



Telephone: (02) 6263 3311
Facsimile: (02) 6263 3104

THE TREASURY

Information Unit
The Treasury
Langton Crescent
PARKES ACT 2600

15 October, 2003
File: ER2002/000645

The Committee Chairman
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Sir,

REQUEST FOR INFORMATION ON COMPUTER RELATED SECURITY BREACHES

In response to your correspondence of 16 September 2003 to Dr Ken Henry, the following information is provided. Responses are listed for each agency within the Treasury portfolio.

Australian Bureau of Statistics (ABS)

The losses of hardware since 1998 are as follows:

Year ended 30 June 1999	1 Laptop computer stolen from residence, not recovered.
Year ended 30 June 2000	1 Laptop computer was lost in the field. 3 Laptop computers were stolen: 2 from residences and 1 from office. None recovered.
Year ended 30 June 2001	1 Laptop computer was lost in transit by courier. 4 Laptop computers were stolen: 1 from residence, 2 from office and 1 from hotel. None recovered, replacement value recovered from hotel.
Year ended 30 June 2002	2 Laptop computers were stolen from residences. One Palm Pilot was lost, and one desktop PC (owned by a contractor) was also stolen. None recovered.
Year ended 30 June 2003	1 Laptop computer was lost. 6 laptop computers were stolen: 1 from office, 3 from residences, 1 from hotel and 1 from vehicle. 1 lost. None recovered.
2003/04 Financial YTD	3 Laptop computers were stolen: 2 from residences and 1 from vehicle.

All thefts of ABS equipment listed above were reported to police. To date, no response has been received from police in any State or Territory for any incident.

All ABS laptops are secured by DSD approved security software. This software encrypts the whole hard drive and locks down the BIOS. This means that anyone without authorised access to the Notebook cannot access any data/software on the hard drive. The laptops are also marked with security paint.

For the period specified, ABS has detected no incidents of unauthorised access to ABS computer systems.

There was a significant amount of inappropriate use of ABS systems detected late in 1998. This was investigated and disciplinary actions carried out.

In August 2003, the ABS network was infected by a computer worm which resulted in a shutdown of the ABS network for an afternoon. ABS has now increased its anti-virus defences.

Australian Consumer Competition Commission (ACCC)

ACCC has suffered the loss or theft of three notebook computers since July 1998.

The details are as follows:

- A notebook computer was found to be missing in April 1999 from our Brisbane Office. An internal investigation found that theft was the likely cause. The item has not been recovered.
- Two notebook computers were stolen from our Sydney Office in April 2001. Police were called to investigate. No action has been taken to date and the items have not been recovered.
- One notebook computer was stolen from the Sydney home of one of our staff. Police were called to investigate. The item has not been recovered.

There were no other security issues.

Australian Prudential Regulation Authority (APRA)

1. Losses of hardware and software are described in detail in the response to Senate Questions QoN 2090 and 2072.
2. No unauthorised access to APRA computer systems have been detected or reported in the financial years 2001-02 and 2002-03. No records exist of any such breaches in prior years.
3. APRA has experienced no significant technology related security breaches in the financial years 2001-02 and 2002-03. No records exist of any such breaches in prior years.

Australian Securities & Investment Commission (ASIC)

The losses of hardware since 1998 are as follows:

Year ended 30 June 1999	2 Laptop computers were stolen. The losses were reported to the Police, but perpetrator(s) could not be identified.
-------------------------	---

Year ended 30 June 2000	2 Laptop computers were stolen. The losses were reported to the Police, but perpetrator(s) could not be identified.
Year ended 30 June 2001	Nil
Year ended 30 June 2002	One Desktop computer. The loss was reported to the Police, but perpetrator(s) could not be identified.
Year ended 30 June 2003	2 Laptop computers were stolen. The losses were reported to the Police, but perpetrator(s) could not be identified.

Desktops are protected by DSD approved security software rendering the hard disk unusable, user login and password protection on all PC's and by ASIC's physical security arrangements

Laptops are protected by DSD approved security software rendering the hard disk unusable. This includes PC vault to encrypt hard disks on all laptops and home PC's, secure remote for VPN connection to the ASIC network and user login and password protection.

In relation to the question concerning unauthorised access to computer systems, there has only been one reported unauthorised access to ASIC systems during this period and this occurred in the ASIC Brisbane office in August 2003. A staff member inappropriately demonstrated the ASIC investigation system to a visiting officer from the Queensland Police without ASIC approval. The staff member has been dismissed.

In relation to the question inviting comment on any other significant events involving information technology security, ASIC has nothing to report on this area.

The Committee might be interested to know that during 2001, the Defence Signals Directorate (DSD), conducted a security audit of ASIC systems and controls and concluded that these were appropriate. The audit focused on the "perimeter security" of ASIC's computer systems in order to ensure that external operators cannot "hack" into the network. ASIC understands that the DSD will be conducting another audit along similar lines in the near future.

Australian Taxation Office

Losses of software and/or hardware

The tables hereunder provide information relating to the hardware component of the request. The ATO is unable, without significant further research, to supply information which pre-dates the outsourcing of the ATO's information and communications technology infrastructure services to EDS in 1999. This data is not readily available as prior to 1999 no central register was held.

Period	Servers	Workstations		Laptops	
	Stolen	Lost	Stolen	Lost	Stolen
1 July 99 to 30 June 00	1	0	0	3	15
1 July 00 to 30 June 01	0	0	14 (14)	6 (0)	31 (26)

Period	Servers	Workstations		Laptops	
	Stolen	Lost	Stolen	Lost	Stolen
1 July 01 to 30 June 02	0	0	0	8 (0)	36 (26)
1 July 02 to 30 June 03	0	0	2 (0)	4 (0)	31 (23)
1 July to 29 September 03	0	0	0	1 (1)	2 (2)

Note 1: The ATO Services Agreement with its outsourcer continues to include the Child Support Agency even though that agency is no longer part of the Treasury portfolio. The figures provided above exclude CSA losses and thefts.

Note 2: () Bracketed figures indicate number of cases reported to the police.

Note 3: The numbers of incidents reported to the police are not readily available for the 1999/2000 financial year.

In relation to the software component of the request:

- Software does not reside on workstation hard drives but on servers;
- The stolen server had Web enabling software only loaded; and
- Current encryption software encrypts the hard drive and any information stored on laptop computers, thereby preventing access to software and data. Prior to September 2001, laptop design prevented full encryption of the hard drive. However, encryption of the boot sector of the hard drive prevented access to software and data by password protecting the access.

Encryption software is DSD (Defence Signals Directorate) accredited and the expertise and equipment needed to break the code is extremely high. It is extremely unlikely that any individual would possess the resources to break the code and therefore an opportunistic theft would pose almost no threat of access to the data.

Unauthorised access to computer systems

In identifying and supplying information in relation to unauthorised access to ATO computer systems, this response considers both internal and external access to ATO computer systems and/or systems data.

The ATO Fraud Prevention and Control Section (FP&C) is responsible for the investigation of allegations of ATO staff accessing taxpayer information or data in breach of the secrecy provisions contained in S.16 of the *Income Tax Assessment Act 1936*.

The FP&C Section have provided the following records for the period July 1999 to the current time (provision of records prior to July 1999 would require a manual review of all FP&C case files):

- FP&C has investigated 574 cases of alleged information access in breach of the secrecy provisions;
- The allegations contained in 507 of the cases were found to be unsubstantiated;
- 67 of the investigations resulted in disciplinary action being taken against the subject officer; and

- 18 of the investigations resulted in the DPP instituting criminal proceedings against the subject officer. (Note: every criminal prosecution entails a disciplinary process in relation to the subject officer).

The ATO Trusted Access (ATA) Branch has responsibility for the development and maintenance of the ATO's e-business gateway environment, including the monitoring of unauthorised attempts to breach this environment. ATA employ a third party contractor (SecureNet) to monitor the ATO gateway environment 24 x 7. This monitoring service constitutes the first level of support for the ATO's IT Security critical incident response capability. This capability extends to varying levels of ATO technical, management and executive support personnel and calls upon the expert services of external Government agencies, including the Defence Signals Directorate and the Australian Federal Police.

The SecureNet team have maintained records of unsuccessful and successful security breaches within the ATO's e-business or external gateway environment since June 2002 and these records are grouped into four separate categories:

Incident Category	Description
1	These incidents include events that cannot be definitely identified as an attack. Record but no further action required.
2	These incidents are unsuccessful attacks; they have no effect on system operations. Record and maintain a watching brief.
3	These are successful attempts to breach security policy with minor consequences to system operations. Initiate primary critical incident response processes.
4	These are successful attempts with major consequences. Initiate critical incident response processes.

To date, the monitoring team have recorded:

- Category 1 – 165,921,014 events
- Category 2 – 73,778,442 events
- Category 3 – 4 events
- Category 4 – 0 events

The four category 3 events recorded include three instances of infection of ATO equipment by a potentially harmful Worm program. In each case, these were identified, isolated and removed with minor consequence or impact on ATO systems.

The fourth category 3 event relates to a breach of data backup tape handling procedure which presented zero consequence or impact to ATO computing systems, but which may potentially have resulted in data loss or compromise. Analysis of the event concluded that it was a procedural error only and it was confirmed that no ATO data had been compromised or lost.

Any other significant events involving information technology security

It is the opinion of the ATO Trusted Access Branch that the ATO has to date not experienced any other events which would be considered "significant" in regard to IT security. To qualify this statement, with reference to qualitative measures of consequence or impact (see table below) contained in the

Australian/New Zealand Standard AS/NZS 4360:1999 – Risk Management, the ATO has not experienced an IT security event which has delivered higher than a Minor level of consequence or impact to the ATO.

Descriptor	Example Detail Description
Insignificant	No injuries, low financial loss
Minor	First aid treatment, on-site release immediately contained, medium financial loss
Moderate	Medical treatment required, on-site release contained with outside assistance, high financial loss
Major	Extensive injuries, loss of production capability, off-site release with no detrimental effects, major financial loss
Catastrophic	Death, toxic release off-site with detrimental effect, huge financial loss

Productivity Commission

Loss of software and/or hardware

There has been one incident involving the loss in transit by a courier of a Canon L280 facsimile/printer valued at \$977. Steps taken by the Commission to recover costs from the courier proved unsuccessful. Use of this particular courier has been curtailed and courier items are now insured when it is cost effective to do so.

Unauthorised access to computer systems

Nil.

Any other significant events involving information technology security

Nil.

The Treasury

Loss of Software and/or hardware

Year ended 30 June 2000

1 Laptop computer was lost or stolen. The loss was reported, but equipment was not recovered.

Year ended 30 June 2001

1 Laptop computer was lost or stolen. The loss was reported, but equipment was not recovered.

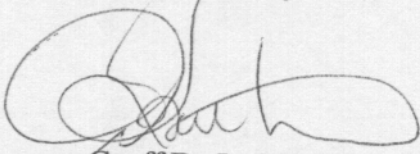
Unauthorised Access to Computer Systems

Treasury has experienced two security incidents relating to Internet websites. In March 2000 the home page of the Treasury website was defaced and replaced with a message from a Brazilian hacker group. The hackers exploited a weakness in the operating system software. A software hotfix was obtained and installed prior to the site being put back online.

The second incident occurred in June 2000 and involved the GST Startup website. This site listed companies that were registered to provide assistance with the implementation of GST .By manipulating the information in the URL Address, a registered user of the site was able to display BSB and Bank Account details of other registered users. The website was updated and independently audited prior to relaunch.

If you require further information or wish to clarify any particular issue, please contact me on 02 6263 3311 or by e-mail at gdelamotte@treasury.gov.au.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Geoff De La Motte', written in a cursive style.

Geoff De La Motte
Manager
Information Unit