be performed with increasing speed and accuracy.

1.3 With the increased efficiency of computers and electronic communication comes different risks. Greater efficiencies in data processing and communication mean that more information is potentially available to a party that has gained unauthorised access to an electronic information system. Easier access to data increases the risk of unauthorised access and theft. Being able to store more data in one place means that more data can be lost in a fire or natural disaster. On the other hand, improvements in information technology (IT) design have provided new opportunities to manage the security of information.

The Setting

1.4 As Commonwealth agencies increasingly rely on the internet to conduct business with the public, they must adopt strategies to protect data transfers from unauthorised access.

1.5 Similarly, the integrity of the Commonwealth's electronic data must be protected from:

- theft and malicious damage;
- electronic attacks, such as viruses and worms;
- negligence and human error; and
- natural disasters, such as fires or earthquakes.

1.6 Rapid advances in computer hardware and software add another challenge. Electronic information may be lost or become inaccessible because of the degradation or obsolescence of the data format or storage medium.

1.7 In addition to its obligation to the Australian people, the Commonwealth has an international obligation to protect the privacy and integrity of electronic information. It has agreed to implement Guidelines adopted in 1980 by the Organisation for Economic Co-operation and Development (OECD) for the Protection of Privacy and Transborder Flows of Personal Data.

1.8 In a recent publication *Guidelines for the Security of Information Systems and Networks*, the OECD outlined the information security problem:

> … As a result of increased interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security. For these reasons, these guidelines … suggest the need for a greater awareness and understanding of security issues and the need to develop a "culture of security".[1]

1.9 In a similar vein, the Australian National Audit Office (ANAO) commented:

> The Commonwealth's use of computer software permeates every aspect of daily business from email to accounting and payroll. It is pervasive in the delivery of services by all entities and is rapidly

[1] Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD, Paris, 2002, p. 7.

> changing the way the public interacts with entities through the ongoing growth of Internet enabled services.[2]

1.10 Reliance on electronic information storage and transmission is growing so quickly that it is essential that the Commonwealth build public and private confidence in the management and use of electronic information by government such as the maintenance of personal records. This can best be accomplished by protecting the privacy, security and integrity of electronic information under Commonwealth control.

1.11 The National Archives of Australia (NAA) addressed this situation in its submission to the inquiry, when it said:

> The Australian community needs to be confident that these records, while in the custody of the agency that collected or created them or with the Archives if they are assessed as being of enduring value, will be secure and retain their integrity.[3]

1.12 The physical security of the information and the equipment it is stored on also cannot be overlooked. The Committee found that more than a thousand laptop computers had been lost by Commonwealth agencies in the last five years. Among the equipment reported lost or stolen were:

- 537 laptops and PCs from the Department of Defence
- 117 laptops and 94 PCs from the Department of Family and Community Services (FaCS).

1.13 These examples are from large agencies and were numerically significant losses. However, the Committee noted that even among smaller agencies, which operate IT resources on a much smaller scale, the loss rate was often still high. Quite apart from the financial aspect of such losses, the danger of information held on the missing equipment being compromised is an issue of significant concern. A more detailed examination of this issue follows in Chapter 2.

1.14 In an effort to encourage a quality of record keeping which protects the privacy, confidentiality and integrity of commonwealth records, the NAA released, in March 2000, the *e-permanence* suite of best-practice recordkeeping standards, manuals and guidelines.[4]

1.15 The standards outlined for recordkeeping call for the institution of:

[2] ANAO, *Capitalisation of Software*, Audit Report No. 54 2002-2003, p. 13.

[3] NAA, *Submission No. 22* (http://naa.gov.au/recordkeeping/, 27 October 2003), p. 3.

[4] NAA, *Submission No. 22*, p. 3.

> … policies, procedures and practices that produce records which have the characteristics of:
>
> - authenticity;
> - reliability;
> - integrity; and
> - useability.[5]

1.16 The NAA considers that present agency practices for record keeping do not provide a full, accurate, reliable, accessible and durable record of government activity. NAA said it is a situation '… where the essential evidence of government decisions and transactions is often kept in the hard drives, e-mail in-boxes and shared folders of individual[s] … or work groups.'[6]

1.17 The NAA concluded that the successful adoption of the *e-permanence* regime is essential for the proper management and maintenance of electronic information in the Commonwealth.[7] Support for this conclusion came from the ANAO. In 2002 it carried out an audit of recordkeeping in four Commonwealth agencies and the findings showed that none of the agencies satisfied the audit criteria.[8]

1.18 Electronic records were a particular focus of concern for the ANAO, which found that agencies were not sure that all essential electronic records were being captured. Most agencies were relying on individuals to print the records to paper but ANAO found that '… in practice, there were significant risks relating to capture of e-mail and electronic documents from personal workspace.'[9]

The Committee's Inquiry

1.19 The Joint Committee of Public Accounts and Audit (JCPAA) has a statutory duty to 'examine all reports of the Auditor-General', and the powers to report to Parliament 'on any items or matters' in the Commonwealth's 'accounts, statements and reports, or any circumstances connected with them'.[10]

[5] NAA, *Submission No. 22*, p. 3.

[6] NAA, *DIRKS – A Strategic Approach to Managing Business Information, Part 1 – The DIRKS Methodology : A User's Guide*, NAA, Canberra, September 2001, p. 5.

[7] NAA, *Submission No. 22*, p. 4.

[8] NAA, *Submission No. 22*, p. 2.

[9] ANAO, *Recordkeeping*, Audit Report No.45 2001-2002, pp. 18-19.

[10] *Public Accounts and Audit Committee Act 1951*, Sections 8(1) (c) & (d).

1.20 The Committee resolved in October 2002 to review the management and integrity of the Commonwealth's electronic information. This decision arose out of the Committee's review of a number of reports by the Auditor-General that addressed, wholly or in part, the issues of the management and integrity of electronic information held by the Commonwealth. A list of these reports, together with later reports on related issues, is shown in Appendix A.

1.21 The Committee established its own terms of reference, which are listed at page xii. The following paragraphs from the preamble to the terms of reference reflected the Committee's concerns:

> The Committee shall inquire into and report on the potential risks concerning the management and integrity of the Commonwealth's electronic information.
>
> The Commonwealth collects, processes and stores a large amount of private and confidential data about Australians. This information is held by various Commonwealth agencies and private bodies acting on behalf of the Commonwealth. For example, the Australian Taxation Office keeps taxpayer records, the Australian Electoral Commission keeps electoral roll information and Centrelink keeps social security, family and health information.
>
> The Committee is concerned that the Commonwealth's electronic information is kept securely and in a manner that ensures its accuracy.

1.22 Invitations to provide submissions to the inquiry were advertised in the national press on 30 October 2002. In response, 103 submissions have been received – a list can be found at Appendix B. Exhibits are listed at Appendix C.

1.23 The Committee held public hearings in Canberra and Sydney between March and October 2003. A list of witnesses at the hearings can be found at Appendix D.

1.24 In August 2003 the theft of two computer servers from the Australian Customs Service (Customs) facility at Mascot Airport was reported in the media. The Committee became aware of this incident during a public hearing into aviation security[11] but only after Customs had completed its evidence. Customs was recalled to explain why it had failed to advise the Committee of the breach during its evidence.

[11] *Transcript,* 5 September 2003, pp. 42-46.

1.25 The incident had serious ramifications for the management and integrity of electronic information and the Committee decided to reopen the evidence gathering phase of the inquiry. The Committee had an additional public hearing in October and also wrote to Commonwealth agencies for details of IT thefts and security breaches suffered since July 1998. The data collected from these replies reinforced the Committee's growing concerns about the physical security of IT equipment and the data stored on it.

Report Structure

1.26 In addition to this introductory chapter the report is divided into seven parts:

- Chapter 2, Examines the physical security of IT equipment and the information stored on that equipment.
- Chapter 3, Outsourcing, considers the advantages and problems in outsourcing IT functions.
- Chapter 4, Risk Management, considers the issue of risk management as a response to the threats posed to the security and integrity of the Government's electronic information.
- Chapter 5, Data Preservation, examines the problems of long term storage of information and agencies' plans for business continuity and disaster recovery.
- Chapter 6, Looks at Public Key Cryptography and how it is used to protect Commonwealth information in transit.
- Chapter 7, Evaluation of Products under Australasian Information Security Evaluation Program, is an examination of the process used to evaluate software products for use in Commonwealth systems.
- Chapter 8, Other Issues. This chapter covers three additional topics: the National Information Infrastructure, a Report by the Management Advisory Committee, and the debate on Commercial versus Open Source Software.

Existing Legislation

1.27 There is a body of legislation and supporting material that directly or indirectly covers the integrity of electronic information held by the Commonwealth. This includes:

- The *Financial Management and Accountability Act 1997* (FMA Act), which provides a framework for the proper management of public money and public property. Section 42 of the Act states that an official or Minister may be held civilly responsible for the loss of any public property, including information, that is in their custody. Each department and agency is responsible for protecting the electronic information that they hold.[12]

- The *Electronic Transactions Act 1999*, which provides a regulatory framework that facilitates the use of electronic transactions and enables business and the community, to use electronic communications in their dealings with government. Division 1 of the Act makes electronic transactions workable by giving them the same legal validity as regular transactions. Division 2 allows a person to use an electronic communication when required to provide information to the Government. Division 3, section 14, defines the time and place of the dispatch and receipt of an electronic communication. The Act also holds the purported sender of an electronic communication responsible for that communication, so long as it was actually sent by them.

- The *Privacy Act 1988*, which protects the privacy of individuals. Division 2 addresses the issue of information privacy, including electronic information. This division provides eleven Information Privacy Principles (IPPs) that set privacy standards for the keeping of personal information by Commonwealth and Australian Capital Territory government agencies. The Privacy Commissioner has responsibilities under the Privacy Act to pursue complaints of privacy breaches.

- The *Privacy Amendment (Private Sector) Act 2000*, which amends the *Privacy Act 1988* to set privacy standards for the collection, holding, use, correction, disclosure and transfer of personal information by private sector organisations. The amendment added ten National Privacy Principles, which provide a framework for the protection of personal information.

- The *Copyright Act 1968*, which relates to copyright of, among other things, electronic information. Sections 10AB, 10AC and 10AD of the Act describe the circumstances in which it is legal to copy electronic information. Sections 44E, 44F and 112DA describe the circumstances in which it is legal to import and sell copies of computer programs and copies of electronic literary or music items. Sections 49, 50, 51, 51AA and 51A describe the circumstances in which it is legal to electronically reproduce and communicate works for various purposes. Division 2A

[12] NOIE, *Submission No. 20*, p. 7.

covers circumvention devices and electronic rights management information.

1.28 This body of legislation is supported by a number of Commonwealth Government guidance documents. These include the:

- *Protective Security Manual* issued by the Attorney-General's Department, disseminates Commonwealth protective security policies, principles, standards and procedures, to be followed by all Commonwealth agencies for the protection of official resources. Part C specifically addresses information security;
- *Australian Communications Electronic Security Instruction 33*, developed by the Defence Signals Directorate, provides guidance to Australian Government agencies on protecting their information systems; and
- ANAO Better Practice Guide, *Internet Delivery Decisions: A Government Program Manager's Guide*, identifies key questions and issues for managers to consider when deciding whether and how their agency should use the internet.

1.29 The legislation and the guidance documents will be referred to through the following chapters as appropriate.