2002

Rapport de la

vérificatrice générale du Canada

à la Chambre des communes

AVRIL

Chapitre 3

La sécurité des technologies de l'information

Le Rapport d'avril 2002 de la vérificatrice générale du Canada comporte huit chapitres, ainsi qu'un Avant-propos et les Points saillants. Vous trouverez la table des matières principale à la fin du présent document.

Dans le présent Rapport, le genre masculin est utilisé sans aucune discrimination et uniquement dans le but d'alléger le texte.

Le Rapport est également disponible sur notre site Web à www.oag-bvg.gc.ca.

Pour obtenir des exemplaires de ce rapport et d'autres publications du Bureau du vérificateur général, adressez-vous au :

Bureau du vérificateur général du Canada
240, rue Sparks, arrêt 10-1
Ottawa (Ontario)
K1A 0G6

Téléphone : (613) 952-0213, poste 5000, ou 1-888-761-5953
Télécopieur : (613) 954-0696
Courriel : distribution@oag-bvg.gc.ca

This document is also available in English.

Nº de catalogue FA1-2002/1-3F
ISBN 0-662-86988-5

Chapitre

3

La sécurité des technologies de l'information

Les travaux de vérification dont traite ce chapitre ont été menés conformément au mandat législatif, aux politiques et aux méthodes du Bureau du vérificateur général du Canada. Ces politiques et méthodes respectent les normes recommandées par l'Institut Canadien des Comptables Agréés.

Table des matières

La sécurité des technologies de l'information

Points saillants

3.1 La version révisée de la Politique du gouvernement sur la sécurité, entrée en vigueur en février 2002, remplace la Politique instaurée en 1994. Elle met fortement l'accent sur la sécurité des technologies de l'information (TI) et contribue largement à l'amélioration de la régie de la sécurité au sein du gouvernement.

3.2 Nous avons constaté que les normes de sécurité des TI qui étayent la Politique sont désuètes et qu'un plan de mise à jour doit encore être dressé. La politique sur la sécurité ne sera pleinement efficace que si les normes sont actualisées et prescrivent les exigences minimales auxquelles les ministères et les organismes doivent satisfaire. Les normes sont un instrument essentiel à l'utilisation de saines pratiques pour la sécurité des TI au sein du gouvernement.

3.3 Qui plus est, on a peu surveillé l'application de la Politique de 1994. En conséquence, le gouvernement ne possède pas suffisamment d'information pour évaluer l'état actuel de la sécurité des TI. Il ne dispose pas non plus d'une base adéquate pour déterminer la mesure dans laquelle les pratiques actuellement utilisées dans l'administration fédérale sont acceptables, ni une base de référence appropriée pour mesurer les progrès futurs. En outre, la version révisée de la Politique prévoit que l'on rende compte de l'efficacité de son application, mais pas avant l'été 2004. Selon nous, ce rapport doit être présenté plus tôt.

3.4 Le gouvernement a pris l'engagement d'offrir aux Canadiens un accès en direct à ses services. Le projet Gouvernement en direct a été lancé pour atteindre cet objectif. Ce projet a suscité des préoccupations majeures au chapitre de la sécurité et de la protection des renseignements personnels, et il importe que les autorités agissent promptement à cet égard afin d'appuyer le projet Gouvernement en direct.

Contexte et autres observations

3.5 Les cybermenaces sont une réalité et elles peuvent causer d'importants dommages. Les attaques récentes au moyen de virus et d'autres types de programmes malveillants ont fait rehausser le profil de la sécurité des TI. Dans le contexte de la sensibilisation accrue à la sécurité nationale, la sécurité des TI est considérée par beaucoup comme vitale pour protéger l'infrastructure essentielle du pays.

3.6 La vérification que nous avons menée dans quatre ministères a révélé un certain nombre de faiblesses qui pourraient donner une certaine idée de l'état actuel de la sécurité des TI au sein du gouvernement. Ces faiblesses pourraient en effet aider le gouvernement à établir des priorités concernant les normes opérationnelles et techniques qu'il élabore à l'appui de la version révisée de sa politique sur la sécurité.

3.7 Les ministères ont mis en place un cadre de régie, mais ils doivent en améliorer la mise en œuvre pour qu'il soit vraiment efficace. C'est particulièrement le cas dans les ministères au sein desquels la responsabilité des systèmes d'information est décentralisée et dans les ministères qui ont formé des partenariats stratégiques et/ou conclu des ententes d'impartition avec d'autres organismes gouvernementaux. Parmi les améliorations qui doivent être apportées pour remédier à certaines faiblesses, nous avons relevé les suivantes :

- mener des évaluations des risques à grande échelle et donner aux employés une formation pertinente afin de les sensibiliser à la sécurité de l'information;
- s'assurer que la sécurité des TI est prise en compte au début du cycle de développement des systèmes et qu'on effectue une surveillance continue de portée adéquate;
- effectuer régulièrement des vérifications et voir à ce que des examens soient menés par des organismes indépendants de façon périodique, notamment des essais techniques pour déceler la vulnérabilité éventuelle des systèmes de réseaux.

Réaction du gouvernement. Le Secrétariat du Conseil du Trésor, au nom du gouvernement, a dans l'ensemble approuvé les recommandations. Le chapitre présente les responses du gouvernement, dans lesquelles celui-ci indique les mesures qu'il prend ou a l'intention de prendre pour donner suite aux recommandations.

Introduction

Les cybermenaces et leurs conséquences éventuelles

3.8 La plupart des grands organismes et des gouvernements sont tributaires des systèmes d'information pour exercer leurs fonctions ou offrir des services. L'utilisation d'Internet prend de l'ampleur à l'échelle mondiale et de nombreux gouvernements commencent à offrir leurs services en direct.

3.9 Au Canada, les systèmes gouvernementaux sont de plus en plus interconnectés. Cette réalité offre de nouvelles possibilités de collaboration, mais s'accompagne également de nouveaux risques pour les ressources d'information. Celles-ci incluent les ordinateurs, les logiciels, le matériel de réseau et de télécommunications et, surtout, les données sous forme électronique.

3.10 Les cyberincidents peuvent faire énormément de dommages au sein d'un organisme. Ils peuvent détériorer les ressources d'information et perturber les activités. Certains incidents nuisent à la productivité; d'autres peuvent entraîner une perte de confiance des consommateurs, nuire à la réputation et à la crédibilité, ou mener directement à la fraude.

3.11 Des mesures relatives à la sécurité des technologies de l'information (TI) s'imposent pour réduire les risques au minimum. En plus de protéger les ressources d'information, la sécurité des TI vise à maintenir la confidentialité, l'intégrité et la disponibilité de l'information — des objectifs importants pour les activités gouvernementales. La plupart des ministères et des organismes gouvernementaux ont en main de l'information de nature délicate, qui exige des restrictions en matière d'accès et est dotée d'exigences liées à la protection des renseignements personnels auxquelles ils doivent satisfaire. L'intégrité des données est fondamentale pour s'assurer que la gestion et l'exécution des programmes s'appuient sur une information valable. Les systèmes d'information font partie de l'infrastructure essentielle du gouvernement, et celui-ci sera de plus en plus tributaire de tels systèmes à mesure qu'il offrira de nouveaux services en direct. Il est désormais absolument nécessaire d'assurer la disponibilité des systèmes d'information pour offrir un service ininterrompu au public.

Les cyberincidents sont une réalité et ils deviennent de plus en plus fréquents

3.12 Les virus informatiques et d'autres programmes malveillants ont récemment mobilisé l'attention des médias et du public. En février 2000, des cyberattaques ont été lancées avec succès contre un certain nombre de sites Web commerciaux très en vue, comme Yahoo! et Amazon.com. Les responsables des attaques ont ciblé les systèmes d'information d'un grand nombre d'organismes dans le monde et ont utilisé ces systèmes pour attaquer simultanément les sites Web visés et les mettre hors d'état.

3.13 De nombreux autres virus et attaques ont été signalés depuis lors, notamment le virus « I love you », qui a surgi en mai 2000, ainsi que les attaques attribuables à « Code Red» et à « Nimda » en 2001. Pour que

certaines attaques soient fructueuses, les victimes sans méfiance doivent ouvrir les pièces jointes au courrier électronique, mais dans le cas d'autres attaques plus insidieuses, il suffit de visualiser le message pour les déclencher.

3.14 De telles attaques peuvent coûter cher aux victimes. Par exemple, les réparations et la perte de production occasionnées par le seul virus « I love you » ont coûté approximativement 8,7 milliards de dollars américains. De plus, il est parfois impossible de déterminer la valeur de l'information perdue.

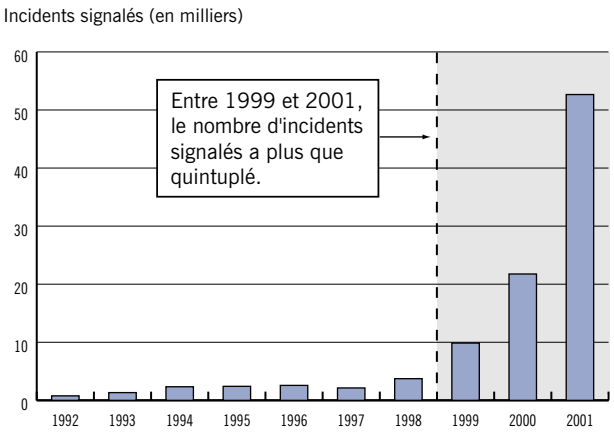
3.15 Les responsables de la sécurité des TI savent qu'il existe des outils logiciels faciles à obtenir et à utiliser pour perpétrer de telles attaques. Les pirates informatiques sont très fiers de les utiliser pour pénétrer dans les systèmes d'information et/ou les mettre hors d'état.

3.16 Les données dont on dispose sur les cyberincidents signalés révèlent l'ampleur de la menace. Des données d'origine américaine indiquent une hausse alarmante des incidents, en particulier ces dernières années. Comme le montre la pièce 3.1, le nombre d'incidents signalés aux États-Unis a plus que quintuplé entre 1999 et 2001, passant de 10 000 environ à quelque 52 700.

3.17 Le gouvernement du Canada a lancé un projet au cours de l'été 1999 afin d'évaluer l'ampleur de la cybermenace à sa présence dans Internet. Un point d'occupation dans Internet de chacun des six ministères a été surveillé, pour une période allant jusqu'à trois mois, et le trafic inhabituel sur le réseau a été relevé et analysé. Cette surveillance a mis en évidence plus de 80 000 alarmes. Une analyse plus poussée des alarmes a permis de repérer plus de 500 tentatives de pénétration dans les systèmes ministériels. La plupart de ces tentatives consistaient en des essais par d'éventuels agresseurs, et un grand nombre d'entre eux avaient utilisé des instruments informatisés.

Point d'occupation dans Internet — Installation ou appareil qui permet d'accéder par Internet aux systèmes de réseaux d'un organisme.

Pièce 3.1 Hausse du nombre de cyberincidents signalés aux États-Unis



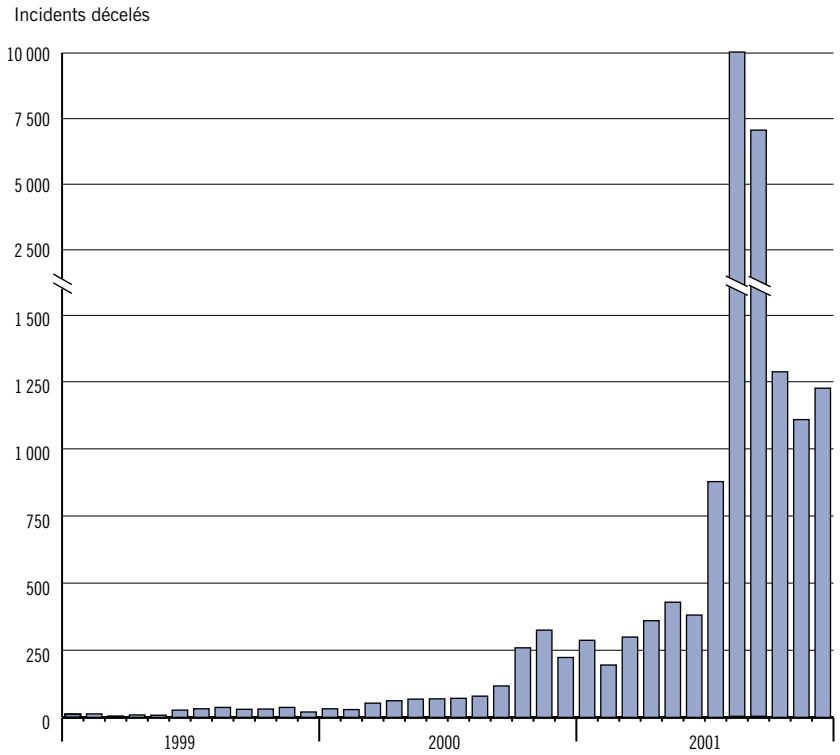
Note : Le Centre compile le nombre de cyberincidents décelés et signalés par des tierces parties.

Source : CERT Coordination Center (États-Unis)

3.18 Même si nous ne disposons pas d'autres données portant précisément sur les systèmes gouvernementaux, la tendance à la hausse du nombre de cyberincidents constatée au Canada (voir la pièce 3.2) se compare à la tendance observée aux États-Unis. Selon les données de CanCERT, un service qui surveille et signale les cyberincidents au Canada, 10 000 incidents ont eu lieu en août 2001 et 7 000, en septembre 2001; les données pour ces deux mois dominent totalement les statistiques de l'année entière (voir la pièce 3.3). Dans un contexte de sensibilisation accrue à la sécurité nationale, les organismes d'exécution de la loi et le public accordent désormais beaucoup plus d'importance aux cyberalertes et aux préoccupations liées à la sécurité des TI.

3.19 Les reportages sur les cyberattaques et l'augmentation phénoménale du nombre de cyberincidents signalés indiquent que les cybermenaces sont une réalité et représentent un danger croissant pouvant occasionner des dommages importants au sein d'un organisme. Qui plus est, étant donné que les systèmes d'information font partie de l'infrastructure essentielle du pays, les cyberattaques font partie des menaces terroristes à la sécurité nationale. La sécurité des TI constitue par conséquent une importante priorité et une grande responsabilité de gestion.

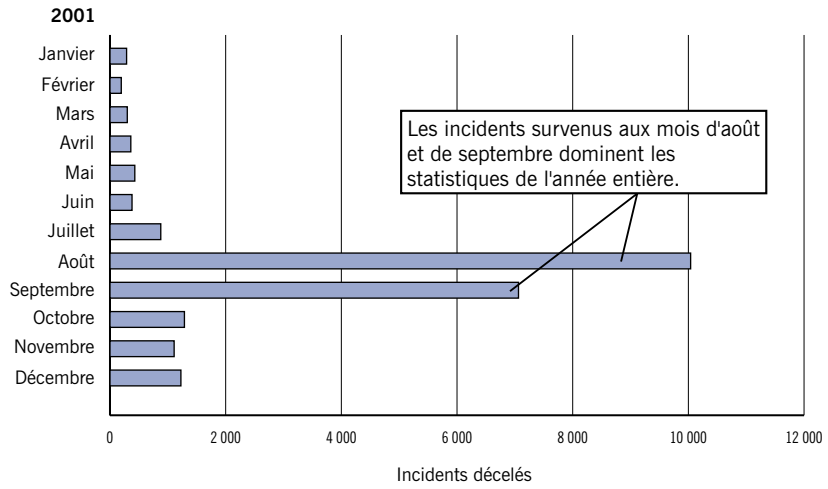
Pièce 3.2 Cyberincidents au Canada de 1999 à 2001



Note : Au Canada, CanCERT surveille les cyberincidents et compile le nombre d'incidents qu'il a décelés.

Source : CanCERT

Pièce 3.3 **Cyberincidents au Canada en 2001**



Source : CanCERT

Objet de la vérification

3.20 La vérification avait pour objectif d'évaluer le cadre de sécurité des technologies de l'information mis en place au sein du gouvernement afin de protéger les ressources d'information et d'assurer la prestation fiable et ininterrompue des services électroniques aux Canadiens. Nous avons examiné le cadre de sécurité des TI à l'échelle gouvernementale ainsi que les pratiques connexes de quatre ministères ou organismes. Les ministères choisis ne devaient pas constituer un échantillon représentatif, mais donner une meilleure idée des pratiques de sécurité des TI au sein du gouvernement.

3.21 Nous avons interviewé le personnel des organismes qui jouent un important rôle directeur dans le domaine de la sécurité des TI à l'échelle gouvernementale et passé en revue des documents et des dossiers connexes. Dans les quatre ministères, nous avons eu des entretiens avec les employés exerçant des responsabilités liées à la sécurité et/ou aux TI. Nous avons soumis les réseaux de quelques ministères à des tests techniques à distance.

3.22 La section intitulée À propos de la vérification, à la fin du chapitre, présente des détails additionnels sur l'objectif, l'étendue, la méthode et les critères de la vérification.

Observations et recommandations

Cadre à l'échelle de l'administration fédérale

3.23 Au même titre que les autres questions importantes qui touchent tous les ministères et organismes, la sécurité des TI exige un bon cadre de régie, qui définit les responsabilités en matière de leadership, précise les rôles des divers organismes responsables et de chaque ministère, et établit les liens redditionnels. La Politique du gouvernement sur la sécurité (PGS) présente le cadre de régie pour tous les aspects de la sécurité, y compris la sécurité des TI.

Le Secrétariat du Conseil du Trésor est responsable de la Politique, dont les dispositions s'appliquent à tous les ministères et organismes.

3.24 La Politique du gouvernement sur la sécurité et les directives qui s'y rattachent se subdivisent en trois niveaux. La politique de sécurité globale occupe le niveau supérieur. Elle prescrit les exigences concernant la protection du personnel et des biens du gouvernement, ainsi que les rôles et les responsabilités des organismes responsables. Le deuxième niveau présente les normes et les pratiques opérationnelles en matière de sécurité, et le troisième niveau définit les normes et les pratiques techniques à ce chapitre.

Mise à jour complète de la Politique du gouvernement sur la sécurité

3.25 La première version de la Politique du gouvernement sur la sécurité est entrée en vigueur en 1986, et elle a été révisée en 1994. Depuis 1994, les technologies de l'information ont fait d'énormes progrès. Au Canada, l'utilisation d'Internet et de diverses applications est devenue un phénomène important. Pour respecter l'engagement qu'il a pris de devenir le gouvernement le plus branché avec ses citoyens, le gouvernement fédéral a lancé le projet Gouvernement en direct afin d'offrir ses services dans Internet. Cette évolution n'est pas sans nouveaux risques et défis pour la sécurité. En outre, à la fin des années 1990, le gouvernement a commencé à définir l'infrastructure essentielle du Canada. Les responsables de la révision de la PGS en 1994 n'avaient pas envisagé toutes ces questions liées à la sécurité des TI.

Gouvernement en direct — Projet du gouvernement du Canada, dont l'objectif est d'assurer la prestation en direct des services à la population canadienne.

3.26 Le Secrétariat du Conseil du Trésor a reconnu que la Politique ne couvrait pas suffisamment les questions courantes liées aux technologies de l'information et à l'infrastructure essentielle. En avril 2000, il a amorcé un examen complet de la Politique, en quatre étapes. La première étape consisterait à déceler les lacunes de la Politique en vigueur. La deuxième étape viserait à formuler des recommandations sur la portée de la révision afin de combler les lacunes et à apporter les changements préconisés. La troisième étape consisterait en une présentation au Conseil du Trésor aux fins de l'approbation de la version révisée de la Politique, et la quatrième étape viserait à communiquer la version révisée de la Politique et les normes connexes et à en assurer la mise en œuvre.

3.27 Après avoir mené un sondage auprès des ministères et des organismes, le Secrétariat a répertorié les lacunes de la Politique de 1994, tâche qu'il a achevée en juin 2000. La deuxième étape a fait appel à une centaine de participants, de tous les secteurs du gouvernement, qui ont siégé à des groupes de travail et à des comités. En novembre 2000, ils ont recommandé que la version révisée de la politique sur la sécurité couvre les sujets suivants :

- les exigences concernant la sécurité des TI à l'échelle gouvernementale, pour protéger les systèmes interconnectés et assurer la prestation électronique sécurisée des services à la population canadienne;
- la disponibilité et l'intégrité de l'information et des systèmes de TI;
- un cadre de régie clair prévoyant le contrôle accru de la Politique et une surveillance renforcée de la part de la haute direction;

- une présélection de sécurité améliorée et une protection accrue du personnel contre les menaces et les actes de violence.

Des ébauches de la Politique ont été mises en circulation au sein des ministères et des organismes. Les consultations se sont terminées en octobre 2001. Le Conseil du Trésor a donné son aval à la version révisée de la Politique et l'a approuvée le 6 décembre 2001. La version révisée de la Politique du gouvernement sur la sécurité est entrée en vigueur le 1er février 2002.

Le cadre de régie pour la sécurité des technologies de l'information au sein du gouvernement est défini dans la version révisée de la Politique

3.28 Le document principal de la Politique de 1994 fait très peu allusion à la sécurité des TI. Plus précisément, on ne définit pas le cadre de régie pour la sécurité des TI à l'échelle du gouvernement. Les administrateurs généraux étaient chargés d'assurer la protection des employés et des biens de leur ministère, mais la responsabilité de la sécurité des TI à l'échelle de l'administration fédérale était limitée. L'examen de la Politique en 2000 a fait ressortir cette lacune, et on a recommandé qu'elle soit comblée dans le cadre du processus de révision.

3.29 La version de la Politique de 2002 tient toujours les administrateurs généraux responsables de la mise en œuvre de la Politique et de la protection des employés et des biens qui relèvent de leur compétence. Nous avons remarqué que le Secrétariat du Conseil du Trésor avait un rôle de leadership précis dans le domaine de la sécurité des TI à l'échelle de l'administration fédérale. Parmi ses responsabilités, mentionnons l'élaboration et la mise à jour de la Politique, l'établissement d'une orientation stratégique, le leadership et la prestation de conseils, ainsi que la surveillance de la mise en œuvre de la Politique et la présentation de rapports au Conseil du Trésor sur son application et l'état de la sécurité au gouvernement.

3.30 Le personnel du Secrétariat a fait savoir qu'il avait l'intention de recourir aux groupes de travail et aux comités qui ont élaboré la Politique de 2002 pour préparer des directives et des conseils sur les questions liées à la sécurité des TI. La structure proposée prévoit un comité consultatif de la politique sur la sécurité, un comité de coordination de la politique et plusieurs groupes de travail s'occupant de la sécurité.

3.31 Dans la version révisée de la Politique du gouvernement sur la sécurité, les rôles et les responsabilités des dix ministères et organismes qui jouent un rôle d'organisme responsable en matière de sécurité ont été mis à jour. Outre les trois organismes responsables que nous avons interviewés — la Gendarmerie royale du Canada, le Centre de la sécurité des télécommunications et le Bureau de la protection des infrastructures essentielles et de la protection civile — les dix ministères et organismes en question comptent le Service canadien du renseignement de sécurité, le ministère de la Défense nationale et le ministère des Affaires étrangères et du Commerce international.

3.32 Le cadre de régie pour la sécurité des TI, qui est défini dans la version révisée de la Politique, comble une importante lacune de la Politique de 1994. Il précise le leadership et le soutien requis pour instaurer et conserver des pratiques efficaces en matière de sécurité des TI au gouvernement. Qui plus est, il traite précisément de l'importance que revêt la sécurité des TI pour la sécurité globale au sein du gouvernement. La sécurité des TI comporte plusieurs objectifs, dont la protection de la confidentialité, de l'intégrité et de la disponibilité des ressources d'information — tous des éléments importants pour les opérations gouvernementales. Le cadre de régie défini dans la version révisée de la Politique du gouvernement sur la sécurité de 2002 est un point de départ important; il répond à nos attentes car il prévoit un leadership et un soutien adéquats pour assurer une sécurité des TI cohérente et rentable à l'échelle de l'administration fédérale.

Il faut accélérer la mise à jour des normes et des pratiques liées à la sécurité des technologies de l'information

3.33 La Politique du gouvernement sur la sécurité comporte trois niveaux. Le niveau supérieur fournit le cadre obligatoire et s'appuie sur les normes opérationnelles et techniques des deux autres niveaux. Les énoncés de politique se rapportent aux exigences de base en matière de sécurité, auxquelles les ministères et les organismes doivent satisfaire, c'est-à-dire des normes minimales. Selon la version révisée de la Politique, le Secrétariat peut approuver la mise à jour des normes opérationnelles sans obtenir l'autorisation préalable du Conseil du Trésor.

3.34 Nous nous attendions à ce que les normes et les pratiques opérationnelles et techniques liées à la sécurité des TI soient tenues à jour et à ce qu'elles correspondent aux niveaux actuels de risques et de menaces pour la sécurité des TI.

3.35 Les normes opérationnelles en vigueur pour la sécurité des TI ont été publiées en 1994 et la dernière mise à jour date de 1995. Les normes et les pratiques en question ne précisent pas les exigences liées à la protection contre les risques et les menaces qui découlent de l'interconnectivité et de l'utilisation croissantes d'Internet au gouvernement. La *Norme de sécurité technique dans le domaine de la technologie de l'information*, publiée par la Gendarmerie royale du Canada (GRC) en 1997, constitue actuellement un ensemble d'exigences de troisième niveau de la Politique du gouvernement sur la sécurité. Ces normes ont été élaborées avant que le projet Gouvernement en direct soit lancé, et elles ne sont pas à jour.

3.36 Le Secrétariat du Conseil du Trésor est chargé de diriger et de coordonner la mise à jour des normes opérationnelles et techniques relatives à la sécurité des TI. Pendant la vérification, nous avons constaté que le Secrétariat avait commencé à s'attaquer aux lacunes décelées dans les normes et pratiques de sécurité des TI, dans le cadre de la révision de la Politique de 1994. Néanmoins, il s'est ensuite occupé surtout à terminer le document de politique de premier niveau, si bien que les travaux concernant les normes et les pratiques ont peu progressé.

3.37 Nous avons demandé à consulter les plans et le calendrier du Secrétariat pour la mise à jour des normes de 1995 et de 1997. À la fin de notre vérification, ces plans et ce calendrier n'étaient pas encore terminés. Quant aux plans de communication et de mise en œuvre de la Politique du gouvernement sur la sécurité de 2002, ils étaient toujours en cours d'élaboration.

3.38 Des normes opérationnelles et techniques à jour sont essentielles à la sécurité des TI au sein du gouvernement. Elles constituent les exigences de base et sont le fondement de la prise de mesures cohérentes pour la sécurité des TI dans l'ensemble de l'administration fédérale. De plus, elles sont un moyen de contrôler et de surveiller les pratiques de sécurité. Nous avons constaté que certains éléments des normes opérationnelles de 1995 ne sont pas entièrement compatibles avec la version révisée de la Politique. Le Secrétariat du Conseil du Trésor nous a informés qu'il a mis l'accent sur un certain nombre de grands projets pour soutenir Gouvernement en direct. Ces projets permettent d'élaborer certaines normes de sécurité et, une fois achevés, ils contribueront à offrir un milieu sûr pour la prestation de services en direct à la population canadienne.

3.39 Les ministères et les organismes doivent connaître les exigences de base pour déterminer les mesures de sécurité à prendre et les ressources nécessaires pour les mettre en œuvre. L'absence de normes opérationnelles et techniques à jour nuira à l'efficacité de la Politique du gouvernement sur la sécurité de 2002. Il est donc important d'accélérer la mise à jour de ces normes.

3.40 **Recommandation.** Le Secrétariat du Conseil du Trésor devrait accélérer l'élaboration d'exigences de base pour la sécurité des technologies de l'information afin de soutenir la Politique du gouvernement sur la sécurité de 2002. Il devrait envisager d'accorder la priorité à diverses exigences en matière de sécurité et de mettre à jour les normes selon leur pertinence.

Réponse du gouvernement. Le Secrétariat du Conseil du Trésor convient qu'il est nécessaire d'accélérer l'élaboration de normes pour la sécurité des technologies de l'information afin de soutenir la Politique du gouvernement sur la sécurité et il s'y engage dans la mesure où il dispose de ressources à cette fin. Le Secrétariat pense aussi qu'il fallait, avant que l'on puisse élaborer des normes pour la sécurité afin de répondre aux besoins du gouvernement dans son ensemble et des ministères, achever la plupart des travaux entrepris au cours des dernières années dans le cadre du projet Gouvernement en direct — par exemple la conception de l'Infrastructure à clés publiques, le Programme d'architecture fédérée et la Voie de communication protégée — et effectuer l'examen détaillé des questions liées à la sécurité des TI qui a mené à la refonte de la Politique du gouvernement sur la sécurité. Cette approche est conforme à la documentation publiée dans les secteurs privé et public, qui recommande d'utiliser des plans d'architecture au niveau de l'entreprise pour l'élaboration des normes, des exigences de base au niveau du réseau et de la politique de sécurité globale.

Contrôle et surveillance

3.41 Lors de la vérification, c'étaient la Politique du gouvernement sur la sécurité de 1994 et les normes opérationnelles de 1995 sur la sécurité des TI qui étaient en vigueur. La version révisée de la Politique n'a pris effet qu'en février 2002, alors que notre vérification était terminée. Nous avons mené notre vérification en regard des exigences de contrôle de la Politique de 1994 et examiné les dispositions révisées relatives au contrôle et à la surveillance. Dans les deux cas, nous nous attendions à ce que les pratiques de sécurité des TI soient contrôlées et évaluées, et à ce que des mesures correctives soient prises au besoin.

Le contrôle et la surveillance à l'échelle de l'administration fédérale ont fait défaut

3.42 Un contrôle permanent et des rapports périodiques permettent d'informer la direction de la pertinence et du bien-fondé des mesures prises pour assurer la sécurité des systèmes de TI et de l'information qu'ils contiennent.

3.43 La Politique de 1994 obligeait les ministères et les organismes à effectuer, au moins une fois tous les cinq ans, des vérifications internes portant sur la sécurité des TI. Les normes opérationnelles de 1995 appuyaient cette exigence. Les vérifications internes devaient porter sur l'efficacité des mesures de sécurité des TI et sur la conformité à la Politique et aux normes opérationnelles connexes. Les ministères et les organismes devaient soumettre leurs rapports de vérification interne au Secrétariat du Conseil du Trésor.

3.44 Nous avons cherché les rapports de vérification interne sur la sécurité des TI présentés au Secrétariat au cours des cinq dernières années. Des quelque 90 ministères et organismes assujettis à la Politique du gouvernement sur la sécurité, seulement 10 avaient présenté des rapports. La majorité des ministères (à peu près 90 p. 100) avaient omis de se conformer à cette exigence de la Politique.

3.45 Nous n'avons trouvé aucune information prouvant que le Secrétariat avait exercé un suivi pour s'assurer que des vérifications internes sur la sécurité des TI étaient effectuées régulièrement. En outre, aucune indication ne laissait entendre que le Secrétariat avait examiné et analysé les résultats des dix rapports qui lui avaient été soumis, de façon à s'informer de l'état de la sécurité des TI dans ces ministères et organismes.

3.46 La Politique de 1994 et les normes relatives à la sécurité des TI exigeaient également que les ministères et les organismes demandent à la GRC d'examiner, au moins une fois tous les cinq ans, leurs pratiques de sécurité des TI. Qui plus est, les examens de la GRC devaient être effectués encore plus fréquemment lorsque les systèmes d'information contenaient une information classifiée ou des renseignements considérés comme extrêmement délicats.

3.47 Nous avons constaté que, depuis 1996, seulement 14 ministères et organismes avaient demandé à la GRC d'examiner leurs pratiques de sécurité des TI. Environ 85 p. 100 des ministères assujettis à la Politique avaient omis de se conformer à cette exigence.

3.48 La Politique de 1994 exigeait qu'à la demande du Secrétariat du Conseil du Trésor, la GRC lui présente un rapport sur l'état de la sécurité des TI au gouvernement, rapport que la GRC devait préparer en s'appuyant sur ses examens. La dernière fois que la GRC a présenté un tel rapport remonte à 1995. Le Secrétariat n'a plus formulé ce genre de demande depuis.

3.49 La portée des lacunes décelées ne se limite pas à la non-conformité à la politique gouvernementale. Faute de rapports de vérification interne ministériels et de rapports préparés par la GRC, le gouvernement ne disposait pas de l'information requise pour évaluer l'état global de la sécurité des TI. Sans cette information, il n'était pas en mesure d'assurer un contrôle et une surveillance efficaces de la sécurité des TI dans l'ensemble des ministères.

Les dispositions révisées n'exigent pas de surveillance en temps opportun

3.50 La Politique du gouvernement sur la sécurité de 2002 apporte un certain nombre de changements aux exigences concernant le contrôle et la surveillance. En effet, le Secrétariat est désormais chargé de surveiller la mise en œuvre de la Politique et de déterminer l'état de la sécurité au sein du gouvernement, y compris la sécurité des TI, et d'en rendre compte au Conseil du Trésor.

3.51 Selon la version révisée de la Politique, les ministères et les organismes doivent surveiller activement leurs programmes de sécurité, effectuer des vérifications internes et communiquer les résultats au Secrétariat du Conseil du Trésor. Toutefois, l'obligation de mener une vérification interne au moins une fois tous les cinq ans a été supprimée. La Politique ne définit pas clairement la notion de « surveillance active ». Des normes opérationnelles doivent encore être mises à jour et aucune autre directive n'est fournie.

3.52 Le principal document de politique ne rend plus la GRC responsable des examens de la sécurité des TI au sein des ministères et des organismes. À titre de mesure préventive contre les menaces à la sécurité, les ministères sont tenus de faire évaluer régulièrement leurs programmes et leurs pratiques de sécurité par un organisme indépendant. Là encore, il n'existe plus d'exigence quant à la fréquence minimale de ces évaluations indépendantes.

3.53 Étant donné l'importance de la sécurité des TI et l'incidence éventuelle des menaces à celle-ci, nous nous attendions à ce que la surveillance soit renforcée à l'issue de la révision de la Politique du gouvernement sur la sécurité. Ce n'est toutefois pas le cas.

3.54 La majorité des ministères et organismes ont omis de se conformer à l'exigence établie en vertu de la Politique de 1994 quant à la fréquence minimale des vérifications internes et des examens par la GRC portant sur la sécurité des TI. Maintenant qu'on ne précise plus la fréquence minimale des vérifications et des évaluations indépendantes, il est moins sûr que les pratiques de sécurité des TI dans les ministères et les organismes soient suffisamment contrôlées.

3.55 Qui plus est, un grand nombre de ministères et d'organismes font face au défi consistant à s'assurer que leurs services de vérification interne possèdent la capacité et l'aptitude à se conformer à la Politique de vérification interne adoptée récemment. Dans le passé, la GRC offrait gratuitement un service d'examen de la sécurité des TI aux ministères et aux organismes; seuls le temps supplémentaire et les frais de déplacement étaient facturés. Les évaluations de la sécurité des TI par des tierces parties seront en concurrence avec d'autres priorités des ministères en ce qui a trait à leur financement, car aucuns fonds additionnels n'ont été octroyés aux ministères ou organismes pour la mise en œuvre de la Politique de 2002.

3.56 Dans le cadre de la surveillance globale, le Secrétariat est tenu de produire un rapport de mi-parcours au Conseil du Trésor pour l'informer de l'efficacité de la Politique du gouvernement sur la sécurité. Étant donné que la Politique vient d'entrer en vigueur, le Secrétariat n'est pas tenu de présenter un rapport avant l'été 2004.

3.57 Au sein d'une organisation aussi vaste et diversifiée que le gouvernement du Canada, il n'est pas déraisonnable de mettre à jour tous les 24 mois l'information sur l'état de la sécurité des TI. Néanmoins, depuis la révision de la Politique du gouvernement sur la sécurité de 1994, le contrôle et la surveillance à l'échelle de l'administration fédérale ont été limités. En conséquence, l'information de base sur l'état de la sécurité des TI à l'échelle du gouvernement est limitée.

3.58 Faute d'information suffisante, il est difficile de repérer les éventuelles lacunes concernant la sécurité de l'infrastructure des TI au sein du gouvernement. Il est également difficile de déterminer la mesure dans laquelle la politique sur la sécurité des TI, ainsi que les normes et les directives connexes, sont suffisantes et pertinentes. Qui plus est, il faudra absolument disposer de données de base convenables pour mesurer les progrès réalisés au fil du temps dans les pratiques utilisées au sein du gouvernement pour assurer la sécurité des TI.

3.59 Les hauts fonctionnaires reconnaissent l'importance que revêt la sécurité des TI. Les systèmes et les ressources d'information sont une importante composante de l'infrastructure essentielle du pays. En outre, la sécurité des TI est un enjeu de taille qui s'inscrit dans le projet Gouvernement en direct, lequel a pour objectif de brancher les Canadiens et de leur offrir des services en direct. Nous craignons que l'information de base sur l'état de la sécurité des TI au sein du gouvernement ne soit pas disponible ou communiquée avant 2004.

3.60 **Recommandation.** Le gouvernement devrait recueillir et analyser de l'information sur la sécurité des technologies de l'information au sein des ministères et des organismes afin d'évaluer, plus tôt que ne l'exige actuellement la politique sur la sécurité, l'état de la sécurité à l'échelle de l'administration fédérale. Cela permettra :

- d'établir des priorités en ce qui a trait à l'élaboration de directives concernant les normes et les pratiques;

- d'établir une base de référence pour déterminer les améliorations qui s'imposent et évaluer les progrès ultérieurs;
- de s'attaquer aux principales lacunes suffisamment tôt pour soutenir le projet Gouvernement en direct.

Le gouvernement devrait également songer à préciser, dans sa politique sur la sécurité, la fréquence à laquelle devraient être effectuées les vérifications internes et les évaluations indépendantes des pratiques de sécurité des TI.

Réponse du gouvernement. Le Secrétariat du Conseil du Trésor (SCT) approuve cette recommandation dans l'ensemble. Au moment de la refonte de la Politique du gouvernement sur la sécurité, le SCT a tenu de vastes consultations auprès des ministères et des organismes sur les capacités et les exigences ministérielles en matière de sécurité des TI et convient qu'il est souhaitable de recueillir l'information de manière plus systématique. En février 2001, le gouvernement a créé le Bureau de la protection des infrastructures essentielles et de la protection civile (BPIEPC) qui constituera une capacité centrale pour les stratégies de surveillance et correctives « en temps réel » concernant les atteintes à la sécurité des TI au niveau des réseaux et du ministère. De plus, le SCT commence à élaborer de nouveaux outils d'évaluation que les ministères pourront utiliser pour évaluer et surveiller de manière continue la sécurité des TI et les pratiques de gestion de la sécurité. Le SCT estime, cependant, que les ministères sont les mieux placés pour déterminer quand et à quelle fréquence il y a lieu de faire des vérifications internes et des évaluations indépendantes de la sécurité des TI, comme il est indiqué dans la Politique révisée du gouvernement sur la sécurité.

Soutien à l'échelle de l'administration fédérale

La révision de la Politique a permis de combler des lacunes et d'éliminer le chevauchement dans les rôles de soutien

3.61 Dans le cadre de régie, la Politique de 2002 énonce les responsabilités des dix ministères et organismes qui jouent un rôle de chef de file en matière de sécurité.

3.62 La Politique attribue les mêmes responsabilités à un certain nombre de ministères et organismes directeurs qui ont toujours apporté un soutien au chapitre la sécurité des TI. Par exemple, la GRC est toujours chargée de fournir des conseils sur la façon de mener des examens, des inspections et des vérifications de la sécurité des TI.

3.63 La Politique du gouvernement sur la sécurité de 2002 a permis de régler les problèmes de double emploi qui existaient dans la Politique de 1994. Selon la version révisée de la Politique, la GRC est le seul organisme chargé de fournir des conseils sur le processus d'évaluation de la menace et des risques. Les rôles en matière de formation et de sensibilisation ont aussi été clarifiés. La GRC prépare des programmes de formation et de sensibilisation aux TI et les offre aux utilisateurs des systèmes et au personnel de soutien technique ainsi qu'aux agents chargés de la sécurité des TI. Le Centre de la sécurité des télécommunications est pour sa part chargé de la formation technique et spécialisée dans des domaines comme la sécurité des

Évaluation de la menace et des risques — Processus permettant à un organisme d'établir la valeur d'une application et d'évaluer les risques inhérents qu'elle présente en matière de sécurité.

communications, la vulnérabilité des réseaux et d'autres mesures de protection techniques. Qui plus est, la Politique révisée clarifie les responsabilités respectives de plusieurs organismes directeurs représentant le gouvernement fédéral au sein de comités nationaux et internationaux œuvrant dans le domaine de la sécurité.

3.64 La Politique énonce également les nouvelles responsabilités en matière de soutien. Par exemple, le Bureau de la protection des infrastructures essentielles et de la protection civile est le centre qui reçoit les comptes rendus des ministères sur les menaces réelles ou imminentes, et il donne des alertes et des avis aux ministères et aux organismes. Dans son rôle de soutien, le Bureau fournit des conseils sur l'établissement et la tenue de plans de continuité des opérations.

Plan de continuité des opérations — Plan prévoyant la reprise des opérations essentielles après la perte ou la détérioration sérieuse des installations d'un organisme ou des conditions de travail.

Certains rôles de soutien demandent davantage de temps pour devenir pleinement efficaces

3.65 De nombreux rôles de soutien définis dans la version révisée de la Politique sont exercés depuis un certain temps déjà. Les organismes conseils ont déjà les capacités requises pour fournir ce soutien et sont en mesure de le faire. Voici quelques exemples :

- le Centre de la sécurité des télécommunications évalue l'équipement cryptographique et accrédite les installations d'essai et d'évaluation du secteur privé;
- le Service canadien du renseignement de sécurité mène des enquêtes sur les menaces à la sécurité nationale et les analyse;
- la GRC élabore des technologies pour la sécurité des TI et des mesures pour contrer la cybercriminalité.

3.66 Ce n'est que récemment que l'on a attribué certains rôles de soutien. Par exemple, le Bureau de la protection des infrastructures essentielles et de la protection civile est un nouvel organisme qui a vu le jour en février 2001, et qui a pour mandat d'élaborer et de mettre en œuvre une méthode globale afin de protéger l'infrastructure essentielle du Canada. Il exerce plusieurs nouvelles fonctions, essentielles à l'appui de la sécurité des TI au gouvernement. Outre les fonctions déjà décrites, le Bureau aide les ministères et les organismes à évaluer la vulnérabilité de leurs réseaux informatiques et il offre des conseils sur la protection des systèmes d'information et des infrastructures essentielles aux activités gouvernementales. Ce nouvel organisme a déterminé et obtenu les ressources dont il a besoin pour remplir son mandat, mais il lui faudra du temps avant de pouvoir apporter un soutien total en sa qualité d'organisme responsable en matière de sécurité. Le Bureau doit notamment recruter des employés spécialisés. Dans son rôle de soutien, il dépend en grande partie de l'efficacité de la coordination et de la coopération avec les ministères et les organismes, mais il faudra du temps pour y parvenir.

3.67 Le partage des bonnes pratiques aide les ministères et les organismes à prendre connaissance des solutions adoptées par d'autres ministères en matière de sécurité et leur permet de tirer parti de l'expérience de ces ministères en regard de ces solutions. Le gouvernement dispose d'un certain nombre de mécanismes pour partager l'information sur la sécurité des TI et il

arrive que les participants en profitent pour partager les pratiques et les solutions. Toutefois, la version révisée de la Politique ne définit aucun rôle de soutien en ce qui touche l'acquisition de bonnes pratiques en matière de sécurité des TI ou leur partage et leur promotion au sein de l'administration fédérale.

3.68 La Politique du gouvernement sur la sécurité de 2002 ne prévoit pas l'évaluation de la fonction de soutien. Selon nous, il est utile d'examiner la pertinence du soutien offert par les organismes responsables en matière de sécurité, de façon que le gouvernement puisse cibler des efforts et des investissements supplémentaires, au besoin, pour améliorer le soutien aux ministères et aux organismes.

3.69 **Recommandation.** Le gouvernement devrait planifier un examen du soutien que fournissent les organismes responsables en matière de sécurité des TI afin d'en déterminer la pertinence et, le cas échéant, d'améliorer ce soutien. De plus, le gouvernement devrait explorer et définir des moyens d'acquérir et de partager les bonnes pratiques en matière de sécurité des TI au sein des ministères et des organismes.

Réponse du gouvernement. Le budget du 10 décembre 2001 prévoyait d'importants investissements, destinés aux organismes responsables en matière de sécurité, pour un large éventail de projets liés à la sécurité, y compris la sécurité des TI; pour sa part, la Politique du gouvernement sur la sécurité précise leurs rôles et responsabilités. Le gouvernement reconnaît qu'il est nécessaire de trouver et de définir des moyens de mieux déterminer et de mieux communiquer aux ministères et organismes les meilleures pratiques de sécurité des TI. Les programmes éducatifs et les activités d'apprentissage offerts par la Gendarmerie royale du Canada et le Centre de la sécurité des télécommunications (y compris le symposium international annuel du Centre) jouent un rôle important en ce qui concerne la sécurité du gouvernement, les TI et les programmes. Ils complètent le choix très varié de cours et de conférences offerts par le secteur privé et les associations professionnelles. En outre, le BPIEPC nouvellement créé a déjà montré qu'il s'acquitte de sa responsabilité en diffusant l'information la plus récente sur les menaces, les tendances et les meilleures pratiques au moyen de conférences téléphoniques régulières, de services offerts sur son site Web et d'alertes ponctuelles. Le Secrétariat du Conseil du Trésor a commencé à préparer des plans pour un répertoire des meilleures pratiques recommandées de même qu'un portail de sécurité des TI afin de faciliter l'échange régulier d'information entre les ministères et les organismes.

La régie et la gestion des risques dans les ministères

3.70 Nous nous sommes penchés sur les questions de sécurité des TI à l'échelle du gouvernement, mais nous avons également examiné les pratiques de sécurité des TI dans quatre ministères et organismes, à savoir Pêches et Océans Canada, Développement des ressources humaines Canada (DRHC), Industrie Canada et la Commission nationale des libérations conditionnelles.

3.71 Ces quatre entités présentent divers milieux opérationnels. À DRHC et à Industrie Canada, la gestion des infrastructures technologiques est centralisée tandis qu'à Pêches et Océans Canada, l'approche est

décentralisée. La Commission nationale des libérations conditionnelles a conclu un partenariat stratégique avec Service correctionnel Canada, et elle utilise les systèmes de réseaux et les opérations informatiques de celui-ci.

3.72 Notre examen avait pour objectif de donner un aperçu des pratiques actuelles de sécurité des TI au gouvernement (consulter la partie intitulée À propos de la vérification). Il ne visait pas à tirer des conclusions au niveau ministériel ou gouvernemental, et nous n'avons tiré aucune conclusion de cet ordre.

Il faut mettre à jour les politiques et améliorer la mise en œuvre du cadre de régie à l'échelle ministérielle

3.73 Une politique globale sur la sécurité des technologies de l'information établit le cadre qui permet d'assurer une protection adéquate des ressources d'information et de l'infrastructure technologique. Étant donné la rapide évolution des technologies de l'information, nous nous attendions à ce que des politiques et des normes sur la sécurité des TI soient non seulement élaborées, mais tenues à jour.

3.74 La Politique du gouvernement sur la sécurité ainsi que les normes opérationnelles et techniques connexes établissent les exigences minimales que les ministères et les organismes doivent respecter. Ceux-ci sont tenus de s'appuyer sur ces normes de base pour élaborer leurs propres politiques, qui répondent aux besoins de sécurité particuliers de leurs activités.

3.75 Les quatre ministères que nous avons examinés se sont dotés de politiques sur la sécurité des TI. DRHC a utilisé la Politique du gouvernement sur la sécurité et les normes connexes pour élaborer ses propres politiques et normes sur la protection contre les menaces visant ses ressources d'information et ses activités. Nous avons constaté que les politiques avaient été actualisées et que des efforts étaient déployés pour les tenir à jour.

3.76 Les trois autres ministères utilisent essentiellement la Politique du gouvernement sur la sécurité et les normes connexes. Leurs dirigeants ont trouvé cette politique et les normes acceptables pour leur organisme, mais nous n'avons trouvé aucun document ni analyse étayant cette décision. Comme nous l'avons déjà fait remarquer, la dernière mise à jour de la Politique du gouvernement sur la sécurité effectuée avant février 2002 remonte à 1994, et l'élaboration des normes est antérieure à de nombreux développements qui ont récemment touché l'utilisation d'Internet. Industrie Canada et Pêches et Océans Canada publient tous les deux des bulletins sur des questions précises concernant la sécurité des TI. Toutefois, ces bulletins sont préparés de façon ponctuelle. Ils pourraient ne pas avoir une portée suffisante pour constituer, avec les politiques et les normes sur la sécurité, une série complète et à jour de politiques et de normes. Nous avons également remarqué que les ministères avaient repéré des lacunes dans la politique, mais n'avaient pas encore pris de mesures pour les combler.

3.77 En vertu de la Politique du gouvernement sur la sécurité, les administrateurs généraux sont responsables de la sécurité dans leur sphère de compétence. La Politique exige également que chaque ministère et que chaque organisme nomme un agent de sécurité ministériel ainsi qu'un coordonnateur de la sécurité des TI.

3.78 Nous avons constaté que les quatre ministères avaient nommé des coordonnateurs de la sécurité des TI qui, dans une certaine mesure, entretiennent des liens hiérarchiques avec les agents de sécurité ministériels. Toutefois, ce n'est qu'à Industrie Canada et à DRHC que les coordonnateurs ont défini des rôles et des responsabilités visant à faciliter l'élaboration, la mise en œuvre et le respect des politiques sur la sécurité des TI.

3.79 À Pêches et Océans Canada, le coordonnateur de la sécurité des TI est chargé d'élaborer le programme de sécurité des TI pour le Ministère. Néanmoins, ce coordonnateur a des pouvoirs limités pour en assurer le respect. Nous avons constaté que la conformité à la politique dans la région du Pacifique du Ministère était sélective. Par exemple, il a mis en œuvre certains aspects de la politique portant sur les mots de passe pour accéder aux réseaux, sans toutefois exiger que ces mots de passe soient changés tous les 90 jours. Il se pourrait que le Ministère ait des raisons justifiant cette omission, mais elles n'étaient pas consignées, et nous ne voyons aucune raison de ne pas suivre la procédure régulière.

3.80 La Commission nationale des libérations conditionnelles a conclu un partenariat stratégique avec Service correctionnel Canada, et elle utilise les réseaux et les opérations informatiques de celui-ci. L'efficacité de son programme de sécurité des TI dépend donc de son partenaire. Selon cette entente de partenariat, Service correctionnel Canada est appelé à gérer des données délicates de la Commission concernant les libérations conditionnelles. Nous avons remarqué que la Commission n'a pas fait part à son partenaire de ses exigences en matière de sécurité des TI ni cherché à obtenir l'assurance que ses ressources d'information étaient suffisamment protégées.

Les évaluations des risques tendent à n'avoir qu'un seul objectif

3.81 Les responsables de la sécurité des TI admettent depuis longtemps que les pratiques de sécurité des TI sont liées à la gestion des risques. Il n'est ni faisable ni rentable d'éliminer tous les risques ou toutes les menaces pesant sur les ressources d'information. Qui plus est, comme toute priorité, la sécurité des TI a des ressources limitées; les évaluations des risques facilitent l'affectation des ressources aux activités qui la justifient. Nous avons par conséquent examiné, dans les quatre ministères, les procédés et les pratiques qui servaient à déceler, à évaluer et à gérer les risques. Nous nous sommes renseignés sur leurs plans de continuité des opérations, qui leur permettraient de poursuivre leurs activités en cas d'interruption des opérations courantes pour une raison quelconque, notamment une panne ou la non-disponibilité des systèmes d'information.

3.82 La Politique du gouvernement sur la sécurité de 1994 a établi que les nouveaux systèmes devaient faire l'objet d'une analyse de sensibilité et d'une évaluation de la menace et des risques (EMR), en mettant l'accent tout particulièrement sur la sécurité des TI. De plus, la GRC a élaboré, à l'intention des ministères et des organismes, des lignes directrices sur la façon d'effectuer des EMR.

3.83 Nous avons remarqué que les quatre ministères avaient fait des EMR, mais seulement de façon ponctuelle (consulter également la partie du chapitre qui commence au paragraphe 3.92). Les évaluations ont tendance à porter sur une seule application ou, dans certains cas, sur un changement majeur survenu dans l'infrastructure des TI. Nous n'avons pas été en mesure de trouver une analyse qui avait porté sur les risques et les menaces à la sécurité globale des TI dans les ministères. Les évaluations de la menace et des risques par les ministères se déroulent à différents moments. Il arrive aussi que le milieu opérationnel change en parallèle avec la technologie. Une analyse menée dans une vaste perspective peut mettre en relief des lacunes et un chevauchement des efforts. Elle peut aussi permettre de s'assurer qu'on a bien tenu compte des préoccupations concernant l'incidence sur les activités et la protection des renseignements personnels. En vertu de la Politique du gouvernement sur la sécurité et des normes qui s'y rattachent, ou encore selon les politiques de sécurité des TI des quatre ministères, la tenue d'analyses de grande portée n'est pas requise. À notre avis, des analyses périodiques seraient un moyen de renforcer la sécurité des TI au sein des ministères.

3.84 Le plan de continuité des opérations (PCO) est un important outil de gestion des risques qui permet aux ministères de planifier une éventuelle interruption des activités et d'en assurer la reprise. Lorsqu'ils se sont préparés au passage à l'an 2000, la plupart des organismes ont dressé des PCO. Dans notre Rapport de décembre 1999, nous avons recommandé que les ministères mettent ses plans à l'essai et les tiennent à jour.

3.85 Notre vérification a confirmé qu'en 1999, les quatre ministères avaient établi des plans de continuité des opérations pour se préparer au passage à l'an 2000. Toutefois, ils n'ont pas tenu leurs plans à jour. En prévision de la Politique du gouvernement sur la sécurité de 2002 et en réponse à une directive publiée après le 11 septembre 2001, les quatre ministères ont amorcé la mise à jour de leurs plans. Nous avons également constaté qu'aucun d'eux n'avait procédé à des essais périodiques de leurs plans de continuité des opérations.

3.86 Pêches et Océans Canada met actuellement à jour sa liste de personnes-ressources et détermine les ressources dont il a besoin pour maintenir son plan de continuité des opérations et le mettre régulièrement à jour. Au cours de l'été 2001, Industrie Canada a mis en place une nouvelle unité opérationnelle à laquelle il a confié son PCO. Le plan englobera plusieurs unités opérationnelles et bureaux du Ministère partout au Canada. DRHC est pour sa part occupé à mettre à jour tous ses PCO locaux et détaillés et à les regrouper en une seule base de données ministérielle.

Les divers plans seront éventuellement réunis pour former un seul plan ministériel. La Commission nationale des libérations conditionnelles a préparé l'ébauche d'un cadre pour la mise à jour de son plan.

Il n'existe pas de programme officiel de formation à des fins de sensibilisation à la sécurité des technologies de l'information

3.87 La formation à des fins de sensibilisation à la sécurité des TI constitue une étape importante dans la mise en œuvre d'un programme de sécurité des TI. Tous les employés doivent en effet comprendre l'aspect délicat de l'information qu'ils traitent, les menaces éventuelles et leur responsabilité consistant à réduire ces menaces au minimum. Un programme de formation à des fins de sensibilisation à la sécurité des TI est un moyen d'aider les employés à comprendre les exigences des politiques de leur ministère sur la sécurité des TI ainsi que l'incidence que la non-conformité peut avoir sur la sécurité de leurs ressources d'information.

3.88 Un plan de formation type comprend les éléments suivants :

- des séminaires et des séances de formation sur la sécurité;
- des documents d'information et des présentations sur la sécurité;
- la publication d'un guide sur la sécurité;
- la diffusion d'information sur le site Web et intranet;
- la distribution de brochures, de vidéos et d'affiches;
- la publication de bulletins et de notes de rappel sur la sécurité;
- l'utilisation d'économiseurs d'écran et de panneaux d'ouverture de session.

3.89 Nous avons remarqué que DRHC s'était doté d'un programme de formation à des fins de sensibilisation à la sécurité, qui englobe la plupart de ces éléments. Les trois autres ministères possèdent certains éléments, mais n'ont pas instauré de programme officiel de formation continue à des fins de sensibilisation.

3.90 Les pratiques que nous avons relevées dans les quatre ministères en matière de régie et d'évaluation des risques à la sécurité des TI reflètent les lacunes éventuelles à ce chapitre dans l'ensemble du gouvernement. À notre avis, il conviendrait de se pencher sur ce problème dans le cadre de la prochaine mise à jour des normes opérationnelles sur la sécurité des TI.

3.91 **Recommandation.** Le gouvernement devrait songer à publier d'autres directives, dans le cadre de la mise à jour des normes de sécurité des technologies de l'information, pour s'assurer que les ministères et les organismes disposent de cadres adéquats pour la régie de la sécurité des TI et la gestion des risques à la sécurité. Les directives devraient notamment inclure la nécessité de mettre les politiques ministérielles à jour, d'effectuer des évaluations générales des risques à intervalles réguliers et d'instaurer un programme officiel de formation pour sensibiliser les employés.

Réponse du gouvernement. Le gouvernement approuve cette approche, qui est aussi prévue dans la nouvelle version de la Politique du gouvernement sur la sécurité. Au cours des prochains mois, le Secrétariat du Conseil du Trésor,

en collaboration avec les organismes responsables en matière de sécurité, diffusera la PGS et fera connaître les obligations ministérielles, y compris le besoin de sensibiliser et de former les employés. La GRC offre déjà sur demande des séances de sensibilisation à la sécurité des TI et une formation spécialisée.

La gestion des pratiques de sécurité dans les ministères

La sécurité des technologies de l'information est une question qu'il faut considérer dès le départ

3.92 Dans tout programme de sécurité des TI, une étape primordiale consiste à mettre en place et en œuvre un contrôle efficace des menaces et des risques liés aux TI. Les contrôles préventifs sont plus efficaces lorsque les préoccupations en matière de sécurité sont réglées au début du processus de conception de nouveaux programmes ou de mise au point et de modification des systèmes d'information. En outre, le fait de tenir dûment compte de la sécurité en temps opportun permet de réduire les coûts au minimum à long terme. Dans les quatre ministères, nous nous sommes intéressés aux pratiques qui soutiennent ces principes et à certains contrôles essentiels reposant sur diverses normes de l'industrie relatives à la sécurité des TI.

3.93 La Politique du gouvernement sur la sécurité de 1994 exigeait que l'élaboration des systèmes commence par une analyse de sensibilité d'un système de TI envisagé, suivie d'une évaluation de la menace et des risques afin d'appuyer toutes les grandes décisions en matière d'élaboration des systèmes, en particulier celles portant sur la sécurité. La Politique révisée exige que les ministères certifient et accréditent les systèmes d'information avant leur première utilisation et qu'ils pratiquent une saine gestion de la configuration des systèmes et de leurs dispositifs de protection.

3.94 Notre vérification a montré que les quatre ministères et organismes avaient pris un ensemble de mesures diverses, qui avaient donné des résultats mitigés. Ils ont tous les quatre assujetti certains nouveaux systèmes et certains changements dans l'infrastructure à des évaluations ponctuelles de la menace et des risques à la sécurité. Jusqu'à tout récemment, aucun ne possédait de politique exigeant la conduite d'EMR au début du cycle de mise au point des systèmes. Qui plus est, les ministères n'ont ni défini ni fourni de lignes directrices sur la façon de déterminer si la mise au point d'une application ou un changement dans l'infrastructure est suffisamment important pour justifier une EMR. Les décisions concernant la réalisation d'évaluations étaient subjectives et ponctuelles. En conséquence, la haute direction ne peut avoir la certitude que des évaluations de la menace et des risques ont été effectuées lorsqu'il le fallait et que des contrôles rentables et préventifs ont été envisagés et mis en place dès le début.

3.95 À Industrie Canada, nous avons remarqué qu'une nouvelle politique était entrée en vigueur en juin 2001, et qu'elle rendait obligatoires les évaluations de la menace et des risques (EMR) lors de l'élaboration de chaque nouveau système. Toutefois, un nombre limité d'évaluations ont été menées à ce jour. DRHC, qui est un organisme de grande taille, a effectué de nombreuses EMR portant sur les changements apportés à ses systèmes.

3.96 Nous avons examiné plusieurs évaluations de la menace et des risques pour obtenir de l'information sur les analyses du coût des options, et notamment de l'option proposée, et sur l'acceptation ultérieure des risques résiduels par la direction. Nous n'avons trouvé aucun élément de preuve indiquant que les conséquences financières avaient été prise en considération dans le cadre des EMR, ou que la direction avait approuvé l'option proposée.

3.97 Une pratique de sécurité généralement reconnue consiste à permettre aux employés d'accéder à un système seulement lorsqu'ils doivent le faire pour mener à bien les fonctions qui leur sont confiées. Les contrôles exercés pour prévenir l'accès non autorisé à des applications ou à des systèmes de réseaux consistent notamment à définir et à mettre en place des droits et des permissions d'accès, et à surveiller l'accès via l'authentification des utilisateurs, souvent grâce à des mots de passe.

3.98 Nous avons remarqué que la gestion des permissions d'accès était dispersée dans chacun des ministères, et que les permissions ne faisaient pas l'objet d'examens périodiques. Selon l'opinion générale, et celle des utilisateurs en particulier, un accès moins restreint est plus efficace pour les activités courantes. Lors de la configuration des nouvelles applications, le principe de l'accès en fonction des besoins est souvent appliqué de façon non rigoureuse, un problème que vient aggraver l'utilisation de diverses plates-formes matérielles incompatibles et d'applications ayant évolué avec le temps. En conséquence, les permissions d'accès peuvent être fragmentées selon les applications et les plates-formes technologiques.

Permission d'accès — Mesure dans laquelle une personne ou un appareil peut visualiser, augmenter, modifier ou supprimer les données versées dans un système informatique.

3.99 La gestion des mots de passe n'est pas une activité futile, mais une nécessité. Dans bon nombre de cas, nous avons remarqué que les mots de passe n'avaient pas été changés régulièrement. Dans quelques cas, lorsque les employés quittaient l'organisme ou étaient mutés à de nouveaux postes, les mots de passe qui leur donnaient accès aux systèmes n'avaient pas été changés ou annulés dans de brefs délais. Dans d'autres cas, l'organisme n'exigeait pas que les mots de passe respectent des règles strictes — par exemple des règles établissant un nombre minimal de caractères, exigeant l'utilisation de caractères spéciaux ou interdisant l'utilisation de mots de passe par défaut ou de mots courants. Qui plus est, la plupart des employés possèdent plusieurs mots de passe pour accéder à divers systèmes et applications, ce qui peut les amener à être moins enclins à changer régulièrement leurs mots de passe et à en assurer la confidentialité. À l'issue des résultats de l'un des examens qu'il a menés sur la sécurité, DRHC a amorcé un projet qui vise à rationaliser la gestion des mots de passe au sein de l'organisme, quel que soit l'emplacement ou le système.

3.100 Pêches et Océans Canada n'a pas de politique globale prescrivant une sécurité minimale sur l'accès à distance aux systèmes ministériels, et de nombreux employés ont un accès à distance. Dans un rapport de vérification interne paru en avril 2000, on fait remarquer qu'environ 2 500 employés ont eu accès aux réseaux du Ministère à partir d'emplacements autres que leur bureau. Plus de 1 800 employés se sont branchés aux réseaux en utilisant du matériel informatique n'appartenant pas au Ministère. Le matériel qui

Accès à distance — Accès à un système ou à un dispositif réseau à distance, au moyen de lignes téléphoniques ou d'Internet.

n'appartient pas au Ministère échappe à son contrôle de la configuration et pourrait présenter des risques et une vulnérabilité additionnels pour ses réseaux. La vérification interne a également permis de constater que l'accès à distance différait d'une région à une autre.

3.101 Nous nous sommes rendus dans les bureaux de Pêches et Océans Canada situés dans la région du Pacifique et dans celle de la capitale nationale. Dans la région du Pacifique, nous avons constaté l'absence de politiques ou de procédures sur l'accès à distance. En fait, les employés se branchaient de la même façon aux services en réseau, qu'ils le fassent à distance ou dans leur bureau. Durant nos entretiens avec la direction régionale, celle-ci a admis que l'octroi généralisé de permissions d'accès à distance non seulement accroît les risques d'atteinte à la sécurité des réseaux, mais entraîne aussi des coûts importants. Durant notre visite en décembre 2001, le bureau régional étudiait la possibilité d'élaborer une politique visant à réduire le coût de l'accès commuté sans frais à ses réseaux.

Il faut élargir la portée du contrôle permanent

3.102 Des programmes de sécurité des TI efficaces englobent des contrôles de détection et de prévention. Les contrôles de détection aident à vérifier la mesure dans laquelle les contrôles de prévention fonctionnent comme prévu. Ils permettent de détecter l'accès non autorisé ou les types d'activité inhabituels, pour que des mesures correctives soient prises en temps opportun. Bien souvent, les contrôles de détection prennent la forme d'un contrôle permanent — par exemple le contrôle des journaux d'exploitation, l'installation de dispositifs de détection des intrusions et l'analyse de leurs résultats, et la conduite de ratissages de sécurité pour vérifier la conformité aux politiques. De plus en plus d'outils informatisés sont mis à la disposition de la direction et des agents de sécurité pour analyser le trafic consigné dans les journaux d'exploitation.

3.103 Pendant la vérification, nous nous sommes intéressés aux contrôles de détection des quatre ministères. Nous avons constaté que lors du contrôle des journaux d'exploitation, les ministères avaient tendance à mettre l'accent sur l'utilisation acceptable d'Internet. C'était particulièrement évident dans les trois plus grands ministères, y compris les bureaux régionaux dans lesquels nous nous sommes rendus. Les journaux d'exploitation étaient assujettis à un contrôle permanent pour s'assurer que les employés ne faisaient pas une utilisation abusive des privilèges d'accès à Internet avec les systèmes ministériels. Les trois ministères ont des procédures sur l'utilisation des systèmes à mauvais escient. DRHC a analysé les journaux d'exploitation pour déceler l'accès aux systèmes qui posaient un problème particulier de sécurité pour les gestionnaires de programme, de façon à pouvoir faire le suivi de l'utilisation malveillante ou abusive des données.

3.104 Dans les quatre ministères, nous avons constaté que les agents de sécurité des TI tenaient compte des alertes et faisaient attention aux attaques par des virus informatiques. Les pratiques de sécurité ministérielles comportent notamment des mesures de protection des ressources

d'information. Pendant nos visites dans les régions, nous avons remarqué que deux ministères prenaient des mesures pour parer aux attaques par des virus.

3.105 Toutefois, nous avons décelé des cas où la fonction d'enregistrement du système n'était pas activée. Nous avons aussi relevé des cas où les journaux d'exploitation n'étaient pas analysés systématiquement. Les menaces à la sécurité des technologies de l'information ne viennent pas seulement des employés qui accèdent à des sites Web non indiqués, ou des virus et autres programmes malveillants. Les ministères doivent se doter de mesures de protection contre les attaques externes dont ils seraient la cible particulière et contre l'utilisation malveillante ou la mauvaise conduite à l'interne, que celles-ci soient intentionnelles ou non.

Système de détection des intrusions — Système qui détecte le trafic pouvant présenter une menace et en avertit la direction.

3.106 Les systèmes de détection des intrusions (SDI) sont un contrôle de détection qui facilite le repérage d'un trafic éventuellement malveillant sur les réseaux. En 1999, le Centre de la sécurité des télécommunications a demandé qu'une étude soit menée dans six ministères à l'aide des SDI, afin d'évaluer la menace pesant sur les réseaux. Le Centre en est arrivé à la conclusion que les systèmes d'information gouvernementaux étaient réellement sujets à des menaces provenant de l'extérieur, apparemment de grande envergure et pour lesquelles des moyens d'attaque informatisés avaient été utilisés. En septembre 2000, le Centre a recommandé que les ministères se dotent d'une capacité de détection des intrusions dans les réseaux. Sur les quatre ministères qui ont fait l'objet de notre vérification, seul Industrie Canada a mis en place une certaine capacité à cet égard.

3.107 Un ratissage de sécurité est une inspection visant à s'assurer que les employés suivent les procédures de sécurité. Dans le cadre de ce ratissage, on s'assure notamment que les employés suivent la procédure de fermeture de session lorsqu'ils n'utilisent plus leurs ordinateurs, et qu'à la fin de la journée de travail ils sécurisent leurs ordinateurs et protègent convenablement les supports d'information amovibles. Nous avons constaté que les ministères ne procèdent pas régulièrement à des ratissages de sécurité.

3.108 Assurer une bonne sécurité des TI consiste également à prendre des mesures préétablies visant à réagir aux atteintes à la sécurité et à les signaler. Lorsqu'il y a atteinte à la sécurité des TI, le personnel doit promptement reconnaître qu'un incident s'est produit, réagir rapidement pour corriger la situation et signaler l'incident aux agents de sécurité compétents. Pour ce faire, les ministères doivent avoir des procédures bien établies et un personnel formé à la prise de mesures décisives et judicieuses.

3.109 Aucun des quatre ministères n'avait défini ce qu'est une atteinte à la sécurité des TI. L'établissement d'une atteinte à la sécurité est laissée au soin du personnel et des gestionnaires, et il n'existe aucune procédure pour veiller à ce que le personnel réagisse promptement, de façon cohérente et adéquate.

3.110 Dans chacun des quatre ministères, la responsabilité des mesures à prendre pour réagir à un incident est assumée conjointement par le personnel affecté aux systèmes, aux réseaux et aux programmes d'activités. Industrie Canada a du personnel chargé des TI et de la sécurité, qui communique par

téléphone au besoin. Le gestionnaire de la sécurité des TI reçoit un courrier électronique chiffré qui l'avertit lorsque les techniciens du réseau décèlent un problème.

3.111 La gestion des pratiques de sécurité des TI au moyen d'un contrôle permanent aide les ministères et les organismes à déceler les attaques portées contre leurs systèmes et à déterminer si la sécurité de ces systèmes est compromise. Bien que le contrôle permanent exercé dans les quatre ministères puisse ne pas être représentatif de la situation au sein du gouvernement, il reflète néanmoins les écarts possibles entre la version révisée de la Politique du gouvernement sur la sécurité, d'une part, et les pratiques de sécurité des TI utilisées par les ministères et organismes, d'autre part. Selon nous, il conviendrait de déceler les écarts importants et d'en tenir compte lors de la mise en œuvre de la Politique révisée.

3.112 **Recommandation.** Le gouvernement devrait déceler les écarts importants entre les pratiques actuelles de sécurité des TI utilisées dans les ministères et la Politique du gouvernement sur la sécurité de 2002, et en tenir compte dans le plan de mise en œuvre de la Politique.

Réponse du gouvernement. Les organismes responsables s'efforcent de déceler les écarts entre les pratiques de sécurité ministérielles et la Politique du gouvernement sur la sécurité et ils élaborent, de concert avec le Secrétariat du Conseil du Trésor, des procédures d'intervention et de rapport d'incidents, des niveaux de préparation à la sécurité des TI (STI), un guide opérationnel d'auto-évaluation de la STI, des lignes directrices pour la certification et l'accréditation et des profils de service pour les besoins fonctionnels essentiels.

Vérifications et examens périodiques

Les examens par des organismes indépendants et les vérifications de la sécurité des technologies de l'information ont été insuffisants

3.113 Les examens par des organismes indépendants et les vérifications sont une façon de garantir à la direction que les opérations ministérielles répondent aux objectifs des programmes; ils font également ressortir les secteurs où il faut apporter des améliorations. Les examens indépendants et les vérifications de la sécurité des TI servent de mécanisme permettant de faire régulièrement le point sur l'état de la sécurité des TI au sein des ministères.

3.114 En vertu de la Politique du gouvernement sur la sécurité de 1994, les ministères devraient faire des vérifications internes de la sécurité des TI au moins une fois tous les cinq ans. Nous avons remarqué que seuls Pêches et Océans Canada et DRHC avaient effectué des vérifications de la sécurité des TI à l'échelle ministérielle. Les deux autres ministères ont omis de satisfaire à cette exigence de la Politique.

3.115 La sécurité des TI a constitué un des éléments de la vérification de la sécurité menée en 1995 à Pêches et Océans Canada. Une deuxième vérification de la sécurité des TI a été menée et, dans le rapport publié en 2000, on note un certain nombre de faiblesses déjà décelées en 1995 — par exemple, des contrôles peu rigoureux sur l'accès à distance et le matériel

branché au réseau. Le Ministère a dressé un plan d'action pour donner suite aux recommandations découlant de la vérification. Quant à DRHC, il a effectué une vérification de la sécurité des TI à grande échelle en 1999. Le rapport de vérification comporte un certain nombre d'observations et de recommandations. Par exemple, on y fait remarquer que les procédures établies pour la sécurité des TI varient, et que les rôles, les responsabilités, la reddition de comptes et les compétences en matière de sécurité ne sont pas clairs. DRHC a préparé un plan d'action dans lequel il donne suite aux observations formulées.

3.116 Selon la pratique établie, la GRC effectuait des examens de sécurité des TI pour les ministères et les organismes. La Politique du gouvernement sur la sécurité de 1994 stipulait que les ministères devaient demander à la GRC d'examiner leurs programmes de sécurité des TI au moins une fois tous les cinq ans, et à des intervalles plus rapprochés lorsque les programmes et les systèmes contenaient une information classifiée et/ou extrêmement délicate.

3.117 Toutefois, la GRC n'a mené aucun examen des pratiques de sécurité des TI à Pêches et Océans Canada ni à Industrie Canada au cours des cinq dernières années. La GRC a effectué un examen partiel au sein de la Commission nationale des libérations conditionnelles, pour satisfaire à une exigence obligatoire avant de permettre à la Commission d'accéder à quelques-uns de ses systèmes sur l'exécution de la loi. DRHC était le seul ministère, parmi les quatre, qui avait demandé à la GRC d'effectuer un examen, mais le dernier remonte à 1997.

Peu de tests techniques sont menés pour déceler la vulnérabilité des réseaux

3.118 Il existe un certain nombre de techniques que les ministères peuvent utiliser pour déterminer l'efficacité de la sécurité entourant leurs systèmes de réseaux. Les techniques sont une composante essentielle d'un programme global de gestion de la sécurité des TI. Elles consistent en des tests visant à déceler les modems non autorisés par l'entremise de la composition automatique de numéros de téléphone (voir la composition intensive de numéros de téléphone) et le repérage des points d'accès aux systèmes de réseaux qui présentent une faiblesse (voir l'évaluation de la vulnérabilité). Les tests, qui constituent une forme de vérification et de surveillance, facilitent le repérage des faiblesses et des points vulnérables éventuels, qui pourraient aboutir à une atteinte à l'intégrité. Les tests périodiques sont une pratique privilégiée de sécurité des TI.

Composition intensive de numéros de téléphone — Test effectué à l'aide d'outils informatisés pour composer un ensemble de numéros de téléphone afin de repérer les modems non sécurisés.

Évaluation de la vulnérabilité — Série de tests visant à déceler les points vulnérables des systèmes de réseaux avant qu'une atteinte à la sécurité ne se produise.

3.119 Nous avons constaté que deux des quatre ministères ont fait peu de tests techniques – voire aucun – de leurs systèmes de réseaux pour déceler les modems non autorisés et la vulnérabilité éventuelle. Industrie Canada a effectué quelques tests, bien que restreints, pour repérer toute vulnérabilité des réseaux. DRHC s'est doté d'outils techniques pour mener des évaluations de la vulnérabilité.

3.120 Notre examen a fait ressortir l'insuffisance des vérifications et des examens indépendants de la sécurité des TI. Qui plus est, la plupart des ministères et des organismes ont omis de satisfaire aux exigences de la Politique. Selon nous, dans le cadre de la version révisée de la Politique du gouvernement sur la sécurité, il faut s'attaquer à cette lacune afin de renforcer la sécurité des TI à l'échelle de l'administration fédérale.

3.121 **Recommandation.** Le gouvernement devrait songer à fixer la fréquence minimale des évaluations des pratiques de sécurité des technologies de l'information qui doivent être menées dans les ministères et exiger, dans ses normes techniques, que les ministères soumettent leurs systèmes à des évaluations de la vulnérabilité.

Réponse du gouvernement. Le gouvernement approuve en principe cette recommandation, mais selon la Politique du gouvernement sur la sécurité, il incombe à l'administrateur général d'une institution gouvernementale de déterminer la fréquence de ces évaluations périodiques. Par l'intermédiaire du processus d'élaboration des normes de sécurité des TI, le Secrétariat du Conseil du Trésor et les organismes responsables en matière de sécurité prépareront des directives sur les exigences en matière d'analyse de la vulnérabilité et de fréquence optimale des évaluations périodiques. Ces directives seront fondées sur les meilleures pratiques en ce qui a trait à la gestion des risques et à la disponibilité des ressources.

L'évaluation de la vulnérabilité des réseaux

Les tests techniques ont permis d'établir l'existence éventuelle de points vulnérables

3.122 Nous avons procédé à une composition intensive de numéros de téléphone à l'aide d'un échantillon dans certains ministères, et à des tests à distance pour déceler la vulnérabilité des réseaux à leurs points d'occupation dans Internet. Dans les deux cas, nous avons essayé de repérer les points vulnérables sans toutefois les exploiter pour pénétrer dans les réseaux ministériels. Nous n'avons pas effectué de tests à partir des systèmes de réseaux internes des ministères.

3.123 Nous avons transmis les résultats détaillés de nos tests directement aux ministères pour qu'ils puissent corriger les faiblesses éventuelles que nous avions repérées. Les résultats des tests que nous présentons dans ce chapitre sont globaux et ne concernent pas un ministère en particulier.

3.124 En ce qui touche les tests par composition intensive de numéros de téléphone, nous avons retenu 10 000 numéros de téléphone correspondant à des bureaux des ministères dans la région de la capitale nationale et dans une autre région, et nous avons utilisé des outils informatisés pour repérer les modems. Nous avons trouvé 97 appareils permettant d'accéder aux réseaux ministériels. Il se pourrait qu'un sous-ensemble de ceux-ci soit des modems non autorisés qui présentent un risque élevé pour les ministères. Nous avons fourni une information détaillée aux ministères à des fins de suivi.

3.125 Nous avons mené des évaluations de la vulnérabilité de 260 systèmes hôtes, dont l'emplacement a été trouvé à l'aide de l'information fournie par les ministères. Au moyen d'une batterie d'instruments techniques, nous avons recueilli de l'information sur les systèmes et nous l'avons analysée pour déceler toute vulnérabilité pouvant ouvrir la porte à un accès non autorisé.

3.126 Nous avons remarqué que sur les 260 systèmes, 85 présentaient des points vulnérables qui, dans la plupart des cas, pourraient compromettre l'intégrité des systèmes lors d'une cyberattaque ciblée. Une faiblesse en particulier nous a préoccupés, car elle présentait une menace imminente, et nous l'avons signalée immédiatement au ministère. Nous avons fourni toutes les autres données ainsi que les résultats de notre analyse aux ministères, après avoir terminé les tests.

3.127 Bien que nous ayons trouvé des points d'accès qui pourraient être faciles à exploiter, nous n'avons pas essayé de pénétrer dans les systèmes. Par conséquent, nous ne sommes pas en mesure de nous prononcer sur l'incidence qu'auraient ces faiblesses. Les études de cas présentées dans « Nos évaluations de la vulnérabilité font ressortir des faiblesses » fournissent quelques exemples des faiblesses relevées.

Nos évaluations de la vulnérabilité font ressortir des faiblesses

Applications désuètes et systèmes non protégés

Plusieurs systèmes hôtes utilisaient des applications désuètes connues pour présenter des points vulnérables pouvant ouvrir la porte à un accès non autorisé. Dans un cas, nous avons remarqué que le mot de passe de l'administrateur de réseau n'était pas établi, ce qui permettait à tout utilisateur d'Internet d'accéder au système.

Les possibilités d'accès non autorisé sont nombreuses :

- Les données délicates enregistrées dans un système peuvent être visualisées et utilisées de façon frauduleuse.
- Les données ou les programmes peuvent être modifiés ou supprimés.
- L'accès à un système ministériel pourrait permettre d'accéder à un autre système.
- Des programmes pourraient être installés pour attaquer d'autres systèmes dans Internet. Les attaques donneraient ainsi l'impression de provenir du gouvernement.
- Les systèmes pourraient être utilisés pour partager des fichiers; le gouvernement donnerait alors l'impression qu'il approuve le contenu des fichiers.

Information pouvant être l'objet de cyberattaques

L'information concernant la configuration des systèmes et l'identité des utilisateurs n'était pas à l'abri des attaques. Cette information pourrait servir à planifier une cyberattaque ou à accéder à des systèmes et à des données sans en avoir la permission.

L'information suivante était accessible dans les systèmes :

- le type de système d'exploitation et la version utilisés;
- le nom du système hôte;
- la configuration du système pour partager les fichiers (permettait-elle une « relation de confiance » qui donnerait un accès direct à d'autres systèmes?);
- une liste de noms d'utilisateur valides;
- les noms et prénoms des utilisateurs.

3.128 Les résultats de nos tests soulignent l'importance des évaluations par des organismes indépendants et des vérifications. Ils justifient aussi notre recommandation, à savoir que le gouvernement intègre la composition intensive de numéros de téléphone et les évaluations de la vulnérabilité dans les normes techniques et opérationnelles qu'il élabore pour la sécurité des TI.

Conclusion

3.129 La version révisée de la Politique du gouvernement sur la sécurité est entrée en vigueur en février 2002, pour remplacer la Politique de 1994. La version révisée met fortement l'accent sur la sécurité des TI et constitue une étape importante pour renforcer la sécurité à l'échelle du gouvernement. Toutefois, nous avons remarqué que les normes opérationnelles et techniques relatives à la sécurité des TI ne sont pas encore mises à jour et que les plans et le calendrier d'actualisation ne sont pas encore terminés. La Politique ne sera pleinement efficace que si elle s'accompagne de normes à jour, qui précisent les exigences minimales auxquelles les ministères et les organismes doivent satisfaire.

3.130 Nous avons également constaté que les ministères ne se sont pas conformés à l'exigence de la Politique de 1994 consistant à mener des vérifications internes et à demander à la GRC d'examiner la sécurité des TI au moins une fois tous les cinq ans. En conséquence, le gouvernement ne possède pas suffisamment d'information sur l'état de la sécurité des TI à l'échelle des ministères et des organismes. Il s'agit d'une information essentielle pour déterminer si l'état actuel de la sécurité est acceptable et pour établir une base de référence afin d'évaluer les progrès futurs.

3.131 Notre examen au sein des quatre ministères a fait ressortir certaines pratiques de sécurité des TI peu rigoureuses, qui pourraient traduire l'existence de faiblesses dans d'autres ministères. Elles peuvent souligner, pour le Secrétariat du Conseil du Trésor et d'autres organismes responsables en matière de sécurité, des aspects de la gestion et du soutien sur lesquels il faudrait peut-être se concentrer. Nos tests techniques ont mis en évidence d'éventuels points vulnérables qui pourraient compromettre l'intégrité des systèmes de réseaux gouvernementaux. Les résultats des tests renforcent notre observation selon laquelle il est nécessaire que des examens indépendants et des vérifications de la sécurité des TI soient menés à intervalles réguliers.

3.132 Notre vérification a permis de définir un certain nombre de questions sur lesquelles le gouvernement doit se pencher pour améliorer la sécurité des TI dans les ministères et les organismes. Lorsqu'il a lancé le projet Gouvernement en direct, le gouvernement a présenté les questions de sécurité et de protection des renseignements personnels comme un enjeu majeur. Il est important, pour le succès du projet, que des mesures opportunes soient prises afin d'améliorer la sécurité des TI, de façon que des pratiques de sécurité adéquates soient en place pour garantir un accès en direct sécurisé à tous les services gouvernementaux.

À propos de la vérification

Objectif, étendue et méthode

La vérification avait pour objectif d'évaluer le cadre de sécurité des technologies de l'information que le gouvernement a mis en place pour protéger les ressources d'information et assurer une prestation ininterrompue des services. La protection des ressources d'information consiste non seulement à protéger la valeur des biens eux-mêmes, mais aussi à tenir confidentielle toute information classifiée et désignée, et à préserver l'intégrité des données et de l'information tenues sur support électronique.

Pour évaluer le cadre de sécurité des TI à l'échelle de l'administration fédérale, nous avons mené notre vérification essentiellement au Secrétariat du Conseil du Trésor. Nous avons aussi interviewé des membres de la Gendarmerie royale du Canada, du Bureau de la protection des infrastructures essentielles et de la protection civile et du Centre de la sécurité des télécommunications.

Notre examen a porté non seulement sur le cadre qui s'applique à l'échelle pangouvernementale, mais aussi sur les pratiques de sécurité des TI utilisées dans quatre ministères et organismes : Pêches et Océans Canada, Développement des ressources humaines Canada, Industrie Canada et la Commission nationale des libérations conditionnelles.

Il s'agit de quatre ministères différents du point de vue de la taille, qui fournissent ensemble des services aux particuliers et aux entreprises. Certains ont une gestion centralisée de leur infrastructure des TI alors que d'autres ont une gestion décentralisée. Nous les avons choisis pour avoir un aperçu de l'état de la sécurité des TI au gouvernement. Néanmoins, en raison de la diversité de leurs mandats et de leurs activités, y compris leurs infrastructures et systèmes de TI, nos constatations ne peuvent être considérées comme représentatives et elles ne donnent pas une vue globale des pratiques de sécurité des TI au gouvernement. La partie de la vérification menée au sein des ministères s'est déroulée dans les bureaux de la région de la capitale nationale des quatre ministères et dans les bureaux de la région du Pacifique de Pêches et Océans Canada et d'Industrie Canada.

Nous avons assujetti les réseaux de certains ministères à des tests techniques à distance pour détecter toute vulnérabilité, mais nous n'avons pas exploité les points vulnérables décelés.

Critères

Les critères généraux qui suivent ont été utilisés aux fins de la vérification.

- Le cadre de sécurité des technologies de l'information devrait permettre de s'assurer que les biens liés aux TI sont protégés et soutiennent la prestation sécurisée et ininterrompue des services gouvernementaux.
- La structure de régie de la sécurité des TI devrait intégrer un leadership et un soutien forts de la part des organismes centraux et des organismes responsables en matière de sécurité, ainsi que des pratiques de sécurité des TI cohérentes et rentables dans l'ensemble du gouvernement.
- Les politiques, les normes et les pratiques devraient correspondre aux niveaux actuels des risques et des menaces à la sécurité des TI.
- En fonction des risques évalués et des exigences actuelles en matière de sécurité, les mesures prises par les ministères et les procédés utilisés devraient permettre de prévenir et de détecter les menaces aux TI, et de réagir en conséquence.
- Les pratiques de sécurité des TI devraient être surveillées et réévaluées régulièrement, et toute vulnérabilité devrait être traitée.

Équipe de vérification

Vérificateur général adjoint : Douglas Timmins
Directrice principale : Nancy Cheng
Directeurs : Richard Brisebois, Greg Boyd, Tony Brigandi, Guy Dumas

Chantal Berger

Pour obtenir de l'information, veuillez joindre le service des Communications, en composant le 613-995-3708 ou le 1-888-761-5953 (sans frais).

Rapport de la vérificatrice générale du Canada à la Chambre des communes — Avril 2002

Table des matières principale