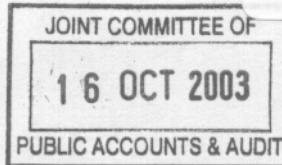


16 OCT 2003

Submission No. 78



Australian Government
Department of Industry
Tourism and Resources



20 Allara Street
CANBERRA ACT 2600

GPO Box 9839
Canberra ACT 2601 Australia

Phone: 6213 6328
Facsimile: 6213 7800

Email: tim.mackey@industry.gov.au

Web: www.industry.gov.au

ABN: 51 835 430 479

Mr Bob Charles MP
Chairman
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Mr Charles

Request for Information on Computer Related Security Breaches

I refer to your letter on 16 September 2003 in which you requested the Department of Industry, Tourism and Resources and its associated agencies provide information on computer related security breaches since 1 July 1998.

Attached for your information are details of the losses of software/and or hardware; unauthorised access to computer systems; and other significant events involving information technology security. Investigation results into these incidents are also contained in the attachment.

Yours sincerely

Tim Mackey
Deputy Secretary
14 October 2003

Information on Computer Related Security Breaches since July 1998 – the Department of Industry, Tourism and Resources and its associated agencies

Losses of software and/or hardware

There has been no recorded incident of lost or stolen software in the Industry Tourism and Resources (ITR) portfolio since 1 July 1998.

The ITR portfolio has identified that the following equipment has been lost or stolen since 1 July 1998.

1998-1999

There have been 2 items of stolen equipment in the Industry Science and Resources (ISR) portfolio. These incidents were reported to the Police. One machine has been recovered.

1999-2000

There have been 87 items of lost or stolen equipment in the ISR portfolio, 44 from CSIRO, 24 from ISR and 19 from agencies. 5 laptops have been recovered and 5 offenders apprehended.

Agency	Number of lost items	Number of stolen items	Total
CSIRO	0	44	44
ASC	0	9	9
ISR	11	13	24
AUSLIG	0	0	0
AGSO	0	3	3
ATC	1	3	4
IPA	0	0	0
ANSTO	0	3	3
AIMS	0	0	0
ASDA	0	0	0
AGAL	0	0	0
Total	12	75	87

2000-2001

There have been 68 items of lost or stolen equipment in the ISR portfolio, 20 from CSIRO, 10 from ISR and 38 from agencies. 7 Laptop have been recovered and 1 offender has been apprehended.

Agency	Number of lost items	Number of stolen items	Total
CSIRO	0	20	20
ASC	0	13	13
ISR	5	5	10
AUSLIG	0	8	8
AGSO	1	5	6
ATC	0	5	5
IPA	0	2	2
ANSTO	0	1	1
AIMS	0	1	1
ASDA	0	1	1
AGAL	0	1	1
Total	6	62	68

2001-2002

There have been 17 items of lost or stolen equipment in the ITR portfolio, 4 from ITR and 13 from agencies.

Agency	Lost items	Stolen items	Total
DITR	0	4	4
GA	0	3	3
AGAL	0	2	2
IPA	0	5	5
ATC	1	2	3
NSC	0	0	0
Total	1	16	17

2002-2003

There have been 28 items of lost or stolen equipment in the ITR portfolio, 8 from ITR and 20 from agencies. 1 monitor was recovered.

Agency	Lost items	Stolen items	Total
DITR	2	6	8
GA	0	8	8
AGAL	0	8	8
IPA	0	4	4
ATC	0	0	0
NSC	0	0	0
Total	2	26	28

Total losses since 1 July 1998:

- 138 laptops
- 42 desktop PC's
- 3 printers
- 11 monitors
- 2 CD drives
- 1 floppy Drives
- 2 zip drives
- 1 data projector
- 1 interface card
- 1 docking station

All of the above incidents have been reported to the relevant authorities and where appropriate, investigations have taken place. 6 offenders have been apprehended. 13 laptops and 1 monitor have been recovered.

Unauthorised Access to Computer Systems

There has been one recorded incident of unauthorised access from the internet to an ITR machine which happened on 17 April 2002. The investigation showed there was no evidence that the integrity of any ITR information was compromised, nor evidence of access to sensitive information. ITR has identified and fixed the security hole.

No offender has been identified.

The ATC recorded an incident on March 13 2002 which did not adversely affect the Australia.com production site. The site was hacked and the content of a non-critical file was replaced with Portuguese text attacking the U.S. Government. The production site did not stop serving pages as a result, and the affected file was at no time visible to the public audience. Once identified, the ATC switched traffic of the site to the unaffected contingency site where Australia.com pages were served until March 21 2002. A full investigation into the security breach and level of damage was then conducted. The Australia.com production web servers were rebuilt during this time and the security breach closed.

No offender has been identified.

Other Significant Events Involving Information Technology Security

Denial of Service Attack

There has been one recorded incident of a successful Denial of Service attack which resulted in the ABRpublic web site being unavailable for short periods on 1 May 2003 (between 5.53am and 9.00am and between 5.30pm and 5.45pm). Relevant security fixes have been implemented. There has been an investigation and no offender has been identified.

Virus Attacks

There have been three recorded incidents of virus attacks on the ITR portfolio. These attacks were contained quickly and resulted in limited disruption to the Department's functionality. Relevant security measures and patching have been implemented.

Loss of Data Tapes

A serious breach of IT security, involving the loss of a quantity of backup tapes by Telstra Enterprise Services (TES) Pty Ltd, occurred in March 2003. TES is the outsourced Information Technology and Telecommunications (IT&T) service provider for Group 5 agencies of which this department is a member.

The loss of the backup tapes was due to a major breakdown in TES's tape handling procedures. The backup tapes have not been recovered.

Dr Shergold wrote to Dr Ziggy Switkowski, CEO Telstra, to express the Group's extreme concern with the extent of this security breach and the negligence of TES staff in the protection of Commonwealth information. Dr Switkowski assured Group 5 that Telstra and TES were very concerned with the seriousness of the breach and had revised the procedures and processes for backup to ensure that all agency information would be handled appropriately, as is required under the contract. Group 5 is undertaking random inspections of the backup facility.

The Australian Federal Police (AFP), Defence Signals Directorate (DSD) and ASIO were informed immediately of the security incident once TES became aware of it. The AFP made an initial assessment of the incident and determined that there was no evidence to suggest criminal conduct. DSD will alert the AFP at once if there is any evidence of the tapes being found and used.

Group 5 agencies have also conducted an independent audit to review the circumstances surrounding the event. This confirmed TES's account of the circumstances. We are agreed that the most likely explanation is that the tapes were accidentally disposed of as rubbish.

Glossary of Acronyms

AGAL:	Australian Government Analytical laboratories
AGSO:	Australian Geological Survey Organisation
AIMS:	Australian Institute of Marine Science
ANSTO:	Australian Nuclear Science and technology Organisation
ASDA:	Australian Sports Drug Agency
ASC:	Australian Sports Commission
ATC:	Australian Tourist Commission
AUSLIG:	Australian Survey and Land Information Group
CSIRO:	Commonwealth Scientific and Industrial Research Organisation
DITR:	Department of Industry, Tourism and Resources
GA:	Geoscience Australia
IPA:	IP Australia
ISR:	Department of Industry, Science and Resources
NSC:	National Standards Commission