2002

Report of the

Auditor General of Canada

to the House of Commons

APRIL

Chapter 3
Information Technology Security

The April 2002 Report of the Auditor General of Canada comprises eight chapters, a Foreword and Main Points. The main table of contents is found at the end of this publication.

The Report is available on our Web site at www.oag-bvg.gc.ca.

For copies of the Report or other Office of the Auditor General publications, contact

Office of the Auditor General of Canada
240 Sparks Street, Stop 10-1
Ottawa, Ontario
K1A 0G6

Telephone: (613) 952-0213, ext. 5000, or 1-888-761-5953
Fax: (613) 954-0696
E-mail: distribution@oag-bvg.gc.ca

Ce document est également disponible en français.

Cat. No. FA1-2002/1-3E
ISBN 0-662-31961-3

Chapter

3

Information Technology Security

The audit work reported in this chapter was conducted in accordance with the legislative mandate, policies, and practices of the Office of the Auditor General of Canada. These policies and practices embrace the standards recommended by the Canadian Institute of Chartered Accountants.

Table of Contents

Information Technology Security

Main Points

3.1 The revised Government Security Policy came into effect in February 2002, replacing the 1994 policy. It has a strong focus on information technology (IT) security and is an important step toward improving the governance of security across government.

3.2 We found that the IT security standards that support the Government Security Policy are out-of-date and a plan to update them has yet to be completed. The security policy will not be fully effective without updated standards, setting out the minimum requirements that departments and agencies must meet. The standards are an essential tool for supporting appropriate IT security practices across government.

3.3 Moreover, there was little monitoring of the 1994 policy. As a result, the government does not have enough information to assess the overall state of IT security. It does not have an adequate basis for determining whether current practices across government are acceptable, nor does it have an appropriate baseline for measuring future progress. Furthermore, the revised policy calls for a report on its effectiveness but not before summer 2004. In our view, a report is needed sooner.

3.4 The government has made a commitment to connect Canadians and provide them with on-line access to services. The Government On-Line initiative was launched to accomplish these goals. Security and privacy concerns have been identified as a key issue in this initiative. It is important that the government promptly address those concerns in order to support Government On-Line.

Background and other observations

3.5 Cyber threats are real and can do significant damage. Recent attacks using viruses and other types of malicious code have raised the profile of IT security. With the heightened awareness of national security, IT security is widely seen as essential to protecting our critical infrastructure.

3.6 Our audit of four departments found a number of weaknesses that could provide some insight into the state of IT security across government. They could help the government set priorities for the operational and technical standards it develops to support the revised Government Security Policy.

3.7 Although the departments have established a governance framework, they need to implement it better to make it fully effective. This is especially true in departments where responsibilities for information systems are decentralized and in departments with strategic partnerships and/or outsourcing relationships with other government organizations. Other improvements needed to address some weaknesses we identified include the following:

- conducting broad-based risk assessments and providing employees with adequate training in information security awareness;
- ensuring that IT security is considered at the start of a system development life cycle and that ongoing monitoring is carried out with appropriate scope; and
- carrying out audits and independent reviews periodically, including technical testing for potential vulnerabilities in network systems.

The government has responded. The Treasury Board Secretariat, on behalf of the government, has generally agreed with the recommendations. The government's responses, including the action that it is taking or intends to take to address the recommendations, are set out in the chapter.

Introduction

Cyber threats and their potential consequences

3.8 Most large organizations and governments depend on information systems to carry out business functions or deliver government services. With use of the Internet increasing worldwide, many governments are moving to deliver services on-line.

3.9 In Canada, government systems are increasingly interconnected, creating new opportunities for collaboration but also new risks to information assets. Information assets include computers, software, network and telecommunications equipment and, more important, data in electronic format.

3.10 Cyber incidents can do significant damage to an organization. They can impair information assets and disrupt business operations. Some incidents result in lost productivity; others can lead to loss of consumer confidence, a tarnished reputation and loss of credibility, or outright fraud.

3.11 Information technology (IT) security measures are necessary to minimize the risks. In addition to safeguarding information assets, IT security is aimed at maintaining the confidentiality, integrity, and availability of information—important objectives in government operations. Most government departments and agencies have sensitive information that requires restrictions on access, and privacy requirements that they have to meet. Data integrity is critical to ensuring that program administration and delivery are based on proper information. Information systems are a part of the government's critical infrastructure; its reliance on them will increase as it provides on-line access to more services. Keeping information systems available is now essential for uninterrupted service to the public.

Cyber incidents are real and on the rise

3.12 Computer viruses and other malicious codes have caught the recent attention of the media and the public. In February 2000, successful cyber attacks were launched against a number of high-profile commercial Web sites such as Yahoo! and Amazon.com. Those responsible attacked the information systems of many organizations worldwide, and used those systems to simultaneously attack and disable the targeted Web sites.

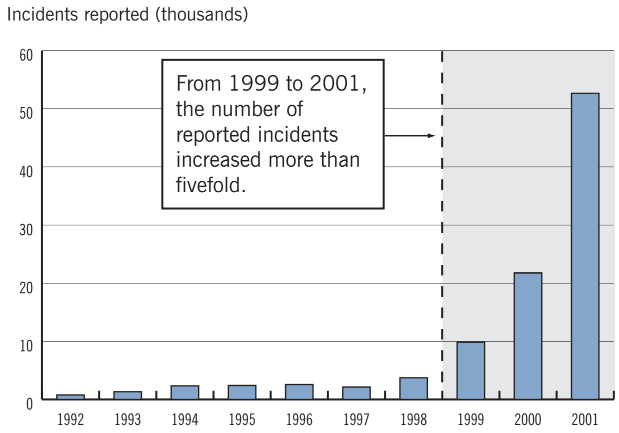
3.13 Many other viruses and attacks have been reported since then, from the "I love you" virus in May 2000 to the "Code Red" and "Nimda" attacks in 2001. Unsuspecting victims had to open attachments to electronic mail for some of those attacks to work, but other attacks were more insidious and required only that a victim view the mail message.

3.14 The costs to the victims of these attacks can be high. For example, repairs and lost productivity associated with the "I love you" virus alone cost an estimated US$ 8.7 billion. And the value of any lost information may never be determined.

3.15 The IT security community knows that readily available and easy-to-use software tools can be used to perpetrate attacks. Hackers take pride in using them to break into information systems and/or disable them.

3.16 The data on reported cyber incidents show the extent of the threat. Data from the United States show a dramatic rise in reported incidents, particularly in recent years. As Exhibit 3.1 illustrates, from 1999 to 2001 the number of reported incidents in that country increased more than fivefold, from about 10,000 to about 52,700.

Exhibit 3.1 Rise in reported cyber incidents in the U.S.



Note: The Centre tabulates the number of cyber incidents detected and reported by third parties.

Source: CERT Coordination Center (U.S.)

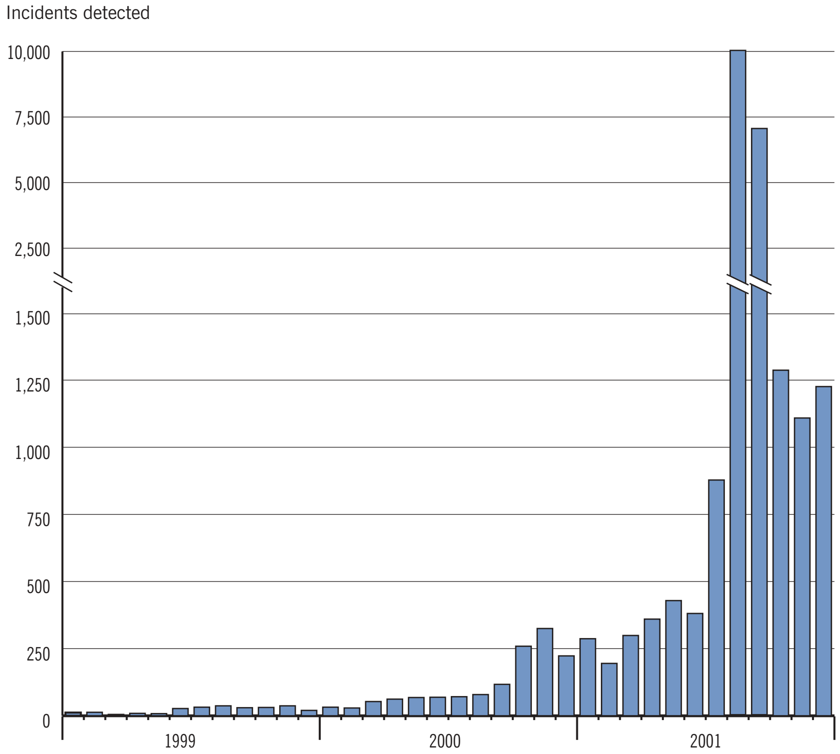
Point of presence on the Internet—A facility or device that allows Internet access to an organization's network systems.

3.17 Canada's federal government began a project in summer 1999 to assess the level of cyber threat to its Internet presence. A single point of presence on the Internet for each of six departments was observed for up to three months and unusual network traffic noted and analyzed. The test generated over 80,000 alarms. Further analysis of those alarms showed more than 500 attempts to penetrate departmental systems. Most of those attempts involved probes by potential attackers, many of them using automated tools.

3.18 Although there are no other data specifically on government systems, the rising Canadian trend in the number of cyber incidents (Exhibit 3.2) parallels the U.S. trend. Data from CanCERT, a service that tracks and reports cyber incidents in Canada, show 10,000 incidents in August 2001 and 7,000 in September 2001, overwhelmingly dominating the entire year's statistics (Exhibit 3.3). With the heightened awareness of national security, law enforcement agencies and the public have given cyber alerts and IT security concerns a much higher profile.

3.19 Media reports on cyber attacks and the dramatic increase in reported cyber incidents show that cyber threats represent a real and growing danger and can have a significant impact on an organization. Moreover, as information systems form part of our critical infrastructure, cyber attacks form part of a terrorist threat to our national security. This makes IT security an important management priority and responsibility.

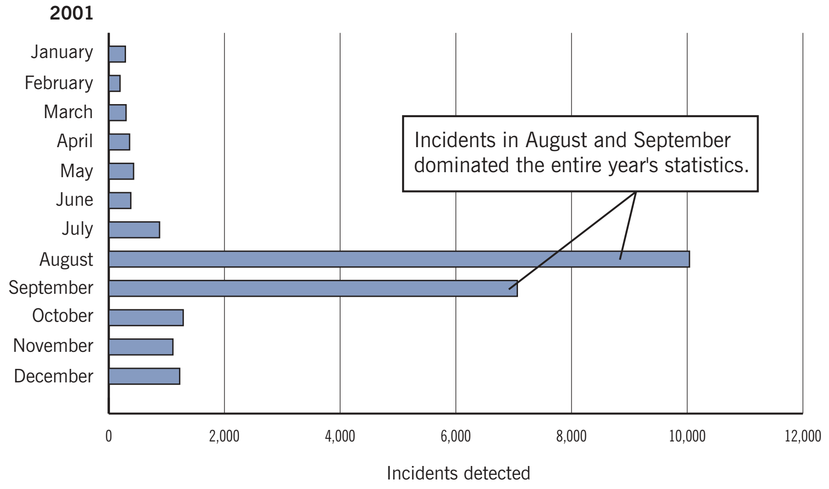
Exhibit 3.2 Canadian cyber incidents, 1999–2001



Note: In Canada, CanCERT tracks cyber incidents and tabulates the number of incidents that it has detected.

Source: CanCERT

Exhibit 3.3 Canadian cyber incidents in 2001



Source: CanCERT

Focus of the audit

3.20 The objective of our audit was to assess the framework for information technology security that the government has in place to protect its information assets and provide for secure, uninterrupted delivery of electronic services to Canadians. We examined the government-wide IT security framework and reviewed the IT security practices of four departments or agencies. The selected departments were not intended to be a representative sample but to provide an insight into government IT security practices.

3.21 We interviewed staff from agencies that have a lead role in IT security across government and examined related documents and files. In the four departments, we met staff who have security and/or IT responsibilities. We also conducted remote technical tests of networks in some departments.

3.22 Further information about the audit objective, scope, approach, and criteria can be found at the end of the chapter in About the Audit.

Observations and Recommendations

Government-wide framework

3.23 Like other important issues that affect all departments and agencies, IT security requires a good governance framework, one that defines leadership responsibilities, articulates the roles of various lead agencies and each department, and sets out accountability relationships. The Government Security Policy provides the governance framework for all aspects of security, including IT security. The Treasury Board Secretariat is responsible for the policy, and its provisions apply to all departments and agencies.

3.24 The Government Security Policy and its directives have three levels. At the top is the overall security policy that sets out the requirements for protection of government assets and personnel and the roles and responsibilities of lead agencies. The second level sets out the operational security standards and practices, and the third level the technical security standards and practices.

Comprehensive update of the Government Security Policy

3.25 The first version of the Government Security Policy (GSP) came into effect in 1986 and was revised in 1994. Information technology has advanced rapidly since 1994. The use of the Internet and various on-line applications in Canada has grown significantly. To meet its commitment to become the government most connected with its citizens, the federal government launched its Government On-Line initiative to make its services accessible on the Internet. Along with those developments came new risks and challenges to security. Moreover, the government began in the late 1990s to define Canada's critical infrastructure. The 1994 revision of the GSP did not contemplate all of those IT security issues.

Government On-Line—A Government of Canada initiative to use the Internet to provide on-line services to Canadians.

3.26 The Treasury Board Secretariat recognized that the policy did not adequately cover current issues of information technology and critical infrastructure. In April 2000 it began a comprehensive review to revise the policy in four phases. Phase 1 would identify deficiencies in the current policy. Phase 2 would develop recommendations on the scope of the revision to correct the deficiencies and would make the recommended changes. Phase 3 would present a submission to the Treasury Board for its approval of the revised policy. Finally, phase 4 would communicate and implement the revised policy and the related standards.

3.27 After surveying departments and agencies, the Secretariat finished identifying the 1994 policy's deficiencies in June 2000. In phase 2, it involved over 100 participants from across government, who served on working groups and committees. By November 2000, they had recommended that the revised security policy address the following:

- government-wide IT security requirements to protect interconnected systems and enable secure Internet delivery of services to Canadians;
- availability and integrity of information and IT systems;
- a clear governance framework with improved policy monitoring and more oversight by senior management; and
- improved security screening and protection of personnel against threats and acts of violence.

Drafts of the policy were circulated to departments and agencies, and the consultation process was completed in October 2001. The Treasury Board endorsed the revised policy and approved it on 6 December 2001. The revised Government Security Policy came into effect on 1 February 2002.

Revised security policy defined the governance framework for information technology security across government

3.28 The main policy document of the 1994 policy had made very few specific references to IT security. In particular, it did not define the governance framework for IT security across government. Although deputy heads were responsible for protecting their departments' employees and assets, accountability for IT security government-wide was limited. The 2000 review of the Government Security Policy identified this weakness and recommended that it be corrected during the revision.

3.29 The 2002 policy still makes deputy heads accountable for implementing it as well as for protecting the employees and safeguarding the assets under their responsibility. We noted that the Treasury Board Secretariat has a defined leadership role in matters of government-wide IT security. Among others, it is responsible for developing and updating the security policy; providing strategic direction, leadership, and advice; and monitoring and reporting to the Treasury Board on policy implementation and the state of security in the government.

3.30 Secretariat staff indicated that they plan to use the structure of working groups and committees that developed the 2002 policy to develop guidance and advice on IT security matters. The proposed structure includes a security policy advisory committee, a security policy co-ordinating committee, and several security working groups.

3.31 The revised Government Security Policy updated the roles and responsibilities of 10 departments that act as lead security agencies. In addition to the three lead agencies we interviewed—the Royal Canadian Mounted Police, the Communications Security Establishment, and the Office of Critical Infrastructure Protection and Emergency Preparedness—the 10 include notably the Canadian Security Intelligence Service, National Defence, and the Department of Foreign Affairs and International Trade.

3.32 The governance framework for IT security defined in the revised policy fills a significant gap that existed in the 1994 policy. It articulates the leadership and support required to implement and maintain effective IT security practices in government. Moreover, it specifically considers the importance of IT security to government security overall. Among the objectives for IT security is the protection of the confidentiality, integrity, and availability of information assets, all aspects that are important to the government's operations. The governance framework defined in the 2002 Government Security Policy is an important starting point, and met our expectations in providing for proper leadership and support of consistent, cost-effective IT security across government.

Update of information security technology standards and practices needs to be accelerated

3.33 We have noted three levels at which the Government Security Policy operates. The top level provides the overarching framework for security and is supported by the operational and technical standards of the two other levels. The policy statements refer to baseline security requirements that departments and agencies must meet, that is, the minimum standards. Under the revised policy, the Secretariat can approve updates to the operational standards without going to the Treasury Board for approval.

3.34 We would expect operational and technical standards and practices for IT security to be kept up-to-date and commensurate with current levels of risk and threats to IT security.

3.35 The existing operational standards for IT security were published in 1994 and were last updated in 1995. Those standards and practices do not specify requirements for security against the risks and threats introduced by growing interconnectedness and Internet use across the government. The Technical Security Standard for Information Technology, published by the Royal Canadian Mounted Police (RCMP) in 1997, serves at present as a set of third-level requirements of the Government Security Policy. Those standards were developed before the Government On-Line initiative and are not up-to-date.

3.36 The Treasury Board Secretariat is responsible for directing and co-ordinating the update of operational and technical standards for IT security. During the audit, we noted that it had started to address gaps in IT security standards and practices as the 1994 policy was being revised. But much of its effort then focussed on completing the top-level policy document, so work on the standards and practices remains at an early stage.

3.37 We asked to see the Secretariat's plans and timetable for updating the 1995 and 1997 standards. At the end of our audit, the plans and timetable have yet to be completed. The plans for communicating and implementing the 2002 Government Security Policy were still being developed as well.

3.38 Up-to-date operational and technical standards are essential to IT security in the government. They set out the baseline requirements and provide a basis for consistent IT security measures across government. In addition, they form the yardstick for the monitoring and oversight of security practices. We found that some elements of the 1995 operational standards are not fully consistent with the revised policy. The Treasury Board Secretariat advised us that it has focussed on a number of major projects to support the Government On-Line initiative. The projects provide a basis for developing certain security standards; on completion, those projects will also help provide a secure environment for delivering on-line services to Canadians.

3.39 Departments and agencies need to know the baseline requirements to determine the security measures they need and the resources it will take to implement them. The lack of up-to-date standards at the operational and technical levels will reduce the effectiveness of the 2002 Government Security Policy. It is important that they be updated on an accelerated basis.

3.40 **Recommendation.** The Treasury Board Secretariat should accelerate the development of baseline requirements for information technology security to support the 2002 Government Security Policy. It should consider prioritizing various security requirements and update the standards in order of their criticality.

Government's response. The Treasury Board Secretariat agrees that the development of IT security standards must be accelerated in support of the Government Security Policy, and undertakes to do so within available resources. The Secretariat is also of the view that much of the work undertaken over the past few years as part of the Government On-Line initiative—such as the development of the Public Key Infrastructure, the Federated Architecture Program, and the Secure Channel—in addition to the comprehensive review of IT security issues leading to the renewal of the Security Policy of the Government of Canada had to be completed before IT security standards could be developed to meet both government-wide and departmental business and security needs. This approach is consistent with commercial and public sector literature that recommends the use of enterprise-wide architecture plans in developing standards, network-wide requirements, and overall security policy.

Monitoring and oversight

3.41 During the audit, the 1994 Government Security Policy and the 1995 IT security operational standards were in force. The revised policy came into effect only in February 2002, after we had completed our audit. We audited against the monitoring requirements of the 1994 policy and reviewed the revised provisions for monitoring and oversight. In either case, we would expect that IT security practices would be monitored and assessed and corrective action taken as appropriate.

Monitoring and oversight across government have been lacking

3.42 Ongoing monitoring and periodic reporting provide management with information on the adequacy and appropriateness of measures to protect the security of IT systems and the information they contain.

3.43 The 1994 policy required departments and agencies to conduct internal audits of IT security at least once every five years. The 1995 operational standards for IT security supported that policy requirement. The scope of internal audit work was to include the effectiveness of IT security measures and compliance with the policy and its operational standards. Departments and agencies were required to submit their internal audit reports to the Treasury Board Secretariat.

3.44 We looked for internal audit reports on IT security submitted to the Secretariat in the last five years. Of some 90 departments and agencies subject to the Government Security Policy, only 10 had submitted reports. The majority of departments (almost 90 percent) had not complied with the policy requirement.

3.45 We found no evidence of any follow-up by the Secretariat to ensure that internal audits of IT security were carried out periodically. Nor did we see any indication that the Secretariat had reviewed and analyzed the findings of the 10 reports that were submitted to inform itself about the state of IT security in those departments and agencies.

3.46 The 1994 policy and the IT security standards also required that departments and agencies ask the RCMP for an independent review of their IT security practices at least once every five years. Further, RCMP reviews were to be conducted more often where information systems contained classified information and information designated as extremely sensitive.

3.47 We found that only 14 departments and agencies have had the RCMP review their IT security practices since 1996. About 85 percent of the departments that are subject to the policy failed to comply with this requirement.

3.48 The 1994 policy required that at the Treasury Board Secretariat's request, the RCMP submit a report to the Secretary of the Treasury Board on the state of IT security in government, based on its reviews. The last time the RCMP submitted such a report was in 1995; the Secretariat has not requested any reports since then.

3.49 The significance of these gaps goes beyond non-compliance with government policy. In the absence of departmental internal audit reports and RCMP annual reports, the government did not have the information it needed to assess the overall state of IT security. Without that information, it was not positioned for effective monitoring and oversight of IT security across departments.

Revised provisions do not require timely oversight

3.50 The 2002 Government Security Policy includes a number of changes in the requirements for monitoring and oversight. The Secretariat is now responsible for monitoring the implementation of the policy and the state of security in government, including IT security, and reporting to the Treasury Board.

3.51 The revised policy requires departments and agencies to actively monitor their security programs, conduct internal audits of them, and report the results to the Treasury Board Secretariat. However, the requirement for an internal audit at least once every five years has been removed. The policy is not clear on what constitutes "active monitoring." The operational standards have yet to be updated and no other guidance is provided.

3.52 The main policy document no longer makes the RCMP responsible for reviews of IT security in departments and agencies. As a preventive measure against security threats, departments are required to have an independent third party assess their security programs and practices periodically. Once again, there is no longer a requirement that stipulates the minimum frequency of such independent assessments.

3.53 Given the importance of IT security and the potential impact of threats to it, we would expect that oversight would be strengthened as the Government Security Policy was revised. However, this has not been the case.

3.54 Under the 1994 policy, a majority of departments and agencies did not comply with the requirement on the minimum frequency of internal audit and RCMP review of IT security. Now that the required frequency of audits and independent assessments is no longer stipulated, there is less assurance that IT security practices in departments and agencies will be monitored adequately.

3.55 Furthermore, many departments and agencies face the challenge of ensuring that their internal audit groups have the capacity and capability to comply with the recently adopted Policy on Internal Audit. In the past, the RCMP provided the IT security review service to departments and agencies at no charge except its overtime and travel costs. The third-party assessments of IT security will have to compete against other funding priorities of departments, as individual departments and agencies have received no new funding to implement the 2002 security policy.

3.56 As part of overall monitoring, the Secretariat is required to produce a midterm report to the Treasury Board on the effectiveness of the Government Security Policy. Because the policy just came into effect, no reporting is required before summer 2004.

3.57 In an enterprise as large and diverse as the Government of Canada, it is not unreasonable to update information on the state of IT security every 24 months. However, since the 1994 revision of the Government Security Policy, government-wide monitoring and oversight have been limited. As a result, there is little baseline information on the state of IT security across government.

3.58 Without adequate baseline information, it is hard to identify potential gaps in the security of IT infrastructure across the government. It is also difficult to determine whether IT security policy, standards, and guidance are sufficient and appropriate. Furthermore, appropriate baseline data will be essential to measure the progress of IT security practices in the government over time.

3.59 Senior management in government acknowledges the importance of IT security. Information systems and assets are an important part of our critical infrastructure. Further, IT security is a top issue in the Government On-Line initiative to connect Canadians and provide government services on-line. We are concerned that appropriate baseline information on the state of IT security across government will not be available or reported before 2004.

3.60 **Recommendation.** The government should collect and analyze information on information technology security in departments and agencies to assess the state of security across the government sooner than its security policy presently requires, in order to do the following:

- set priorities for developing standards and practice guidance;
- establish a baseline for determining required improvements and measuring future progress; and
- address key gaps soon enough to support the Government On-Line initiative.

The government should also consider defining in the Government Security Policy how frequently internal audits and independent assessments of IT security practices are to be conducted.

Government's response. The Treasury Board Secretariat (TBS) generally concurs with this recommendation. In the course of renewing the Government Security Policy, TBS has consulted widely and extensively with departments and agencies on departmental IT security capabilities and requirements and agrees that more systematic collection of information is desirable. In February 2001, the government established the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), which will provide a central capacity for "real time" monitoring and remediation strategies with respect to network and departmental IT security incidents. In addition, TBS is starting the development of new assessment tools for use by departments to continually assess and monitor their IT security posture and security management practices. TBS is of the view, however, that departments are in the best position to determine when and how frequently internal audits and independent assessments of their IT security posture are to be conducted, as is stated in the renewed Government Security Policy.

Government-wide support

Revised security policy addressed gaps and overlaps in support roles

3.61 As part of the governance framework, the 2002 Government Security Policy states the responsibilities of 10 departments and agencies that act as lead security agencies.

3.62 The policy assigns the same responsibilities to a number of the lead departments and agencies that all along have provided support for IT security. For example, the RCMP is still responsible for providing advice on how to conduct reviews, inspections, and audits of IT security.

Threat and risk assessment—A process that allows an organization to evaluate the value of an application and its inherent security risks.

3.63 The 2002 Government Security Policy addressed duplications that existed in the 1994 policy. Under the revised policy, the RCMP is the only agency responsible for providing advice on the process of conducting threat and risk assessments. Roles in training and awareness have also been clarified. The RCMP develops and provides IT security training and awareness for systems users and technical support staff as well as for IT security officers. The Communications Security Establishment is responsible for specialized and technical training in areas such as communications security, network vulnerability, and other technical safeguards. Moreover, the revised policy clarifies the respective responsibilities of several lead agencies in representing the federal government on national and international committees involved in security.

Business continuity plan—A plan for resuming essential business activities following the loss or serious deterioration of an organization's facilities or work conditions.

3.64 The policy sets out new responsibilities for support as well. For example, the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) is assigned to be the centre for reporting by departments on real or imminent cyber threats and for issuing alerts and advisories to departments and agencies. Among other support roles, the OCIPEP provides advice on developing and maintaining business continuity plans.

Some support roles need more time to become fully effective

3.65 Many support roles defined under the revised policy have existed for some time. In those cases, the lead agencies already have the capabilities and are in a position to provide the support. Typical examples include

- the Communications Security Establishment, which evaluates cryptography products and certifies private sector testing and evaluation facilities,
- the Canadian Security Intelligence Service, which investigates and analyzes threats to national security, and
- the RCMP, which develops IT security technologies and countermeasures against cyber crime.

3.66 Responsibilities for some support roles have been assigned only recently. For example, OCIPEP is a new agency formed in February 2001 to develop and implement a comprehensive approach to protecting Canada's critical infrastructure. It carries out several new, essential functions that support IT security in government. In addition to those already described, it is to help departments and agencies assess vulnerabilities in their computer networks and to offer advice on protecting information systems and infrastructures critical to government operations. As a new organization, it has defined and obtained the resources it needs to discharge its mandate, but it will need time before it can support others fully as a lead security agency. In addition to recruiting specialized staff, much of its support role depends on effective co-ordination and co-operation with departments and agencies, which will take time to develop.

3.67 Sharing good practices helps departments and agencies learn of security solutions in other departments and gives them the benefit of experience with those solutions. The government has a number of forums for sharing information on IT security, and sometimes the participants share practices and solutions in those forums. Nevertheless, the revised policy has not defined a support role for capturing good IT security practices and sharing and promoting them across government.

3.68 The 2002 Government Security Policy does not stipulate that the support function will be assessed. In our view, it is worthwhile to review the adequacy of the support provided by the lead security agencies so the government can target additional efforts and investments where needed to improve support to departments and agencies.

3.69 **Recommendation.** The government should plan to review the adequacy of the support that the lead security agencies provide for IT security in order to improve that support where necessary. In addition, the government should explore and define ways to capture and share good IT security practices among departments and agencies.

Government's response. The 10 December 2001 Budget provided significant investments in the lead security agencies for a wide range of security-related initiatives, including IT security; for its part, the Government Security Policy clarifies their roles and responsibilities. The government recognizes the need to explore and define ways in which IT security best practices can most effectively be identified and disseminated to departments and agencies. Educational programs and learning events offered by the Royal Canadian Mounted Police and the Communications Security Establishment (including the latter's annual international symposium) are important to the government security, IT, and program communities. They supplement the rich selection of courses and conferences offered by the private sector and professional associations. In addition, the recently created OCIPEP has already demonstrated its informational role by disseminating the latest information on threats, trends, and best practices, by way of regular conference calls, Web site services, and timely advisories. Plans are under way by the Treasury Board Secretariat to develop a repository of recommended best practices as well as an IT security portal to facilitate the regular exchange of information among departments and agencies.

Departmental governance and risk management

3.70 In addition to examining IT security issues in the government as a whole, we reviewed IT security practices at four departments and agencies, namely Fisheries and Oceans Canada, Human Resources Development Canada (HRDC), Industry Canada, and the National Parole Board.

3.71 The four entities together provided a variety of operating environments. In HRDC and Industry Canada, the management of technology infrastructures is centralized, while Fisheries and Oceans Canada takes a decentralized approach. The National Parole Board has a strategic partnership with Correctional Service Canada and relies on that organization for its network systems and computer operations.

3.72 The purpose of our review was to provide an insight into current IT security practices in government (see About the Audit). It was not intended as the basis for drawing conclusions at the departmental or the government-wide level and we have drawn no such conclusions.

Need to update policies and improve implementation of departmental governance framework

3.73 A comprehensive policy on information technology security establishes the framework for ensuring that information assets and the technology infrastructure are properly protected. With the rapid pace of change in information technology, we would expect IT security policies and standards to be not only developed but also kept current.

3.74 The Government Security Policy and the related operational and technical standards set out the minimum requirements that departments and agencies must meet. They are required to build on these baseline standards and develop their own policies that meet the specific security needs of their operations.

3.75 All four departments we examined have IT security policies. HRDC used the Government Security Policy and the related standards to develop its own policies and standards that would guard against the threats to its information assets and operations. We noted that the policies had been updated and efforts made to keep them current.

3.76 The three other departments rely primarily on the Government Security Policy and standards. Management decided to accept them as appropriate for their organizations, but we found no documents or analysis to support that decision. As already noted, until February 2002 the last update of the Government Security Policy had been in 1994, and the standards predate many recent developments in the use of the Internet. Both Industry Canada and Fisheries and Oceans Canada issue security bulletins on specific IT issues. However, they prepare them on an ad hoc basis. The bulletins may not be broad enough to ensure that with the security policies and standards, they constitute an up-to-date and comprehensive set of policies and standards. We also noted that departments have identified policy gaps but have yet to develop policies that address them.

3.77 The Government Security Policy stipulates that deputy heads are accountable for security in their areas of responsibility. The policy also requires that each department and agency appoint a departmental security officer and an IT security co-ordinator.

3.78 We found that all four departments have appointed IT security co-ordinators with some form of reporting relationship to the departmental security officers. However, only in HRDC and Industry Canada do the co-ordinators have defined roles and responsibilities to facilitate developing, implementing, and enforcing IT security policies.

3.79 In Fisheries and Oceans Canada, the IT security co-ordinator is responsible for establishing the corporate IT security program. However, he has limited authority to ensure compliance. We noted that compliance in the Department's Pacific Region was selective. For example, the Region implemented certain aspects of the policy on network passwords but not the requirement to change those passwords every 90 days. There may have been an appropriate justification for this but it was not documented, nor was it evident to us.

3.80 The National Parole Board has a strategic partnership with Correctional Service Canada and relies on it for its networks and computer operations. The effectiveness of its IT security program is thus dependent on its partner. In this partnership arrangement, however, Correctional Service Canada manages sensitive parole data owned by the Board. We found that the Board has not articulated its IT security requirements to its partner or sought assurance that its information assets are safeguarded adequately.

Risk assessments tend to have a single focus

3.81 The IT security community has long acknowledged that IT security practices revolve around risk management. It is neither feasible nor cost-effective to eliminate all risks or threats to information assets. Moreover, like any priority, IT security has access to limited resources; risk assessments help direct resources to areas that warrant them. We therefore looked in the four departments for processes and practices to identify, assess, and manage risks. We also asked about their business continuity plans, which would help them continue operating if normal operations were interrupted for any reason, including failure or unavailability of information systems.

3.82 The 1994 Government Security Policy set an expectation that new systems were to undergo sensitivity analysis and threat and risk assessment (TRA), with a specific focus on IT security. In addition, the RCMP has developed guidelines for departments and agencies on conducting TRAs.

3.83 We found that all four departments have prepared TRAs but only on an ad hoc basis (see also the section of this chapter beginning at paragraph 3.92). The assessments tend to focus on a single application or, in some cases, on a major change in IT infrastructure. We were not able to find any analysis that considered threats and risks to departmental IT security overall. The departments' threat and risk assessments were conducted at different times. Business environments change from time to time along with technology. An analysis with a broad perspective can highlight gaps and duplication of efforts. It can also ensure that concerns about business impacts and privacy have been addressed adequately. Although such broad-based analyses are not required by the Government Security Policy and standards or by the IT security policies of the four departments, in our view conducting them periodically would add strength to departmental IT security.

3.84 A business continuity plan (BCP) is an important risk management tool that allows a department to plan for business disruptions and to recover from them. While preparing for the Year 2000 computer problem, most organizations also developed BCPs. In our December 1999 Report, we recommended that departments test those plans and keep them up-to-date.

3.85 Our audit confirmed that in 1999, all four departments developed business continuity plans in preparing for Year 2000. However, they have not updated the plans since then. In anticipation of the 2002 Government Security Policy and in response to a directive issued after 11 September 2001, all four departments are preparing to update their plans. We also noted that none of the departments have conducted periodic tests of their business continuity plans.

3.86 Fisheries and Oceans Canada is updating its contact list and determining the resources it needs to maintain its business continuity plan and update the plan regularly. In summer 2001, Industry Canada created a new business unit to be responsible for its BCP; the plan will take into account various business units and locations of the Department across Canada. HRDC is updating and centralizing all local and detailed business continuity plans in a single corporate database. The individual plans will eventually be rolled up into a corporate plan. The National Parole Board has developed a draft framework for updating its plan.

No formal program for awareness training in information technology security

3.87 Awareness training in IT security is an important step in implementing an IT security program. All employees need to understand the sensitivity of the information they handle, the potential threats, and their responsibility to minimize the threats. A program of training in IT security awareness is a way to help employees understand the requirements of their departmental IT security policies and the potential impact of non-compliance on the security of their information assets.

3.88 A typical awareness training program includes the following:

- holding security training sessions and seminars;
- giving security briefings and presentations;
- disseminating a security handbook;
- providing information on a Web site and Intranet;
- distributing pamphlets, videos, and posters;
- issuing security bulletins and reminders; and
- using screen savers and login banners.

3.89 We found that HRDC has a security awareness training program that includes most of those elements. The three other departments have some of the elements but have not established a formal program of ongoing awareness training.

3.90 The practices we observed in IT security governance and risk assessment in the four departments are symptoms of potential weaknesses in IT security practices across government. In our view, they merit consideration in the upcoming update of IT security operational standards.

3.91 **Recommendation.** The government should consider providing further guidance in its update of information technology security standards to ensure that departments and agencies have appropriate frameworks for governance of IT security and for management of security risks. Considerations should include the need to keep departmental policies up-to-date; the need for periodic, broad-based risk assessments; and the need for a formal program of employee awareness training.

Government's response. The government agrees with this approach, which is reflected in the renewed Government Security Policy. Over the next few months, the Treasury Board Secretariat will be working with the lead security agencies to communicate the GSP and departmental obligations, including the need for employee awareness and training. The RCMP already provides IT security awareness and specialized training, on demand.

Managing security practices in departments

Early consideration of information technology security needed

3.92 A key step in any IT security program is to develop and practise effective control of IT threats and risks. Preventive controls are most effective when security concerns are considered and dealt with early on in designing new business programs or developing and changing information systems. Further, timely and due regard to security minimizes costs in the long term. At the four departments, we looked for practices that support these principles and for some essential controls that various industry standards for IT security support.

3.93 The 1994 Government Security Policy required that system development start with a sensitivity analysis of a contemplated IT system, followed by a threat and risk assessment that supports all key development decisions, especially decisions about security. The revised policy requires that departments certify and accredit information systems before they begin operating and that they practise sound configuration management of systems and their safeguards.

3.94 Our audit showed a mix of actions taken by the four departments and agencies, with mixed results. All four have conducted ad hoc threat and risk assessments (TRAs) of some new systems and some infrastructure changes. Until recently, none had a policy requiring TRAs at the start of a system development life cycle. Moreover, departments have not defined or provided guidelines on how to identify an application development or infrastructure change that is substantive enough to warrant a TRA. Decisions to conduct assessments were subjective and ad hoc. As a result, senior management does not have full assurance that threat and risk assessments were conducted where needed and that cost-effective, preventive controls were considered and put in place right from the start.

3.95 At Industry Canada we noted a new policy that came into effect in June 2001, making threat and risk assessments mandatory in all new systems development. However, few have been conducted so far. As a large entity, HRDC has done many TRAs of changes to its systems.

3.96 We reviewed several threat and risk assessments to look for cost analyses of options, including the proposed option, and management's subsequent acceptance of residual risks. We found no evidence that cost implications had been considered in the TRAs and that management had approved the proposed option.

3.97 It is a generally accepted security practice to allow employees access to a system only as needed to carry out their assigned duties. Controls to prevent unauthorized access to applications or network systems include defining and implementing access rights and privileges and controlling access through user authentication, often by passwords.

Access privilege—The extent to which an individual or device can view, add, change, or delete data on a computer system.

3.98 We found that the management of access privileges was spread throughout each department, and those privileges were not reviewed periodically. The general mentality, especially among the users, is that broader access is more efficient for day-to-day operations. In configuring new applications, the principle of access as needed is often not applied stringently, a problem further compounded by the use of diverse and incompatible hardware platforms and applications that have evolved over time. Consequently, access privileges can be fragmented across different applications and technology platforms.

3.99 Password management is not trivial but essential. We found in many cases that passwords are not changed regularly. In some cases, when employees leave the organization or move on to new assignments, the passwords to which they had access are not changed or cancelled promptly. In some other cases, the organization does not use rules-based, strong passwords—with rules, for example, that set a minimum number of characters, require the use of special characters, and forbid the use of default passwords or common words. Furthermore, most employees have several passwords to access various networks and applications, which can lead them to be less vigilant about changing their passwords and keeping them confidential. In response to what it found in one of its security reviews, HRDC has a project under way to streamline password management across the Department, irrespective of location or system.

Remote access—Access to a system or network device from a distance, using telephone lines or the Internet.

3.100 Fisheries and Oceans Canada has no department-wide policy for minimum security over remote access to departmental systems, and many employees use remote access. An April 2000 internal audit report noted that about 2,500 staff accessed the Department's networks from outside office premises. Over 1,800 employees accessed the networks using computer equipment not owned by the Department. Equipment that the Department does not own is not subject to its configuration control and could introduce additional risks and vulnerability to its networks. The internal audit also noted that delivery of remote access differed from one region to another.

3.101 We visited Fisheries and Oceans Canada in its Pacific Region as well in the National Capital Region. In the Pacific Region, we found no policies or procedures governing remote access. Employees are granted the same access to network services from a remote location as they have on departmental premises. In our discussions, regional management acknowledged that global granting of remote network privileges not only increases the risks of compromising its network security but also carries a significant cost. As we concluded our visit in December 2001, the Region was considering developing a policy to reduce the cost of toll-free dial-up access to its networks.

Needs to broaden ongoing monitoring

3.102 Effective IT security programs include detective as well as preventive controls. Detective controls help to verify whether preventive controls function as planned. They can detect unauthorized access or unusual patterns of activity so that timely corrective action can be taken. Detective controls often take the form of ongoing monitoring—for example, monitoring system logs, installing intrusion detection sensors and analyzing their results, and conducting security sweeps for compliance with policies. Automated tools are increasingly available to management and security officers for analyzing log traffic.

3.103 During the audit, we looked for detective controls in the four departments. We found that in monitoring logs, they tend to focus on acceptable use of the Internet. This was particularly evident in the three larger departments, including the regional offices we visited. They monitored logs on an ongoing basis to ensure that employees had not abused Internet privileges on departmental systems. The three departments have procedures to address any inappropriate use by staff. HRDC analyzed logs to identify access to systems whose security was of specific concern to program managers so it could follow up on misuse and abuse of the data.

3.104 In all four departments, we noted that IT security officers heed IT security alerts and are on guard against virus attacks. Departmental security practices include measures to protect information assets. During our regional visits, we observed two departments taking steps to ward off a virus attack.

3.105 However, we found instances where the system logging function was not activated. We noted instances where the logs were not analyzed systematically. Threats to information technology security are not limited to employees accessing inappropriate Web sites or to viruses and other forms of malicious code. A department needs to have proper safeguards against external attacks that target it specifically as well as internal misuse or misconduct, unintentional or otherwise.

Intrusion detection system—A system that detects potentially hostile traffic and warns management.

3.106 Intrusion detection systems are a detective control that helps identify potentially malicious network traffic. In 1999 the Communications Security Establishment (CSE) commissioned a network threat assessment study of six departments, using intrusion detection systems. The CSE concluded that external threats to government information systems were real and appeared to be global, and that automated attack tools had been used. In September 2000, the CSE recommended that departments implement a network intrusion detection capability. Of the four departments we audited, only Industry Canada has developed some internal capability for intrusion detection.

3.107 A security sweep is an inspection to verify that employees are following security procedures. The procedures include making sure that they log off their computers when not using them and at the end of a work day, that they secure computers physically, and that removable media are properly protected. We noted that the departments do not conduct regular security sweeps.

3.108 Good IT security also includes following predefined steps to respond to and report security incidents. When an IT security incident occurs, staff have to recognize it as an incident, react quickly to correct the situation, and report it to the appropriate security officers. This requires that departments have procedures established and personnel trained to take decisive and appropriate action.

3.109 In none of the four departments did we find a definition of what constitutes an IT security incident. Declaring that an incident is a security incident is left to staff and managers, and there are no procedures established to ensure that staff will react appropriately, consistently, and promptly.

3.110 In each of the four departments, responsibility for responding to an incident is shared by systems, network, and business program staff. Industry Canada has a team of IT and security staff that communicates by telephone as needed. The IT security manager also receives an encrypted electronic mail alert when the network engineers detect a problem.

3.111 Managing IT security practices through ongoing monitoring helps departments and agencies detect any attack on their systems and determine whether they have been compromised. Although the ongoing monitoring in the four departments may not be representative of the government, it is symptomatic of likely gaps between the revised Government Security Policy and the IT security practices of departments and agencies. In our view, it would be appropriate to identify any significant gaps and consider them when implementing the revised policy.

3.112 **Recommendation.** The government should identify any significant gaps between present information security practices in departments and the 2002 Government Security Policy and address them in its plan for implementing the policy.

Government's response. Lead agencies are actively engaged in identifying gaps between departmental security practices and the Government Security Policy, and are working with the Treasury Board Secretariat to develop incident response and reporting procedures; IT security (ITS) readiness levels; an organizational ITS self-assessment guide; certification and accreditation guidelines; and secure service profiles for critical business requirements.

Audits and periodic reviews

Audit and independent reviews of information technology security have been limited

3.113 Audits and independent reviews provide assurance to management that departmental operations meet program objectives; they also highlight areas that need to be improved. Audits and independent reviews of IT security serve as periodic checks on the state of IT security in a department.

3.114 The 1994 Government Security Policy required that departments conduct internal audits of IT security at least once every five years. We found that only Fisheries and Oceans Canada and HRDC have audited IT security department-wide. The two other departments have not complied with the policy requirement.

3.115 A 1995 audit of security at Fisheries and Oceans Canada included IT security as a specific component. A second audit of IT security was completed and a report issued in 2000 that noted some of the same weaknesses as in 1995—for example, weak controls over remote access and equipment connected to the network. The Department has prepared an action plan to address the audit recommendations. HRDC carried out a broad-based audit of IT security in 1999, and the audit report made a number of observations and recommendations. For example, it noted that procedures for IT security varied; and roles, responsibilities, accountabilities, and authority for security were unclear. HRDC has prepared an action plan and is addressing those observations.

3.116 Traditionally, the RCMP conducted independent reviews of IT security for departments and agencies. The 1994 Government Security Policy stipulated that departments were to request RCMP reviews of their IT security programs at least once every five years, and more often where programs and systems involved classified and/or extremely sensitive information.

3.117 Contrary to the policy, however, no RCMP reviews of IT security practices have been conducted at Fisheries and Oceans Canada or Industry Canada in the last five years. The RCMP conducted a partial review of the National Parole Board as part of a mandatory requirement before it would allow the Board access to some of its law enforcement systems. HRDC was the only one of the four departments that had requested an RCMP review, but the last one was conducted in 1997.

Few technical tests to check for network vulnerabilities

War dialing—A test that uses automated tools for dialing a set of telephone numbers to find unsecured modems.

Vulnerability assessment—A set of tests that looks for vulnerabilities in network systems before a security breach occurs.

3.118 A number of techniques are available for departments to test the effectiveness of security for their network systems. The techniques are an essential part of a comprehensive program for managing IT security. They include testing for unauthorized modems by automated dialing of telephone lines (war dialing) and checking for weak access points in network systems (vulnerability assessments). A form of audit and monitoring, the tests can help identify weaknesses and potential vulnerabilities that could be compromised. Periodic testing is a preferred IT security practice.

3.119 We found that two of the four departments have done little or no technical testing of their network systems for unauthorized modems and potential vulnerabilities; Industry Canada did some limited testing for network vulnerabilities. HRDC has acquired technical tools to conduct vulnerability assessments.

3.120 Our examination showed that audit and independent review of IT security are weak. Furthermore, most departments and agencies have not complied with policy requirements. In our view, the revised Government Security Policy needs to address this deficiency to enhance IT security across government.

3.121 **Recommendation.** The government should consider setting a minimum frequency for departments to conduct periodic assessments of information technology security practices and requiring in its technical standards that departments conduct vulnerability assessments of their systems.

Government's response. While the government agrees in principle with this recommendation, the Government Security Policy leaves it to the deputy head of a government institution to determine the frequency of such periodic assessments. Through the IT security standards development process, the Treasury Board Secretariat and lead security agencies will be developing guidance on vulnerability analysis requirements and optimal frequency of periodic assessments. These will be based on best practices with respect to risk management and availability of resources.

Assessing network vulnerabilities

Technical tests identified potential vulnerabilities

3.122 We conducted war dialing on a sample basis in some departments and remote testing for network vulnerabilities at their Internet points of presence. In both cases, we looked for vulnerabilities but did not exploit them to penetrate departmental networks. We did not test from the departments' internal network systems for network vulnerabilities.

3.123 We provided details of our test results directly to the departments so they could address any potential weaknesses we had identified. The test results presented here are global and not attributed to individual departments.

3.124 For the war dialing tests, we selected 10,000 telephone numbers in the National Capital Region and one other region of the departments and used automated tools to search for modems. We found 97 devices that could serve as points of access to departmental networks. A subset of those devices could be unauthorized modems that present a high risk to the departments. We provided the departments with details for follow-up.

3.125 We conducted vulnerability assessments of 260 host systems, located using information provided by the departments. Using a combination of different technical tools, we gathered information about the systems and analyzed it for vulnerabilities that could allow unauthorized access to them.

3.126 We found that 85 of the 260 systems contained vulnerabilities, most of which could allow the systems to be readily compromised by a targeted cyber attack. We were concerned by one weakness in particular that posed an imminent threat, and we reported it immediately to that department. We provided all other data and the results of our analysis to the departments after completing the tests.

3.127 Although we found access points that could readily be exploited, we did not attempt to penetrate the systems. As a result, we cannot conclude what the impact of such weaknesses would be. Examples of weaknesses we found are provided in "Our vulnerability assessments identified weaknesses."

3.128 The results of our tests underscore the value of audits and independent assessments. They also support our recommendation that the government include war dialing and vulnerability assessments in the operational and technical standards it is developing for IT security.

Our vulnerability assessments identified weaknesses

Outdated applications and unprotected systems

Several host systems used outdated applications known to contain vulnerabilities that could be exploited to gain unauthorized access. In one case a system administrator password was not set, thus allowing any Internet user to gain access to the system.

There are many potential abuses of unauthorized access:

- Sensitive data stored on a system can be viewed and used fraudulently.
- Data or programs can be modified or deleted.
- Access to one departmental system could allow access to another.
- Programs could be installed to attack other systems on the Internet. The attacks would appear to be initiated by the government.
- Systems could be used to share files; the government would be seen as endorsing the content of the files.

Information vulnerable to cyber attacks

Information on system set-up and user identity was vulnerable to attacks. This information could be used to plan a cyber attack or to gain unauthorized access to systems and data.

The following information was available on the systems:

- the type and version of operating system in use;
- the name of the host system;
- the configuration of the system for file sharing (did it allow "trust relationships" that would provide direct access to other systems?);
- a list of valid usernames; and
- the first and last names of users.

Conclusion

3.129 The revised Government Security Policy came into effect in February 2002, replacing the 1994 policy. The revised policy has a strong focus on IT security and is an important step in strengthening security across government. However, we observed that the operational and technical standards for IT security are still out-of-date, and plans and a timetable to update them have not been completed. The revised policy will not be fully effective without updated standards, setting out minimum requirements that departments and agencies must meet.

3.130 We also noted that departments have not complied with the 1994 policy requirement to conduct internal audits and request RCMP reviews of their IT security at least once every five years. As a result, the government does not have sufficient information on the state of IT security across departments and agencies. That information is essential to determine whether the present state of security is acceptable and to set a baseline for measuring future progress.

3.131 Our examination of four departments showed some weak IT security practices that could be symptomatic of weaknesses in other departments. They can thus indicate to the Treasury Board Secretariat and other lead security agencies where they may need to focus their management and support. Our technical tests found potential vulnerabilities that could compromise government network systems. The test results reinforce our observation that periodic audits and independent reviews of IT security are needed.

3.132 Our audit has identified a number of issues that the government needs to address to improve IT security across departments and agencies. In launching its Government On-Line initiative, the government identified security and privacy concerns as a key issue. Timely action to improve IT security is important for this initiative so that appropriate security practices can be in place to provide secure on-line access to all government services.

About the Audit

Objective, scope, and approach

The audit objective was to assess the framework for information technology security that the government has in place to protect information assets and ensure the uninterrupted delivery of services. Protecting information assets includes not only protecting the value of the assets themselves but also keeping classified and designated information confidential and safeguarding the integrity of data and information kept in electronic form.

To assess the IT security framework government-wide, we carried out our audit work primarily at the Treasury Board Secretariat. We also met staff of the Royal Canadian Mounted Police, the Office of Critical Infrastructure Protection and Emergency Preparedness, and the Communications Security Establishment.

In addition to reviewing the government-wide framework, we reviewed IT security practices at four departments and agencies: Fisheries and Oceans Canada, Human Resources Development Canada, Industry Canada, and the National Parole Board.

The four departments vary in size and collectively provide services to individuals and to businesses. They include both centralized and decentralized management of IT infrastructure. We selected them for some insight into the state of IT security in government. However, due to the diversity of their mandates and operations, including their IT infrastructures and systems, our findings cannot be considered representative and do not provide an overall view of government IT security practices. Our audit work at the departments included the National Capital Region of all four departments and the Pacific regions of Fisheries and Oceans Canada and Industry Canada.

We also conducted remote technical tests on networks of some departments to detect vulnerabilities, but we did not exploit any vulnerabilities found during the tests.

Criteria

The following general criteria were used in the audit:

- The information technology security framework should ensure that IT assets are protected and support the secure and uninterrupted delivery of government services.
- The IT security governance structure should ensure strong leadership and support from the central and lead agencies and consistent, cost-effective IT security practices across government.
- Policies, standards, and practices should be commensurate with the current state of risks and threats to IT security.
- Consistent with assessed risks and current security requirements, departmental measures and processes should prevent, detect, and respond to IT threats.
- IT security practices should be monitored and periodically reassessed, and vulnerabilities addressed.

Audit team

Assistant Auditor General: Douglas Timmins
Principal: Nancy Cheng
Directors: Richard Brisebois, Greg Boyd, Tony Brigandi, and Guy Dumas

Chantal Berger

For information, please contact Communications at (613) 995-3708 or 1-888-761-5953 (toll-free).

Report of the Auditor General of Canada to the House of Commons—April 2002

Main Table of Contents