Chapter

1

Information Technology Security

All of the audit work in this chapter was conducted in accordance with the standards for assurance engagements set by the Canadian Institute of Chartered Accountants. While the Office adopts these standards as the minimum requirement for our audits, we also draw upon the standards and practices of other disciplines.

Table of Contents

Information Technology Security

Main Points

1.1 Despite encouraging signs of improvement, the government has made unsatisfactory progress in strengthening information technology (IT) security since our audit in 2002. It has laid a foundation by developing IT security policies and standards, and lead agencies and departments are more involved and committed to IT security. However, two and a half years after revising its Government Security Policy, the government has much work to do to translate its policies and standards into consistent, cost-effective practices that will result in a more secure IT environment in departments and agencies.

1.2 The revised 2002 Policy clarified the roles and responsibilities of the various players in IT security. Since then, lead organizations are co-operating to develop standards and provide guidance and assistance to departments in strengthening their IT security practices. However, many standards have yet to be developed and the Treasury Board Secretariat has not completely fulfilled its oversight role as defined in the Policy.

1.3 Departments and agencies have achieved some progress in developing IT security policies and implementing specific security practices, such as vulnerability assessments. However, their IT systems are vulnerable to breaches in security. The majority of departments do not meet the minimum standards set by the Secretariat for IT security. Vulnerability assessments, conducted in departments and agencies over the last two years, have revealed significant weaknesses that, if exploited, could result in serious damage to government information systems.

1.4 We are concerned that, in many departments and agencies, senior management is not aware of the IT security risks and does not understand how breaches of IT security could affect operations and the credibility of the government. If security weaknesses allowed someone to access a database or confidential information, Canadians' trust in the government would be greatly eroded. Further, if a citizen's privacy were violated because of a failure to keep confidential information secure, it could cause that person hardship and seriously undermine the government's efforts to deliver services to Canadians electronically.

Background and other observations

1.5 In 2002, we found that the revised Government Security Policy, which came into effect in February 2002, was an important step in strengthening security across government. However, the IT security standards to support its implementation in departments and agencies were either non-existent or out

of date. Little information on the state of IT security across the government was available because few departments had audited their security programs or monitored their IT security. We also identified other issues that the government needed to address to improve IT security.

Treasury Board Secretariat has responded. The Treasury Board Secretariat's responses to our recommendations are included in this chapter, along with additional information at the end of the conclusion. The Secretariat has responded positively to our recommendations and, in some instances, is already taking action.

Introduction

Cyber incident—Any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource.

1.6 In our April 2002 Report, we reported on the state of information technology (IT) security in the federal government. We noted that IT security should be a high priority for management, given increasing cyber incidents and their potential to disrupt an organization's business.

Key findings in 2002

1.7 The 2002 revised Government Security Policy was an improvement over earlier versions of the Policy. More specifically, it

- updated the roles and responsibilities of the Treasury Board Secretariat, which plays a co-ordination and leadership role, and of the 10 entities that provide security guidance and support to departments and agencies; and
- emphasized the importance of IT security to overall government security.

1.8 However, we did have concerns. The operational standards, which departments and agencies follow to implement the policy, were outdated or did not exist. These standards are critical: they define baseline requirements for instituting consistent security measures across government.

1.9 The government was not monitoring how effective the Policy was in strengthening IT security. It had done little monitoring since 1994, and departments and agencies were generally not complying with Policy requirements. The 2002 Policy no longer required departments to audit their security programs every five years and the Royal Canadian Mounted Police to assess departmental security periodically.

1.10 Since 1994, there had been limited government-wide monitoring and oversight of IT security and, as a consequence, little baseline information existed on the state of IT security across government.

Important changes since 2002

1.11 Since 2002, the use of the Internet in government has grown rapidly. It started to accelerate in 1999 with the launch of the Government On-Line (GOL) initiative. GOL will allow Canadians to access key government information and transaction services on-line by the end of 2005.

1.12 To make services and information more accessible, the government has been streamlining its Internet services under three themes: Canadians, Business, and International Visitors. At the departmental level, it is making its services more client-friendly and providing 130 key services on-line. At the same time, three factors are compounding the risk of delivering services on-line:

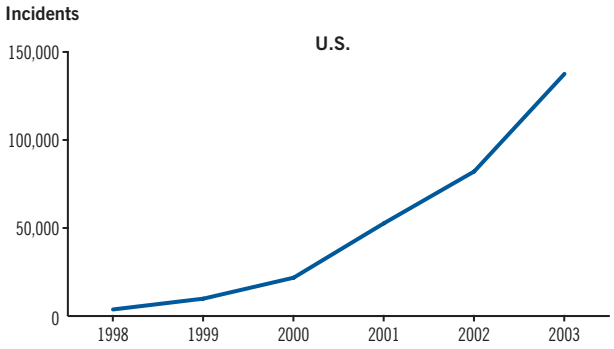
- the availability of on-line tools that can breach the security of IT systems;

- an enormous increase in software and hardware weaknesses that can compromise computer systems and the information they contain; and
- a growing number of people with the knowledge to exploit these weaknesses, often within days of their discovery.

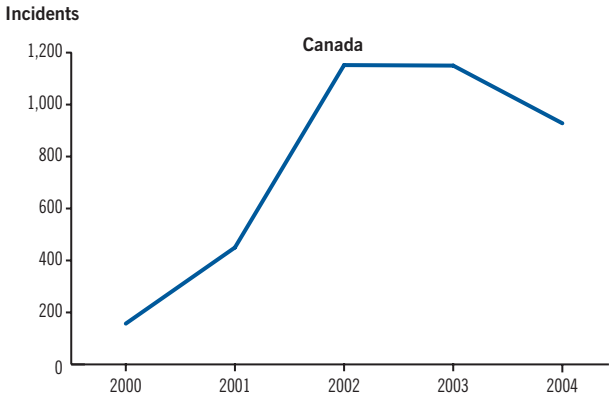
Network attack—A single unauthorized attempt to access or use a network. An **incident**, on the other hand, involves a group of attacks that can be distinguished from other **incidents** by the distinctiveness of the attackers and the degree of similarity of sites, techniques, and timing.

1.13 Cyber incidents have risen significantly since 2001, and the increase and the patterns are similar in Canada and in the U.S. (Exhibit 1.1). However, only a small percentage of incidents are actually reported. Network attacks are a good indicator of the real risks. Since our last 2002 Report, these attacks have increased dramatically, which shows how easily and quickly they can be launched (Exhibit 1.2).

Exhibit 1.1 Cyber incidents detected and reported by third parties in the U.S. and in Canada

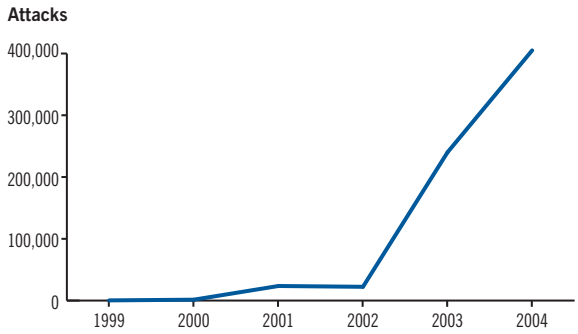


Source: CERT Coordination Centre (U.S.)



Source: CanCERT (Canada)

Exhibit 1.2 **Network attacks detected in Canada**



Note: These network attacks include a variety of incidents detected by sensors across Canada. They are indicative of the malicious activity that most government and commercial networks experience.

Source: CanCERT (Canada)

1.14 The Government of Canada recognizes that Canadians want on-line services that are secure for business and protect their personal information. In response, it initiated the major Crown project, Secure Channel, an infrastructure that connects Canadians and businesses to the government. The Secure Channel

- incorporates common standards for privacy, security, availability, and reliability;
- offers Internet services to all departments and agencies;
- offers client authentication services, which are being used more and more;
- delivers several GOL services since 2002; and
- will allow Canadians to provide confidential information on their census forms on-line in 2006.

1.15 The government also offers services to users with Web-enabled cell phones or personal digital assistants. The range of these services is increasing. For example, Canadians can now obtain toll-free numbers, up-to-date economic forecasts, or contact information for their members of Parliament.

1.16 Before departments and agencies can deliver their services, either by wireless devices or on-line on the Secure Channel network, they will need to meet stringent baseline IT security standards.

Focus of the follow-up

1.17 The objective of this follow-up was to assess the extent to which the Treasury Board Secretariat and departments have implemented the recommendations that we made on IT security in Chapter 3 of our 2002 Report. We looked at the state of IT security across government, and whether departments and agencies have appropriate frameworks for

protecting the security of information and delivering services securely and without interruption. More specifically, we focussed on five key areas:

- co-operation and information-sharing among lead organizations on IT security;
- development and implementation of IT security standards to support policy;
- effectiveness of the Government Security Policy and existing security measures;
- contingency planning; and
- risk management.

1.18 We interviewed staff from agencies that play a lead role in IT security across government and examined documents and files. In the four departments that we audited in 2002, we reviewed IT security practices in the five key areas noted above. We reviewed a Treasury Board Secretariat survey, conducted a survey of selected IT security practices in 82 government entities, and reviewed the results of technical tests conducted in a number of departments and agencies either by consultants or the Communications Security Establishment. In addition, we conducted our own technical tests. However, we did not examine the Secure Channel and national security matters.

1.19 More information about the follow-up objective, scope, approach, and criteria can be found at the end of the chapter in **About the Follow-Up**.

Observations and Recommendations

A revised Government Security Policy

1.20 The revised Government Security Policy has improved IT security across government, and support exists for further progress.

Roles and responsibilities of lead departments and agencies are outlined in the Policy

1.21 The Policy outlines the roles for the Treasury Board Secretariat and the 10 lead departments and agencies and divides responsibility for security among them. It eliminates duplication in the roles and responsibilities of the Royal Canadian Mounted Police (RCMP) and the Communications Security Establishment (CSE), and adds new roles for Public Safety and Emergency Preparedness Canada (formerly the Office of Critical Infrastructure Protection and Emergency Preparedness).

1.22 In 2002, it was too early to know whether the new roles and responsibilities were appropriate and would eliminate duplication. They are an improvement; the lead organizations, government, and agencies consult regularly on IT security. For example,

- the Information Technology Security Committee meets every two months and is co-chaired by the RCMP and the CSE;

- departmental security officers are briefed throughout the year by lead organizations; and
- senior IT and information management (IM) staff attend the Chief Information Officer Council, an advisory body that discusses IT and IM issues.

1.23 The Policy assigns the Treasury Board Secretariat the main responsibilities of co-ordination, leadership, oversight, and monitoring. However, the Secretariat is not adequately fulfilling its role of monitoring and overseeing the state of security in the government (see paragraphs 1.72 and 1.73).

Government-wide co-operation has improved

1.24 In 2002, we found that the Policy had not defined who was responsible for collecting and sharing best IT security practices across government. This has improved with various mechanisms that contribute to effective information sharing. These include courses organized by the RCMP and the CSE, liaison among chief information officers, and meetings of departmental security officers.

Several IT security standards remain to be developed

1.25 IT security standards stipulate what departments and agencies must do to meet the Policy's baseline requirements. They also promote consistency in security measures across departments and sharing of best practices.

1.26 In 2002, the Policy lacked the operational standards that departments and agencies must meet to comply with its various requirements. Since then, the Treasury Board Secretariat, in consultation with the lead security organizations and departments and agencies, developed the Management of Information Technology Security (MITS) standard, published in May 2004. The MITS standard offers guidance on maintaining secure IT systems in the following areas: management controls, risk assessments, dealing with security incidents and weaknesses in systems, auditing security, and business continuity planning. It also defines the roles and responsibilities of key security officers.

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

1.27 The MITS standard refers to a number of other standards that have not been completed (Exhibit 1.3). When these standards are completed, they, along with the MITS standard, should provide departments with the directives they need to comply with the Policy. The Treasury Board Secretariat has set December 2006 as the target date for complying with the MITS standard.

1.28 **Recommendation.** The Treasury Board Secretariat should complete all the security standards that support the Government Security Policy and the MITS standard. More specifically, it should

- prioritize the IT security standards that have been identified but not yet developed,
- prepare an action plan with timelines for each standard, and
- continuously identify IT security areas where standards are needed.

Treasury Board Secretariat's response. The Treasury Board Secretariat agrees. The MITS (Management of Information Technology Security) standard established an overarching set of baseline requirements for all departments and agencies. In conjunction with the lead security agencies (the Communications Security Establishment, Public Safety and Emergency Preparedness Canada, and the Royal Canadian Mounted Police), TBS will complete the Operational Security Standards before the end of 2006. More technical standards, as well as technical and operational guidance, will continue to be developed to meet the changing needs that reflect our dynamic risk environment.

TBS will develop, co-ordinate, and monitor a GoC-wide plan that will identify priorities among standards not yet developed. As well, a specific action plan for each standard will be produced by the appropriate lead agency and timelines agreed upon with TBS. This broad prioritization and planning in conjunction with the lead security agencies has already begun; the plan will be available to all departments and agencies on our Sitescape forum early in the fiscal year 2005–06.

Emerging IT security issues will continue to be identified by many sources, from lead security agencies and line department security professionals to the business and service delivery owners who have service and system needs to be met. While prioritizing these areas for standards development will be a collaborative effort, TBS will continue to play a GoC-wide co-ordination role, including oversight of the development and implementation of action plans to provide standards and guidance where needed.

Exhibit 1.3 Security standards yet to be completed

IT security standards

- Intrusion Detection
- Incident Management

Other security standards that affect IT security

- Security Training and Awareness
- Security in Contracting
- Identification and Categorization of Assets
- Threat and Risk Assessment
- Investigations and Sanctions
- Security Screening
- Departmental Security Program
- Protection of Employees
- Security Outside Canada
- Sharing of Information

Implementing the Policy

Major inconsistencies in compliance exist

1.29 We expected that departments would generally be complying with most of the Government Security Policy requirements. The core requirements of the Policy and standards have changed little since the mid-nineties. For over a decade, departments have been aware of the Policy and its requirement that their IT systems be adequately protected. However, we found that most departments are not complying fully with the Policy, and major inconsistencies in compliance exist. IT security practices vary in departments; examples are provided in special inserts throughout this section.

The security officer's place in the department

The Government Security Policy and the Management of Information Technology Security (MITS) standard require each department to define the roles of its security officers, in particular for IT security, and give them appropriate status in the organization. The extent that departments have met this requirement varies widely.

- At Industry Canada and Social Development Canada, the roles of the departmental security officer (DSO) and the IT security co-ordinator are clearly defined and follow the MITS standard. However, at Social Development Canada, there is no senior committee responsible for approving policies and standards, and making decisions about IT security. At Industry Canada, the DSO is not positioned strategically to provide strategic and decision-making advice to the organization. In addition, the IT security co-ordinator's function within the Chief Information Officer Branch, which controls only a fraction of the IT budget, does not have sufficient authority in the IT security decision-making process. Because of the limited scope of the two positions, the officers have little influence on department-wide security-related decisions, particularly IT security.
- At Fisheries and Oceans, the DSO does not occupy a position at a strategic level, as required by the Policy. An IT security co-ordinator position does exist and has a functional reporting relationship with the DSO. Given that the Department has many business sectors and regions and that communication between its two security officers is lacking, the Department is not able to develop and implement an integrated and well-co-ordinated security program.

1.30 The Policy requires departments to actively monitor their security programs and audit them. In 2003, the Chief Information Officer Branch of the Treasury Board Secretariat developed a self-assessment questionnaire that departments, in accordance with the MITS standard, must use annually to assess their IT security and security management practices. Departments answer questions about their security policies and practices, based on the Policy's baseline requirements, and are scored against a benchmark.

1.31 The questionnaire helps IT and security staff to better understand baseline IT security requirements, measure their current IT security capacity, and identify gaps between their current practices and best practices. The questionnaire also helps the Secretariat assess the effectiveness of the Policy and standards and assess whether departments are complying with their requirements.

1.32 By early 2004, the Secretariat was concerned that many departments were not implementing the current Policy's IT security requirements. In May 2004, using the questionnaire, the Secretariat surveyed more than

90 departments and agencies. Forty-six entities completed the questionnaire and shared their results with the Secretariat. The results indicate that the Secretariat's concerns were well founded. Of the 46 departments that responded, only 1 met all the baseline requirements of the Policy and standards.

1.33 Departmental IT security policies provide the foundation for meeting the Policy's standards for protecting information and information systems. The Secretariat's survey found that

- 16 percent of departments did not have an IT security policy;
- for those departments that did have one, 33 percent indicated that it had not been formally approved by management;
- 35 percent of departments did not have a policy requiring threat and risk assessments;
- 26 percent of departments did not have a policy requiring a business continuity plan for critical systems and services; and
- 12 percent of departments had not yet identified their critical systems.

Security policies in departments

In 2002, we noted that the four departments we had examined should update their security policies and implement a better governance framework for security. Since then, progress has been uneven:

- Industry Canada has made good progress in developing, implementing, and communicating its IT security policies. It has developed standards and guidance to address IT security issues.
- Senior management at Social Development Canada has yet to formally approve several policies on IT security. As a consequence, they are applied inconsistently across the Department.
- Fisheries and Oceans Canada has made progress in developing a security management framework and specific policies. However, none of these have been formally approved by senior management.
- The National Parole Board has recently started a project to review its IT security policies.

1.34 We developed a brief questionnaire that complemented the Secretariat's self-assessment questionnaire, and focussed on specific IT security practices in departments. We surveyed 82 entities and obtained a response rate of 100 percent. Our results corroborate the Secretariat's findings—major inconsistencies exist between the requirements of the Policy and standards, and the current practice of departments.

1.35 For several areas of security, compliance with the baseline requirements of the Policy and standards was significantly less than adequate. For example, although 65 percent of departments had business continuity plans, only 29 percent had tested them in the last two years.

1.36 The staff that we interviewed suggested various reasons for the gaps in IT security:

- a lack of money and people,
- a lack of interest in IT security by senior management, and
- IT security concerns were not part of the culture in their organizations.

1.37 A general lack of concern for IT security risks leaves systems vulnerable, where weaknesses could be exploited. As a result, sensitive data, including information on the privacy of Canadians, payroll and financial transactions, program information, and other mission-critical data are at increased risk of unauthorized disclosure, modification, or loss—possibly without being detected.

Fostering a culture of IT security in departments

Since we looked at the four departments in 2002, their success in promoting awareness of IT security issues and providing security training has been uneven.

Industry Canada has worked to raise awareness of IT security throughout the Department. It publishes security tips and monthly IT bulletins. It has also developed security training and a process for alerting staff to security incidents. The other departments have not been able to maintain awareness of security throughout the organization or have not been able to maintain the momentum.

1.38 **Recommendation.** The departments and agencies, subject to the Government Security Policy, should prepare an action plan indicating when they intend to fully comply with the IT security requirements of the Policy and with the Management of Information Technology Security standard. This IT security action plan should be approved by the deputy head or designate and reported to the Treasury Board Secretariat.

Treasury Board Secretariat's response. TBS agrees with this recommendation. Discussions have already begun with Information Technology Security Coordinators (ITSCs) to develop individual departmental plans for compliance with the IT security requirements of the Government Security Policy (GSP) and Management of Information Technology Security (MITS) standard. These departmental plans must be submitted to TBS by summer 2005, under the signature of the deputy head or designate, thus ensuring the involvement and commitment of senior departmental management.

1.39 **Recommendation.** The Treasury Board Secretariat should require all departments and agencies, subject to the Government Security Policy, to prepare timely IT security action plans, follow up on these plans shortly after December 2006, and report to the Secretary of the Treasury Board on the organizations that are not complying.

Treasury Board Secretariat's response. TBS agrees with this recommendation in line with recommendation 1.38. TBS will work with the departments and agencies in developing a common review and reporting process with a final report prepared for the Secretary of the Treasury Board in early 2007.

IT security measures should reflect the level of risk

1.40 To protect government assets and information, the Policy follows a risk management approach—a set of practices and procedures to manage risks. Departments and agencies are required to comply with the baseline requirements of the Policy and its standards. In addition, departments are required to conduct a threat and risk assessment to determine whether they need safeguards above the baseline level. The MITS standard requires a threat and risk assessment for "every program, system or service." The assessment can be "simple or far more detailed and rigorous, depending on the sensitivity, criticality or complexity of the program, system or service." The requirement is not new; it was part of the 1994 Government Security Policy.

1.41 Allocating resources according to the degree of risk is a common IT security practice. As mentioned in our 2002 Report, "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."

1.42 We were expecting that, in complying with the long-standing requirement of the Policy and its standards, departments and agencies would have done threat and risk assessments to identify risks, and developed strategies for mitigating them.

1.43 In general, departments and agencies have yet to assess threats and risks adequately. Except in the departments where assessments are becoming well-established, they are done inconsistently or not at all. Out of 82 departments and agencies we surveyed, only 37 (45 percent) had performed threat and risk assessments of their programs, systems, or services, as required by the Policy and standards. In addition, only 28 departments had verified that recommendations made in their assessments had been addressed before putting the new programs and systems in place.

Certifying and accrediting systems in departments

The Government Security Policy and its related operational standards require that departments and agencies certify and accredit any new or modified system or application before it is used. Organizations must sign off on the system or application to certify that all the requirements of the risk assessments have been met.

Industry Canada is certifying and accrediting not only new systems and applications that it implements but also major changes to existing ones. Social Development Canada has developed a project life-cycle model that includes certifying and accrediting systems and applications under development. However, IT security is not always taken into consideration at the start of the project. In addition, the risk of failing to meet IT security requirements is increased because senior management, as the project review committee, has not met in over a year.

Fisheries and Oceans Canada and the National Parole Board have yet to comply with this requirement.

1.44 The reasons for not performing threat and risk assessments are unclear. The RCMP has been offering guidance and training for years on how to carry

them out. In 2001, the Secretariat published the Integrated Risk Management Framework to provide departments with guidance on how to take a systematic approach to risk management. Over the last few years, the Communications Security Establishment has also developed methodology and guidance for doing comprehensive assessments. Yet, departments and agencies are not taking full advantage of this support to ensure that their IT resources are well protected in a cost-effective manner.

1.45 Departments and agencies that do not perform threat and risk assessments, as part of their business operations, do not know what risks they are exposed to. As a consequence, if departments and agencies do not consider their IT risks in their risk profile, they may not be directing their efforts and money on the most effective strategies to mitigate their exposure to IT risks, and may not be achieving their objectives.

Exposure—A function of the likelihood that a threat could occur, the consequences if it were to occur, and the safeguards in place.

1.46 **Recommendation.** Senior management in departments and agencies should ensure that IT security risks are included in preparing the corporate risk profile by identifying and assessing the key IT security risks and challenges and determining the level of risk to accept.

Treasury Board Secretariat's response. TBS concurs with this direction, which will encourage departments and agencies to develop an overall corporate risk profile that is reflective of the department as a whole, integrating all risk elements. Senior management oversight will be key to ensuring the success of this way forward. Also refer to recommendation and response 1.47.

1.47 **Recommendation.** The Treasury Board Secretariat should provide departments and agencies with guidance and tools for including IT security as a key component in their corporate risk profile.

Treasury Board Secretariat's response. TBS agrees with this recommendation, which is fundamental to departmental implementation of the Government Security Policy. TBS will work closely with lead security agencies, as well as with line departments, in developing the guidance and tools required to include IT security in an overall integrated corporate risk process, including an updated self-assessment tool.

A key part of this effort is the current project led by the CSE and the RCMP to amalgamate the Threat and Risk Assessment (TRA) guidelines from their respective organizations, thereby providing one common approach that will incorporate both physical and IT security TRA processes. As well, the Security Risk Management standard, planned for completion early in 2005–06, will provide an overall framework for incorporating security risk into the corporate risk profile.

Vulnerability assessments are important in assessing IT security

Vulnerability assessment—A set of procedures to identify and assess weak spots in an organization's security architecture. It uses automated tools to identify if an organization has addressed, or remains exposed to, known security flaws and vulnerabilities in its computing environment.

1.48 Many departments and agencies have carried out vulnerability assessments of their information systems. These assessments complement threat and risk assessments and are done to test systems for particular weaknesses that could compromise security. They do not determine whether

the identified vulnerabilities could be exploited (another test, penetration testing, can determine that). They can be carried out from outside the security perimeter (externally) or within (internally).

1.49 Departments that perform regular assessments often identify weaknesses in networks that had previously been considered to be secure. This happens because new vulnerabilities are continuously being uncovered and exploited with malicious intent. Although many vulnerabilities come from outside an organization, most security incidents (willful or accidental) originate from inside an organization, where individuals have ready access to information and systems.

1.50 We reviewed a number of vulnerability assessments completed by external consultants, the Communications Security Establishment, and our Office (as part of this audit). Most of them revealed significant weaknesses that could be exploited. In some instances, the weaknesses had been exploited and gone undetected. There were also vulnerabilities that had existed for some time in the older versions of products. In such cases, the vulnerabilities cannot be rectified, and the products must be upgraded to ensure adequate protection.

1.51 Exhibit 1.4 shows that 46 departments and agencies (56 percent) from our survey have completed vulnerability assessments in the last two years. The other 36 departments (44 percent) had not completed an assessment in the last two years or had never completed one.

Exhibit 1.4 Organizations that have completed vulnerability assessments over the last two years

Size of organization*	Organizations surveyed	Those that completed one or more assessments	Percentage that completed assessments
Small (under 1,000)	54	27	50%
Medium (over 1,000 and under 10,000)	22	13	59%
Large (over 10,000)	6	6	100%
Total	**82**	**46**	**56%**

*Based on full-time equivalent staff

1.52 We found that the departments and agencies that completed recent assessments had been proactive; they had identified their IT security weaknesses and were prioritizing their efforts to correct those weaknesses. In paragraphs 1.53 to 1.59, we present some of the most important weaknesses reported in the assessments we reviewed. However, we intentionally do not disclose the departments and agencies involved or the exact weaknesses.

1.53 **Access to sensitive data and programs was not adequately controlled.** An important objective for organizations is to prevent

unauthorized people from gaining access to data that support critical operations. Unauthorized access can lead to data being improperly modified, deleted, or disclosed. To effectively control access to data, organizations use software programs to monitor what information on the network is being accessed, and who is accessing it.

1.54 In many cases, the measures to control access to the systems and data were inadequate. We found that the risk associated with weak access controls increased because most organizations did not yet have a comprehensive program for monitoring who was accessing the network.

1.55 **Networks were not secure.** Networks are interconnected devices and software that allow individuals to share data and computer programs. Sensitive programs and data are stored and transmitted on networks. For this reason, networks must be made secure against unauthorized access, manipulation, and use by outsiders. Organizations can secure their networks by limiting the services that are available and installing devices that deny unauthorized requests for access to services and data.

1.56 In many cases, the networks of departments and agencies did not provide a secure operating environment. They used firewalls to protect internal networks from the Internet; however, their current network controls do not provide adequate protection from unauthorized access by outsiders. Without a secure network, departments and agencies are exposed to an increased risk that unauthorized individuals could gain access to sensitive data, and that service could be disrupted or denied.

1.57 **Inadequate network access controls.** Controls that limit access to a network ensure that only authorized individuals in an organization gain access to sensitive and critical data. Effective controls allow only authorized users to access the network from local and remote locations. They also provide safeguards to ensure that users cannot bypass them and cause the network to fail.

Testing for vulnerable passwords

Passwords are used to ensure that only authorized persons gain access to systems. If passwords are not sufficiently robust, they can be compromised by computer programs in what is known as “brute force attacks.” Brute force attacks attempt to guess passwords. These attacks can quickly succeed with passwords that

- consist of only a few characters,
- are the same as the account name,
- use the default password,
- use a common word, or
- are derived from personal information that is readily available (such as a person’s name, address, or favourite sports team).

Many of the vulnerability assessments that we reviewed found instances where passwords were susceptible to brute force attacks. Some of these vulnerable passwords were protecting access to sensitive entry points in mission critical systems.

1.58 We found that many departments and agencies did not have secure controls in place. In many cases, the devices were not configured to consistently prevent unauthorized access to the systems on their networks.

1.59 The Chief Information Officer Branch of the Secretariat has provided departments and agencies with guidance on how to mitigate potential vulnerabilities on network servers. However, we found weaknesses in areas such as managing passwords and assigning rights and permissions to users. For example, in some departments,

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

- default vendor accounts and passwords were still active;
- passwords were not set or not set properly;
- staff had broader access than needed; and
- dangerous services, such as remote execute commands, were available.

Testing for weaknesses in configuring systems

Vulnerability exists when an organization installs commercial off-the-shelf software or hardware and does not change the default settings. The default settings are often very permissive so that a new system can be set up easily. It is best practice to remove functions that are not used, and restrict access to a system administrator who, in turn, grants permissions to users to perform activities. The initial default settings that software and hardware vendors provide usually consist of an administrator account name, a standard set of privileges for the administrator, and a password. It is best practice to change these default settings before a new system component is put into use.

The vulnerability tests, performed by departments on their own systems, have identified instances where the manufacturer's default administrator settings had not been changed. Anyone who uses these default settings, to gain access to the system, with administrator privileges effectively has full control over granting access privileges for others and can modify or remove the functions the system performs. This situation presents a serious vulnerability.

Business continuity planning still needs improvement

1.60 The Government Security Policy requires departments to establish a business continuity planning program. The program ensures that all critical services continue to be available in the event of a major disruption, such as a prolonged power failure or natural disaster. Information technology is a major part of an organization's business continuity planning program.

1.61 Valuable information is obtained in business continuity planning from two activities:

- The business impact analysis identifies critical programs, systems, or services, and assigns priority to the ones that should be restored first, if they are disrupted.
- The threat and risk assessment identifies and categorizes information and related assets according to their sensitivity, assesses related threats and system vulnerabilities, determines the level of risk, and recommends safeguards that will reduce this risk to an acceptable level.

1.62 Government operational standards require departments and agencies to perform both activities and, in particular, to carry out threat and risk assessments for every program, system, or service. The requirement to perform business impact analyses is new; we did not examine this area in our 2002 audit.

1.63 In 2002, we examined the business continuity planning program of four departments. None of the departments had updated its plans since preparing for Y2K or tested them periodically. Both activities represent best practices.

1.64 This audit looked at 82 departments and agencies. We examined how they were managing their business continuity planning program and whether the program meets the baseline requirements of the Policy and standards. We did not examine the adequacy of the plans or their tools—the business impact analysis and the threat and risk assessment. We found that several departments and agencies had made progress in instituting their business continuity planning program. However, based on our survey, progress has varied considerably among departments and agencies.

1.65 In our survey, we found that 53 departments (65 percent) had business continuity plans, but only 24 (29 percent) had tested them over the last two years. Periodic testing ensures that these plans remain effective.

1.66 The extent to which the four departments that we audited had updated and tested their business continuity plans and evaluated and mitigated the risks varied. Social Development Canada and Industry Canada had a good updating and testing regime, while the National Parole Board and Fisheries and Oceans Canada did not. Similarly, we found differences in the way departments had clarified roles and responsibilities for business continuity planning. As well, except for the National Parole Board, the other departments had developed improved decision-making mechanisms for developing and implementing their business continuity planning program.

Some departments have yet to start monitoring their security

1.67 The Government Security Policy requires departments to continuously monitor their security program, audit it, and report the findings to the Treasury Board Secretariat. The requirements for ongoing monitoring and periodic reporting provide management with information on whether measures to protect the security of IT systems are adequate and appropriate.

1.68 Prior to 2002, the Policy required departments and agencies to audit their IT security at least every five years. In 2002, we observed that, of some 90 departments and agencies subject to the Policy, only 10 had submitted internal audit reports. Most departments (almost 90 percent) had not complied with the Policy requirement.

1.69 The revised Policy continues to require departments and agencies to monitor their security programs. However, they are no longer required to audit their programs at least once every five years. It is now up to departments to decide how often they will audit their programs, as part of their overall planning process.

1.70 Consequently, we were concerned that departments and agencies would not periodically audit their IT security practices. However, we noted some improvement in this area. Thirty-seven departments and agencies (45 percent) that we surveyed had audited their IT security program in the last two years (as opposed to 10 percent in 2002).

Monitoring security practices in departments

In the four departments we examined, practices for monitoring IT security varied from unsatisfactory to non-existent. We also found that when departments carry out IT security reviews, they do not always correct the problems they have identified. These reviews often revealed a lack of compliance with basic security requirements, such as instituting strong passwords and correcting weaknesses that have been identified.

For example, Social Development Canada has a new process to monitor and respond to IT security incidents, as required by the Policy. However, the Department has not defined what constitutes an IT security incident. This prevents consistent reporting and analysis of incidents, and consistent enforcement of the policies and standards.

1.71 **Recommendation.** Departments and agencies, subject to the Government Security Policy, should provide the Treasury Board Secretariat with an annual schedule of their planned IT security monitoring activities, including self-assessments, vulnerability assessments, and internal audits. They should also provide the Secretariat with a copy of internal audit reports, within three months of completing them.

Treasury Board Secretariat's response. The Internal Audit Policy requires departments to have at least an annual internal audit plan, which must be copied to TBS. This Policy also requires deputy heads to ensure that copies of completed audit reports are provided in a timely manner to the Treasury Board Secretariat. According to the Government Security Policy, the results of internal audits must be reported to the TBS.

TBS agrees with this recommendation, which will require departments and agencies to submit an annual schedule of IT security monitoring activities. Review of these schedules by TBS will provide a level of assurance that departments and agencies are performing ongoing monitoring of their departmental ITS activities and ensure that TBS does receive internal audit reports in a timely fashion.

The Secretariat's oversight of the Policy

1.72 The Treasury Board Secretariat has no formal process in place for getting departments and agencies to submit their audit reports or analyzing the security findings of these reports. Since 2002, the Secretariat has received only 10 audit reports on IT security and has not issued a mid-term report, as required by the Government Security Policy. Internal audit reports can be an important element in developing an overall picture of IT security in departments and agencies.

1.73 The revised Policy requires the Secretariat, as part of its overall monitoring, to submit a report to the Treasury Board on how effective the Policy is in strengthening security. The report was due in the summer of 2004

but has not been produced. As a result, little baseline information exists on the state of IT security across the government.

1.74 **Recommendation.** The Treasury Board Secretariat should monitor departments to determine whether they are carrying out timely audits and other IT security monitoring activities.

Treasury Board Secretariat's response. TBS agrees with this recommendation and will work collaboratively with the lead security agencies and departmental representatives to develop a monitoring process that meets this recommendation and provides adequate information.

TBS will find the most effective way to collect the information required for this monitoring by reusing information that departments and agencies are currently providing and requesting only supplemental information as necessary.

1.75 **Recommendation.** The Treasury Board Secretariat should complete the mid-term report on the effectiveness of the Government Security Policy in a timely manner, as required by the Policy.

Treasury Board Secretariat's response. The mid-term report is scheduled to be presented to the Treasury Board in early 2005.

Conclusion

1.76 Overall, the government has made unsatisfactory progress in strengthening information technology security since our audit in 2002.

1.77 The government has made good progress in several areas that we had previously raised concerns about. The 2002 Policy clarified the roles and responsibilities of the various players in IT security. Since then, lead organizations have consulted regularly and are co-operating to develop standards to strengthen IT security practices. The Policy lacked operational standards for departments to meet its various requirements. Since then, the Management of Information Technology Security standard has been developed, along with some other associated standards.

1.78 However, a number of IT security standards remain to be developed and the Secretariat has not completed its mid-term evaluation of the effectiveness of the Policy. Business continuity planning still needs improvement, and most departments and agencies have yet to assess threats and risks adequately.

1.79 Since 2002, the use of the Internet has increased, and portable computer devices and wireless technologies have made access to information easy and affordable. Government systems are more connected, and the government is aiming for greater inter-operability and integration of its business processes. This environment provides more opportunities for problems to occur, such as theft of data, malicious attacks, or criminal

actions. The threats have increased significantly since 2002, and they can cause serious damage to an organization.

1.80 Despite a stronger Policy, new standards, and other examples of progress, the government still needs to address serious weaknesses in IT security. The majority of departments and agencies are not complying with the baseline requirements of the Policy and the associated standards.

1.81 A lack of compliance with the Policy and standards, a lack of awareness of IT security risks, and a lack of understanding how breaches of IT security could affect operations have broad implications. The risk of security breaches that could violate the privacy of Canadians increases. These violations could cause hardship to individuals and erode the trust that Canadians have in the ability of their government to transact business on-line, in a secure and confidential environment.

Government's overall response. Treasury Board Secretariat (TBS) offers the following information to better explain the context within which TBS and the Government of Canada (GoC) departments and agencies are working.

The GoC operates in a dynamically changing risk environment that requires an active and continuous defence against cyber attacks, viruses, and other internet-related threats. While policy and standards are necessary to establish a common posture and constitute one of the key components of the overall federal ITS response, TBS and the three lead security agencies (namely the Communications Security Establishment (CSE), Public Safety and Emergency Preparedness Canada (PSEPC), and Royal Canadian Mounted Police (RCMP)) are also providing practical assistance and guidance to departments and agencies to help them improve their overall Information Technology Security (ITS) posture and to support their ability to act quickly and co-operatively to prevent, detect, and respond to security breaches across the GoC. Like all large and geographically diverse organizations, the dependence of the GoC on a networked and interdependent environment continues to grow. Such an environment will increasingly require a "collective" approach to effective IT security, wherein a department's ability to respond rapidly to a security incident and share information about it will become the hallmark of an enhanced security organization in the 21st century.

There is a growing requirement for individual departments and agencies, as well as the GoC at large, to be more resilient in the face of rapid technological change. This will require the engagement and co-operation of personnel across organizational boundaries, sharing information on incidents, issues, and solutions.

TBS and PWGSC, in conjunction with the lead security agencies, are also leading the move toward the provision and use of common and shared IT security infrastructures and services. Measures such as Intrusion Detection (ID), Vulnerability Assessment (VA), software maintenance, and system development methodologies are more efficiently implemented in a common centrally managed IT infrastructure rather than department-by-department

solutions. The significant investments made by the GoC in common IT services are an important contribution to more effective security for the GoC's operations and services.

The Secure Channel provides a set of common and secure infrastructure services protecting the delivery of information and transactions for individuals, businesses, employees, and other governments. At this time, 122 departments and agencies are using one or more of the Secure Channel service offerings in support of their on-line service and information delivery. Building and maintaining the trust and confidence of our citizens, businesses, and other governments with whom we do business is fundamental to effective service delivery.

With the publication of the National Security Policy (NSP) in 2004 and the development of processes, committees, and organizational structures to meet the objectives of that Policy, TBS will ensure that departments and agencies follow a strategy that supports the integration and co-ordination of plans, activities, infrastructures, and operations. To this end, projects that enable the pro-active sharing of information and processes both within the GoC and across jurisdictions will be key to this integration.

About the Follow-Up

Objective

The objective of this follow-up was to determine whether the Treasury Board Secretariat and departments had implemented the recommendations we made in Chapter 3 of our 2002 Report. We assessed whether, in general, departments and agencies had implemented IT security baseline requirements to protect information technology assets and deliver services securely and without interruption.

Scope and approach

Our audit focussed on two levels:

- **Lead security agency level**. We focussed on the Treasury Board Secretariat, which provides co-ordination, leadership and oversight for IT security. We also met staff from the Royal Canadian Mounted Police, Public Safety and Emergency Preparedness Canada, the Communications Security Establishment, and the Canadian Security Intelligence Services.
- **Departmental level**. We reviewed selected security practices in the four departments we had examined in 2002: Fisheries and Oceans Canada, Social Development Canada (formerly Human Resources Development Canada), Industry Canada, and the National Parole Board.

We looked at the results of a self-assessment questionnaire that the Secretariat conducted in 97 departments and agencies. The self-assessment was voluntary; only 46 departments and agencies responded. The responses were not corroborated with evidence. We complemented the Treasury Board Secretariat survey with a survey of 82 departments and agencies on specific security practices. We obtained a 100 percent response rate and, to validate the answers, we corroborated the positive answers in a random sample of 20 departments and agencies.

We assessed the safeguards that departments and agencies use to ensure the security of government assets and information. We reviewed the results of vulnerability assessments and technical tests done by consultants, the Communications Security Establishment, and our Office (for three departments) as part of this audit. We ensured that our technical tests did not harm the systems we tested or the data they contained.

We looked at the extent to which the following areas of IT security had improved:

- co-operation and information-sharing among lead organizations on IT security,
- development and implementation of IT security standards to support policy,
- effectiveness of the Government Security Policy and existing security measures,
- contingency planning, and
- risk management.

We did not examine the Secure Channel as, at the time of the audit, it had not yet received effective project approval by the Treasury Board. We did not examine national security matters, which will be the subject of a separate audit on national security enhancement initiatives to be reported in 2005.

Criteria

As in our 2002 audit, we expected that

- the framework for IT security ensures that IT assets and information are protected and supports the secure and uninterrupted delivery of government services;
- the governance structure for IT security ensures strong leadership and support from the central and lead agencies, and consistent, cost-effective IT security practices across government;

- policies, standards, and practices are commensurate with the current state of risks and threats to IT security;
- consistent with assessed risks and current security requirements, departmental measures and processes prevent, detect, and respond to IT threats; and
- IT security practices are monitored and periodically reassessed, and vulnerabilities are addressed.

In addition, we expected that new IT security risks are identified and addressed.

Audit team

Assistant Auditor General: Douglas G. Timmins
Principal: Richard Brisebois
Directors: Greg Boyd, Tony Brigandi, Guy Dumas

Bernard Battistin
Etienne Robillard

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