2

Physical Security

2.1 The question of the physical security of the Commonwealth's IT equipment, and the data stored on it, sprang into prominence during the course of the inquiry. Evidence taken by the Committee in another inquiry and press reports of the theft of two file servers from Customs underlined the vulnerability of IT equipment and the consequent threat to data security.

2.2 The Committee's concern was increased when evidence came to light of a serious security breach by Telstra Enterprise Services (TES), when backup tapes for several departments disappeared – presumed dumped as rubbish.

Introduction

2.3 The Committee was disturbed about the reports of IT equipment thefts. Although all of the details of the losses were not available, due to ongoing police investigations, there was sufficient information to indicate that lapses in security had occurred.

2.4 To clarify the facts, the Committee held a special public hearing in Canberra on 17 October 2003, taking evidence directly from the departments affected and the agencies involved in the investigation of the thefts.

2.5 In addition, the Committee asked Commonwealth agencies to provide details of all IT equipment, software and related products, lost since July 1998. The agency responses indicated a need to reduce the unacceptably high loss rate of equipment apparent in some departments and agencies. In addition, the difficulties and delays encountered in compiling the

requested data, showed that inventory controls have been neglected in many Commonwealth agencies.

2.6 The data provided by agencies revealed that laptop computers have been by far the most vulnerable equipment to loss or theft – more than 1000 having been lost over the five years surveyed.[1] A list of losses of IT equipment from Commonwealth agencies can be found at Appendix E. What was equally disturbing in the agency responses was the very low rate of recoveries and prosecutions related to these losses.

2.7 The Committee was particularly concerned to receive evidence from the Department of Defence that 'Not all data prior to 2002-03, such as laptops lost or stolen in 2000-01, is available from the asset management database and information prior to 2000 is not available from the investigations database.'[2] The Committee finds it unacceptable that of 64 computers lost or stolen in 2001-02 only 11 of these incidents were reported to federal or state police.[3]

Physical Security of IT Networks

2.8 In examining the evidence before it, the Committee found that the physical security of IT networks has two main aspects:

1) the security of the building itself and measures in place to counter attempts to break-in to secured areas; and

2) the screening process for people seeking access to secured areas and the measures in place to verify their identity and right to be admitted.

2.9 The Committee observed contractual relationships and responsibilities between Commonwealth agencies and IT service providers provide an additional layer of complexity in ensuring the physical security of IT equipment.

Building Security

2.10 One of the difficulties which became apparent during the inquiry, was the problem of maintaining a high level of security in shared office buildings.

---

1 Aggregate figure calculated from responses by Commonwealth Departments and associated agencies to the request made by the JCPAA in mid-October 2003.

2 Minister for Defence, *Submission No. 86,* p. 1.

3 Minister for Defence, *Submission No. 86,* p. 1.

Where Commonwealth agencies do not have full control of a building for security purposes, it is difficult to ensure that an adequate level of security is in place.

2.11 Inadequate building security allowed a break-in at the Department of Transport and Regional Services (DoTaRS) in August 2003, where the thieves used false identification to gain access to the building's public spaces and then physically broke-in to the secured area by smashing glass doors.[4]

2.12 This case shows the need for effective alarm systems in secured areas and for much faster response times from security services. As a result of this incident, DoTaRS is reviewing its security arrangements and, in the meantime, has hired security guards to patrol the area.[5]

2.13 To some extent, attention to physical security has taken second place in agency planning to the high profile task of protecting IT networks from electronic attacks. Electronic Data Services (EDS), an IT contractor to Commonwealth agencies including Customs, commented in its evidence that most of the focus is on stopping attacks on networks and that '… there is an assumption that physical security around key systems is going to be in place.'[6]

2.14 The Committee is concerned that this climate of complacency is addressed very quickly.

Visitor Identification

2.15 It is an essential link in the security chain that staff controlling access to secured areas are completely satisfied about the identity of anyone admitted to that area.

2.16 The Committee emphasises that, as in many aspects of security, the weak point in the system is the human factor. The best system possible cannot protect a site adequately against a security staff member who fails to carry out the correct procedures. This fact stresses the need for careful selection and training of security staff.

2.17 The theft from Customs is an excellent illustration of this principle – the thieves gained access to the building with false identification and then were allowed to enter a secure area unescorted. Neither of these errors

4 Mr Fisher, Mr Yuile, Mr Banham, *Transcript*, 17 October 2003, pp. 351-2.

5 Mr Fisher, *Transcript*, 17 October 2003, p. 364.

6 Mr Smith, *Transcript*, 17 October 2003, p. 321.

would have remained undetected if the prescribed security procedures had been followed.

2.18 When questioned by the Committee about the incident, Customs responded:

> We have a comprehensive set of security practices that are required to be followed – and are generally followed – which, I think, meet the standards that any external agency would set. In essence, what happened was a breakdown in the process in a particular location.
>
> We have taken physical steps to deal with access to the building; security steps in relation to the computer room; and steps in relation to accompanying people when they go on site. … So we are having a comprehensive look at security throughout Customs, with one of the major requirements being security plans which will be site specific – so that each site will need to have a security plan and an obligation that the security plan is complied with.[7]

2.19 EDS agreed with Customs that the security process and policy in place at the site was 'sound and robust' and that the problem was a local practice that negated the system:

> I would say that the approach being taken within Customs, defined by the policy and the processes that were in place, was sound, robust and sufficient to secure the equipment. What occurred was a breakdown in that process.[8]

2.20 The evidence suggests to the Committee that security procedures should be tailored to each location, as intended by Customs. In addition, to ensure that security procedures are followed correctly, regular staff training in security awareness should be conducted.

2.21 Appropriate security procedures provide a necessary condition for the safeguarding of electronic information, but the Committee is of the view that this by itself will not guarantee effective protection. To be fully effective, procedures must be underpinned by a strong security culture among departmental officials.

---

7 Mr Woodward, *Transcript*, 17 October 2003, p. 369.

8 Mr Smith, *Transcript*, 17 October 2003, p. 321.

Recommendation 1

2.22 **The Defence Signals Directorate (DSD) in conjunction with other agencies where appropriate, ensure that Commonwealth agencies institute without delay, physical security plans for each of their information technology systems. Additional plans may be necessary for key information technology centres. DSD to advise the Committee within six months of the tabling of this report, on the status and adequacy of these plans.**

2.23 The security lapses examined by the Committee have revealed that there is a need for clear and active channels of communication between agencies and outsourced service providers. In the context of this inquiry, contracts should place obligations on both parties to inform each other when an IT security incident occurs.

Recommendation 2

2.24 **The Australian Government Information Management Office advise all Commonwealth agencies that new or renegotiated contracts for outsourcing of information technology services need to pursue best practice and include the following:**

- **clear information sharing protocols that require each party to inform the other when an information technology security incident occurs that, directly or indirectly, affects the security of agency information technology networks;**
- **prohibition of unauthorised subcontracting of information technology services;**
- **provision for a graduated hierarchy of sanctions in response to security breaches.**

Survey of Equipment Losses

2.25 The responses from Commonwealth agencies to the Committee's request for details of lost or stolen IT equipment revealed that those losses had reached alarming levels. The value of the lost equipment and the cost of

replacing it, together represent a very substantial cost to the Commonwealth. This could either be in direct replacement costs or increased insurance premiums.

2.26 When the threat to data security is also considered, it becomes obvious that this is an area where all Commonwealth agencies have a need to ensure that their procedures and accountability are brought up to best practice as quickly as possible.

2.27 Even where the equipment is, in fact, owned by a contractor rather than the agency itself, the contract would no doubt have built-in to it an additional cost factor in anticipation of likely losses. It is in the Commonwealth's interest to institute practices which minimise that anticipated cost and hence the contract loading.

2.28 DSD has said that losses of IT equipment rate as Level 3 incidents under the Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS) and should all, therefore, be reported to DSD. Agencies seem to be unaware of this assessment and very few cases have, in fact, been reported without prompting from DSD.[9]

2.29 Customs offered the opinion that it is almost impossible to completely eliminate theft – but high quality internal security systems in IT equipment could ensure the protection of the data. In giving evidence Customs said:

> … it is going to be extremely difficult for any agency or private sector organisation to come up with a foolproof mechanism that prevents theft from either buildings or homes. What it does do is put a lot more pressure on those who design systems to enable appropriate protection and a series of layers of security to be built into those computers, and into the software that lies behind them, in the event they are stolen. I just do not believe there will ever be a solution to theft. We do the best we can.[10]

IT Equipment Lost by Agencies

2.30 A summary table of the IT equipment reported lost or stolen from Commonwealth agencies can be found at Appendix E. The following paragraphs, however, look at some of the more serious cases revealed in those reports. The Committee notes that IT assets are in some cases the property of the contracted service provider which can add a level of complexity to lines of responsibility.

9 Mr Burmeister, *Transcript*, 17 October 2003, p. 392.

10 Mr Woodward, *Transcript*, 17 October 2003, p. 370.

2.31 For sheer volume the quantity of equipment lost by the Department of Defence stands out. Although the losses reflect, to some extent, the scale of its operations compared to other departments, the loss of 537 personal computers and laptops in five years is alarming.

2.32 A particularly worrying aspect of the Defence losses is that three of the computers lost contained material classified as secret. Even though these machines were recovered, these incidents represent significant security breaches. In addition, there were more than thirty additional security breaches which did not involve national security level data.

2.33 FaCS also reported large quantities of equipment lost in the five year period. FaCS lost 117 laptops and 94 PCs and when the extremely personal nature of the data handled by this department is considered, these statistics represent a potentially substantial breach of individual privacy. The other aspect to be considered is that over half the laptops and almost three quarters of the personal computers, were lost in the last two years. This indicates that FaCS security position is worsening.[11]

2.34 Within the Treasury portfolio, the Australian Taxation Office (ATO) reported that in the period from 1 July 1999 to 29 September 2003, over one hundred laptops were stolen and twenty-two were lost. Fortunately, in this case Treasury reported that the hard drives of all laptops are encrypted with DSD approved software and would be very difficult to access.[12]

2.35 The Department of Industry, Tourism and Resources portfolio reported the loss of 138 laptops and 42 personal computers, 64 of these items were lost from the Commonwealth Scientific and Industrial Research Organisation (CSIRO) and the rest from the department itself.[13]

2.36 The equipment listed by departments was lost or stolen in a variety of locations. Personal computers were most often stolen from offices; while for laptops, thefts from offices, private homes, vehicles and hotel rooms were common. Laptops were also prone to be left in taxis and lost at airports. Several laptops were lost in the Canberra bushfires in January 2003.

2.37 Losses which were particularly disturbing were a laptop and a printer / facsimile machine stolen in separate incidents, while being

11 FaCS, *Submission No. 87*, p. 1.

12 Treasury, *Submission No. 82,* pp. 3-4.

13 DITR, *Submission No. 78,* pp. 2-4.

transported by courier services and a briefcase containing an encryption modem stolen while in transit in aircraft baggage. [14]

2.38 Although many of the thefts and losses were reported to police, the recovery and prosecution rate is best described as disappointing. The Committee believes Commonwealth agencies should report all thefts of laptops, personal computers and other valuable IT equipment to the police. This strategy will reinforce the significance of IT losses on those responsible for the safekeeping of the equipment.

Telstra Incident

2.39 The case involving TES reinforced the need for staff to adhere closely to security guidelines. In this case, backup tapes holding e-mail traffic for several departments, were routinely stored for a brief time in a wheelie bin, while awaiting movement to a secure storage area. On this occasion there was a changeover in staff and the new staff member presumed that the normal transfer to secure storage had proceeded as usual. Several weeks later it was discovered that the tapes were not in the secure storage area.[15]

2.40 Telstra have been unable to trace the tapes and it is presumed that they were thrown out in the course of the normal rubbish collection – although no-one can be certain of this.[16]

2.41 The Committee has reviewed the comments made by TES on this incident and was dissatisfied with their vagueness. For example, asked where the incident occurred, TES representatives were unable at first to say which city the problem occurred in. They were also unable to definitely state whether or not press reports that Telstra staff had searched rubbish tips for the lost tapes, were accurate or not.[17]

2.42 It was left to the Department of the Prime Minister and Cabinet (PM&C) to explain that, in fact, since the loss was not discovered for some time, no physical search was made because by then, the dumping area would have been covered by several metres of landfill.[18]

---

14 Attorney-General's Department, *Submission No. 75*, pp. 3 and 5 and Treasury, *Submission 82*, p. 6.

15 Dr Ball, *Senate Hansard Transcript*, 4 November 2003, F&PA, pp. 65-6.

16 Mr Scales, *Senate Hansard Transcript*, 3 November 2003, ECITA, p. 41.

17 Mr Scales, *Senate Hansard Transcript*, 3 November 2003, ECITA, p. 42.

18 Dr Ball, *Senate Hansard Transcript*, 4 November 2003, F&PA, p. 66.

Laptop Computers

2.43 Laptop computers have proved to be the most attractive target for thieves and also, because of their small size, easy portability and marketability, the item of equipment most frequently lost. The Committee considered that reducing the loss rate for laptops should be a priority for all agencies – not only because of the monetary value of the equipment, but also because of the value of the information that may be lost or disclosed.

2.44 Each agency will need to make its own assessment of the best ways of achieving this aim. The Committee discussed with a number of witnesses, possible means of achieving tighter control over laptops and thus reducing the loss rate.

2.45 Several departments reported that their laptops were protected by encryption software, approved by DSD, which locked down their hard drives and operating systems to prevent unauthorised access. The Committee believes this policy should be adopted by any agency which has a need to carry classified information on its laptops.

2.46 DSD suggested that, given that the equipment is specifically designed for easy transport from place to place, the focus should be on better asset controls and on making individuals responsible for their safekeeping.[19]

2.47 The Committee considered which agency would be the most appropriate to introduce tighter security requirements for the use of portable electronic devices across government. The agencies considered were:

- the Department for Communications, Information Technology and the Arts and its portfolio agency National Office for the Information Economy (NOIE), which is responsible for promoting 'e-security';
- the Attorney-General's Department because unauthorised access to the information held on lost or stolen equipment could have national security implications;
- the Department of Finance and Administration (DoFA) because the loss of items in such numbers has financial management and asset management implications; and
- PM&C because it administers the *Public Service Act 1999* which outlines standards of behaviour expected of public servants.

2.48 Given the role of the Management Advisory Committee (MAC), the Committee concluded that PM&C is the most appropriate agency, particularly given that the implementation of the recommendation below

19 Mr Merchant, *Transcript*, 17 October 2003, p. 368.

will require the promotion of a broad change in behaviour towards greater security awareness across agencies.

2.49 In framing the recommendation below the Committee recognises the value of laptop computers in enabling flexible working arrangements such as working from home.

Recommendation 3

2.50 **The Department of Prime Minister and Cabinet introduce regulations that address the issuing and use of laptop computers and other portable electronic devices by Commonwealth agencies. The regulations should require that:**

- **such equipment is only issued to officers on a needs basis;**
- **such equipment is assigned to an individual, rather than to a work area, to ensure clear accountability;**
- **portable electronic devices are given password protection and, where they hold sensitive information, that data should be suitably encrypted;**
- **movement logs are made mandatory for valuable equipment taken outside agency premises ('valuable' here includes the significance of the information involved, as well as the monetary value);**
- **all thefts are reported to the police and to a central reporting body such as the Defence Signals Directorate; and**
- **regular inventory audits are conducted.**

Committee Comment

2.51 In relation to the reporting of security incidents, the Committee wishes to remind agencies of their responsibility to advise DSD of level 3 and 4 security breeches, which includes the loss of IT equipment. DSD should not have to chase agencies to obtain a report.

2.52 While acknowledging that complete elimination of theft may be impossible, the Committee expects agencies to reduce the level of theft through improved security procedures and better training.

2.53 Similarly it expects agencies to impress on their staff the responsibility they have to safeguard IT resources. The Committee anticipates that a security awareness program, combined with individuals taking greater responsibility for equipment assigned to them, will help to reduce IT losses. To aid the cultural change, IT security should also be included in all staff induction programs and staff members should be given regular refresher sessions thereafter.

2.54 The Committee has recommended that the theft of any piece of IT related equipment, whether a mobile phone or a laptop computer, should be reported to the police. In addition, IT thefts and security breaches should also be reported to agencies' audit committees to ensure there is 'whole of agency' recognition of the problem and of the impact on agency business.

2.55 Agencies should review back up storage plans including whether they need to encrypt all data in back-up storage, especially data stored off-site with an external provider. The necessity for this step will depend on the agency concerned, but the Committee believes agencies should err on the side of caution.

Asset Registration

2.56 Among other things, the recent incidents have shown that there are serious flaws in the system of asset registration and accounting in a number of agencies.

2.57 In the Customs case, it became apparent to the Committee that control of the asset register maintained by EDS was inadequate. On 28 August 2003 Customs inquired of EDS as to the possible loss of any equipment besides the two file servers that were originally notified as stolen.[20] It was not until 15 October 2003 that EDS confirmed to Customs that two desktop computers and a battery charger had been stolen at the same time as the file servers.[21] In giving evidence, EDS admitted that it was unable to immediately establish just what equipment had been stolen.[22]

2.58 This apparent lack of control of valuable assets (or, at the least, a sad lack of communication), was of concern to the Committee. A considerable amount of time went by after the theft was discovered before Customs

20 Ms Batman, Mr Woodward, *Transcript*, 17 October 2003, pp. 368-72.

21 Mr Woodward, Ms Batman, *Transcript*, 17 October 2003, pp. 374-5.

22 Mr Merchant, *Transcript*, 17 October 2003, p. 351.

and EDS both knew exactly what had been lost.[23] The Committee considers this unacceptable.

2.59 The lack of precision in the assets register was clearly illustrated when Customs said:

> We did not do a reconciliation between the previous asset register with the current one – I think the assumption … is that assets remain where they are forever. These assets are being moved around all the time-
>
> … It is not an unusual situation for PCs … to not be in the place you think they are, in an environment like this.[24]

2.60 Further evidence came from the Department of Defence, when it was unable to provide a detailed breakdown of its equipment losses prior to 2002-03.[25]

2.61 The potential seriousness of the loss of portable IT equipment was demonstrated by an incident in the United Kingdom in December 1990. A Ministry of Defence laptop, which had been left unattended in a private car, was stolen. The laptop contained extremely sensitive military plans on the upcoming Desert Shield campaign in Iraq. The incident also demonstrates the importance of a robust security culture.[26]

2.62 The impression of an overall lack of control and accountability of IT assets is heightened when the lengthy list of lost equipment reported by agencies, is considered. The Committee suggests that this would be a suitable area for review by ANAO in the near future.

23 Mr Woodward, Ms Batman, *Transcript*, 17 October 2003, pp. 352-7.

24 Mr Harrison, *Transcript*, 17 October 2003, p. 359.

25 Minister for Defence, *Submission No. 86*, p. 1.

26 *The Independent*, 31 December 1990.

Recommendation 4

2.63 **The Australian Government Information Management Office (AGIMO) ensure that Commonwealth agencies:**

- **have up-to-date asset registers of all IT equipment owned by them and used on their premises; and**
- **undertake a regular audit and reconciliation program of all owned and leased IT equipment.**

AGIMO should advise the Committee, in an Executive Minute, of the completeness of the registers and the audit procedures that have been established.

2.64 The publicity on the theft of IT equipment that resulted from this Committee's inquiry, particularly the loss of the two servers from the Customs facility at Mascot Airport, has dramatically changed department security procedures. The Chief Executive Officer of Customs stated that:

> We have taken physical steps to deal with access to the building [at Mascot] security steps in relation to the computer room and steps in relation to accompanying people when they go on site … we are having a comprehensive look at security throughout Customs, with one of the major requirements being security plans that will be site specific – so that each site will need to have a security plan and an obligation that the security plan is complied with.[27]

2.65 This incidence of reporting of the breaching of the security of Commonwealth electronic information systems clearly demonstrates the link between transparency and increased accountability of agencies.

27 Mr Woodward, *Transcript*, 17 October 2003, p. 368.