INTERNET SECURITY MANAGEMENT

ISSN 1036-7632

ISBN 0 644 39000 X

Canberra ACT
27 November 1997

Australian National
Audit Office

Dear Madam President
Dear Mr Speaker

In accordance with the authority contained in the *Audit Act 1901*, the Australian National Audit Office has undertaken a financial control and administration audit of Internet Security management and administration across a number of Commonwealth entities.

Financial control and administration audit findings are reported generically. The findings and recommendations contained in this report are not therefore necessarily attributable to any one entity, based as they are on a range of entity experience. The nature and delivery of these types of audits are set out in the *Financial Control and Administration Audit Charter* published in 1995.

This report concentrates on findings which have an 'across the board' perspective and relevance. A companion better practice guide *Internet Security Management* has been developed in the course of the audit (a summary of which has been reproduced in Appendix 1 of this report). The guide draws on experience from both the private and public sectors.

I present this report to the Parliament. The report is titled *Internet Security Management*

Yours sincerely

P. J. Barrett
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

Contents

Abbreviations / Glossary vii

PART ONE ix

Summary of Key Findings and Recommendations xi
- Background xi
- Scope xii
- Audit Conclusion xiii
- Summary of Key Findings xiii
- Summary of Key Recommendations xiv
- Future Directions xiv
- Recommendations xv

PART TWO 1

Detailed Findings and Recommendations 3
- Introduction 3
- Planning an internet Connection 3
- Securing an Internet Connection 5

PART THREE 11

Appendix 1 Internet Security Principles 13

Appendix 2 Objectives, Scope and Focus of the Audit 18

Series Titles 1997-98 20

Financial Control and Administration Audits

- *are concerned with improving the quality of public sector administration. They are intended to assist public sector managers in meeting their responsibilities and to inform the Parliament about aspects of public administration; and*
- *deal with those systems and procedures implemented to support and assist in the delivery and monitoring of the products and services provided by the public sector. They aim to identify, develop and report better practice for broader application.*

Auditor-General reports are available from Commonwealth Government Bookshops. Recent titles are shown at the back of this report. For further information please contact :

The Reports and Publications Officer
Australian National Audit Office
GPO Box 707
Canberra ACT 2601
telephone (02) 6203 7537
fax (02) 6203 7777
e-mail library@anao.gov.au

Information on ANAO audit reports and activities is available at the following Internet address: http://www.anao.gov.au

The Auditor-General is head of the Australian National Audit Office. The ANAO assists the Auditor-General to carry out his duties under the Audit Act to undertake performance audits and financial statement audits of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

Auditor-General reports are available from Commonwealth Government Bookshops. Recent titles are shown at the back of this report. For further information contact:

The Publications Manager
Australian National Audit Office
GPO Box 707 Canberra ACT 2601
telephone (02) 6203 7537
fax (02) 6203 7798

Information on ANAO audit reports and activities is available at the following Internet address:
http://www.anao.gov.au

Glossary of Terms

Authentication	Verification of the identity of a computer user or another computer. This is usually achieved through the use of user ids and passwords.
Browser	A client application that lets users view and interact with information from the Internet.
Control	In general terms, it is a mechanism used to ensure various processes/systems operate as designed.
Data Warehouse	An orderly and accessible repository of facts and related data that is used as a basis for making management decisions.
Dial-up	A facility used to obtain remote access to an agency’s network through telephone facilities.
Electronic commerce	A method to conduct, manage and execute business related transactions using computer and telecommunications technology.
Email	A facility to send messages electronically.
Encryption	Encoding information to prevent unauthorised access.
Firewall	A specific mechanism(s) that controls access between two networks.
General IT controls	Controls that relate to the operation of an agency’s systems and are not peculiar or special to the Internet connection.

Hacker	Person who attempts to gain unauthorised access to an agency’s computing facilities and systems.
Incident Response Capability	The ability of an agency to detect, identify and respond to any suspected breach of the agency’s Internet security.
Information Resources	Covers information in electronic form, hardware and software of the agency’s systems and networks and the documentation supporting them.
Internet	A worldwide public communication facility that provides an email facility and an electronic pipeline for information between governments, businesses, consumers and individuals.
Log	A mechanism which is used to record events, transactions or user activity.
Network	Consists of more that one computer, linked by communication lines to share information and other facilities.
Repudiate	Refusal to acknowledge sending or receiving a transaction.
System Software	Software used to operate the computer.
Viruses	Programs that alter the way a computer works without the permission or knowledge of the user.
Virus Prevention Capability	The ability of an agency to prevent, detect and recover from infection by computer viruses.
Web page	A structured and formatted electronic document containing information from the Internet.

PART ONE

Summary of Key Findings and Recommendations

Summary of Key Findings and Recommendations

1.1 The Internet comprises the on-line world of the information highway. It is a public communication facility that provides an email facility and an electronic pipeline for information between governments, businesses, consumers and individuals.

1.2 This report deals with the management of Internet security in Commonwealth public sector entities, including departments and similar agencies, and commercial and non-commercial statutory authorities.

1.3 The objective of this audit was to form an opinion on the effectiveness of Internet security measures within the Commonwealth public sector.

1.4 The second objective was to provide better practice guidance for managing an Internet connection.

Background

1.5 The Internet has expanded rapidly in recent years and is expected to continue to do so. Between 1996 and 1999 it is estimated that the number of Internet users worldwide will increase from 38 million to 200 million[1]. In July 1996 A G B McNair conducted a survey which estimated that 1.2 million Australians aged 18 years old and over have access to the Internet at home and at least 20% of Australians have accessed the Internet at some stage (40% of Australians between 18 and 24 have used the Internet)[2].

1.6 The use of the Internet will continue to grow due to :

- improving communication speed and reliability;
- decreasing costs of technology;
- increasing computer literacy; and
- increasing services being provided.

1.7 Historically, the main uses of the Internet have been limited to electronic mail and research with the principal users being universities and other research and education bodies. However, increasingly, the Internet is being used for more commercial purposes such as selling goods and services, electronic banking and marketing.

[1] Price Waterhouse, Information Technology Forecast 1997

[2] This survey covered a nationally representative sample of people aged 18 years and over.

1.8 Commonwealth government agencies have been developing their Internet capabilities over a number of years. In line with experience in the general community, Internet usage by the Commonwealth has, to date, been restricted to electronic mail and research. However, several agencies are currently planning to provide commercial services and payment facilities via the Internet (ie: electronic commerce).

1.9 Using the Internet is subject to the following risks:

- outside users ('hackers') using the Internet to gain unauthorised access to data or functions held on internal networks;
- disruption or sabotage of information technology related equipment and services;
- provision of inappropriate and banned material for general access (eg pornographic and violent themes);
- computer viruses being imported from the Internet to the internal network;
- unauthorised interception of confidential or sensitive material transmitted over the Internet;
- loss of reputation due to security related incidents becoming publicly known; and
- different legal requirements, interpretations and jurisdictions.

1.10 Agencies using the Internet need to ensure that an appropriate control framework has been implemented to minimise these risks. With the use of the Internet continuing to evolve, the control frameworks that are satisfactory today may not be adequate in the future. As agencies expand their use of the Internet they will need to review continuously the adequacy of security provided and necessary controls to ensure that risks continue to be adequately addressed.

1.11 Some risks can be reduced through the establishment of a separate computer network dedicated for Internet use only. This prevents Internet users from obtaining access to an agency's corporate database, data warehouse and other corporate systems. Such a standalone system would only include information that is publicly available. This report primarily considers Internet security in respect to networked access to the Internet.

Scope

1.12 The audit covered a range of Commonwealth agencies which had established an Internet facility. It specifically addressed the following matters :

- Internet security policies;
- site management - including change control processes, virus prevention and detection strategies, and incident response plans;

- controls over access to the Internet site and to data sources connected to the site; and
- user education and training.

Audit Conclusion

1.13 Based on the results of the audit, it is concluded that:

- most agencies had some of the core elements required for effective Internet management; however, improvement was required in several key areas; and
- a small number of agencies were operating and managing their Internet facilities at or near identified better practice.

Summary of Key Findings

1.14 The above conclusions are based on the findings summarised below. Each of these is dealt with in Part 2 of this report.

Planning an Internet Connection

1.15 A secure and effectively managed Internet connection requires detailed planning prior to establishment. Planning includes the formulation of policies; conducting a risk assessment and analysis; and the design of control activities which, when implemented, will achieve an appropriate level of security.

1.16 Most of the agencies audited were found not to have undertaken a comprehensive process of planning their Internet connections. In particular:

- security policies and supporting procedures (eg Internet Security Plans) to define standards for secure Internet usage had not been developed. These included agencies with long established Internet connections *(refer paragraphs 2.5 to 2.7)*; and
- a risk assessment and analysis had not been completed prior to connecting to the Internet. As a result, risk management and contingency plans had not been formulated *(refer paragraphs 2.8 to 2.11)*.

Securing an Internet Connection

1.17 As a consequence of the above lack of planning, few agencies were found to have selected and implemented controls commensurate with the risks associated with their Internet connection. In particular :

- the configuration, operation and management of 'firewalls' could be improved (*refer paragraphs 2.21 to 2.27*);
- while most agencies had adequate security logging capabilities, only some undertook regular monitoring and analysis of these logs or used specialised tools or software for the security

audit function *(refer paragraphs 2.29 to 2.31);*

- the overall incident response capability could be improved *(refer paragraphs 2.34 to 2.36)*; and
- several agencies did not have adequate policies covering virus prevention and did not have tools or software installed on their 'firewalls' for the detection of viruses (*refer paragraphs 2.38 to 2.40*);

1.18 To some extent these findings arise because, at the time of the initial connection, the risks were minimal and it is not surprising therefore that controls were not fully considered. Now that the risks associated with Internet usage have increased, agencies need to reconsider their control frameworks.

1.19 On the positive side the audit found most agencies had some of the core elements for effective Internet site management in place. In particular:

- physical security over Internet facilities was generally good—access was controlled at all times, equipment and other items were located in secure areas, and the removal of equipment and other items was recorded and tracked; and
- all agencies had technically skilled staff who had an awareness of the need for security and its requirements.

Summary of Key Recommendations

1.20 The ANAO considers that more effective Internet security can be achieved by most agencies. The key recommendations contained in this report focus on:

- careful planning of the connection to the Internet and the establishment of Internet facilities (eg e-mail, web page browsers, file transfer, and secure dial-up). The fundamentals of this approach apply equally to those agencies with existing connections;
- documentation of all policies, plans and procedures necessary for the secure operation and management of an Internet facility;
- fully utilising suitable available hardware, software and other security tools; and
- ensuring management and staff remain vigilant and are kept aware of all relevant security issues.

1.21 The ANAO made a number of detailed, specific recommendations to those agencies included in the audit. In accordance with the FCA Charter these recommendations and agency responses have been reported to each relevant Minister.

1.22 The table at the end of this Part summarises the recommendations contained in Part 2 of this Report. These recommendations are considered to have relevance to all Commonwealth agencies with, or contemplating, an Internet connection. They are framed against the key findings summarised above.

Future Directions

1.23 Currently, a number of agencies are planning to provide services or make payments via the Internet in their move to electronic commerce. These proposed activities will increase the risk of unauthorised access, sabotage or fraud.

1.24 Agencies will need to consider further security measures such as encryption or authentication procedures to mitigate these increased risks, although this will depend in part on future government action.

1.25 Agencies should work with security authorities such as Defence Signals Directorate (DSD) to ensure that adequate encryption and authentication procedures are implemented. The development of common encryption and authentication procedures across the Commonwealth public sector may be a possible approach to this issue. This may need to be considered in a whole of government approach by the Office of Government Information Technology (OGIT).

1.26 The provision of services and payments over the Internet will also expose agencies to a number of legal issues such as:[3]

- which legal jurisdiction applies to Internet transactions given that the Internet is a global electronic environment that makes geographic locations irrelevant;
- what documentation is required to support transactions given the electronic nature of the Internet;
- how to prove who the counterparty to a transaction is and ensure they cannot repudiate acceptance at a later date;
- when is a contract formed between supplier and customer in Internet transactions; and
- what is the legal status of information held on web pages.

1.27 Agencies must ensure that they fully consider and address legal issues before they implement commercial services on the Internet.

Recommendations

Planning an Internet Connection

Recommendation No. 1
Para. 2.15

It is recommended those Commonwealth agencies considering an Internet connection and the provision of Internet facilities, and those agencies with a connection

[3] Arthur Robinson & Hedderwicks, *Doing Business On The Internet* by Michael Pattison, August 1996

who have not already done so, should:

- develop and distribute an Internet Security policy covering the use of the Internet connection. This policy should define the level of protection for the agency's computerised data, computer programs and Internet facilities;
- undertake a Risk Review and Analysis and document risks identified in a Risk Management Plan or equivalent document; and
- adequately document the security controls and other measures designed to mitigate the risks that arise through connection to, and use of, the Internet (including a usage and publishing policy).

Securing an Internet Connection

Recommendation No. 2
Para. 2.28

It is recommended those agencies that use a firewall to assist in securing their Internet facilities:

- obtain accreditation by an independent agent if not already done (subject to risk assessment and cost-effectiveness considerations);
- restrict access to firewall settings to a minimum number of authorised users; and
- log and review all configuration changes to the firewall, the review to be undertaken by an independent person.

Recommendation No. 3
Para. 2.32

It is recommended agencies should, as their circumstances dictate, further develop their security audit function to focus on the logging of significant transactions, using specialised tools where appropriate.

Recommendation No. 4
Para. 2.33

It is further recommended that the security audit function include ensuring the security monitoring and log analysis are performed on a regular basis and that executive management is made aware of the results, at least on an 'exception' basis.

Recommendation No. 5
Para. 2.37

It is recommended that an effective incident response capability, including a forensic plan which preserves evidence for legal purposes, be established by agencies that have not already done so. This capability should be documented as Contingency and/or Incident Response Plans, tested and evaluated.

Recommendation No. 6
Para. 2.41

It is recommended that agencies develop a Virus Prevention Plan that consists of a collection of policies and/or procedures to address virus threats. This plan should be tested and evaluated to ensure that it will operate effectively.

Recommendation No. 7

Para. 2.42

It is further recommended that agencies install proven virus detection software on their firewalls and network servers.

Part Two

Detailed Findings and Recommendations

Detailed Findings and Recommendations

Introduction

2.1 The following discussion considers the audit findings in depth. A better practice 'model' (see Appendix 1), developed as part of the audit, was the benchmark of Internet site security management against which the findings were framed.

2.2 The major findings of this audit relate to issues dealing with planning for an Internet connection and the requirements for securing such a connection.

Planning an Internet Connection

2.3 A secure and effectively managed connection to the Internet requires detailed planning, prior to establishment, to ensure that risks (such as those noted in the Background comments in Part 1) are adequately addressed.

2.4 The results of this audit confirmed those agencies that carefully planned their connection to the Internet went on to establish better managed and more secure Internet facilities.

Formulation of Policies

2.5 An Internet Security Policy is the foundation on which an effective control framework for the development, implementation and management of a secure Internet connection is based. It is important that a specific Internet security policy be developed to ensure uniform procedures and that use of the Internet is consistent with an agency's overall policies and standards.

2.6 This audit found that most agencies, including some with long established Internet connections, had not developed an Internet Security Policy nor supporting policies.

2.7 For those agencies that did not have an Internet security policy in place, formal procedures over the use of the Internet had developed on an ad-hoc basis and, in some areas, did not exist at all.

Risk Review and Analysis

2.8 Another key element of an effective security control framework is a formal risk review and analysis. This process enables the agency to establish:

the value of its ‘information resources’[4]

- the probable threats to those resources; and the vulnerability of its processing systems to such threats.

2.9 Based on its risk analysis an agency should be able to design adequate security control measures that will reduce risks to an acceptable level, in a manner that balances competing objectives, such as, security, cost-effectiveness, user needs and productivity.

2.10 One output of this process is an ‘IT Risk Management Plan’ that will document, amongst other things, what risks must be minimised and to what degree; and what risks are acceptable. This should be an integral part of overall risk management planning.

2.11 The audit found that few agencies had undertaken the Risk Review and Analysis process. Without undertaking this process, an agency is not in a position to decide the level of risk that is acceptable and therefore cannot be confident that the security measures in place over the Internet connection will be sufficient to cover actual risks nor their implications for the agency’s programs and activities.

Design and Documentation of Plans and Procedures

2.12 The security control measures selected by an agency and the plans and procedures developed to counteract risks should be documented to provide a reference for their implementation, for staff information and for any future review. A separate ‘Internet Security Plan’ is one approach to documentation—it defines the sum of all logical, physical and management controls that ensure the secure operation of the Internet facilities and protection of the agency’s information resources.

2.13 Few agencies had developed Internet Security Plans or equivalent documentation. This was a further indication that most agencies had not selected and implemented suitable controls according to the assessed risks associated with an agency’s Internet connection.

2.14 The lack of rigor in planning and documentation is likely to have resulted in certain risks not being adequately addressed by appropriate controls and security measures. For example, some agencies who did not have these plans in place were also found to lack comprehensive facilities for logging and examining suspicious activity and traffic across the Internet connection. In addition most agencies did not undertake regular independent reviews of these logs.

[4] In this context ‘information resources’ means not only information in electronic form but also the hardware and software of the agency’s systems and networks and the documentation supporting them.

Recommendations

2.15 It is **recommended** those Commonwealth agencies considering an Internet connection and the provision of Internet facilities, and those agencies with a connection who have not already done so, should:

- develop and distribute an Internet Security policy covering the use of the Internet connection. This policy should define the level of protection for the agency's computerised data, computer programs and Internet facilities;
- undertake a Risk Review and Analysis and document risks identified in a Risk Management Plan or equivalent document; and
- adequately document the security controls and other measures designed to mitigate the risks that arise through connection to, and use of, the Internet (including a usage and publishing policy).

Securing an Internet Connection

2.16 In securing an Internet connection agencies should employ a series of controls and security measures designed to protect against the risks associated with the Internet connection and services. A major source of risk is associated with the activities of outside 'intruders' or 'hackers'. Successful hacking attacks may not only compromise classified information, but may also result in lost productivity and damage or denial of access to data to users with possible significant implications for agency programs.

2.17 Another threat that should receive greater prominence where an Internet connection exists and is generally available to staff, is the unintentional introduction of viruses and other maleficent software. The Internet can be a major 'disease carrier' and an insecure Internet connection is the primary vehicle for transmission of such viruses and software into an agency. The costs of 'cure' can be significant.

2.18 The control measures put in place to address these threats and risks can be categorised as 'preventative' (that is, they stop the event occurring) and 'detective' (that is, those which detect and correct security breaches which arise from the Internet connection).

2.19 Many of these controls relate to the operation of an agency's systems and, to this extent, are not 'peculiar' or special to the Internet connection. These include controls, both physical and logical, over access to hardware, software and information. They also include controls over changes to system software and activity logging.

2.20 While such controls are characterised as General IT controls, they have the potential to take on more significance where an agency has established an Internet site. The creation of a gateway that allows outside access to an agency's systems and the existence of 'hackers' whose 'vocation' revolves around breaking into networks, places an increased premium on the effectiveness of an agency's General IT controls.

Firewalls

2.21 Firewalls are the primary mechanism for securing Internet connections. A firewall, for the purpose of this audit, is a specific mechanism(s) that controls access between two networks. It is basically a piece of computing hardware/ software.

2.22 Firewalls should be used by agencies who have, or are planning to have, the Internet connected to networks that are linked to their corporate and operational information systems.

2.23 Firewalls are not relevant to an Internet connection that operates on a separate computer or network dedicated for Internet use only. Such 'stand-alone' systems should have no information on them that cannot be publicly released. It is, however, necessary that the information contained on "stand alone' systems should be protected from unauthorised changes. Physical separation is the alternate protection.

2.24 The configuration, operation and management of the firewall are vital to ensure a secure Internet connection. This is a complex task with many considerations. However, the essence of an accurately configured, operated and managed firewall involves:

- accreditation or guidance by an independent agent such as Defence Signals Directorate (this is mandatory for some agencies; for others this will depend on an independent risk assessment of the site);
- access to the firewall being restricted to a minimum number, ideally two, authorised staff (more may be needed for larger sites); and
- changes to the firewall configuration being logged and reviewed by an independent person.

2.25 The audit noted most agencies could improve the configuration, operation and management of their firewalls. Specifically, the firewalls of several agencies had not been accredited by an independent agent and the logs of changes to the firewall configuration were not being reviewed regularly in many of them.

2.26 Accreditation provides an agency with a degree of certainty that the firewall used to control access between the agency's internal network and the Internet is sufficient to address the associated risks. Accreditation is needed for agencies that intend to use the Internet for commercial and financial purposes or hold information that is of a sensitive or private nature. Other agencies with Internet sites of a low risk nature may not require accreditation if the costs are considered to exceed the benefits of doing so. However, agencies should be careful not to define such costs and benefits too narrowly at the possible expense of their programs and public creditability and confidence.

2.27 Failure to regularly review the log of changes to the firewall configuration may compromise the security measures implemented. In addition, providing access to a large number of staff to the firewall settings could result in unauthorised changes being made to the firewall settings that may also compromise the security measures implemented. Such changes may not be detected until some time after the event. Robust corporate-based controls are essential to protect corporate data bases from such changes.

Recommendations

2.28 It is **recommended** those agencies that use a firewall to assist in securing their Internet facilities:

- obtain accreditation by an independent agent (subject to broadly- based risk assessment and cost-effectiveness considerations);
- restrict access to firewall settings to a minimum number of authorised users; and
- log and review all configuration changes to the firewall, the review to be undertaken by an independent person.

Security Audit

2.29 Security audit refers to the function of monitoring compliance with the agency's Internet security policies and operational procedures, and reviewing the mechanisms adopted to enforce those policies. It is a complex task, that needs to be performed by independent and technically skilled staff. It should consist of the following elements to be efficient and effective:

- the use of logs to record significant transactions (these can be used to identify events requiring confirmation, suspicious activity or incidents that may have occurred);
- the use of specialised tools to assist in log analysis, automatically notifying administrators when suspicious activity or incidents may be occurring and authenticating the configuration of the site;
- protection of the log data and specialised tools; and
- management of the security audit function, including ensuring log analysis is performed regularly and management made aware of the results, support staff have the appropriate technical skills, and the monitoring schedule is varied.

2.30 The audit found that although most agencies had adequate security logging capabilities, only some agencies undertook regular monitoring and analysis of these logs or used specialised tools or software to support the security audit function.

2.31 If regular monitoring and analysis are not undertaken, any unauthorised or suspicious activity originating from the Internet connection may not be detected. Successful hacker attempts may have been undertaken into these agency networks but, as the hacker did not change any data or programs, they have not been detected. In addition, by not using log analysis tools the review of logs could become time consuming and tedious. This increases the risk of incidents not being detected by the reviewer.

Recommendation

2.32 It is recommended agencies should as their circumstances dictate further develop their security audit function to focus on the logging of significant transactions, using specialised tools where appropriate.

2.33 It is further recommended that the security audit function include ensuring that security monitoring and log analysis are performed on a regular basis and that executive management is made aware of the results at least on an 'exception' basis.

Incident Response Capability

2.34 An incident response capability refers to the ability of an agency to detect, identify and respond to any suspected breach of the agency's Internet security. Until an incident has occurred and been detected, it is difficult to assess this capability. An adequate incident response capability will possess the following elements:

- a Contingency and/or Incident Response Plan that has been tested and evaluated;
- an Incident Response Team and/or arrangements with specialist response teams such as the Australian Computer Emergency Response Team (AUSCERT) or Defence Signals Directorate (DSD); and
- measures for the detection of incidents, concentrating on the security audit function.

2.35 The audit found there were many agencies whose incident response capability could be improved. Some agencies did not have Contingency and/or Incident Response Plans in place, including the identification of Incidence Response Teams.

2.36 Those agencies that did not have Contingency and/or Incident Response Plans in place or whose plans required significant improvement may not be able to recover quickly from any disaster including hacker, virus or sabotage attack. It may also be difficult to trace, identify and re-establish the integrity of key data and systems. It is simply a matter of good risk management and the determination of the 'cost of insurance'.

Recommendation

2.37 It is **recommended** that an effective incident response capability, including a forensic plan which preserves evidence for legal purposes, be established by agencies. This capability should be documented as Contingency and/or Incident Response Plans, that are periodically tested and evaluated.

Virus Prevention Capability

2.38 Viruses are programs that alter the way a computer works without the permission or knowledge of the user. A virus prevention capability refers to the ability of an agency to prevent, detect and recover from infection by computer viruses. While the principles are similar to incident response, there are factors unique to virus prevention that must be addressed.

2.39 Viruses are prevalent on the Internet and habitually 'infect' the networks and computers of agencies. To counteract this threat, an agency must have an adequate virus prevention capability in place with the following elements:

- a Virus Prevention Plan that has been tested and evaluated which specifies the agency's objectives, procedures, requirements and designated staff with responsibility to investigate any detected incident;
- education of staff concerning the threats and risks of viruses;
- tools for the detection of, and recovery from viruses; and
- an Information and Back-up Recovery Strategy that ensures backup copies of critical programs and data are securely held and known to be free from viruses.

2.40 The audit found that agencies generally had satisfactory virus prevention capabilities in place. However, several agencies did not have policies covering virus prevention and did not have tools for the detection of viruses installed on their firewalls or network servers.

Recommendation

2.41 It is **recommended** that agencies develop a Virus Prevention Plan that consists of a collection of policies and/or procedures to address virus threats. This plan should be periodically tested and evaluated to ensure that it will operate effectively.

2.42 It is further recommended that agencies install proven virus detection software on their firewalls and network servers.

P. J. Barrett

Auditor-General
Canberra ACT

Part Three

Appendices

Appendix 1

Internet Security Principles

The objective of Internet security risk management is to protect agency assets from risks associated with connecting to the Internet by implementing a control framework.

Effective Internet security risk management requires:

- identifying the type and likelihood of risks;
- identifying the value and nature of agency assets to be protected;
- planning an appropriate control framework; and
- implementing the planned control framework.

Identifying Internet Risks

Any agency using the Internet will be subject to risks which will vary depending on the circumstances associated with an agency's site.

Risk	Description	Factors Increasing Risk
Hackers	Outside users ('hackers') using Internet access to gain unauthorised access to agency data or functions held on internal agency networks.	Profile of the agency. Connection between the Internet server and internal agency networks. Attractiveness of information or services.
Viruses	Viruses being imported from the Internet to the internal agency network	Connection between the Internet server and internal agency networks. Poor staff awareness of virus risk.
Sabotage	Disruption or sabotage of agency information technology services.	Profile of the agency. Connection between the Internet server and internal agency networks.
Information Disclosure	Unauthorised interception of confidential or sensitive material transmitted over the Internet	Poor staff awareness of Internet risks. Use of Internet for Email.
Legal Uncertainty	Lack of legal certainty over commercial transactions performed on the Internet due to different legal interpretation, jurisdictions and enforcement ability.	Provision of services or receipt of payments via the Internet.
Public Embarrassment	Loss of reputation due to security related incidents becoming publicly known.	Profile of the agency

Effective Internet risk management requires an accurate assessment of the nature and likelihood of risks affecting an agency's Internet site.

Identifying Assets At Risk

Agencies must identify the value and nature of assets at risk by the Internet connection. Different assets will primarily be affected by different risk types.

Asset	**Description**	**Main Risks**
Information	Information held by an agency such as data on clients and suppliers or research performed	Hackers Information Disclosure Public Embarrassment
Public Image	The reputation of an agency in the mind of the public especially for being soundly controlled and able to protect sensitive information.	Public Embarrassment Information Disclosure Sabotage
Service Delivery	The ability of an agency to deliver its services to its clients especially those dependent on information technology.	Sabotage Viruses
Financial Assets	The monetary assets of the agency such as cash and liabilities.	Hackers Legal Uncertainty

Agencies must decide what level of risk to their assets they are willing to accept as part of their risk management approach.

Planning for connecting to the Internet

A secure and effectively managed connection to the Internet requires careful planning prior to establishment. This planning process will involve developing:

- An *Internet Security Policy* which provides the foundation by which a framework for the development, implementation and management of a secure Internet connection can be achieved.
- A *Threat and Risk Assessment* to identify the nature and extent of the threats and risks of the Internet.
- *Controls, Plans and Procedures* to counteract those risks identified in the *Threat Risk Assessment* in a manner that balances security, cost-effectiveness and user needs.

The risks and corresponding controls should be documented in a *Internet Site Security Plan.*

Implementing an Internet Control Framework

The *Control Framework* is the combination of policy, procedures, controls and security measures implemented by an agency to minimise the risks to its assets to an acceptable level. The *Control Framework* will involve:

- *Internet Site Management* to ensure the Internet site is configured and managed correctly with vulnerability assessments, accreditation, resourcing, training, policies, plans and procedures.
- *Firewalls* to control access between an agency's internal network and the Internet The *firewalls* need to be correctly configured and managed with access restricted and logged. Accreditation of firewalls by an independent agent may be required for higher risk sites.
- *Physical Security* of Internet facilities so that access is controlled at all times, equipment and other items are located in secure areas and removal of equipment and other items is controlled.
- *Access Security* to ensure that information resources are only available to authorised users.
- Internet *Change Control* procedures overseen by a change control committee which address the procedures for the application and implementation of all changes to the Internet configuration.
- *Education and Training* of staff using and operating the Internet facilities including the promotion of security policies.

- ***Security Audit*** by independent and technically skilled staff to monitor compliance with the agency’s Internet security policies and operational procedures.
- ***Incident Response Capability*** to detect, identify and respond to any suspected breach of the agency’s Internet Security. This should be documented, tested and evaluated.
- ***Virus Prevention Capability*** to prevent, detect and recover from infection by computer viruses by using detection and recovery tools and educating users of virus threats and risks.

With the use of the Internet continuing to evolve, the control frameworks that are satisfactory today may not be adequate in the future. As agencies expand their use of the Internet, they will need to constantly review the adequacy of security and controls to ensure that risks continue to be adequately addressed.

Appendix 2

Objectives, Scope and Focus of the Audit

Background

Commonwealth government agencies have been developing their Internet capabilities over a number of years. In line with the general community, Internet usage by the Commonwealth has, to date, been restricted to electronic mail and research. However, several agencies are currently planning to provide commercial services and payment facilities via the Internet.

Given the increased number of Internet users and current plans of many agencies to provide commercial services via the Internet, it was considered appropriate to review the effectiveness of Internet security management.

The Internet security management audit covered ten agencies, including government departments, departmental outriders and commercial and non commercial statutory authorities based in Canberra, Melbourne and Sydney. The audit team also undertook an extensive review of relevant literature.

Scope and focus

The audit of Internet security encompassed all forms of Commonwealth agency, with the exception of Government Business Enterprises and Departmental Commercial Undertakings. A number of agencies were included to obtain a contrast of Internet usage.

The subject of the audit was the security management of Internet connections within Commonwealth agencies. Connections via stand-alone personal computers and connections to internal agency networks were included in the review.

The audit field work undertaken in agencies addressed the adequacy of planning, policies, management practices, access control and user education in relation to the Internet.

Objectives

The objectives of the audit were to:

- assess the effectiveness of Internet security measures within the Commonwealth public sector; and
- identify, develop and report current better practice in Internet security management for use across the public sector.

The first objective is addressed in this report by expression of an overall opinion which is supported by detailed conclusions, findings and recommendations in Chapter 1.

The second objective is addressed through the preparation of a Better Practice Guide issued separately but in conjunction with this report. The Better Practice Guide is based on a set of Internet security management principles (Appendix 1) which provide the criteria against which achievement of the above objectives were measured and upon which the audit opinion is based.

Audit Methodology

The audit was undertaken in accordance with ANAO Auditing Standards which are consistent with Australian Auditing Standards.

Audit evidence was obtained primarily by means of discussion with staff of the agencies audited and inspection of policies and procedure manuals.

Findings and recommendations were reported to individual agencies for their review and comment. A report was provided to each Minister on the results of the audits on agencies within their portfolios.

Performance information

Arising from the audit, a total of 63 recommendations and findings were made and accepted in the individual reports to agencies. The ANAO was advised that appropriate corrective action would be taken where necessary.

The total cost of the audit including the report to Parliament of the 10 agencies was $139,000.

Series Titles

Titles published in the financial year 1997-98

Audit Report No.1
Audit Activity Report: Jan-Jun 1997
Summary of Audit Outcomes

Audit Report No.2 Performance Audit
Government Business Enterprise Monitoring Practices
Selected Agencies

Audit Report No.3 Performance Audit
Program Evaluation in the Australian Public Service

Audit Report No.4 Performance Audit
Service Delivery in Radio and Telecommunications
Australian Telecommunications Authority
and Spectrum Management Agency

Audit Report No.5 Performance Audit
Performance Management of Defence Inventory
Defence Quality Assurance (preliminary study)

Audit Report No.6 Performance Audit
Risk Management in Commercial Compliance
Australian Customs Service

Audit Report No.7 Followup Audit
Immigration Compliance Function
Department of Immigration and Ethnic Affairs

Audit Report No.8 Performance Audit
The Management of Occupational Stress in Commonwealth Employment

Audit Report No.9 Performance Audit
Management of Telecommunications Services
in Selected Agencies

Audit Report No.10 Performance Audit
Aspects of Corporate Governance
The Australian Tourist Commission

Audit Report No.11 Performance Audit
Austudy
Department of Employment,
Education and Youth Affairs

Audit Report No.12 Performance Audit
Pharmaceutical Benefits Scheme
Department of Health and Family Services

Audit Report No.13 Performance Audit
Third Tranche Sale of the
Commonwealth Bank of Australia