CHAMBRE DES COMMUNES
CANADA

Chapitre 1, La sécurité des technologies de l'information du Rapport de février 2005 du vérificateur général du Canada

Rapport du Comité permanent des comptes publics

John Williams, député
Président

Juin 2005

Les transcriptions des réunions publiques du Comité sont disponibles par Internet : http://www.parl.gc.ca

En vente : Communication Canada — Édition, Ottawa, Canada K1A 0S9

Chapitre 1, La sécurité des technologies de l'information du Rapport de février 2005 du vérificateur général du Canada

Rapport du Comité permanent des comptes publics

John Williams, député
Président

Juin 2005

COMITÉ PERMANENT DES COMPTES PUBLICS

PRÉSIDENT

John Williams

VICE-PRÉSIDENTS

Mark Holland
Benoît Sauvageau

MEMBRES

Dean Allison
Gary Carr
David Christopherson
Brian Fitzpatrick
Sébastien Gagnon
Daryl Kramp
Walt Lastewka
Shawn Murphy
Borys Wrzesnewskyj

GREFFIÈRE DU COMITÉ

Elizabeth B. Kingston

SERVICE D'INFORMATION ET DE RECHERCHE PARLEMENTAIRES
BIBLIOTHÈQUE DU PARLEMENT

Brian O'Neal
Marc-André Pigeon

LE COMITÉ PERMANENT DES COMPTES PUBLICS

a l'honneur de présenter son

QUATORZIÈME RAPPORT

Conformément à l'alinéa 108(3)*g*) du Règlement, le Comité permanent des comptes publics a examiné le Chapitre 1 du rapport du Bureau du vérificateur général du Canada en date de février 2005. Les membres du Comité ont convenu de signaler ce qui suit :

TABLE DES MATIÈRES

LISTE DES RECOMMANDATIONS

RECOMMANDATION 1

Que le Secrétariat du Conseil du Trésor accélère l'élaboration et la mise en œuvre de toutes les normes non encore élaborées de sécurité des TI afin qu'elles soient terminées bien avant l'échéance prévue de décembre 2006.

RECOMMANDATION 2

Qu'à compter de septembre 2005, le Secrétariat du Conseil du Trésor présente au Comité permanent des comptes publics des rapports semestriels sur l'élaboration et la mise en œuvre des dernières normes de sécurité des TI.

RECOMMANDATION 3

Que le Secrétariat du Conseil du Trésor présente au Comité permanent des comptes publics un plan d'action détaillé des mesures qu'il entend prendre pour mettre en œuvre les recommandations de la vérificatrice générale du Canada. Ce plan d'action doit préciser un calendrier de mise en œuvre et être présenté au Comité permanent des comptes publics au plus tard le 30 septembre 2005.

RECOMMANDATION 4

Que le Secrétariat du Conseil du Trésor se conforme aux exigences énoncées à l'annexe A de la Politique du gouvernement sur la sécurité et s'efforce de s'acquitter de sa fonction qui consiste à « fournir des conseils et de l'aide en matière de sécurité » et de surveiller « la mise en œuvre de la [P]olitique et l'état de la sécurité au sein du gouvernement du Canada ».

RECOMMANDATION 5

Que le Secrétariat du Conseil du Trésor présente, dans ses rapports ministériels annuels sur le rendement, de l'information sur ses activités de surveillance exercées conformément aux dispositions de l'annexe A de la Politique du gouvernement sur la sécurité. Il doit indiquer la fréquence et la portée de ses activités de surveillance, les résultats obtenus et les mesures correctives prises. Il doit commencer à fournir ces données

dans son rapport couvrant la période ayant pris fin le 31 mars 2005.

RECOMMANDATION 6

Que le gouvernement vérifie si les ressources et les pouvoirs dont dispose le bureau du dirigeant principal de l'information lui permettent de diriger les activités de sécurité des TI à la grandeur du gouvernement, explore la possibilité de regrouper les ressources et les pouvoirs au sein d'un seul organisme qui assumerait l'entière responsabilité de la sécurité des TI à la grandeur du gouvernement et présente ses conclusions au Comité des comptes publics au plus tard le 31 décembre 2005.

RECOMMANDATION 7

Que le Secrétariat du Conseil du Trésor détermine les raisons du changement fréquent des titulaires du poste de dirigeant principal de l'information, analyse les résultats et présente au Comité des comptes publics un rapport ainsi qu'un plan d'action décrivant les mesures qu'il prendra en vue de porter à cinq ans le mandat du titulaire de ce poste, au plus tard le 31 décembre 2005.

RECOMMANDATION 8

Que le Secrétariat du Conseil du Trésor élabore et mette en œuvre un plan de sensibilisation des cadres supérieurs, surtout des sous-ministres, à l'importance de la sécurité des TI et fournisse au Comité permanent des comptes publics une copie de ce plan au plus tard le 30 septembre 2005.

RECOMMANDATION 9

Qu'un lien hiérarchique direct obligatoire soit établi pour les agents de sécurité ministériels et les coordonnateurs de la sécurité des TI par rapport à leurs sous-ministres.

RECOMMANDATION 10

Que les agents de sécurité ministériels occupent un poste stratégique au sein des ministères et des organismes afin qu'ils puissent exercer une influence réelle sur les stratégies pangouvernementales en matière de sécurité des TI et participer aux décisions budgétaires touchant la sécurité.

RECOMMANDATION 11

Que les ministères et organismes soient tenus d'élaborer, en priorité, un plan de continuité des activités, de le mettre à l'essai au moins tous les deux ans et de communiquer les résultats de l'essai au bureau du dirigeant principal de l'information au Secrétariat du Conseil du Trésor.

RECOMMANDATION 12

Que le bureau du dirigeant principal de l'information effectue un examen pangouvernemental afin de vérifier le niveau total des ressources humaines, technologiques et financières consacrées à la sécurité des TI, au cours de l'exercice financier 2005-2006, au sein des ministères et organismes, qu'il en analyse les résultats afin de déterminer si ces ressources sont adéquates et qu'il présente ses conclusions au Parlement au plus tard le 30 avril 2006.

CHAPITRE 1, LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION DU RAPPORT DE FÉVRIER 2005 DU VÉRIFICATEUR GÉNÉRAL DU CANADA

> 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[1].

INTRODUCTION

Dans son rapport d'avril 2002, la vérificatrice générale présentait les conclusions d'une vérification de la sécurité des technologies de l'information (TI) au sein du gouvernement fédéral. Ces conclusions étaient accablantes. Les normes gouvernementales de sécurité des TI étaient incomplètes et bon nombre des normes en place étaient désuètes. Le gouvernement n'avait aucun plan visant leur mise à jour. Tant que ces normes ne seront pas actualisées, la Politique du gouvernement sur la sécurité de 2002, une version révisée de la politique de 1994, ne sera jamais pleinement efficace.

La vérificatrice générale a également constaté que le gouvernement n'avait pas surveillé l'application de sa politique de 1994 sur la sécurité des TI, de sorte qu'il ne possédait 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[2].

Mme Fraser a fait remarquer que la politique révisée (2002) prévoyait la présentation d'un rapport sur l'efficacité de la politique, mais pas avant l'été 2004. Selon elle, le rapport aurait dû être déposé plus tôt. Une ébauche de rapport a été produite en mai 2005.

De nombreux services gouvernementaux sont offerts en format électronique, ce qui permet aux Canadiens d'y avoir accès, de la maison ou du

---

1 Bureau du vérificateur général, *Rapport Le Point 2005,* février 2005, chapitre 1, paragraphe 37.

2 Bureau du vérificateur général du Canada, *Rapport de la vérificatrice générale du Canada à la Chambre des communes*, avril 2002, chapitre 3, paragraphe 3.3.

travail, au moyen de leur ordinateur ou d'autres dispositifs. Leur faible coût, conjugué à leur facilité et rapidité d'accès pour une population disséminée sur un large territoire, garantit l'augmentation du nombre de ces services en ligne. Plus ces services prennent de l'expansion, plus il y a lieu de se préoccuper de la vulnérabilité des services électroniques et des systèmes de stockage de données. À l'extrême, les cyberattaques pourraient entraîner l'usurpation de renseignements personnels, la destruction de données essentielles, la divulgation de renseignements de nature délicate sur les activités du gouvernement ou l'arrêt des systèmes internes du gouvernement.

Le Comité a décidé d'examiner les conclusions de la vérification de suivi de la vérification de 2002 portant sur la sécurité des TI pour la raison précise que les faiblesses de ces systèmes posent des risques potentiels très graves pour la santé et la sécurité des Canadiens et la capacité fonctionnelle du gouvernement.

Pour faciliter son examen, le Comité a rencontré, le 23 mars 2005, la vérificatrice générale Sheila Fraser qui était accompagnée de M. Douglas Timmins (vérificateur général adjoint), M. Richard Brisebois (directeur principal) et M. Guy Dumas (directeur), du Bureau du vérificateur général du Canada. Au cours de cette rencontre, le Comité a également entendu Helen McDonald, dirigeante principale de l'information par intérim pour le gouvernement du Canada, qui relève du Secrétariat du Conseil du Trésor. M. Simon Gauthier, dirigeant principal adjoint de l'information, et M. Pierre Boucher, directeur principal adjoint, Architecture d'entreprise et normes, également du Secrétariat du Conseil du Trésor, accompagnaient Mme McDonald.

OBSERVATIONS ET RECOMMANDATIONS

Au terme de son examen, le Comité exprime de vives préoccupations qui nécessitent une solution dans les domaines suivants : l'état actuel des normes utilisées à l'appui de la sécurité des TI, le rôle du Secrétariat du Conseil du Trésor dans la surveillance de l'état de la sécurité des TI, le rôle des ministères et des organismes ainsi que les ressources disponibles à l'appui de la sécurité des TI.

Normes de sécurité des TI

Les normes gouvernementales de sécurité des TI prescrivent les exigences minimales que doivent respecter tous les ministères et organismes pour s'assurer que leurs systèmes sont protégés contre une intrusion de l'extérieur et la perte de données. En 2002, la vérificatrice générale avait fait savoir au Parlement que ces normes étaient désuètes, une observation troublante face à l'évolution rapide de la technologie de l'information. En 2005, malgré les signes d'amélioration constatés, la vérificatrice générale a fait savoir que dans l'ensemble, le gouvernement n'avait pas fait de « progrès satisfaisants » dans le renforcement de la sécurité des TI depuis sa vérification de 2002 (1.1).

La Politique du gouvernement sur la sécurité (la Politique) énonce des exigences générales en matière de sécurité dans un vaste éventail de domaines, dont les technologies de l'information. Ces exigences sont étayées par des « normes de sécurité » qui précisent ce que doivent faire les ministères et les organismes pour se conformer aux exigences de base de la Politique. Selon la vérificatrice générale, ces normes, de par leur existence, « … encouragent l'instauration de mesures de sécurité uniformes et l'échange de pratiques exemplaires entre les ministères » (1.25).

En 2002, au moment de l'entrée en vigueur de la Politique révisée, beaucoup des 40 normes à l'appui de la sécurité des TI n'étaient pas encore élaborées tandis que d'autres étaient désuètes. En mai 2004, le gouvernement a publié la *Norme de gestion de la sécurité des technologies de l'information* (GSTI). La GSTI porte sur 28 des 40 normes, il en reste donc 12 à élaborer. Les ministères et les organismes doivent attendre que les normes soient terminées avant d'évaluer dans quelle mesure ils respectent la Politique.

Le Secrétariat du Conseil du Trésor (SCT, le Secrétariat) a fait savoir que ces 12 normes recevraient la priorité dans un plan qu'il dévoilera au début de l'exercice financier 2005-2006. La dirigeante principale de l'information par intérim, Helen McDonald, a informé le Comité que 3 des 12 normes sont maintenant à l'état d'ébauche et que le SCT prévoyait les avoir toutes finalisées d'ici décembre 2006.

Le Secrétariat du Conseil du Trésor s'attend à ce que les ministères et les organismes se conforment à la norme GSTI d'ici décembre 2006. Il s'engage à surveiller l'élaboration des normes restantes et la conformité des ministères à ces normes.

Ce témoignage doit être placé dans son contexte. Lorsque l'ancienne dirigeante principale de l'information, Michelle d'Auray, s'est adressée au Comité au sujet de la vérification de la sécurité des TI effectuée en 2002, elle a reconnu que le gouvernement devait accélérer l'élaboration des norms. Mme d'Auray a également dit au Comité — il y a plus de deux ans — que le gouvernement avait « maintenant élaboré un plan exhaustif qui établit l'ordre de priorité des principales normes à mettre en place ».

Il y a donc trois questions à examiner. La première concerne l'établissement des normes dans les délais; ces normes prescrivent les exigences minimales que doivent respecter les ministères et les organismes pour assurer la sécurité de leurs systèmes de TI; sans ces normes, il est impossible de vérifier avec exactitude l'état actuel de la sécurité des TI à la grandeur du gouvernement. La deuxième est le roulement élevé au poste de dirigeant principal de l'information qui empêche le titulaire de faire des prévisions exactes et éclairées du temps et des efforts requis pour effectuer un changement urgent. Et la dernière question, qui découle de la précédente, concerne la crédibilité des déclarations similaires formulées par le SCT aujourd'hui.

Aucun retard n'est excusable dans le contexte actuel. C'est pourquoi le gouvernement doit s'empresser d'assurer la sécurité des TI. Le Comité recommande donc :

RECOMMANDATION 1

Que le Secrétariat du Conseil du Trésor accélère l'élaboration et la mise en œuvre de toutes les normes non encore élaborées de sécurité des TI afin qu'elles soient terminées bien avant l'échéance prévue de décembre 2006.

Dans un contexte en évolution, il est difficile de prévoir avec exactitude le temps nécessaire pour mener à terme des projets complexes. Toutefois, lorsque les représentants du Secrétariat du Conseil du Trésor prennent des engagements devant un comité parlementaire, ils doivent s'efforcer d'être précis et, par la suite, ne ménager aucun effort pour respecter leurs engagements. Lorsque, pour diverses raisons, leurs prévisions s'avèrent trop optimistes et compromettent les engagements pris en fonction de ces prévisions, ils doivent alors en informer le Parlement. C'est seulement de cette manière que le SCT pourra s'acquitter pleinement de son obligation redditionnelle et établir sa crédibilité — ou, dans le cas présent, la rétablir. Le Comité recommande donc :

RECOMMANDATION 2

Qu'à compter de septembre 2005, le Secrétariat du Conseil du Trésor présente au Comité permanent des comptes publics des rapports semestriels sur l'élaboration et la mise en œuvre des dernières normes de sécurité des TI.

Le Comité constate en outre qu'en 2002, le Secrétariat a approuvé toutes les recommandations de la vérificatrice générale. Étant donné que l'espoir suscité par cette réponse est déçu par les conclusions inacceptables de la récente vérification, le Comité recommande :

RECOMMANDATION 3

Que le Secrétariat du Conseil du Trésor présente au Comité permanent des comptes publics un plan d'action détaillé des mesures qu'il entend prendre pour mettre en œuvre les recommandations de la vérificatrice générale du Canada. Ce plan d'action doit préciser un calendrier de mise en œuvre et être présenté au Comité permanent des comptes publics au plus tard le 30 septembre 2005.

Rôle du Secrétariat du Conseil du Trésor

Le bureau du dirigeant principal de l'information se trouve au Secrétariat du Conseil du Trésor, l'organisme central chargé d'assurer la coordination, le leadership, la surveillance et le contrôle de la sécurité des TI à la grandeur du gouvernement.

Le Secrétariat est tenu, aux termes de la Politique du gouvernement sur la sécurité (la Politique), de surveiller les vérifications internes de sécurité des TI et de présenter au Conseil du Trésor un rapport semestriel sur l'efficacité de la Politique.

Le Comité a donc été troublé de constater que le Secrétariat « ne joue pas pleinement son rôle » de contrôle et de surveillance de l'état de la sécurité au sein des ministères et des organismes (1.23). La vérification a permis de constater, par exemple, que le Secrétariat n'avait pas « de processus officiel en place pour demander aux ministères et aux organismes de présenter leurs rapports de vérification [sur la sécurité interne des TI] ou pour analyser les constatations communiquées dans ces rapports » (1.72). Depuis 2002, le Secrétariat n'a reçu que 10 rapports de vérification (1.72); or, la vérificatrice générale a constaté que 37 ministères et organismes avaient vérifié leurs programmes de sécurité des TI au cours des deux dernières années (1:70). Autrement dit, le Secrétariat n'a aucun mécanisme officiel pour obliger ces derniers à produire leurs rapports de vérification des systèmes de sécurité des TI. Cela semble s'expliquer par l'empressement du Secrétariat à refiler aux ministères et organismes le fardeau de la conformité à ses politiques, dans l'espoir que tout se passera bien.

Le Comité est convaincu que, comme dans bien d'autres domaines relevant de sa responsabilité, le Secrétariat du Conseil du Trésor doit abandonner cette approche passive et surveiller activement l'application des politiques qu'il adopte. Le Comité recommande donc :

RECOMMANDATION 4

Que le Secrétariat du Conseil du Trésor se conforme aux exigences énoncées à l'annexe A de la Politique du gouvernement sur la sécurité et s'efforce de s'acquitter de sa fonction qui consiste à « fournir des conseils et de l'aide en matière de sécurité » et de surveiller « la mise en œuvre de la [P]olitique et l'état de la sécurité au sein du gouvernement du Canada ».

RECOMMANDATION 5

Que le Secrétariat du Conseil du Trésor présente, dans ses rapports ministériels annuels sur le rendement, de l'information sur ses activités de surveillance exercées conformément aux dispositions de l'annexe A de la Politique du gouvernement sur la sécurité. Il doit indiquer la fréquence et la portée de ses

activités de surveillance, les résultats obtenus et les mesures correctives prises. Il doit commencer à fournir ces données dans son rapport couvrant la période ayant pris fin le 31 mars 2005.

Le Comité se préoccupe de la capacité du Secrétariat à appliquer la Politique. Il constate que le personnel affecté au bureau du dirigeant principal de l'information (DPI) est peu nombreux et que les titulaires du poste changent fréquemment. Il constate également que la responsabilité de la sécurité des TI est souvent répartie entre le Secrétariat du Conseil du Trésor et les 10 principaux organismes. Paul Rummell, un ancien dirigeant principal de l'information, a dit que la sécurité des TI continuera de poser un problème pour le gouvernement tant que la responsabilité de la mise en œuvre de la politique et des opérations ne sera pas confiée à un organisme unique[3]. Même si la vérificatrice générale a constaté une amélioration de la coopération et de la coordination entre les organismes, le Comité partage l'inquiétude de M. Rummel. Il recommande donc :

RECOMMANDATION 6

Que le gouvernement vérifie si les ressources et les pouvoirs dont dispose le bureau du dirigeant principal de l'information lui permettent de diriger les activités de sécurité des TI à la grandeur du gouvernement, explore la possibilité de regrouper les ressources et les pouvoirs au sein d'un seul organisme qui assumerait l'entière responsabilité de la sécurité des TI à la grandeur du gouvernement et présente ses conclusions au Comité des comptes publics au plus tard le 31 décembre 2005.

RECOMMANDATION 7

Que le Secrétariat du Conseil du Trésor détermine les raisons du changement fréquent des titulaires du poste de dirigeant principal de l'information, analyse les résultats et présente au Comité des comptes publics un rapport ainsi qu'un plan d'action décrivant les mesures qu'il prendra en vue de porter à cinq ans le mandat du titulaire de ce poste, au plus tard le 31 décembre 2005.

Rôle des ministères et organismes

Conformément à la Politique du gouvernement sur la sécurité, les sous-ministres doivent s'assurer que leur ministère a les moyens de se conformer aux exigences de la Politique et de ses normes connexes. Cette responsabilité englobe la conduite d'évaluations des menaces et des risques afin de déterminer si

[3] "Feds respond to Auditor General's IT security critique," ITBusiness.ca, 18 février 2005 (Le gouvernement fédéral répond à la critique de la vérificatrice générale concernant la sécurité des TI).

les ministères ont besoin de garanties autres que celles prescrites par la Politique. La Politique oblige également les ministères à surveiller activement la mise en œuvre de leur programme de sécurité, à faire des vérifications internes périodiques et à en communiquer les résultats au Secrétariat du Conseil du Trésor.

La vérificatrice générale a fait savoir que les systèmes informatiques ministériels étaient vulnérables et que la majorité des ministères ne « satisfaisaient pas aux normes minimales de sécurité » fixées par le Secrétariat du Conseil du Trésor (1.3). Le Comité a notamment été troublé d'apprendre que dans bon nombre de ministères et d'organismes, la haute direction n'est pas « au courant des risques liés à la sécurité des TI et qu'elle ne sait pas comment les atteintes à la sécurité informatique risquent de nuire aux activités et de miner la crédibilité du gouvernement » (1.4).

Les sous-ministres ont pourtant la responsabilité de déterminer l'importance que les ministères accordent à la sécurité des TI et le niveau des ressources affectées à cette fin. La situation ne pourra pas s'améliorer tant que les sous-ministres ne seront pas pleinement au courant de l'état de la sécurité des TI et des risques associés aux lacunes non résolues au sein de leur ministère respectif.

Conformément à la Politique du gouvernement sur la sécurité, le Secrétariat du Conseil du Trésor a la responsabilité de coordonner les activités de formation et de sensibilisation dans le domaine de la sécurité. Conscient de la nécessité de sensibiliser les cadres supérieurs à l'importance de la sécurité des TI, le Secrétariat oblige les sous-ministres à approuver des plans d'action visant à assurer la conformité de leur ministère aux normes d'ici l'automne 2005. Le Comité est d'avis que ces activités devraient s'insérer dans un vaste effort de sensibilisation des cadres supérieurs. Il recommande donc :

RECOMMANDATION 8

Que le Secrétariat du Conseil du Trésor élabore et mette en œuvre un plan de sensibilisation des cadres supérieurs, surtout des sous-ministres, à l'importance de la sécurité des TI et fournisse au Comité permanent des comptes publics une copie de ce plan au plus tard le 30 septembre 2005.

Tous les ministères et organismes ont désigné un agent ministériel de la sécurité et un coordinateur de la sécurité des TI, mais il n'existe aucune assurance que ces personnes rendent compte directement au sous-ministre. Puisque ces personnes doivent nécessairement avoir un accès direct au sous-ministre pour lui faire part de l'état de la sécurité et des besoins à cet égard afin que des mesures soient prises, le Comité recommande :

RECOMMANDATION 9

Qu'un lien hiérarchique direct obligatoire soit établi pour les agents de sécurité ministériels et les coordonnateurs de la sécurité des TI par rapport à leurs sous-ministres.

Le Comité constate également que certains agents de sécurité ministériels ne sont pas en mesure d'influencer les décisions à l'échelle du ministère en matière de sécurité. Il s'agit là d'une grave lacune qui doit être corrigée le plus rapidement possible. Le Comité recommande donc :

RECOMMANDATION 10

Que les agents de sécurité ministériels occupent un poste stratégique au sein des ministères et des organismes afin qu'ils puissent exercer une influence réelle sur les stratégies pangouvernementales en matière de sécurité des TI et participer aux décisions budgétaires touchant la sécurité.

Malgré les meilleures mesures de précaution et de surveillance, les systèmes essentiels de TI des ministères risquent toujours d'être mis hors de service en cas de cyberattaque. C'est pourquoi la Politique du gouvernement sur la sécurité oblige les ministères et les organismes à élaborer des plans de continuité des activités afin de pouvoir demeurer fonctionnels même en cas d'attaque. La vérificatrice a constaté que plus de la moitié des ministères (53 sur 82, soit 65 p. 100) avaient élaboré un tel plan, mais que seulement 24 l'avaient mis à l'essai au cours des deux dernières années. Cela est inacceptable. Le Comité recommande :

RECOMMANDATION 11

Que les ministères et organismes soient tenus d'élaborer, en priorité, un plan de continuité des activités, de le mettre à l'essai au moins tous les deux ans et de communiquer les résultats de l'essai au bureau du dirigeant principal de l'information au Secrétariat du Conseil du Trésor.

Ressources disponibles à l'appui de la sécurité des TI

Les décisions relatives à la répartition des ressources dans le budget de fonctionnement des ministères incombent aux sous-ministres. La vérification a démontré que de nombreux sous-ministres ne connaissaient pas l'état de la sécurité des TI au sein de leur propre ministère ou n'y attachaient pas suffisamment d'importance. Cette constatation permet de conclure que la sécurité des TI au sein des ministères ne reçoit pas les ressources requises pour faire face aux défis de plus en plus nombreux dans ce domaine. Le Comité recommande donc :

RECOMMANDATION 12

Que le bureau du dirigeant principal de l'information effectue un examen pangouvernemental afin de vérifier le niveau total des ressources humaines, technologiques et financières consacrées à la sécurité des TI, au cours de l'exercice financier 2005-2006, au sein des ministères et organismes, qu'il en analyse les résultats afin de déterminer si ces ressources sont adéquates et qu'il présente ses conclusions au Parlement au plus tard le 30 avril 2006.

CONCLUSION

Au Canada comme ailleurs, les faiblesses inhérentes à l'utilisation des communications informatiques, au stockage des données et aux systèmes de transmission de données sont très connus. Les menaces à l'endroit de ces systèmes se multiplient au fur et à mesure que notre société et nos gouvernements deviennent plus dépendants de ces systèmes pour gérer et fournir une énorme quantité de transactions et de services publics et privés. Bon nombre de ces transactions sont d'une nature commerciale ou financière ou encore concernent la santé et la sécurité du public.

Le gouvernement fédéral est la plus importante entité au Canada. Le volume de ses échanges avec des groupes et des particuliers est énorme et, comme la population est disséminée sur un vaste territoire, il ne pourra faire autrement que de grossir. Les services deviendront plus complexes, plus étendus et, du point de vue des consommateurs, moins chers et plus faciles à obtenir et à utiliser.

En plus de stocker une vaste quantité de données sensibles, le gouvernement est l'un des principaux fournisseurs de services et de renseignements aux Canadiens par voie électronique. Bon nombre de ses services sont considérés essentiels, par exemple, le Régime de pensions du Canada, le Régime d'assurance-emploi et d'autres prestations sociales, les paiements aux fournisseurs, les transferts de fonds à d'autres paliers de gouvernement, les communications inter- et intra-gouvernementales concernant la santé, la sécurité et d'autres enjeux d'importance.

Dans ce contexte, il est impératif d'assurer un niveau maximal de sécurité afin de protéger ces interactions et la multitude de données contre toute intrusion. Toute lacune ou défaillance du système de sécurité des TI aurait de graves conséquences sur les citoyens canadiens et la disponibilité des services de tout genre dont ils dépendent. En outre, comme dans tout régime démocratique, les institutions du gouvernement ne fonctionnent que dans la mesure où elles sont perçues comme légitimes et dignes de confiance par les citoyens. À titre de gardien de données parmi les plus personnelles de ses citoyens, le gouvernement doit donc prendre des précautions extrêmes pour conserver ces renseignements.

Autrement, selon la vérificatrice générale, « 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 » (1.4).

De l'avis du Comité, il est impossible de sous-estimer les répercussions néfastes susceptibles de découler d'une incapacité à protéger efficacement les systèmes de TI du gouvernement contre une intrusion ou une panne. Ceux qui se sont vu confier la responsabilité de protéger ces systèmes — les titulaires de postes de direction au sein des organismes centraux et des ministères et organismes — doivent être pleinement conscients des risques élevés associés à tout défaut d'exercer une surveillance adéquate des systèmes de sécurité des TI et de prendre les mesures correctives immédiates lorsque des lacunes sont constatées.

Dans les semaines qui ont suivi l'examen du Comité, les résultats d'une vérification interne, obtenus suite à une demande d'accès à l'information, indiquaient qu'il y avait des motifs de s'inquiéter. Selon un article de journal, une vérification interne menée en 2004 à l'Agence du revenu du Canada a révélé que les ordinateurs portatifs utilisés à l'extérieur du bureau n'étaient pas verrouillés correctement, que les renseignements confidentiels contenus dans les ordinateurs étaient à la merci des pirates et que les employés ignoraient qu'ils étaient tenus de signaler toute activité criminelle. Des 3 000 employés interrogés, plus de la moitié ne savaient pas comment signaler un incident mettant en péril la sécurité. Les gestionnaires ont indiqué qu'ils ne savaient pas quoi faire pour surveiller les systèmes informatiques de l'Agence[4]. L'article ajoute que quatre ordinateurs volés en 2003 dans un bureau de l'Agence du revenu de Laval (Québec) contenaient des données sur 120 000 Canadiens, dont leur numéro d'assurance sociale. Cet article et les conclusions de l'enquête de la vérificatrice générale démontrent clairement que la sécurité des TI est menacée dans toutes les entités gouvernementales, y compris dans les grandes institutions responsables du traitement des données personnelles les plus sensibles concernant les citoyens canadiens.

Le Comité s'attend donc à ce que le gouvernement et le Secrétariat du Conseil du Trésor s'acquittent, de toute urgence, des engagements qu'ils ont pris pour régler les lacunes en ce qui concerne la sécurité des TI, mettent en œuvre les recommandations de la vérificatrice générale et s'assurent que les Canadiens ont un accès sûr et digne de confiance aux programmes et services électroniques du gouvernement.

---

[4] Security Report blasts tax collectors, *Globe and Mail*, 25 avril 2005. (Un rapport sur la sécurité fait bondir les percepteurs d'impôts).

ANNEXE A
LISTE DES TÉMOINS

Organismes et individus	Date	Réunion
Bureau du vérificateur général du Canada	23/03/2005	25
Richard Brisebois, directeur principal		
Guy Dumas, directeur		
Douglas Timmins, vérificateur général adjoint		
Secrétariat du Conseil du Trésor du Canada		
Pierre Boucher, directeur principal, Architecture, Normes et Ingénierie		
Simon Gauthier, dirigeant principal associé de l'information		
Helen McDonald, dirigeant principal de l'information		

DEMANDE DE RÉPONSE DU GOUVERNEMENT

Conformément à l'article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au rapport.

Un exemplaire des Procès-verbaux pertinents (*réunions n^{o} 25 et 40 incluant le présent rapport*) est déposé.

Respectueusement soumis,

Le président
John Williams, député

PROCÈS-VERBAL

Le mercredi 1 juin 2005
(*Séance n^{o} 40*)

Le Comité permanent des comptes publics se réunit aujourd'hui à huis clos à 15 h 32, dans la pièce 237-C de l'édifice du Centre, sous la présidence de John Williams, président.

Membres du Comité présents : Dean Allison, Gary Carr, David Christopherson, Brian Fitzpatrick, Sébastien Gagnon, Mark Holland, Daryl Kramp, l'hon. Shawn Murphy, Benoît Sauvageau, John Williams et Borys Wrzesnewskyj.

Membre substitut présent : L'hon. Robert Thibault pour L'hon. Walt Lastewka.

Aussi présent : *Bibliothèque du Parlement* : Brian O'Neal, analyste.

Conformément à l'article 81(7) du Règlement, le Comité reprend l'étude du Rapport sur les plans et priorités 2005-2006 du Bureau du vérificateur général du Canada.

Le Comité entreprend l'étude d'une ébauche de rapport.

Il est convenu, — Que le Comité adopte l'ébauche de rapport comme le rapport du Comité à la Chambre.

Il est convenu, — Que, conformément à l'article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au rapport.

Il est convenu, — Que, dans la mesure où cela ne modifie pas le contenu du rapport, le président, le greffier et les analystes soient autorisés à apporter au rapport les modifications jugées nécessaires (erreurs de grammaire et de style).

Il est convenu, — Que le président présente le rapport à la Chambre dès que possible après l'expiration de la période de révision de quarante-huit (48) heures.

Il est convenu, — Que le greffier et les analystes émettent, en accord avec le président, un communiqué.

Conformément à l'article 108(3)g) du Règlement, le Comité reprend l'étude du chapitre 1, La sécurité des technologies de l'information du Rapport de février 2005 du vérificateur général du Canada renvoyé au Comité le 15 février 2005.

Le Comité entreprend l'étude d'une ébauche de rapport.

Il est convenu, — Que le Comité adopte l'ébauche de rapport comme le rapport du Comité à la Chambre.

Il est convenu, — Que, conformément à l’article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au rapport.

Il est convenu, — Que, dans la mesure où cela ne modifie pas le contenu du rapport, le président, le greffier et les analystes soient autorisés à apporter au rapport les modifications jugées nécessaires (erreurs de grammaire et de style).

Il est convenu, — Que le président présente le rapport à la Chambre dès que possible après l’expiration de la période de révision de quarante-huit (48) heures.

Il est convenu, — Que le greffier et les analystes émettent, en accord avec le président, un communiqué.

À 16 h 43, le Comité s’ajourne jusqu’à nouvelle convocation de la présidence.

La greffière du Comité

Elizabeth B. Kingston