Chapitre

1

La sécurité des technologies de l'information

Tous les travaux de vérification dont traite le présent chapitre ont été menés conformément aux normes pour les missions de certification établies par l'Institut Canadien des Comptables Agréés. Même si le Bureau a adopté ces normes comme exigences minimales pour ses vérifications, il s'appuie également sur les normes et pratiques d'autres disciplines.

Table des matières

La sécurité des technologies de l'information

Points saillants

1.1 Malgré d'encourageants signes d'amélioration, le gouvernement n'a pas fait de progrès satisfaisants dans le renforcement de la sécurité des technologies de l'information (TI) depuis notre vérification de 2002. Il a posé les fondements en élaborant des politiques et des normes en la matière, et les ministères et organismes responsables sont plus actifs et plus déterminés à s'en occuper. Par ailleurs, deux ans et demi après avoir révisé sa politique sur la sécurité, le gouvernement a encore beaucoup à faire pour concrétiser ses politiques et ses normes en pratiques cohérentes et rentables, propres à assurer aux ministères et aux organismes un environnement informatique plus sécuritaire.

1.2 La version révisée de la Politique du gouvernement sur la sécurité de 2002 est venue préciser les rôles et les responsabilités des divers intervenants. Depuis lors, les organisations responsables travaillent de concert afin d'élaborer des normes et d'offrir aide et orientation aux ministères pour le renforcement de leurs pratiques de sécurité des TI. Malgré tout, il reste encore beaucoup de normes à élaborer, et le Secrétariat du Conseil du Trésor ne joue pas pleinement son rôle de surveillant, tel que le prévoit la Politique.

1.3 Les ministères et les organismes ont réalisé certains progrès en préparant des politiques sur la sécurité des TI et en mettant en place certaines pratiques de sécurité, telle l'évaluation de la vulnérabilité. Cependant, les systèmes informatiques restent vulnérables. La majorité des organisations ne satisfont pas aux normes minimales fixées par le Secrétariat. Les évaluations de vulnérabilité effectuées au cours des deux dernières années ont révélé de graves lacunes qui, si elles étaient exploitées, pourraient causer de sérieux dommages aux systèmes d'information du gouvernement.

1.4 Nous nous inquiétons du fait que, dans plusieurs ministères et organismes, la haute direction ne soit pas au courant des risques liés à la sécurité des TI et qu'elle ne sache pas comment les atteintes à la sécurité informatique risquent de nuire aux activités et de miner la crédibilité du gouvernement. Si, en raison d'une faiblesse du côté de la sécurité, une personne arrivait à accéder à une base de données ou à des renseignements confidentiels, la confiance des Canadiens à l'endroit du gouvernement serait sérieusement ébranlée. De plus, s'il y avait atteinte à la vie privée à cause d'une protection déficiente des renseignements personnels, la personne concernée pourrait en subir de graves préjudices. Qui plus est, les efforts déployés par le gouvernement pour fournir des services électroniques aux Canadiens s'en trouveraient sérieusement minés.

Contexte et autres observations

1.5 En 2002, nous avions constaté que la version révisée de la Politique du gouvernement sur la sécurité, entrée en vigueur en février 2002, représentait une étape importante dans le renforcement de la sécurité au sein de l'administration fédérale. Cependant, les normes de sécurité des TI qui devaient soutenir la mise en œuvre de la Politique dans les ministères et les organismes étaient inexistantes ou périmées. Il n'y avait que peu d'information sur l'état de la sécurité des TI au sein de l'administration fédérale parce qu'un petit nombre seulement d'organisations avaient vérifié leur programme en la matière ou surveillé leurs mesures de sécurité des TI. Nous avions également recensé d'autres questions sur lesquelles le gouvernement devait se pencher afin d'améliorer la sécurité des TI.

Réaction du Secrétariat du Conseil du Trésor. Les réponses du Secrétariat du Trésor à nos recommandations sont insérées dans le chapitre. Le gouvernement fournit également de l'information complémentaire, qui figure à la fin de la section « Conclusion ». Il accepte toutes nos recommandations et prend déjà des mesures dans certains cas.

Introduction

Cyberincident — Tentative non autorisée, réussie ou non, visant à accéder à un réseau ou à un système informatique ou visant à le modifier, à le détruire, à le supprimer ou à le rendre non disponible.

1.6 En avril 2002, nous avons fait rapport sur l'état de la sécurité des technologies de l'information (TI) au sein de l'administration fédérale. Nous avions alors signalé que ce sujet devait être une priorité pour les gestionnaires, compte tenu du nombre sans cesse grandissant de cyberincidents susceptibles de nuire aux activités d'une organisation.

Principales constatations de 2002

1.7 La version révisée de la Politique du gouvernement sur la sécurité de 2002 représentait une amélioration par rapport aux versions antérieures. De façon particulière, cette version :

- a mis à jour les rôles et les responsabilités du Secrétariat du Conseil du Trésor, qui est chargé de la coordination et du leadership, et ceux des 10 entités qui donnent des directives et du soutien en matière de sécurité aux ministères et aux organismes;
- a accentué l'importance de la sécurité des TI pour la sécurité globale au sein du gouvernement.

1.8 Par ailleurs, certains aspects nous préoccupaient. Les normes opérationnelles sur lesquelles les ministères et organismes devaient s'appuyer pour appliquer la Politique étaient périmées ou inexistantes. Or, ces normes sont essentielles car elles définissent les exigences de base à satisfaire pour instaurer des mesures de sécurité uniformes dans l'administration fédérale.

1.9 Le gouvernement ne surveillait pas le degré d'efficacité de la Politique pour ce qui est du renforcement de la sécurité des TI. Il avait exercé peu de surveillance depuis 1994, et les ministères et organismes ne satisfaisaient pas aux exigences de la Politique. La version révisée de 2002 n'exigeait plus que les organisations vérifient leurs programmes de sécurité tous les cinq ans; en outre, elle n'exigeait plus que la Gendarmerie royale du Canada (GRC) procède à une évaluation périodique de la sécurité des organisations.

1.10 Depuis 1994, les activités de contrôle et de surveillance de la sécurité des TI dans l'ensemble de l'administration fédérale étaient limitées. Il existait donc très peu d'information de base sur l'état de la sécurité des TI au sein de l'administration fédérale.

Changements importants depuis 2002

1.11 Depuis 2002, l'utilisation d'Internet au sein du gouvernement s'est accrue rapidement. Ce phénomène a débuté lors du lancement de Gouvernement en direct (GED) en 1999, l'objectif étant de donner aux Canadiens, d'ici la fin de 2005, la possibilité d'accéder en ligne aux informations importantes de même qu'aux services essentiels du gouvernement.

1.12 Pour rendre les services et les renseignements plus accessibles, le gouvernement a simplifié l'accès à ses services par Internet en trois avenues principales : Canadiens et résidents, Entreprises canadiennes, et

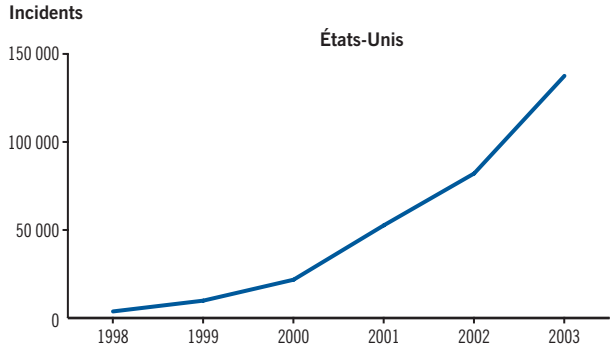
Non-Canadiens. Les ministères et organismes rendent leurs services plus conviviaux et offrent quelque 130 services clés en ligne. Par ailleurs, trois facteurs ajoutent au risque inhérent de la prestation de services en ligne :

- la présence d'outils en ligne susceptibles de causer des atteintes à la sécurité dans les systèmes informatiques;
- une forte augmentation des déficiences des logiciels et du matériel, susceptibles de porter atteinte aux systèmes informatiques et à l'information qu'ils abritent;
- un nombre grandissant de personnes aptes à exploiter ces déficiences, souvent dans les jours qui suivent la découverte de celles-ci.

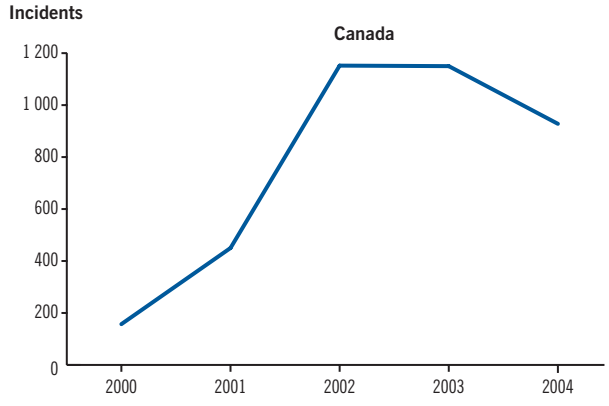
Attaque contre un réseau informatique — Tentative unique, non autorisée, visant à accéder à un réseau ou à l'utiliser. Un **incident** suppose quant à lui une série d'attaques qui se distinguent des autres **incidents** par la nature des « attaquants » et le degré de similarité des sites, des techniques et du moment choisi.

1.13 Le nombre de cyberincidents a beaucoup augmenté depuis 2001. Leur hausse et leur évolution au Canada et aux États-unis sont comparables (voir la pièce 1.1). Cependant, un faible pourcentage seulement des incidents sont signalés. Les attaques contre un réseau informatique donnent une bonne indication des risques réels. Depuis notre dernier rapport sur le sujet, publié en 2002, le nombre d'attaques a augmenté dangereusement, ce qui montre à quel point il est facile et rapide de lancer ces attaques (voir la pièce 1.2).

Pièce 1.1 Cyberincidents détectés et signalés par des tierces parties, aux États-Unis et au Canada

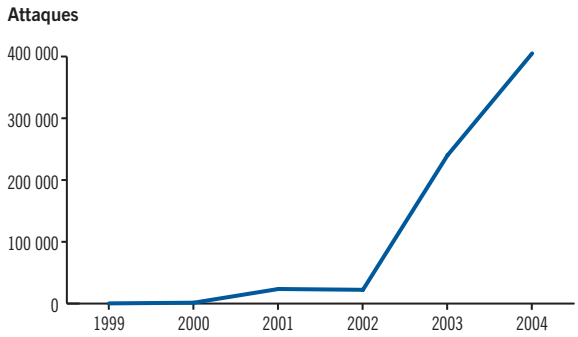


Source : CERT Coordination Centre (É.-U.)



Source : CanCERT (Canada)

Pièce 1.2 Attaques contre un réseau informatique détectées au Canada



Note : Ces attaques contre un réseau informatique comportent divers incidents détectés par des capteurs dans l'ensemble du Canada. Elles signalent des activités malveillantes dont font l'objet la plupart des réseaux gouvernementaux et commerciaux.

Source : CanCERT (Canada)

1.14 Le gouvernement du Canada reconnaît que les Canadiens veulent des services en ligne qui leur permettent de faire des transactions de manière sûre et confidentielle. C'est pourquoi il a lancé le grand projet d'État appelé la « Voie de communication protégée », une infrastructure qui assure le lien entre les Canadiens et les entreprises, d'une part, et le gouvernement, d'autre part. La Voie de communication protégée :

- instaure des normes communes en matière de protection des renseignements personnels, de sécurité, de disponibilité et de fiabilité;
- met les services Internet à la disposition de tous les ministères et organismes;
- offre des services d'authentification des clients, qui sont de plus en plus utilisés;
- offre plusieurs services GED depuis 2002;
- permettra aux Canadiens de communiquer des renseignements confidentiels à même le formulaire de recensement en ligne en 2006.

1.15 Le gouvernement offre aussi des services aux utilisateurs de téléphones mobiles ou d'assistants numériques personnels ayant accès à Internet. La gamme de ces services va s'élargissant. Ainsi, les Canadiens peuvent maintenant obtenir des numéros sans frais, des prévisions économiques de dernière heure, ou des informations utiles pour joindre leur député.

1.16 Avant de pouvoir offrir leurs services au moyen de dispositifs sans fil ou en ligne sur la Voie de communication protégée, les ministères et les organismes devront d'abord satisfaire à des normes de base rigoureuses en matière de sécurité des TI.

Objet du suivi

1.17 Le suivi avait pour objectif d'évaluer la mesure dans laquelle le Secrétariat du Conseil du Trésor et les ministères et organismes ont donné

suite aux recommandations formulées dans le chapitre 3 du Rapport de 2002, sur la sécurité des technologies de l'information. Nous avons examiné l'état de la sécurité des TI dans l'ensemble de l'administration fédérale et vérifié si les organisations disposaient du cadre voulu pour assurer la sécurité de l'information et offrir des services de façon sécuritaire et ininterrompue. Nous nous sommes attardés plus particulièrement sur les cinq secteurs suivants :

- la collaboration et l'échange d'informations entre les organisations responsables en matière de sécurité des TI;
- l'élaboration et la mise en œuvre de normes de sécurité des TI visant à soutenir la politique;
- l'efficacité de la Politique du gouvernement sur la sécurité, ainsi que les mesures de sécurité existantes;
- la planification des mesures d'urgence;
- la gestion des risques.

1.18 Nous avons interviewé des employés des organismes qui jouent un rôle de chef de file dans la sécurité des TI au gouvernement. Nous avons aussi examiné des documents et des dossiers. Dans les quatre organisations qui avaient fait l'objet d'une vérification en 2002, nous avons examiné les pratiques en matière de sécurité des TI, dans les cinq secteurs susmentionnés. Nous avons examiné un sondage effectué par le Secrétariat du Conseil du Trésor, fait une enquête auprès de 82 entités du gouvernement au sujet de pratiques choisies en matière de sécurité des TI et examiné les résultats des tests techniques réalisés dans un certain nombre de ministères et d'organismes par des consultants ou par le Centre de la sécurité des télécommunications (CST). Nous avons également exécuté nos propres tests techniques. Toutefois, nous n'avons examiné ni la Voie de communication protégée ni les questions de sécurité nationale.

1.19 La section intitulée **À propos du suivi,** à la fin du chapitre, fournit des détails additionnels sur l'objectif, l'étendue, la méthode et les critères du suivi.

Observations et recommandations

La version révisée de la Politique du gouvernement sur la sécurité

1.20 La version révisée de la Politique du gouvernement sur la sécurité améliore la sécurité des TI au sein de l'administration fédérale et offre une base pour d'autres progrès.

Les rôles et les responsabilités des ministères et organismes responsables sont définis dans la Politique

1.21 La Politique définit les rôles du Secrétariat du Conseil du Trésor et des 10 ministères et organismes responsables. Elle répartit entre ces entités la responsabilité à l'égard de la sécurité. Elle élimine le chevauchement des attributions de la GRC et du CST et donne des rôles à Sécurité publique et Protection civile Canada (qui remplace le Bureau de la protection des infrastructures essentielles et de la protection civile).

1.22 En 2002, il était trop tôt pour savoir si les nouveaux rôles et les nouvelles responsabilités étaient adéquats et s'ils allaient éliminer les chevauchements. Ils représentent, de fait, un pas en avant : les organisations responsables, le gouvernement et les organismes se consultent régulièrement au sujet de la sécurité des TI. À titre d'exemples :

- le Comité sur la sécurité des technologies de l'information tient une réunion tous les deux mois, sous la coprésidence de la GRC et du CST;
- les agents de sécurité des ministères sont informés des faits nouveaux en matière de sécurité tout au long de l'année par les organisations responsables;
- le personnel principal de gestion de l'information et des TI participe au Conseil des dirigeants principaux de l'information, organe consultatif qui s'occupe des questions relatives aux TI et à la gestion de l'information.

1.23 Selon la Politique, les responsabilités principales de coordination, de leadership, de surveillance et de contrôle relèvent du Secrétariat du Conseil du Trésor. Cependant, ce dernier ne joue pas pleinement son rôle de surveillance et de contrôle de l'état de la sécurité au sein de l'administration fédérale (voir les paragraphes 1.72 et 1.73).

On observe une plus grande coopération au sein de l'administration fédérale

1.24 En 2002, nous avions constaté que la Politique ne précisait pas à qui revenait la responsabilité de recueillir et de faire connaître les pratiques exemplaires en matière de sécurité des TI au gouvernement. Cet aspect s'est amélioré grâce à des moyens destinés à assurer des échanges efficaces d'information : cours offerts par la GRC et le CST, réseau de communication reliant les dirigeants principaux de l'information et réunions des agents de sécurité des ministères.

Il reste encore plusieurs normes de sécurité des TI à élaborer

1.25 Les normes de sécurité des TI énoncent ce que les ministères et les organismes doivent faire pour satisfaire aux exigences de base de la Politique. Les normes encouragent l'instauration de mesures de sécurité uniformes et l'échange de pratiques exemplaires entre les ministères.

1.26 En 2002, la Politique n'était pas assortie de normes opérationnelles auxquelles les ministères et les organismes devaient se plier pour se conformer aux diverses exigences. Depuis lors, le Secrétariat du Conseil du Trésor, en consultation avec les organisations responsables de la sécurité ainsi que les ministères et les organismes, a élaboré, et publié en mai 2004, la norme opérationnelle de sécurité appelée Gestion de la sécurité des technologies de l'information (GSTI). Cette norme donne des lignes directrices sur la manière de maintenir des systèmes informatiques sécuritaires dans des domaines tels que le contrôle de la gestion, l'évaluation des risques, la gestion des incidents liés à la sécurité et des faiblesses observées dans les systèmes, la vérification de la sécurité et l'élaboration d'un plan de continuité des activités. Elle définit également les rôles et les responsabilités des agents principaux de sécurité.

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

1.27 La norme GSTI renvoie à un certain nombre d'autres normes qui ne sont pas encore prêtes (voir la pièce 1.3). Ces normes, ainsi que la GSTI, fourniront aux ministères et aux organismes des lignes directrices qu'ils devront suivre pour se conformer à la Politique. Le Secrétariat du Conseil du Trésor a accordé aux organisations jusqu'en décembre 2006 pour se conformer à la norme GSTI.

Pièce 1.3 Normes de sécurité qui restent à élaborer

Normes de sécurité des TI

- Détection des intrusions
- Gestion des incidents

Autres normes de sécurité ayant une incidence sur la sécurité des TI

- Formation et sensibilisation en matière de sécurité
- Sécurité de la passation des marchés
- Identification et classement des biens
- Évaluation des menaces et des risques
- Enquêtes et sanctions
- Enquêtes de sécurité des employés
- Programme de sécurité des ministères
- Protection des employés
- Sécurité à l'étranger
- Échange d'information

1.28 **Recommandation.** Le Secrétariat du Conseil du Trésor devrait terminer l'élaboration de toutes les normes de sécurité soutenant la Politique du gouvernement sur la sécurité et la norme GSTI. Il devrait, en particulier,

- traiter en priorité les normes de sécurité des TI qui ont été identifiées et qui ne sont pas encore élaborées;
- préparer pour chaque norme un plan d'action assorti d'un échéancier;
- identifier de façon continue les aspects de la sécurité des TI pour lesquels des normes sont requises.

Réponse du Secrétariat du Conseil du Trésor. Le Secrétariat du Conseil du Trésor souscrit à cette recommandation. La norme de Gestion de la sécurité des technologies de l'information (GSTI) impose un ensemble d'exigences minimales à tous les ministères et organismes. Conjointement avec les trois organismes responsables de la sécurité (le Centre de la sécurité des télécommunications, Sécurité publique et Protection civile Canada et la Gendarmerie royale du Canada), le Secrétariat mettra la dernière main aux normes de sécurité opérationnelle avant la fin de 2006. D'autres normes techniques, de même que des directives techniques et opérationnelles, seront aussi mises au point pour combler les besoins changeants qui reflètent notre environnement à risque dynamique.

Le Secrétariat du Conseil du Trésor développera, coordonnera et supervisera un plan pangouvernemental qui recensera les priorités en ce qui a trait aux normes qui restent à élaborer. En outre, l'organisme responsable pertinent élaborera un plan d'action propre à chaque norme et le calendrier sera établi avec le Secrétariat. Cet exercice général d'établissement des priorités et de planification effectué conjointement avec les organismes responsables de la sécurité est déjà en cours. Le plan sera à la disposition de tous les ministères et organismes sur le forum Sitescape au début de 2005-2006.

Les questions émergentes de sécurité des TI continueront d'être cernées par plusieurs sources, qu'il s'agisse des organismes responsables de la sécurité, des professionnels de la sécurité au sein des ministères hiérarchiques ou des propriétaires d'entreprises de service qui ont des besoins à combler au chapitre des services et des systèmes. Même si l'établissement de l'ordre de priorité de l'objet des normes à élaborer sera un effort collectif, le Secrétariat continuera d'assurer la coordination à l'échelle de l'administration fédérale, et notamment de superviser le développement et l'exécution de plans d'action afin de fournir les normes et les consignes nécessaires.

La mise en œuvre de la Politique

D'importantes incohérences sont observées au chapitre de la conformité

1.29 Nous nous attendions à ce que les ministères et organismes se conforment à la plupart des exigences de la Politique du gouvernement sur la sécurité. Depuis le milieu des années 1990, les exigences fondamentales de la Politique et des normes ont très peu changé. Cela fait donc plus de dix ans que les ministères et organismes sont au courant de l'existence de la Politique et de ses exigences en matière de protection des systèmes informatiques. Cependant, nous avons constaté que peu d'entre eux se conforment en tous points à la Politique et qu'il y a des incohérences importantes sur le plan de la conformité. Les pratiques de sécurité des TI varient d'une entité à l'autre; des exemples en sont donnés dans des encarts tout au long de cette section du chapitre.

1.30 En vertu de la Politique, les ministères et organismes sont tenus de surveiller l'exécution de leurs programmes de sécurité et de les vérifier. En 2003, la Direction du dirigeant principal de l'information du Secrétariat du Conseil du Trésor a préparé un questionnaire d'autoévaluation que les ministères et organismes doivent remplir une fois par année conformément à la norme GSTI, pour évaluer la sécurité de leurs TI et leurs pratiques de gestion de la sécurité. Les organisations répondent aux questions, fondées sur les exigences de base de la Politique, au sujet de leurs politiques et de leurs pratiques en matière de sécurité et reçoivent une cote établie à partir d'une échelle de référence.

La place de l'agent de sécurité au sein de l'organisation

En vertu de la Politique du gouvernement sur la sécurité et de la norme de Gestion de la sécurité des technologies de l'information (GSTI), chaque ministère et organisme doit définir les rôles des agents de sécurité, en particulier ceux chargés de la sécurité des TI, et leur attribuer la place qui leur revient dans l'organisation. Le degré de conformité à cette exigence varie grandement d'une organisation à l'autre.

- À Industrie Canada et à Développement social Canada, les rôles de l'agent de sécurité du ministère (ASM) et du coordonnateur de la sécurité des TI sont clairement définis et vont dans le sens de la norme GSTI. Cependant, à Développement social Canada, il n'existe pas de comité supérieur chargé d'approuver les politiques et les normes et de prendre les décisions qui touchent la sécurité des TI. À Industrie Canada, l'ASM n'occupe pas un poste stratégique qui lui permettrait de donner à l'organisation des conseils sur des stratégies ou des décisions. De plus, la fonction du coordonnateur de la sécurité des TI à la Direction du dirigeant principal de l'information, qui contrôle une partie seulement du budget informatique, n'a pas suffisamment de pouvoir dans le processus décisionnel en matière de sécurité des TI. À cause de la portée restreinte de leurs postes, les agents concernés n'ont qu'une faible influence sur les décisions relatives à la sécurité intéressant l'ensemble du Ministère, et en particulier la sécurité des TI.
- À Pêches et Océans Canada, l'ASM n'occupe pas un poste stratégique, comme l'exige la Politique. Le poste de coordonnateur de la sécurité des TI existe, et ses rapports avec l'ASM sont fonctionnels. Vu que le Ministère est actif dans un grand nombre de secteurs et de régions et qu'il n'y a pas de communication entre les deux agents de sécurité, le Ministère n'est pas en mesure d'élaborer et de mettre en place un programme de sécurité intégré et bien coordonné.

1.31 Le questionnaire aide le personnel des TI et celui de la sécurité à mieux comprendre les exigences de base en matière de sécurité des TI, à mesurer leurs capacités actuelles à ce chapitre, ainsi qu'à repérer les écarts entre leurs propres pratiques et les pratiques exemplaires. Le questionnaire aide également le Secrétariat à évaluer le degré d'efficacité de la Politique et des normes et à déterminer si les ministères et organismes se conforment aux exigences de ces dernières.

1.32 Au début de 2004, le Secrétariat s'inquiétait du fait que bon nombre de ministères et organismes ne mettaient pas en œuvre les exigences de la Politique en matière de sécurité des TI. En mai 2004, il a procédé à une enquête, à l'aide du questionnaire, auprès de plus de 90 ministères et organismes. En tout, 46 organisations ont rempli le questionnaire et répondu au Secrétariat. D'après les résultats recueillis, le Secrétariat avait toutes les raisons de s'inquiéter puisque seule une de ces 46 organisations satisfaisait aux exigences de base de la Politique et des normes.

1.33 Les politiques ministérielles en matière de sécurité des TI établissent le fondement permettant de satisfaire aux normes de la Politique qui régissent la protection de l'information et des systèmes d'information. L'enquête du Secrétariat a révélé ce qui suit :

- 16 p. 100 des organisations n'avaient pas de politique en matière de sécurité des TI;
- 33 p. 100 des organisations qui avaient une politique ont répondu que celle-ci n'avait pas été officiellement approuvée par la direction;

- 35 p. 100 des organisations n'avaient pas de politique exigeant l'évaluation des menaces et des risques;
- 26 p. 100 des organisations n'avaient pas de politique exigeant un plan de continuité des activités pour les systèmes et services essentiels;
- 12 p. 100 des organisations n'avaient pas encore recensé leurs systèmes essentiels.

Politiques sur la sécurité des organisations

En 2002, nous avions signalé que les quatre organisations examinées devaient actualiser leurs politiques en matière de sécurité et mettre en place un meilleur cadre de régie (ou de gouvernance) pour la sécurité. Depuis lors, les progrès ont été inégaux :

- Industrie Canada a fait des progrès marqués : il a élaboré, mis en œuvre et fait connaître ses politiques en matière de sécurité des TI. Il a préparé des normes et des lignes directrices sur les questions relatives à la sécurité des TI.
- À Développement social Canada, la haute direction doit encore approuver plusieurs politiques sur la sécurité des TI. Par conséquent, leur application manque d'uniformité dans l'ensemble du Ministère.
- Pêches et Océans Canada a fait des progrès : il a développé un cadre de gestion de la sécurité et des politiques bien précises. Cependant, ni le cadre ni les politiques n'ont été approuvés officiellement par la haute direction.
- La Commission nationale des libérations conditionnelles a récemment entamé un projet visant à examiner ses politiques sur la sécurité des TI.

1.34 Nous avons préparé un court questionnaire, qui complète celui du Secrétariat et porte sur des pratiques précises en matière de sécurité des TI dans les ministères et organismes. Nous avons envoyé ce questionnaire à 82 organisations, qui y ont toutes répondu. Les résultats obtenus corroborent les constatations du Secrétariat, à savoir qu'il existe de grandes incohérences entre les exigences de la Politique et des normes, d'une part, et les pratiques observées dans les différentes organisations, d'autre part.

1.35 Sous plusieurs aspects, la conformité aux exigences de base de la Politique et des normes était loin d'être adéquate. À titre d'exemple, 65 p. 100 des organisations avaient un plan de continuité des activités, mais seulement 29 p. 100 l'avaient mis à l'essai au cours des deux dernières années.

1.36 Le personnel que nous avons interviewé a fourni diverses raisons sous-tendant cet état de fait :

- le manque d'argent et de ressources humaines;
- le manque d'intérêt de la part de la haute direction pour les questions de sécurité des TI;
- l'absence de préoccupation à l'égard de la sécurité des TI dans la culture de l'organisation.

1.37 En raison de l'absence généralisée de préoccupation au sujet des risques rattachés à la sécurité des TI, les systèmes comportent des faiblesses dont il est facile de tirer avantage. Il s'ensuit que l'organisation concernée court davantage le risque que des données de nature délicate, notamment des

renseignements personnels sur des Canadiens, des données sur la paie, des opérations financières, de l'information sur les programmes et d'autres données essentielles soient divulguées ou modifiées sans autorisation, ou encore perdues, sans que l'incident ne soit détecté.

Favoriser l'émergence d'une culture intégrant le souci de la sécurité des TI

Depuis notre examen des quatre organisations en 2002, les efforts de formation et de sensibilisation aux questions de sécurité des TI de la part des entités ont connu un succès mitigé.

Industrie Canada s'est efforcé de hausser le niveau de sensibilisation du Ministère aux questions de sécurité des TI. Il a publié des conseils en matière de sécurité et un bulletin mensuel en technologie de l'information. Il a aussi mis au point un cours de formation sur la sécurité et un processus d'avertissement lorsque surviennent des incidents de sécurité. Les autres organisations n'ont pas été en mesure de maintenir le niveau de sensibilisation sur les questions de sécurité dans l'organisation, ou n'ont pas été capables de poursuivre sur cette lancée.

1.38 **Recommandation.** Les ministères et organismes assujettis à la Politique du gouvernement sur la sécurité devraient préparer un plan d'action donnant le calendrier qu'ils entendent suivre pour se conformer pleinement aux exigences en matière de sécurité des TI de la Politique et de la norme sur la gestion de la sécurité des technologies de l'information. Ce plan d'action devrait être approuvé par l'administrateur général ou son délégué et présenté au Secrétariat du Conseil du Trésor.

Réponse du Secrétariat du Conseil du Trésor. Le Secrétariat du Conseil du Trésor souscrit à cette recommandation. Les discussions avec les coordonnateurs de la sécurité des TI visant à élaborer des plans ministériels de respect des exigences de sécurité des TI énoncées dans la Politique du gouvernement sur la sécurité et la norme de gestion de la sécurité des technologies de l'information ont débuté. Les ministères devront soumettre ces plans au Secrétariat d'ici l'été 2005, et ces documents devront être signés par l'administrateur général ou son délégué pour garantir la participation et l'engagement de la haute direction des ministères.

1.39 **Recommandation.** Le Secrétariat du Conseil du Trésor devrait exiger que les ministères et organismes assujettis à la Politique du gouvernement sur la sécurité préparent des plans d'action opportuns en matière de sécurité des TI, faire un suivi de l'exécution de ces plans peu après décembre 2006, et signaler au secrétaire du Conseil du Trésor les organisations qui ne s'y conforment pas.

Réponse du Secrétariat du Conseil du Trésor. Le Secrétariat du Conseil du Trésor souscrit à cette recommandation, de concert avec la recommandation 1.38. Il collaborera avec les ministères et les organismes pour mettre au point un mécanisme commun d'examen et de rapport, et un rapport final sera transmis au secrétaire du Conseil du Trésor au début de 2007.

Les mesures de sécurité des TI devraient tenir compte du niveau de risque

1.40 Dans le souci de protéger les biens et les données du gouvernement, la Politique propose une stratégie de gestion des risques, c'est-à-dire une série de méthodes et de procédures conçues à cette fin. Les ministères et organismes sont tenus de se conformer aux exigences de base de la Politique et de ses normes. De plus, ils sont tenus d'effectuer une évaluation des menaces et des risques en vue de déterminer si le contexte justifie le recours à des mesures de protection plus poussées que les mesures de base. Selon la norme GSTI, les organisations doivent effectuer une évaluation des menaces et des risques « pour chaque programme, système ou service ». L'évaluation peut être « soit simple et concise, soit détaillée et rigoureuse, selon le degré de délicatesse, d'importance et de complexité du programme, du système ou du service faisant l'objet de l'évaluation ». Cette exigence n'est pas nouvelle, puisqu'elle était déjà prévue dans la Politique du gouvernement sur la sécurité de 1994.

1.41 L'affectation des ressources en fonction du niveau de risque est une pratique courante dans la gestion de la sécurité des TI. Comme nous l'avons mentionné dans notre rapport de 2002, « 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. »

1.42 Nous nous attendions à ce que les ministères et organismes se soient conformés à cette exigence de la Politique et des normes, en vigueur depuis longtemps, qu'ils aient effectué une évaluation des menaces et des risques en vue d'identifier les risques et qu'ils aient élaboré des stratégies d'atténuation.

1.43 En général, les ministères et organismes n'ont pas encore évalué les menaces et les risques de manière convenable. À l'exception des organisations où les évaluations sont bien établies, celles-ci sont effectuées de manière non uniforme, voire pas du tout. Des 82 ministères et organismes qui faisaient partie de notre enquête, seulement 37 (soit 45 p. 100) avaient effectué, conformément à la Politique et aux normes, une évaluation des menaces et des risques pesant sur leurs programmes, systèmes et services. De plus, seulement 28 organisations avaient vérifié que les recommandations énoncées dans leurs évaluations avaient été prises en compte avant de mettre en place leurs nouveaux programmes ou systèmes.

1.44 Les motifs sous-tendant la non-évaluation des menaces et des risques sont vagues. Depuis plusieurs années, la GRC offre de l'orientation et de la formation sur la manière de procéder à cette évaluation. En 2001, le Secrétariat a publié le Cadre de gestion intégrée du risque, conçu dans le but de donner aux ministères des lignes directrices sur l'adoption d'une approche systématique de gestion du risque. Au cours des dernières années, le Centre de la sécurité des télécommunications a aussi préparé une méthode et des lignes directrices pour l'exécution d'une évaluation complète. Malgré tout, les ministères et les organismes ne tirent pas pleinement parti de ces outils pour s'assurer que leurs ressources en matière de TI sont bien protégées et ce, de manière rentable.

Certification et accréditation des systèmes des organisations

En vertu de la Politique du gouvernement sur la sécurité et des normes opérationnelles connexes, les ministères et les organismes doivent certifier et accréditer tout système ou application nouveau ou modifié, avant son utilisation. Les organisations doivent approuver par écrit, ou certifier, que toutes les exigences relevées dans l'évaluation des risques ont été satisfaites.

Industrie Canada certifie et accrédite les nouveaux systèmes et les nouvelles applications, de même que les changements majeurs apportés aux applications ou systèmes existants. Développement social Canada a mis au point un modèle de projet fondé sur le cycle de vie qui prévoit la certification et l'accréditation des systèmes et des applications en développement. Cependant, la sécurité des TI n'est pas toujours prise en compte au début du projet. De plus, le risque de ne pas satisfaire aux exigences en matière de sécurité des TI est plus grand parce que la haute direction, à titre de comité d'examen des projets, n'a pas tenu de réunion depuis plus d'un an.

Pêches et Océans Canada et la Commission nationale des libérations conditionnelles ne se conforment toujours pas à cette exigence.

1.45 Les ministères et les organismes qui n'effectuent pas d'évaluation des menaces et des risques dans le cadre de leurs activités ne connaissent pas les risques auxquels ils sont exposés. Par conséquent, si ces organisations ne tiennent pas compte des risques qui pèsent sur leurs TI dans leur profil de risque, il se pourrait qu'elles n'orientent pas leurs efforts ou ne dirigent pas leurs ressources financières vers les stratégies susceptibles d'atténuer le plus efficacement possible leur exposition aux risques liés aux TI, et donc qu'elles ne réalisent pas leurs objectifs.

Exposition — Paramètre mesurant la probabilité qu'une menace se concrétise, les conséquences possibles et les mesures de protection en place.

1.46 **Recommandation.** La haute direction des ministères et des organismes devrait s'assurer que les risques liés à la sécurité des TI sont pris en compte lors de la préparation du profil de risque de l'organisation, et ce en identifiant et en évaluant les principaux risques et enjeux liés à la sécurité des TI et en déterminant le niveau de risque acceptable.

Réponse du Secrétariat du Conseil du Trésor. Le Secrétariat du Conseil du Trésor souscrit à cette recommandation, qui encouragera les ministères et les organismes à élaborer un profil de risque qui tienne compte de la situation de l'ensemble de l'organisation et de tous les facteurs de risque. Le succès de cette mesure dépendra de la supervision exercée par la haute direction. Voir aussi la recommandation 1.47 et la réponse à cette dernière.

1.47 **Recommandation.** Le Secrétariat du Conseil du Trésor devrait fournir aux ministères et aux organismes des lignes directrices et des outils pour qu'ils intègrent la sécurité des TI en tant qu'élément essentiel dans le profil de risque de leur organisation.

Réponse du Secrétariat du Conseil du Trésor. Le Secrétariat du Conseil du Trésor souscrit à cette recommandation, qui est déterminante pour la mise en œuvre de la Politique du gouvernement sur la sécurité. Le Secrétariat travaillera en étroite collaboration avec les principaux organismes responsables de la sécurité, de même qu'avec les ministères hiérarchiques, pour mettre au point les consignes et les outils nécessaires pour inclure la

sécurité des TI dans le processus d'élaboration du profil de risque des organisations, y compris un outil d'auto-évaluation à jour.

Un volet clé de cet effort est le projet en cours dirigé par le Centre de la sécurité des télécommunications et la Gendarmerie royale du Canada en vue de regrouper les lignes directrices de leurs organismes respectifs sur l'évaluation des menaces et des risques (EMR) afin d'instaurer une approche commune qui englobera des processus d'EMR axés sur la sécurité matérielle et des TI. En outre, la norme de gestion du risque de sécurité, qui devrait être au point au début de 2005-2006, fournira un cadre global pour l'intégration du risque de sécurité aux profils de risque des ministères et des organismes.

L'évaluation de la vulnérabilité est un élément important de l'évaluation de la sécurité des TI

Évaluation de la vulnérabilité — Ensemble de procédures servant à recenser et à évaluer les points faibles dans la structure encadrant la sécurité. L'évaluation se fait à l'aide d'outils automatisés permettant d'établir si l'organisation a colmaté les brèches et éliminé les points vulnérables connus de son environnement informatique ou si elle y est toujours exposée.

1.48 Plusieurs ministères et organismes ont effectué une évaluation de la vulnérabilité de leurs systèmes d'information. Cette évaluation, qui vient compléter celle des menaces et des risques, permet de tester dans les systèmes la présence de faiblesses précises, susceptibles de compromettre la sécurité. Elle ne permet pas, par ailleurs, de déterminer si les points vulnérables repérés pourraient être exploités (le test de pénétration couvre cet aspect). On peut exécuter cette évaluation de l'extérieur ou de l'intérieur du périmètre de sécurité.

1.49 Les organisations qui font une évaluation régulière repèrent souvent des faiblesses dans des réseaux auparavant considérés comme sûrs. Cela est attribuable au fait que de nouveaux points de vulnérabilité sont continuellement découverts et exploités dans l'intention de nuire. Bien qu'un certain nombre de points de vulnérabilité viennent de l'extérieur de l'organisation, la plupart des incidents de sécurité (intentionnels ou accidentels) proviennent de l'intérieur, là où les personnes ont facilement accès à l'information et aux systèmes.

1.50 Nous avons examiné un certain nombre d'évaluations de la vulnérabilité effectuées par des consultants de l'extérieur, le Centre de la sécurité des télécommunications et notre bureau (dans le cadre du présent suivi). La plupart font ressortir de graves faiblesses susceptibles d'être exploitées. Dans certains cas, c'est ce qui s'est produit à l'insu des organisations. Il y avait aussi des points faibles qui existaient depuis quelque temps dans d'anciennes versions de produits. Dans ces cas-là, il n'est pas possible d'y remédier et il faut procéder à une mise à niveau des produits pour assurer une protection adéquate.

1.51 La pièce 1.4 montre que, parmi les ministères et organismes faisant partie de notre enquête, 46 (soit 56 p. 100) ont effectué une évaluation de la vulnérabilité au cours des deux dernières années. Les 36 autres organisations participantes (soit 44 p. 100) n'avaient pas fait d'évaluation durant cette période, ou n'en avaient jamais fait.

1.52 Nous avons constaté que les ministères et les organismes ayant effectué une évaluation récemment avaient fait preuve d'une approche progressiste; ils avaient décelé leurs faiblesses en matière de sécurité des TI et s'employaient

Pièce 1.4 Organisations ayant effectué au moins une évaluation de la vulnérabilité au cours des deux dernières années

Taille de l'organisation *	Organisations faisant partie de l'enquête	Organisations ayant effectué une évaluation ou plus	Pourcentage des organisations qui ont fait une évaluation ou plus
petite (moins de 1 000)	54	27	50
moyenne (plus de 1 000 mais moins de 10 000)	22	13	59
grande (plus de 10 000)	6	6	100
Total	**82**	**46**	**56**

* Selon le nombre d'équivalents temps plein (ETP)

en toute priorité à les corriger. Dans les paragraphes 1.53 à 1.59 ci-dessous, nous décrivons les faiblesses les plus graves relevées dans les évaluations que nous avons examinées. Cependant, c'est à dessein que nous ne divulguons ni le nom des organisations en cause, ni des précisions sur les faiblesses.

1.53 **L'accès aux données et aux programmes de nature délicate n'est pas contrôlé comme il se doit.** Les organisations doivent toujours avoir pour objectif d'empêcher les personnes non autorisées d'accéder aux données qui soutiennent les opérations essentielles. Tout accès non autorisé peut mener à une modification, à une suppression ou à une divulgation abusive de données. Pour contrôler l'accès à celles-ci, les organisations utilisent des programmes informatiques permettant de savoir quelles informations sont consultées sur le réseau et par qui elles le sont.

1.54 Dans de nombreux cas, les mesures visant à contrôler l'accès aux systèmes et aux données se sont révélées inadéquates. Nous avons constaté que le risque associé aux contrôles déficients de l'accès augmentait parce que la plupart des organisations n'avaient pas encore de programme complet de surveillance permettant de savoir qui accédait aux réseaux.

1.55 **Les réseaux ne sont pas protégés.** Les réseaux sont composés d'appareils et de logiciels connectés qui permettent aux personnes de partager des données et des programmes informatiques. Les programmes et les données de nature délicate sont conservés sur les réseaux et y transitent. C'est pour cette raison que les réseaux doivent être protégés contre tout accès, manipulation ou utilisation non autorisés, par des personnes de l'extérieur. Les organisations peuvent protéger leurs réseaux en limitant les services offerts et en installant des dispositifs qui bloquent toute demande d'accès aux services et aux données si elle n'est pas autorisée.

1.56 Dans bien des cas, les réseaux des ministères et des organismes ne garantissaient pas un cadre de fonctionnement sécurisé. On y retrouvait des pare-feu visant à protéger d'Internet les réseaux internes; cependant, les

contrôles de réseau en place n'assuraient pas une protection adéquate contre l'accès non autorisé de personnes de l'extérieur. Sans une bonne protection de leurs réseaux, les ministères et les organismes courent un risque accru que des personnes non autorisées accèdent à des données de nature délicate ou que des services soient interrompus ou refusés.

1.57 **Les contrôles de l'accès aux réseaux sont inadéquats.** Les contrôles limitant l'accès à un réseau garantissent que seules les personnes autorisées au sein de l'organisation ont accès aux données essentielles ou de nature délicate. Des contrôles efficaces permettent aux utilisateurs autorisés seulement d'accéder au réseau à distance ou sur place. Ils assurent également des mesures de protection visant à garantir que les utilisateurs ne peuvent contourner les contrôles et causer des pannes de réseau.

Recherche de mots de passe vulnérables

L'utilité des mots de passe est de faire en sorte que seules les personnes autorisées aient accès aux systèmes. Si les mots de passe ne sont pas assez « solides », ils risquent de mettre en péril les programmes informatiques en ouvrant la porte à des « attaques en force ». Par attaque en force, on entend toute tentative visant à deviner le mot de passe d'une personne. Ce genre d'attaque peut réussir rapidement lorsque les mots de passe :

- comportent peu de caractères;
- sont les mêmes que les noms de compte;
- sont les mots de passe implicites (par défaut);
- correspondent à des mots usuels;
- sont dérivés des renseignements connus au sujet de la personne (son nom, son adresse, son équipe sportive préférée, par exemple).

Bon nombre des évaluations de la vulnérabilité que nous avons examinées ont révélé des cas où les mots de passe se prêtaient à des attaques en force. Certains de ces mots de passe servaient à protéger des points d'entrée de nature délicate, dans des systèmes essentiels à la mission de l'organisation.

1.58 Nous avons constaté que dans de nombreux ministères et organismes, les contrôles n'offraient pas la sécurité voulue. Dans bien des cas, les dispositifs n'étaient pas configurés pour empêcher en tout temps l'accès non autorisé aux systèmes installés sur les réseaux.

Droits et autorisations — Étendue de la permission accordée à une personne ou à un dispositif de visionner, d'ajouter, de modifier ou de supprimer des données d'un système informatique.

1.59 La Direction du dirigeant principal de l'information du Secrétariat du Conseil du Trésor a donné aux ministères et aux organismes des lignes directrices sur la manière d'éliminer au maximum les points de vulnérabilité susceptibles de se trouver sur les serveurs de réseau. Cependant, nous avons constaté qu'il y avait des faiblesses dans plusieurs domaines, notamment la gestion des mots de passe et l'attribution des droits et autorisations aux utilisateurs. Citons, à titre d'exemple, quelques situations observées dans certaines organisations :

- les comptes et les mots de passe par défaut du fournisseur étaient encore actifs;
- les mots de passe n'étaient pas définis ou étaient définis incorrectement;

- le personnel bénéficiait d'un accès plus large que nécessaire;
- des services présentant un danger, comme les commandes d'exécution à distance, étaient offerts.

Recherche de faiblesses dans la configuration des systèmes

Il y a vulnérabilité dès qu'une organisation installe des machines ou des logiciels prêts à utiliser et qu'elle ne change pas les paramètres par défaut définis par le fournisseur. Ces valeurs par défaut sont souvent très permissives parce qu'elles sont conçues en vue de faciliter l'installation du nouveau système. Une pratique exemplaire consiste à supprimer les fonctions non utilisées et à restreindre l'accès à un administrateur de système qui, à son tour, autorise les utilisateurs à exécuter certaines opérations. Les valeurs par défaut installées par le fournisseur consistent généralement en un nom de compte d'administrateur, une série standard de privilèges accordés à l'administrateur et un mot de passe. Le fait de changer les valeurs par défaut avant qu'un nouveau composant d'un système soit mis en place constitue également une pratique exemplaire.

Les tests de vulnérabilité exécutés par les ministères sur leurs systèmes ont révélé des cas où les paramètres par défaut de l'administrateur, installés par le fabricant, n'avaient pas été changés. Quiconque utilise ces valeurs par défaut pour entrer dans le système, muni de privilèges d'administrateur, a le parfait contrôle des privilèges accordés aux autres, en plus d'avoir la possibilité de modifier ou de supprimer les fonctions du système. Cette situation est un point de vulnérabilité sérieux.

Il y a lieu d'améliorer davantage la planification de la continuité des activités

1.60 En vertu de la Politique du gouvernement sur la sécurité, les ministères et les organismes doivent établir un programme de planification de la continuité des activités, lequel doit garantir le maintien des services essentiels en cas d'interruption majeure due, par exemple, à une panne de courant prolongée ou à une catastrophe naturelle. Les technologies de l'information constituent une partie importante du programme de planification de la continuité des activités de toute organisation.

1.61 De l'information précieuse pour la planification de la continuité des activités est tirée des deux activités suivantes :

- l'analyse des répercussions sur les opérations, qui permet d'identifier les programmes, systèmes ou services essentiels et d'établir l'ordre de priorité de leur reprise en cas d'interruption;
- l'évaluation des menaces et des risques, qui permet de déterminer et de classer l'information et les biens connexes en fonction de leur nature délicate, d'évaluer les menaces et les points de vulnérabilité qui y sont associés, d'établir le niveau de risque et de recommander les mesures de protection à prendre pour ramener le risque à un niveau acceptable.

1.62 Selon les normes opérationnelles du gouvernement, les ministères et les organismes doivent exécuter ces deux activités, en particulier l'évaluation des menaces et des risques de chacun des programmes, systèmes ou services. L'obligation de procéder à l'analyse des répercussions sur les opérations est nouvelle. Cet aspect n'avait pas fait l'objet de notre vérification en 2002.

1.63 En 2002, nous avions examiné le programme de planification de la continuité des activités de trois ministères et d'un organisme. Aucun d'eux n'avait mis son plan à jour depuis sa préparation au passage à l'an 2000 ni testé ce plan sur une base régulière. Ces deux activités sont des pratiques exemplaires.

1.64 Dans le cadre du présent suivi, nous avons sélectionné 82 ministères et organismes. Nous avons examiné comment les entités gèrent leur programme de planification de la continuité des activités et vérifié si le programme tient compte des exigences de base de la Politique et des normes. Nous n'avons pas examiné le caractère adéquat des plans ou des outils, à savoir l'analyse des répercussions sur les opérations et l'évaluation des menaces et des risques. Nous avons constaté que plusieurs ministères et organismes avaient fait des progrès dans la mise en œuvre de leur programme de planification de la continuité des activités. Cependant, d'après les résultats de notre enquête, les progrès accomplis varient grandement d'une organisation à l'autre.

1.65 Nous avons constaté que 53 entités (soit 65 p. 100) avaient un plan de continuité des activités, mais que seulement 24 (soit 29 p. 100) l'avaient testé au cours des deux dernières années. Les tests, ou mises à l'essai, des plans sur une base régulière sont essentiels pour assurer leur efficacité continue.

1.66 Les quatre organisations qui ont fait l'objet de notre vérification n'avaient pas toutes, dans la même mesure, mis à jour et testé leur plan de continuité des opérations, ni évalué et atténué les risques. Développement social Canada et Industrie Canada étaient dotés d'un bon système de mise à jour et de test, mais ce n'était pas le cas de la Commission nationale des libérations conditionnelles ni de Pêches et Océans Canada. De même, nous avons constaté des différences dans la façon dont les organisations avaient distribué les rôles et les responsabilités concernant la planification de la continuité des activités. Exception faite de la Commission nationale des libérations conditionnelles, les trois ministères avaient amélioré les mécanismes de prise de décisions se rapportant à l'élaboration et à la mise en œuvre de leur programme de planification de la continuité des activités.

Certaines organisations n'ont toujours pas commencé à surveiller la sécurité

1.67 En vertu de la Politique du gouvernement sur la sécurité, les ministères et les organismes doivent exercer une surveillance continue de leur programme de sécurité, en faire la vérification et communiquer leurs constatations au Secrétariat du Conseil du Trésor. Grâce à la surveillance continue et aux comptes rendus périodiques, la direction de l'organisation dispose de l'information voulue sur le caractère adéquat et opportun des mesures prises pour assurer la sécurité des systèmes informatiques.

1.68 Avant 2002, la Politique exigeait des ministères et des organismes qu'ils vérifient la sécurité des technologies de l'information au moins tous les cinq ans. En 2002, nous avions constaté que, des quelque 90 ministères et organismes assujettis à la Politique, seulement 10 avaient présenté des rapports de vérification interne. La plupart des organisations (près de 90 p. 100) ne se conformaient donc pas à cette exigence de la Politique.

1.69 Selon la version révisée de la Politique, les ministères et les organismes doivent toujours surveiller leurs programmes de sécurité, mais ils ne sont plus tenus de les vérifier tous les cinq ans. Ils peuvent maintenant décider de la fréquence des vérifications dans le cadre de leur planification globale.

1.70 Par conséquent, nous nous sommes demandé si les ministères et les organismes n'avaient pas négligé la vérification périodique de leurs pratiques en matière de sécurité des TI. Or, nous avons remarqué des améliorations à ce chapitre. Parmi les ministères et organismes visés par notre enquête, 37 (soit 45 p. 100) avaient vérifié leur programme de sécurité au cours des deux années précédentes (comparativement à 10 p. 100 en 2002).

Pratiques de surveillance des programmes de sécurité dans les organisations

Dans les quatre organisations examinées, les pratiques de surveillance des programmes de sécurité allaient d'insatisfaisantes à inexistantes. Nous avons aussi constaté que lorsque les organisations examinent la sécurité des TI, elles ne corrigent pas toujours les problèmes décelés. Ces examens ont souvent révélé que l'organisation ne se conformait pas à certaines exigences de base, comme instituer des mots de passe « solides » et corriger les faiblesses relevées.

Ainsi, Développement social Canada applique un nouveau processus pour surveiller tout incident de sécurité en matière de TI et y remédier, comme l'exige la Politique. Par contre, il n'a pas défini ce qu'il entend par « incident de sécurité en matière de TI ». Il est donc difficile de signaler et d'analyser les incidents de manière cohérente et de veiller à l'application uniforme des politiques et des normes.

1.71 **Recommandation.** Les ministères et organismes assujettis à la Politique du gouvernement sur la sécurité devraient présenter au Secrétariat du Conseil du Trésor le calendrier annuel de leurs activités prévues en matière de surveillance de la sécurité des TI, y compris les autoévaluations, les évaluations de la vulnérabilité et les travaux de vérification interne. Ils devraient également transmettre au Secrétariat un exemplaire de leurs rapports de vérification interne dans les trois mois qui suivent la vérification.

Réponse du Secrétariat du Conseil du Trésor. En vertu de la Politique sur la vérification interne, les ministères doivent élaborer un plan de vérification au moins une fois par an et en faire parvenir un exemplaire au Secrétariat du Conseil du Trésor. La Politique prévoit en outre que les administrateurs généraux doivent veiller à ce que les exemplaires des rapports sur les vérifications internes achevées parviennent en temps opportun au Secrétariat. Aux termes de la Politique du gouvernement sur la sécurité, les résultats des vérifications internes doivent être communiqués au Secrétariat.

Le Secrétariat du Conseil du Trésor souscrit à cette recommandation, qui obligera les ministères et les organismes à soumettre un calendrier annuel de leurs activités de surveillance de la sécurité des TI. L'examen de ces calendriers par le Secrétariat permettra de s'assurer que les ministères et les organismes surveillent de façon continue leurs activités liées à la sécurité des TI et que le Secrétariat reçoit effectivement les rapports de vérification interne en temps opportun.

La surveillance de la Politique par le Secrétariat du Conseil du Trésor

1.72 Le Secrétariat du Conseil du Trésor n'a pas de processus officiel en place pour demander aux ministères et aux organismes de présenter leurs rapports de vérification ou pour analyser les constatations en matière de sécurité communiquées dans ces rapports. Depuis 2002, le Secrétariat a reçu seulement 10 rapports de vérification sur la sécurité des TI et n'a pas produit de rapport à mi-terme, comme le stipule la Politique. Les rapports de vérification interne pourraient s'avérer des sources d'information précieuses pour brosser un tableau général de la sécurité des TI dans les ministères et les organismes.

1.73 En vertu de la version révisée de la Politique, le Secrétariat est tenu, dans le cadre de ses activités de surveillance générale, de présenter un rapport au Conseil du Trésor sur la mesure dans laquelle la Politique renforce réellement la sécurité. Le rapport devait être remis à l'été de 2004, mais ne l'a pas été. Il existe donc peu d'information de base sur l'état de la sécurité des TI dans l'ensemble du gouvernement.

1.74 **Recommandation.** Le Secrétariat du Conseil du Trésor devrait surveiller les ministères et les organismes afin de s'assurer qu'ils effectuent des vérifications en temps opportun et mènent d'autres activités de surveillance liées à la sécurité des TI.

Réponse du Secrétariat du Conseil du Trésor. Le Secrétariat du Conseil du Trésor souscrit à cette recommandation et collaborera avec les organismes responsables de la sécurité et les représentants des ministères pour mettre au point un mécanisme de surveillance qui respecte cette recommandation et fournit des renseignements adéquats.

Le Secrétariat du Conseil du Trésor trouvera la façon la plus efficace de recueillir l'information nécessaire à l'exercice de cette surveillance en réutilisant les renseignements que les ministères et les organismes fournissent déjà et en ne demandant que l'information supplémentaire requise.

1.75 **Recommandation.** Le Secrétariat du Conseil du Trésor devrait produire sans retard le rapport à mi-terme sur l'efficacité de la Politique du gouvernement sur la sécurité, tel que le prescrit la politique en question.

Réponse du Secrétariat du Conseil du Trésor. Le rapport à mi-terme doit être soumis au Conseil du Trésor au début de 2005.

Conclusion

1.76 Dans l'ensemble, on peut dire que le gouvernement n'a pas fait de progrès satisfaisants dans le renforcement de la sécurité des technologies de l'information depuis notre vérification de 2002.

1.77 Le gouvernement a fait des progrès marqués dans plusieurs secteurs au regard desquels nous avions exprimé des préoccupations. La version révisée de 2002 de la Politique est venue préciser les rôles et les responsabilités des divers intervenants. Depuis lors, les organisations responsables se consultent régulièrement et travaillent ensemble à développer des normes destinées à

renforcer les pratiques de sécurité des TI. La Politique ne contenait pas de normes opérationnelles propres à aider les ministères et les organismes à satisfaire ses diverses exigences. Depuis, la norme opérationnelle appelée Gestion de la sécurité des technologies de l'information a été élaborée, en même temps que d'autres normes connexes.

1.78 Cependant, il reste à élaborer un certain nombre de normes en matière de sécurité des TI, et le Secrétariat n'a pas terminé son évaluation à mi-terme de l'efficacité de la Politique. La planification de la continuité des activités doit être améliorée et la plupart des ministères et des organismes doivent encore faire une évaluation en bonne et due forme des menaces et des risques.

1.79 Depuis 2002, l'usage d'Internet s'est accru, et les ordinateurs portatifs et les technologies sans fil permettent d'accéder à l'information avec facilité et à prix abordable. Il y a davantage de connexions entre les systèmes du gouvernement et celui-ci vise à accroître l'interopérabilité et l'intégration de ses processus administratifs. Dans un tel contexte, il y a un risque accru de voir surgir des problèmes tels que vols de données, attaques malveillantes ou actes criminels. Depuis 2002, les menaces ont proliféré, et celles-ci peuvent causer de graves préjudices à une organisation.

1.80 Malgré une politique plus vigoureuse et en dépit de nouvelles normes et de certains progrès, le gouvernement se doit de corriger de graves faiblesses en matière de sécurité des TI. La majorité des ministères et des organismes ne satisfont pas aux exigences de base de la Politique et des normes connexes.

1.81 Le fait de ne pas se conformer à la Politique ni aux normes, de ne pas être conscient des risques liés à la sécurité des TI et de ne pas savoir comment les atteintes à la sécurité pourraient nuire aux activités est lourd de conséquences possibles. Cela augmente la probabilité que les atteintes à la sécurité violent la confidentialité des renseignements personnels des Canadiens, ce qui pourrait occasionner de sérieux problèmes aux personnes concernées et miner la confiance des Canadiens envers la capacité de leur gouvernement à faire des transactions en ligne dans un environnement sûr et de manière confidentielle.

Réponse globale du gouvernement. Le Secrétariat du Conseil du Trésor fournit les renseignements suivants pour préciser le contexte dans lequel ce dernier et les ministères et organismes du gouvernement du Canada évoluent.

Le gouvernement du Canada œuvre dans un contexte à risque en évolution dynamique qui l'oblige à se protéger activement et en permanence contre les cyberattaques, les virus et les autres menaces propres à Internet. Même s'il faut une politique et des normes pour établir une position commune et si ces documents constituent l'un des éléments clés de la réponse du gouvernement fédéral à l'égard de la sécurité des technologies de l'information (TI), le Secrétariat du Conseil du Trésor et les trois organismes responsables de la sécurité (le Centre de la sécurité des télécommunications, Sécurité publique et Protection civile Canada et la Gendarmerie royale du Canada) fournissent aussi un soutien concret et des directives aux ministères et aux organismes

pour les aider à renforcer leur situation en matière de sécurité des TI et à intervenir promptement et de façon concertée pour prévenir, déceler et contrer toute atteinte à la sécurité à l'échelle de l'administration fédérale. À l'instar de toute autre organisation d'envergure et géographiquement dispersée, le gouvernement du Canada mise de plus en plus sur un contexte en réseau et interdépendant, lequel nécessitera de plus en plus une approche collective en matière de sécurité des TI où la capacité d'un ministère de réagir rapidement à un problème de sécurité et de partager l'information relative à cet incident sera typique d'une entité à sécurité renforcée au XXI^{e} siècle.

Chaque ministère et organisme, de même que l'ensemble du gouvernement du Canada, est de plus en plus tenu de faire preuve de souplesse face à l'évolution rapide de la technologie. Cela nécessitera l'engagement et la collaboration du personnel de toutes les organisations en vue de mettre en commun l'information sur les incidents, les problèmes et les solutions.

De concert avec les organismes responsables de la sécurité, le Secrétariat du Conseil du Trésor et Travaux publics et Services gouvernementaux Canada dirigent aussi la mise en place et l'utilisation d'infrastructures et de services communs de sécurité des TI. Il est plus efficient d'instaurer des mesures comme la détection des intrusions, l'évaluation de la vulnérabilité, l'entretien des logiciels et le développement des systèmes par l'entremise d'une infrastructure commune de TI à gestion centralisée, que de façon différente pour chaque ministère. Les investissements d'envergure du gouvernement du Canada dans les services communs de TI contribuent de façon marquée à rehausser la sécurité de ses opérations et services.

La Voie de communication protégée fournit un ensemble de services d'infrastructure communs et sécuritaires qui protègent la communication de renseignements et l'exécution de diverses opérations pour les particuliers, les entreprises, les employés et les autres administrations. À l'heure actuelle, 122 ministères et organismes recourent à au moins l'un des services offerts par la Voie de communication protégée, à l'appui de leurs propres services, d'information et autres, en ligne. Pour assurer la prestation efficace des services, il faut développer et maintenir la confiance des citoyens, des entreprises et des autres administrations avec lesquelles le gouvernement du Canada traite.

Grâce à la publication, en 2004, de la Politique sur la sécurité nationale et à la mise en place des processus, des comités et des structures organisationnelles connexes nécessaires, le Secrétariat du Conseil du Trésor fera en sorte que les ministères et les organismes appliquent une stratégie propice à l'intégration et à la coordination des plans, des activités, des infrastructures et des opérations. À cet égard, les projets favorisant la mise en commun proactive de l'information et des processus, au sein du gouvernement du Canada et avec les autres administrations, seront déterminants pour cette intégration.

À propos du suivi

Objectif

Le suivi avait pour objectif de déterminer si le Secrétariat du Conseil du Trésor et les ministères avaient donné suite aux recommandations que nous avions formulées dans le chapitre 3 du Rapport de 2002. Nous avons vérifié si, dans l'ensemble, les ministères et les organismes ont mis en place les exigences de base en matière de sécurité des TI visant à protéger les biens et les données informatiques et à assurer la prestation de services de manière sûre et ininterrompue.

Étendue et méthode

Notre vérification a ciblé des entités de deux ordres :

- **Les organismes responsables de la sécurité**. Nous nous sommes intéressés aux activités du Secrétariat du Conseil du Trésor, qui a un rôle de coordination, de leadership et de surveillance à jouer au regard de la sécurité des TI. Nous avons également rencontré des employés de la Gendarmerie royale du Canada, de Sécurité publique et protection civile Canada, du Centre de la sécurité des télécommunications et du Service canadien du renseignement de sécurité.
- **Les ministères et organismes**. Nous avons examiné certaines pratiques de sécurité dans les trois ministères et l'organisme que nous avions examinés en 2002 : Pêches et Océans Canada, Développement social Canada (anciennement, Développement des ressources humaines Canada), Industrie Canada et la Commission nationale des libérations conditionnelles.

Nous avons évalué les résultats du questionnaire d'autoévaluation que le Secrétariat avait envoyé à 97 ministères et organismes. Cette évaluation était volontaire; seulement 46 entités y ont répondu. Les réponses n'étaient pas corroborées. En complément du sondage fait par le Secrétariat, nous avons fait une enquête auprès de 82 ministères et organismes sur certaines pratiques de sécurité. Nous avons obtenu un taux de réponse de 100 p. 100. Nous avons validé les réponses en corroborant les réponses positives d'un échantillon aléatoire de 20 organisations.

Nous avons examiné les mesures de protection établies par les ministères et les organismes pour garantir la sécurité des biens et des données du gouvernement. Nous avons examiné les résultats des évaluations de vulnérabilité et des tests techniques faits par des consultants, le Centre de la sécurité des télécommunications et notre bureau (dans trois ministères). Nous nous sommes assurés que nos tests techniques ne mettaient pas en péril les systèmes visés ou les données qu'ils abritaient.

Nous avons examiné la mesure dans laquelle il y avait eu amélioration dans les secteurs suivants de la sécurité des TI :

- la collaboration et l'échange d'information entre les organisations responsables de la sécurité des TI;
- l'élaboration et la mise en place de normes de sécurité des TI visant à soutenir la politique;
- l'efficacité de la Politique du gouvernement sur la sécurité, ainsi que les mesures de sécurité existantes;
- la planification des mesures d'urgence;
- la gestion des risques.

Nous n'avons pas examiné la Voie de communication protégée, étant donné que ce projet n'avait pas encore officiellement reçu l'aval du Conseil du Trésor au moment de la vérification. En outre, nous n'avons pas examiné les questions de sécurité nationale car celles-ci feront l'objet d'une vérification distincte sur les initiatives d'amélioration de la sécurité nationale, dont les résultats seront communiqués en 2005.

Critères

Comme lors de notre vérification de 2002, nous nous attendions à ce que :

- le cadre de sécurité des technologies de l'information permette de s'assurer que les biens liés aux TI sont protégés et soutiennent la prestation sécurisée et ininterrompue des services gouvernementaux;
- la structure de gouvernance de la sécurité des TI intègre 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 correspondent 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 permettent de prévenir et de détecter les menaces aux TI, et de réagir en conséquence;
- les pratiques de sécurité des TI soient surveillées et réévaluées régulièrement, et que toute vulnérabilité soit traitée.

En outre, nous nous attendions à ce que les nouveaux risques liés à la sécurité des TI soient définis et traités.

Équipe de vérification

Vérificateur général adjoint : Douglas G. Timmins
Directeur principal : Richard Brisebois
Directeurs : Greg Boyd, Tony Brigandi, Guy Dumas

Bernard Battistin
Étienne Robillard

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