Chambre des communes
CANADA

Comité permanent des comptes publics

PACP • NUMÉRO 025 • 1re SESSION • 38e LÉGISLATURE

TÉMOIGNAGES

Le mercredi 23 mars 2005

Président

M. John Williams

Toutes les publications parlementaires sont disponibles sur le
réseau électronique « Parliamentary Internet Parlementaire » à l'adresse suivante :

http://www.parl.gc.ca

Comité permanent des comptes publics

Le mercredi 23 mars 2005

● (1535)

[*Traduction*]

Le président (M. John Williams (Edmonton—St. Albert, PCC)): Bonjour à tous.

Aujourd'hui, la séance est télévisée. Conformément à l'alinéa 108 (3)*g*) du Règlement, nous examinons le chapitre 1, « La sécurité des technologies de l'information », du rapport de février 2005 du vérificateur général du Canada, dont le comité a été saisi le 15 février 2005.

Nous accueillons les représentants suivants du Bureau du vérificateur général du Canada : M. Douglas Timmins, vérificateur général adjoint; M. Richard Brisebois, directeur principal; et M. Guy Dumas, directeur. Nous recevons également des représentants du Secrétariat du Conseil du Trésor : M. Pierre Boucher, directeur principal, architecture, normes et ingénierie; Mme Helen McDonald, dirigeant principal de l'information; et M. Simon Gauthier, dirigeant principal associé de l'information.

Avant d'aller plus loin, je tiens à faire deux commentaires. On m'a informé qu'un rappel au Règlement allait être soulevé. Avant de l'entendre, je tiens à vous rappeler que le comité fédéral des comptes publics rencontre, une fois l'an, les comités des comptes publics des provinces. Cette année, la rencontre va avoir lieu du 21 au 23 août. Un budget sera déposé le 4 avril.

La réunion va se dérouler à Niagara-on-the-Lake, votre ville natale, monsieur Lastewka. J'espère que vous allez nous faire bon accueil quand nous serons là.

L'hon. Walt Lastewka (St. Catharines, Lib.): Absolument.

Le président: Comme je l'ai indiqué, je compte déposer un budget le 4 avril. Je vous invite à inscrire ces dates à votre agenda. Je veux que le comité des comptes publics soit bien représenté, qu'il montre au reste du pays comment se font les choses à Ottawa—à quel point nous faisons bien notre travail.

Quoi qu'il en soit, M. Kramp souhaite invoquer le Règlement.

M. Daryl Kramp (Prince Edward—Hastings, PCC): Je désire soulever aujourd'hui une question très grave qui porte sur les privilèges du comité et la séance à huis clos qu'il a tenue le lundi 21 mars 2005. J'ai été étonné de lire aujourd'hui, dans le quotidien The Gazette de Montréal, à la page A16, ce qui suit :

> ...Mark Holland, député libéral et membre du comité, a affirmé qu'on demandait au comité d'examiner une question qui a déjà été réglée par la vérificatrice générale. Il a dit que c'est pour cette raison qu'il a exercé des pressions afin que le comité entende Dodge et Fraser, ainsi que O'Leary, Cutler et Kinsella.
>
> « Il s'agit d'une tentative visant à se servir du comité pour faire des gains dans un esprit partisan et à traîner devant le comité des gens qui ont des liens avec le premier ministre dans l'espoir de les mettre dans l'embarras de manière partisane. »

Monsieur le président, M. Sauvageau, député du Bloc québécois, est cité dans le même article. Il dit être heureux de voir que le comité a accepté de se pencher sur la question :

> « Nous allons voir que ce n'était pas seulement dans le groupe formé de Guité, (Alfonso) Gagliano et Chrétien qu'il se passait des choses. Des comportements similaires ont été observés, semble-t-il, au sein du ministère des Finances. »

Comme M. Sauvageau ne faisait pas directement référence aux propos tenus au cours d'une séance à huis clos du comité, ses commentaires ne sont pas visés par mon rappel au Règlement.

La divulgation de délibérations à huis clos de comités a déjà fait l'objet d'un examen à la Chambre. Je vous renvoie à la note en bas de page 96, page 68, de Marleau-Montpetit. Par ailleurs, en 1987, le Président a déterminé qu'il y avait à première vue matière à privilège parce que John Parry, le député de Kenora—Rainy River, avait divulgué le résultat d'un vote à huis clos. Je vous renvoie aux Débats du 29 avril 1987, pages 5299, 5329 et 5330, entre autres.

Il est également question de l'affaire John Parry dans la note en bas de page 362, page 130 de Marleau-Montpetit. À l'époque, le comité a renvoyé la question à la Chambre. Dans la note 363, toujours à la même page, on précise que le rapport à la Chambre concluait ce qui suit : « Votre comité estime de son devoir de soumettre cette question à la Chambre afin qu'elle puisse l'étudier, car il y a peut-être eu violation de privilège. »

Monsieur le président, à la lumière des commentaires faits par le député d'Ajax—Pickering, M. Mark Holland, dans le quotidien The Gazette de Montréal, page A16, le 23 mars 2005, alors qu'il a fait allusion aux délibérations à huis clos du Comité permanent des comptes publics et aurait affirmé :

> ...Mark Holland, député libéral et membre du comité, a affirmé qu'on demandait au comité d'examiner une question qui a déjà été réglée par la vérificatrice générale. Il a dit que c'est pour cette raison qu'il a exercé des pressions afin que le comité entende Dodge et Fraser, ainsi que O'Leary, Cutler et Kinsella.
>
> « Il s'agit d'une tentative visant à se servir du comité pour faire des gains dans un esprit partisan et à traîner devant le comité des gens qui ont des liens avec le premier ministre dans l'espoir de les mettre dans l'embarras de manière partisane. »

J'estime qu'une motion doit être présentée afin de signifier qu'il y a eu atteinte aux privilèges du comité ou qu'un outrage a pu se produire. Je demande donc au comité de faire rapport à la Chambre pour indiquer qu'il est d'avis qu'il y a, à première vue, atteinte au privilège ou outrage, et qu'il est de son devoir de soumettre cette question au Président et de permettre à la Chambre d'y réfléchir.

Le président: Merci beaucoup, monsieur Kramp.

M. Holland vient de se joindre à nous; il n'a pas entendu ce que vous avez dit.

Monsieur Holland, M. Kramp a relevé les commentaires que vous avez faits dans le journal The Gazette de Montréal—je pense que c'est l'édition d'aujourd'hui—au sujet de la séance à huis clos que le comité a tenue, lundi. Il vous a cité deux fois. Il a demandé au comité de considérer qu'il pourrait y avoir, de prime abord, atteinte au privilège ou outrage et d'en faire rapport à la Chambre.

Avez-vous quelque chose à dire à ce sujet, monsieur Holland.

M. Mark Holland (Ajax—Pickering, Lib.): Puis-je voir l'article?

Le président: En avez-vous un exemplaire, monsieur Kramp?

M. Daryl Kramp: Peut-être. Oui.

Le président: Le voilà, monsieur Holland.

● (1540)

M. Mark Holland: Tout ce que je peux dire, c'est qu'au cours de notre conversation, Elizabeth Thompson m'a transmis les noms des personnes qui allaient comparaître. J'ai parlé de manière générale du chapitre 5 du rapport de 2003. Je n'ai jamais dit que j'exerçais des pressions afin que le comité entende certains témoins.

J'ai dit que si on allait demander au comité de se pencher sur la question, il faudrait que celui-ci l'examine de manière globale et dans un esprit non partisan. Je pense que la déclaration suivante, « Il s'agit d'une tentative visant à se servir du comité pour faire des gains dans un esprit partisan et à traîner devant le comité des gens qui ont des liens avec le premier ministre dans l'espoir de les mettre dans l'embarras de manière partisane », reflète, grosso modo, les commentaires que j'ai formulés. Je n'ai pas divulgué le contenu de conversations tenues derrière des portes closes.

Le président: C'est en fait le paragraphe qui vient juste avant qui semble poser problème : « Il a dit que c'est pour cette raison qu'il a exercé des pressions afin que le comité entende Dodge et Fraser, ainsi que O'Leary, Cutler et Kinsella. »

M. Mark Holland: Mes propos ont été paraphrasés. Je n'ai mentionné aucun nom. J'ai dit que j'avais exercé des pressions afin que le comité entende un grand nombre de personnes, et pas seulement quelques témoins bien précis. Je n'ai mentionné aucun nom, aucun détail particulier. J'ai exercé des pressions de façon générale. On a paraphrasé mes propos et ajouté des noms.

Le président: Monsieur Fitzpatrick.

M. Brian Fitzpatrick (Prince Albert, PCC): À mon avis, le fait de discuter du sujet en termes généraux constitue une violation du principe du huis clos. Pour moi, le « huis clos » s'applique à tout ce qui se dit à l'intérieur de cette pièce. On ne doit rien répéter à l'extérieur. Même le fait de mentionner qu'il a été question du chapitre 5 correspond à une divulgation de propos tenus à huis clos. Laisser entendre qu'il a été question de stratégies au cours de la réunion, qu'on a exercé des pressions pour que certains témoins soient entendus, ainsi de suite, constitue une violation claire et nette du principe.

La seule question qui me vient à l'esprit est la suivante : s'agit-il d'une erreur ou d'un geste délibéré? S'il s'agit d'un geste délibéré, il y a lieu de s'inquiéter. Les gens peuvent commettre des erreurs, des lapsus, mais à mon avis, tout geste calculé et délibéré constitue un outrage et une atteinte aux privilèges des députés.

Le président: En passant, je tiens à dire aux membres du comité que le rappel de M. Kramp concerne les propos tenus à huis clos. Par conséquent, si, au cours d'une réunion publique, un membre discute de ce qui s'est passé à huis clos, il risque peut-être de se placer dans la même situation que M. Holland, situation qui a été dénoncée par M. Kramp. Vous devez faire très attention quand vous faites référence à une réunion tenue à huis clos. Je vous demande de vous en tenir à ce qui a été rapporté dans les médias, et non à ce qui a été dit à la réunion.

Monsieur Holland, souhaitez-vous ajouter quelque chose?

M. Mark Holland: Oui. J'aimerais faire quelques observations.

D'abord, je ne sais pas comment la journaliste a obtenu la liste des témoins, mais elle l'avait en main à ce moment-là. Je ne sais pas si la liste avait été rendue publique ou non. Je tiens à ce que ce soit clair.

Ensuite, quand elle a communiqué avec moi, je lui ai parlé de façon générale du chapitre 5. Encore une fois, cette question relève du domaine public. De nombreux articles de journaux ont mentionné le fait que le comité comptait examiner ce chapitre en particulier. Tout cela est de notoriété publique. Je lui ai parlé de l'opportunité du comité de s'engager dans l'examen de ce chapitre en particulier. Encore une fois, il en a été question, entre autres, dans The Gazette et La Presse, si je ne m'abuse. On savait fort bien que le comité allait se pencher là-dessus. Je lui ait fait part, en termes généraux, des x inquiétudes que suscitait chez moi cet examen et du fait qu'il fallait entendre un grand nombre de témoins.

Or, elle a paraphrasé mes propos en y ajoutant les noms de témoins. Je ne sais pas d'où provient cette liste. Comme je l'ai mentionné, la journaliste, quand elle a communiqué avec moi, m'a fourni les noms et des personnes qui allaient être convoquées et des témoins que je voulais que le comité entende. Je n'ai pas répété ce qu'elle a dit. Toutefois, elle m'a fourni non seulement la liste des témoins qui ont été proposés à la réunion, mais également la liste de ceux que je voulais que le comité entende. Je n'ai pas mentionné de noms. J'ai dit, en termes très généraux, qu'il ne faudrait pas que le comité, s'il s'engage dans cet examen, entende uniquement des témoins qui ont des liens partisans. Mes propos ont été paraphrasés : on a dit que j'exerçais des pressions afin que le comité entende certains témoins.

● (1545)

Le président: En passant, la greffière me dit que le fait que nous allons examiner le chapitre 5 est de notoriété publique, puisqu'il en est question dans le rapport que le comité de direction a présenté au comité principal. Ce qui pose problème, c'est que les discussions que nous avons tenues à huis clos sur la marche à suivre que nous allions adopter figurent maintenant dans les médias.

Monsieur Kramp.

M. Daryl Kramp: Je suis inquiet, pour plusieurs raisons.

Mon objectif ici est de travailler avec mes collègues de tous les partis à la Chambre. Nous sommes tous humains. Nous commettons tous des erreurs, et nous le savons. Nous l'avons reconnu lors d'une réunion antérieure, quand nous avons discuté à huis clos d'incidents qui s'étaient produits. D'après l'attitude des membres et du président du comité, les choses semblaient assez claires. Si c'était la première fois qu'une telle affaire était portée à l'attention du comité, nous pourrions nous attendre à une certaine latitude et compréhension de sa part.

Toutefois, je crois sincèrement que nos discussions doivent rester confidentielles. La séance à huis clos a pour but de permettre l'examen de questions comme celle-ci. Ce qui me préoccupe au plus haut point, c'est le fait que nous nous retrouvons dans une situation similaire alors que nous venons à peine de tenir une réunion sur le sujet. Nous devons réagir, clore le dossier et aller de l'avant avec nos travaux dans un esprit de collégialité et de compréhension, en prenant les mesures qui s'imposent, littéralement, au nom du comité et du Parlement.

Le président: Monsieur Carr.

M. Gary Carr (Halton, Lib.): Merci, monsieur le président.

J'aimerais avoir des précisions. Je devrais peut-être le savoir, mais est-ce que quelqu'un connaissait le contenu de la liste des témoins, ou est-ce que cette information a elle aussi fait l'objet d'une fuite? La liste a-t-elle été rendue publique, ou a-t-elle fait l'objet d'une fuite?

Le président: Nous avons adopté une motion qui prévoyait la tenue d'une réunion à laquelle seraient convoqués des témoins. La greffière me dit que cette motion a été rendue publique, ce qui fait que l'on connaissait les noms des personnes convoquées. Pour ce qui est de la question de savoir qui a proposé ces noms, comment la liste a été établie, ces renseignements ne relèvent pas du domaine public. Seul le fait qu'une motion a été adoptée et que ces personnes seraient convoquées en vertu de celle-ci était connu du public.

Monsieur Fitzpatrick.

M. Brian Fitzpatrick: Je voudrais que l'on clarifie un point. Toutefois, avant cela, je tiens à préciser que lorsque l'on discute publiquement de propos qui ont été tenus à l'interne, que ce soit avec un journaliste ou une autre personne, on se trouve, dans les faits, à miner le principe du huis clos, parce que le débat est censé se dérouler derrière des portes closes. Se laisser entraîner dans ce genre de discussion avec un journaliste n'est pas la chose à faire.

Plus important encore, la journaliste, dans son article, cite textuellement M. Holland. Elle lui attribue ces propos. M. Holland nie tout. Je tiens à ce que les choses soient bien claires. Est-ce que M. Holland est en train de dire que la journaliste a dénaturé ses propos, ou encore qu'elle ment? À mon avis, la journaliste a cité textuellement M. Holland.

Le président: Monsieur Holland.

M. Mark Holland: Je vais répéter ce que j'ai dit pour que ce soit très clair. Je ne sais pas d'où vient la liste des témoins. Je suis toutefois heureux d'apprendre qu'elle a été rendue publique dans le cadre de la motion. Quand on a communiqué avec moi et qu'on m'a posé des questions au sujet des témoins dont le nom figurait sur la liste, j'ai dit, au cours de la conversation, que j'avais exercé des pressions pour que le comité n'entende pas uniquement des témoins qui ont des liens partisans. Elle a mentionné les noms de Mme Fraser et de M. Dodge. Quand j'ai dit que j'avais demandé que le comité n'entende pas uniquement des témoins qui ont des liens partisans, elle a avancé certains noms. Elle n'a pas menti, mais elle ne m'a pas cité textuellement.

● (1550)

Le président: Monsieur Holland, je tiens à préciser que vous êtes en train de décrire ce qui s'est passé à huis clos, ce qui pose problème. Nous sommes en train de tenir une séance publique et de discuter de ce qui s'est passé à huis clos. Comme je l'ai déjà mentionné, les membres du comité devraient éviter de parler de ce qui s'est dit à la réunion et s'en tenir aux documents qui relèvent du domaine public, c'est-à-dire la motion, qui donne la liste des témoins, et les articles parus dans les journaux. Il n'y aura aucun problème si vous limitez vos propos à ces documents.

M. Mark Holland: Pour que les choses soient bien claires, j'aimerais préciser qu'il y avait deux volets à mon commentaire. D'une part, j'ai fait valoir mon point de vue quant à la pertinence pour nous d'étudier ce chapitre-là; j'ai simplement exprimer mon opinion à ce sujet, ce qui me semble tout à fait être dans mes droits. D'autre part, pour ce qui est des témoins du public, je me suis demandé s'il pouvait s'agir seulement de témoins ayant des liens partisans ou s'il ne serait pas préférable de compter sur un plus large éventail de témoins. J'exprimais mon opinion; je ne régurgitais pas les délibérations du comité. Je voulais faire valoir que, selon moi, nous devons établir une liste de témoins qui ne se limite pas aux seuls partisans; c'est ce que j'ai dit dans cette citation. En exprimant mon opinion, je ne régurgite pas le contenu d'une séance à huis clos. Il y a une différence énorme.

Si vous lisez bien la transcription de cette entrevue, vous constaterez que je ne fais que présenter mon point de vue sur la façon dont les choses devraient se passer. Je ne parle ni du contenu ni du sujet de la séance à huis clos.

Le président: Monsieur Lastewka.

L'hon. Walt Lastewka: Je voudrais continuer dans le sens de l'intervention de M. Carr.

Soit dit en passant, j'ai appris quelque chose : je ne savais pas que les noms reliés à une motion adoptée à huis clos entraient également dans le domaine public. Je pense que c'est un bon enseignement à tirer. Nous avons quelques nouveaux députés dans nos rangs, et je pense que c'est bon que tous l'apprennent.

Je prends très au sérieux les commentaires de M. Kramp, mais j'estime que nous ne devrions pas pousser l'affaire plus loin. Nous devrions simplement reprendre nos travaux, mais en tirer tout de même une bonne leçon.

Le président: Monsieur Fitzpatrick.

M. Brian Fitzpatrick: Je veux simplement revenir à la question de la divulgation des délibérations tenues lors de séances à huis clos. Pour moi, le huis clos est synonyme de confidentialité. Si vous déclarez publiquement qu'un autre participant à une réunion avait présumément une liste de témoins ayant des liens partisans, vous contrevenez au principe du huis clos en diffusant de l'information à l'extérieur de l'enceinte de la réunion.

Le président: Veuillez adresser vos observations à la présidence.

M. Brian Fitzpatrick: C'est ce que je voulais faire valoir. Les débats et les discussions sont tout aussi importants que les détails des délibérations de ces réunions. La faute ne se limite pas, monsieur le président, à la divulgation des détails de nos réunions au public. Si vous portez la teneur des discussions et des débats du comité à l'attention des gens de l'extérieur, vous enfreignez tout autant le principe du huis clos.

Le président: Je ne me réjouis pas particulièrement d'avoir à régler ce genre de situation.

M. Kramp m'avait remis au préalable le texte de sa déclaration et j'ai eu la chance d'en discuter avec notre greffière. Nous ne pouvons pas faire une entorse au règlement ou décider quelles règles s'appliquent à nous; nous devons tous respecter un ensemble commun de règles. C'est ce qui a permis l'évolution du Parlement. C'est pourquoi aussi nous avons le Marleau et Montpetit, avec son millier de pages de précédents nous permettant de déterminer ce qui est acceptable ou non dans un cas particulier. Si on considère la motion déposée par M. Kramp, le Marleau et Montpetit prévoit ce qui suit:

> Si le président du comité estime que la question concerne un privilège... le comité peut alors envisager de présenter un rapport à la Chambre sur la question. Le président du comité recevra alors une motion qui constituera le texte du rapport. On devra y exposer clairement la situation, résumer les faits, nommer les personnes en cause, indiquer qu'il pourrait y avoir atteinte au privilège ou outrage, et demander à la Chambre de prendre les mesures qui s'imposent. La motion peut être débattue et modifiée, et le comité devra l'étudier en priorité. Si le comité décide qu'il y a effectivement lieu de faire rapport de la question à la Chambre, il adoptera le rapport, qu'il présentera à la Chambre au moment prévu au cours des Affaires courantes ordinaires.

D'abord et avant tout, on dit: « Si le président du comité estime que la question concerne un privilège »; c'est donc à moi de trancher. Si j'estime que c'est ce qu'il convient de faire, alors la question est soumise au comité. Si le comité décide qu'il faut aller de l'avant, nous faisons rapport à la Chambre; celle-ci examine la situation et détermine les mesures à prendre.

Le processus est assorti de tout un système de freins et de contrepoids. Selon moi, nous ne pouvons pas laisser des personnes s'en tirer en disant simplement que les règles ne s'appliquent pas à elles et qu'elles peuvent faire des déclarations et des commentaires sur le déroulement de nos séances à huis clos. Pour d'autres personnes, les restrictions sont pourtant bien claires: on ne peut pas parler de ce qui s'est passé lors d'une séance à huis clos parce que, par définition, ces séances sont confidentielles.

Comme je l'ai indiqué, si je décide que c'est ce qu'il faut faire, la décision incombera au comité, qui pourra ensuite faire rapport à la Chambre, laquelle aura alors l'occasion de débattre de la question et de décider de ce qui convient. Je ne vois pas pourquoi je devrais faire obstacle au processus dès le départ. Il y a différentes étapes à franchir, sans compter les appels qui peuvent être entendus.

D'un côté, je lis: « Si le président du comité estime que la question concerne un privilège », et de l'autre, je lis:

> Mark Holland, député libéral et membre du comité, a affirmé qu'on demandait au comité d'examiner une question qui a déjà été réglée par la vérificatrice générale. Il a dit que c'est pour cette raison qu'il a exercé des pressions afin que le comité entende Dodge et Fraser, ainsi que O'Leary, Cutler et Kinsella.

À mon avis, cela semble être une question de privilège. Je vais donc conclure qu'il s'agit bien d'une question concernant un privilège. Il incombe maintenant au comité de décider s'il me donne raison et, le cas échéant, de faire rapport à la Chambre, laquelle se penchera ensuite sur la question.

D'abord et avant tout, je vous demande si la motion est recevable telle que présentée. On indique ici « Je proposerais donc que », alors nous allons présumer que la motion est recevable et peut être débattue.

Monsieur Carr.

● (1555)

M. Gary Carr: Je me demandais simplement si M. Kramp voulait inclure également M. Sauvageau, parce que l'article indiquait que M. Sauvageau était à l'origine de l'examen des contrats de Earnscliffe et qu'il s'est déclaré heureux que le comité ait accepté d'enquêter sur la question. Je demande donc à M. Kramp si, compte tenu de la décision de la présidence, il souhaite que M. Sauvageau soit également visé par la motion.

Le président: M. Kramp a indiqué dans sa déclaration, et je le cite —vous venez juste de citer M. Sauvageau dans l'article, alors je n'ai pas à le faire de nouveau—« Comme M. Sauvageau ne faisait pas directement référence aux propos tenus au cours d'une séance à huis clos du comité, ses commentaires ne sont pas visés par mon rappel au Règlement ».

Par ailleurs, comme je l'ai déjà indiqué, il était connu de tous depuis un bon moment que nous allions nous pencher sur le chapitre 5. En effet, le comité avait adopté une motion en ce sens, et toutes les motions adoptées par les comités font partie du domaine public. Je ne crois pas que les commentaires de M. Sauvageau font référence à des discussions tenues. Il a dit : « Nous apprendrons »; il avançait des hypothèses sur ce que les témoins pourraient raconter au sujet de l'état d'esprit de M. Guité, M. Gagliano et M. Chrétien. Je suis donc d'avis que M. Holland a peut-être porté atteinte aux privilèges de la Chambre, mais je ne crois pas que ce soit le cas pour M. Sauvageau.

● (1600)

M. Gary Carr: Je veux simplement faire une précision; je ne vais pas le répéter parce que je sais que ce n'est pas ce que vous souhaitez. M. Sauvageau a indiqué qu'il était également heureux de la décision prise. Selon cet article, il y aurait eu fuite d'information quant à la personne qui a présenté une motion, alors qui est responsable de cette fuite? Comment ces renseignements ont-ils été divulgués?

J'estime que si des dispositions sont prises, elles devraient s'appliquer de la même façon à M. Sauvageau...selon ce qu'on peut lire dans l'article.

Le président: Je ne sais pas qui est responsable de la divulgation des motions et des autres renseignements. La greffière m'a indiqué que lorsqu'une motion est adoptée lors d'une séance à huis clos, on indique seulement qu'elle a été proposée puis adoptée. On ne précise pas qui l'a proposée ou qui l'a adoptée; c'est une décision de l'ensemble du comité. C'est là que s'arrête l'incursion dans le domaine public.

À ce moment-ci, j'ai seulement été saisi d'une motion de M. Kramp indiquant que M. Holland a porté atteinte aux privilèges de ce comité. Comme je constitue en fait le premier palier dans l'examen de cette motion, j'ai déclaré qu'il ne convenait pas pour moi de faire obstacle à ce débat. Par ailleurs, je suis d'avis également que M. Sauvageau n'a pas porté atteinte aux privilèges du comité en parlant de ses délibérations à huis clos.

M. Gary Carr: C'est deux poids deux mesures.

Le président: Peut-être avez-vous raison, mais M. Sauvageau avançait des hypothèses quant à ce qui pourrait se produire à une date ultérieure, alors il ne pouvait pas parler de ce qui s'était passé auparavant.

Monsieur Kramp.

M. Daryl Kramp: Si vous me permettez, je demanderais l'indulgence de mes collègues sur cette question. Je suis vraiment partagé sur ce point, et peut-être devrais-je faire appel à votre considération à l'égard des propos que je tiendrai.

Je crois vraiment qu'il serait facile de simplement fermer les yeux, parce que c'est un premier faux pas devant ce comité. Il s'agit manifestement d'une autre occasion de se pencher sur la question très importante des orientations futures du comité. En effet, il importe davantage de savoir où on s'en va que de déterminer qui a tort ou qui a commis une faute. Pour le bien de notre comité, compte tenu du travail que nous avons à faire, en considération des invités que nous recevons aujourd'hui, et de concert avec mes collègues, je serais prêt à suggérer que nous déposions cette motion ou alors que je la retire, en comprenant bien qu'un avertissement très clair a été lancé.

M. Lastewka a fait un commentaire très pertinent. Notre comité compte un certain nombre de nouveaux députés, moi le premier; nous avons tous nos limites et nous pouvons commettre des erreurs. Parfois, lorsqu'une situation se répète à plusieurs reprises, on ne peut plus parler d'erreur. Je ne crois pas qu'il s'agisse ici d'une erreur, mais j'estime à ce moment-ci qu'il est plus important pour moi de faire montre de considération à l'égard de mes collègues que de chercher à prendre des mesures punitives à l'égard d'une personne ou d'un collègue alors que nous avons un travail très important à faire.

Si la présidence et mes collègues me le permettent, je serais maintenant disposé à retirer ma motion. Reprenons simplement notre travail. Je ne sais pas ce que vous en pensez, mais il est important pour moi que nous travaillions tous ensemble.

Le président: Vous dites que vous êtes prêt à retirer votre motion, mais c'est à vous de décider. Souhaitez-vous retirer la motion ou maintenir votre proposition?

M. Daryl Kramp: Je retire la motion.

Le président: La greffière vient de m'aviser qu'il nous faut un consentement unanime pour le retrait d'une motion. M. Kramp a demandé le retrait de sa motion. Y a-t-il consentement unanime à cet effet?

Des voix: D'accord.

Le président: Comme personne ne s'y oppose, la motion est retirée. Cette question est maintenant réglée.

M. Holland veut intervenir, mais je veux d'abord préciser à tous les membres du comité, et surtout aux nouveaux députés, que le Parlement du Canada existe depuis quelque 138 ans et a vécu un grand nombre de précédents. Nous dépendons beaucoup de la confiance mutuelle, non seulement envers les collègues de notre propre parti, mais aussi envers tous nos collègues du Parlement. Si nous cessons d'être assujettis à un ensemble de règles, tout le système va s'effondrer. Si nous laissons des gens s'en tirer impunément lorsqu'ils prennent avantage du système et contournent les règles, nous minons tout le processus, et cela est vrai pour tous les membres.

Selon moi, M. Kramp a été magnanime en retirant sa motion et la question est maintenant réglée. Je ne crois pas qu'il sera aussi magnanime si la situation se répète. Nous avons tous eu droit à cet avertissement, alors agissons en conséquence.

Un dernier bref commentaire, monsieur Holland.

● (1605)

M. Mark Holland: Ce n'est pas nécessaire.

Le président: Ceci étant réglé, nous allons maintenant entendre la déclaration préliminaire des représentants du Bureau du vérificateur général.

Monsieur Timmins, nous vous écoutons.

M. Douglas Timmins (vérificateur général adjoint, Bureau du vérificateur général du Canada): Monsieur le président, je vous remercie de me donner l'occasion de discuter des résultats de notre vérification de la sécurité des technologies de l'information.

Comme vous l'avez indiqué, je suis accompagné de Richard Brisebois, directeur principal, et de Guy Dumas, directeur de cette vérification.

Notre dernière vérification de la sécurité des technologies de l'information remonte à 2002. Depuis ce temps, les cybermenaces qui pèsent sur les technologies de l'information ont augmenté de manière inquiétante. En 2002, une version révisée de la Politique du gouvernement sur la sécurité venait tout juste d'être publiée, mais les normes opérationnelles essentielles à la mise en oeuvre de la politique étaient périmées ou inexistantes.

Depuis 2002, le Secrétariat du Conseil du Trésor a élaboré, de concert avec les principaux organismes responsables de la sécurité et certains ministères, plusieurs normes de sécurité opérationnelles et techniques. On a notamment établi des normes sur la continuité des activités et sur la gestion de la sécurité informatique. Cependant, il en reste encore plusieurs à élaborer, la plupart dans d'autres secteurs touchant la sécurité informatique, comme l'évaluation des menaces et des risques, la passation des marchés, la formation et la sensibilisation en matière de sécurité, ainsi que l'identification des biens.

Pour être efficaces, les politiques et les normes doivent se traduire en gestes concrets de la part des ministères et des organismes. En général, nous avons constaté que les ministères et les organismes ne satisfont aux exigences de base de la politique et des normes, ou encore ils y satisfont, mais d'une manière non uniforme d'un secteur à l'autre ou d'une région à l'autre.

[*Français*]

Dans le cours de notre vérification, nous avons examiné les réponses à un questionnaire d'autoévaluation de la sécurité informatique qui a été administré par le Secrétariat du Conseil du Trésor. Des 46 ministères et organismes qui ont répondu, une seule entité disait satisfaire aux exigences de base. Comme complément à cet exercice, nous avons préparé notre propre questionnaire et l'avons envoyé à 82 organisations. Nous avons obtenu des résultats similaires.

[*Traduction*]

Nous avons examiné 20 rapports de tests techniques menés au cours des deux dernières années dans diverses organisations. La plupart de ces rapports ont signalé de graves lacunes dans les systèmes informatiques, qui, si elles étaient exploitées, pourraient provoquer de sérieux bris de sécurité, entraîner la divulgation non autorisée de renseignements et causer des dommages à des entreprises ou à des citoyens non méfiants.

Monsieur le président, nous avons aussi examiné les pratiques en matière de sécurité informatique dans les quatre ministères qui avaient fait l'objet de notre vérification en 2002. Certains ont apporté des changements importants à leurs pratiques, mais aucun ne satisfaisait à toutes les exigences de base de la politique.

Dans notre sondage, nous avons constaté que, des 82 ministères et organismes, seulement 37—soit 45 p. 100—avaient effectué une évaluation des menaces et des risques de leurs programmes, de leurs systèmes ou de leurs services, comme l'exige la politique. Dans la plupart des organisations, la haute direction n'est pas informée des résultats ou n'est pas au courant des risques informatiques, ce qui a pour effet qu'elle n'accorde peut-être pas suffisamment d'importance à la nécessité de les éliminer.

[*Français*]

Nous signalons également dans notre rapport que le Secrétariat du Conseil du Trésor n'a pas entièrement rempli son rôle de surveillance tel qu'il est défini dans la politique. Il n'a pas mis en place les processus nécessaires pour recueillir et analyser les constatations en matière de sécurité soulevées dans les rapports de vérification ministériels. Il n'a pas non plus produit le rapport à mi-terme, destiné au Conseil du Trésor, sur l'efficacité de la politique du gouvernement sur la sécurité, rapport qui devait être remis à l'été de 2004. Il existe donc peu d'information de base sur l'état de la sécurité informatique dans l'ensemble du gouvernement.

● (1610)

[*Traduction*]

Monsieur le président, il est important que des mesures précises visant à dissiper les inquiétudes en matière de sécurité informatique soient prises sans délai. Le comité voudra peut-être poser les questions suivantes au Secrétariat du Conseil du Trésor : Comment s'assurera-t-il que toutes les normes de sécurité informatique nécessaires sont préparées et publiées en temps opportun? Comment s'assurera-t-il que les ministères et les organismes mettent en place un niveau raisonnable de sécurité informatique et qu'ils en rendent compte? Comment jouera-t-il son rôle de surveillant de la sécurité informatique et suivra-t-il les vérifications entreprises par les ministères dans ce domaine? Quand le rapport a mi-terme sur la Politique du gouvernement sur la sécurité sera-t-il préparé?

Monsieur le président, voilà qui conclut ma déclaration d'ouverture. Nous serons heureux de répondre aux questions du comité.

Le président: Merci, monsieur Timmins.

Nous allons maintenant passer à Mme McDonald, dirigeante principale de l'information, qui fera elle aussi une déclaration préliminaire.

Madame McDonald, la parole est à vous.

[*Français*]

Mme Helen McDonald (dirigeant principal de l'information, Secrétariat du Conseil du Trésor du Canada): Merci, monsieur le président.

Bonjour. Je m'appelle Helen McDonald et je suis dirigeant principal de l'information par intérim pour le gouvernement du Canada. Je suis accompagnée de M. Simon Gauthier, dirigeant principal associé, ainsi que de M. Pierre Boucher, directeur principal par intérim, Architecture, normes et ingénierie. M. Gauthier et Boucher m'ont aidée à élaborer la réponse du gouvernement du Canada aux points soulevés dernièrement par la vérificatrice générale.

J'aimerais d'abord vous remercier de me donner la possibilité de parler, au nom du Secrétariat du Conseil du Trésor, de ce chapitre sur la sécurité des technologies de l'information.

J'aimerais premièrement affirmer que le gouvernement du Canada souscrit entièrement aux recommandations de la vérificatrice générale. Nous la remercions, ainsi que son bureau, pour son rapport sur le progrès dans le renforcement de la sécurité des technologies de l'information depuis la vérification de 2002.

[*Traduction*]

En effet, les recommandations de la vérificatrice générale sont conformes aux résultats de l'évaluation de la sécurité des technologies de l'information que nous avons effectuée dans le cadre de nos fonctions de contrôle et de surveillance. À ce sujet, j'aimerais donner au comité un aperçu des travaux réalisés depuis la dernière vérification et de nos activités prévues pour les semaines et les mois à venir relativement à cette importante question.

Le Secrétariat du Conseil du Trésor et les principaux organismes oeuvrant dans le domaine de la sécurité, c'est-à-dire la Gendarmerie royale du Canada, Sécurité publique et Protection civile Canada et le Centre de la sécurité des télécommunications, jouent un rôle essentiel dans l'élaboration et le renouvellement des normes, des documents techniques et des directives en matière de sécurité, en vue de répondre aux défis et possibilités qui se présentent dans le domaine des TI.

Mme Helen McDonald: Par exemple, en mai dernier, le SCT a mis en oeuvre la norme de gestion de la sécurité des technologies de l'information, qui traite des 40 normes répertoriées en 2002 et jugées essentielles à l'efficacité de la sécurité des TI au gouvernement du Canada. La norme de GSTI expose, dans un document succinct rédigé en langage clair, les exigences de base en matière de sécurité des TI pour tous les ministères. Le bureau de la vérificatrice générale l'a utilisée comme critère de conformité dans sa récente vérification. Selon cette norme, tous les ministères et organismes doivent effectuer chaque année une auto-évaluation de la sécurité des TI et élaborer un plan d'action visant à combler les lacunes décelées à cet égard. On s'attend à ce que tous les ministères et organismes se conforment à la norme de GSTI d'ici décembre 2006.

En 2004, le SCT a rendu visite à 90 ministères et organismes afin de passer en revue leurs progrès dans la mise en oeuvre de la Politique du gouvernement sur la sécurité. Ces constatations seront incluses dans le rapport de mi-parcours qui devrait être disponible en mai 2005. Nous avons constaté que, dans l'ensemble, les grandes institutions fédérales avaient déjà instauré de rigoureuses mesures de sécurité ou élaboré des plans relatifs à la Politique du gouvernement sur la sécurité et commencé leur mise en oeuvre.

Le SCT dirige actuellement l'élaboration d'une méthode de mesure du rendement pour la sécurité des TI. Cette méthode précisera les outils, les mesures et les objectifs qui permettront de confirmer la conformité des ministères à la norme de gestion de la sécurité des TI. Nous envisageons également d'intégrer les données provenant des évaluations de la vulnérabilité, de la menace et des risques, des rapports de gestion des incidents et d'auto-évaluation de la sécurité des TI ainsi que des visites effectuées dans les ministères, en vue d'obtenir une image cohérente de l'état de la sécurité des TI au gouvernement du Canada. Nous examinons aussi la possibilité d'inclure la sécurité des TI comme mesure dans le Cadre de responsabilisation de gestion qui est utilisé lors des discussions qui ont eu lieu entre les sous-ministres et le Secrétariat du Conseil du Trésor afin d'évaluer chaque année le rendement.

Conjointement avec les principaux organismes oeuvrant dans le domaine de la sécurité, le CST, la GRC, SPPCC, ainsi qu'avec la participation de Travaux publics et Services gouvernementaux Canada, le SCT s'apprête à mettre en oeuvre et à utiliser des infrastructures et des solutions de services partagées pour les TI; par exemple, la Voie de communication protégée, des solutions communes de détection des intrusions et de gestion des incidents et le partage de données sur les menaces et la vulnérabilité.

En plus de ces mesures, le Secrétariat du Conseil du Trésor a fait plusieurs démarches en vue d'accroître la sensibilisation à la sécurité des TI au gouvernement et d'aider les institutions gouvernementales à se conformer aux normes et politiques à cet égard. Ces efforts comprennent une variété de programmes de formation en sécurité qui sont offerts partout au pays par l'entremise de la GRC, du CST et de l'École de la fonction publique du Canada.

En dépit des défis auxquels doit faire face une organisation de cette taille, le gouvernement du Canada peut maintenant partager l'information entre ses ministères d'une manière plus efficace que jamais auparavant. La Politique du gouvernement sur la sécurité diffusée en 2002 et la création en décembre 2003 de Sécurité publique et Protection civile Canada ont clarifié les rôles et les responsabilités et précisé le leadership dans des secteurs comme le partage de données sur les menaces et la vulnérabilité.

Nous continuons aussi à offrir des possibilités de discussions sur la sécurité des TI dans les communautés d'intérêts, qui comprennent des séances d'information aux agents de sécurité des ministères, des comités sur la sécurité des TI, le Conseil des DPI ainsi que des rencontres avec des spécialistes de la GI-TI et des vérificateurs internes. C'est pourquoi j'ai une grande confiance dans la capacité du gouvernement à réagir rapidement et en collaboration en vue de prévenir, de déceler et d'atténuer les infractions à la sécurité à l'échelle du gouvernement du Canada.

● (1615)

[*Français*]

Nous sommes aussi fermement déterminés à veiller au renforcement de la sécurité des technologies de l'information dans l'ensemble de la fonction publique fédérale. Notre objectif est de consolider la prise de conscience des sous-ministres et de la haute gestion ministérielle de l'importance de la sécurité des technologies de l'information dans les fonctions routinières du gouvernement canadien.

Comme l'a fait la vérificatrice générale, nous voulons aussi assurer les Canadiens et les Canadiennes que leurs transactions en direct ainsi que l'information que détient le gouvernement à leur sujet continuent à être judicieusement protégées. Je suis persuadée que le gouvernement canadien est en mesure d'atteindre son objectif de renforcer et de standardiser ses efforts envers la sécurité des technologies de l'information dans toute la fonction publique.

● (1620)

[*Traduction*]

Mon optimisme à l'égard de notre capacité d'atteindre nos objectifs en ce qui a trait à la sécurité des TI, malgré l'évolution constante du contexte en matière de risque, repose sur le plan d'action global du gouvernement qui comprend les quatre volets suivants : améliorer nos activités de contrôle et de surveillance, ce qui comprend l'achèvement du rapport de mi-parcours dans les semaines à venir ainsi que les auto-évaluations de la sécurité des TI que doivent effectuer annuellement les ministères et organismes; assurer que les institutions gouvernementales prennent en considération les risques en matière de sécurité dans leur Cadre de gestion intégrée du risque; exiger que les ministères et organismes gouvernementaux élaborent des plans d'action signés par les sous-ministres et les dirigeants des organismes, au plus tard à l'été 2005; ajouter de la documentation technique à la norme de gestion de la sécurité des technologies de l'information, au besoin.

Nous nous sommes également engagés à terminer, d'ici décembre 2006, avec la participation de SPPCC, la série de normes relatives à la détection des intrusions et à la gestion des incidents.

Enfin, l'objectif du gouvernement en matière de sécurité des TI est d'améliorer la résilience des systèmes des ministères et organismes afin de garantir la prestation continue des services aux citoyens et entreprises du Canada.

[*Français*]

Monsieur le président, ainsi se termine mon allocution. Il nous fera plaisir de répondre aux questions que les membres du comité voudront bien nous poser.

[*Traduction*]

Le président: Je vous remercie beaucoup, madame McDonald.

Avant de céder la parole à M. Fitzpatrick, je vais poser une question. Vous avez dit dans votre déclaration que vous avez « une grande confiance dans la capacité du gouvernement à réagir rapidement et en collaboration en vue de prévenir, de déceler et d'atténuer les infractions à la sécurité à l'échelle du gouvernement du Canada. » Cela va directement à l'encontre de ce qu'ont déclaré M. Timmins et la vérificatrice générale.

Mme Helen McDonald: La vérificatrice générale a également signalé que les organismes centraux ont clarifié leurs rôles et leurs responsabilités et travaillent beaucoup mieux ensemble, c'est-à-dire qu'ils partagent davantage les renseignements au sujet des incidents et qu'ils réagissent plus rapidement aux menaces qui visent nos systèmes.

Le président: Ne diriez-vous pas, monsieur Timmins, que ce commentaire est un peu trop optimiste?

M. Douglas Timmins: Notre vérification a révélé qu'il existe des menaces et des risques qui ne sont pas gérés. Néanmoins, cela ne nous permet pas de déterminer si les organismes seraient en mesure de réagir de façon appropriée à ces menaces et à ces risques s'ils se concrétisaient.

Le président: Monsieur Fitzpatrick, allez-y; vous disposez de huit minutes.

M. Brian Fitzpatrick: Mes questions vont porter sur un seul sujet, à savoir la menace terroriste. À l'époque à laquelle nous vivons, le terrorisme constitue un danger très réel et très présent dans notre société. Ce qui s'est produit dans le cas d'un avion d'Air India nous a donné une idée de ce qu'allait être l'avenir. Si nous revenions à cette période, nous constaterions, même au sein de la GRC ou des autres organismes de sécurité, que les systèmes de technologie de l'information ont peut-être connu de graves défaillances; si ce n'avait pas été le cas, peut-être aurait-on pu prévenir ce qui s'est produit. Je sais que nous sommes à une autre époque, mais je tenais à faire cette observation.

Je me souviens de la grande panne de courant qui a eu lieu il y a un an, l'été dernier, je crois. Nous pouvons tous imaginer les conséquences graves qu'entraînerait une défaillance des systèmes. Il m'arrive souvent de penser que, si des terroristes voulaient vraiment faire du mal à la société canadienne ou américaine, ils pourraient notamment utiliser des explosifs. Une autre façon serait d'accéder à des systèmes et causer beaucoup de tort. Une panne comme la grande panne de courant que nous avons connue nous montre à quel point nous sommes vulnérables.

Cela m'amène au sixième point du rapport de M. Timmins, quoique ma question s'adresse à Mme McDonald. Il est écrit que, sur 46 ministères, un seul disait satisfaire aux exigences de base. J'interprète les exigences de base comme étant des normes essentielles. Le Bureau du vérificateur général a déclaré qu'il avait sondé 82 autres ministères et que les résultats se sont avérés similaires.

D'après ce que vous avez affirmé lors de votre exposé, c'est-à-dire que tout est sous contrôle et que toutes les exigences sont respectées, vous démontrez beaucoup de confiance, mais diriez-vous, madame McDonald, que, si nous refaisions ces évaluations des risques de façon aléatoire, nous constaterions que tous les ministères et organismes satisferaient aux exigences de base?

Mme Helen McDonald: Ce qui a été fait en 2004, c'est une évaluation du respect des exigences de base liées à la norme de GSTI —gestion de la sécurité des technologies de l'information. Je crois que le Bureau du vérificateur général approuve ces exigences, car il les a utilisées comme outil d'évaluation.

La norme de GSTI a été approuvée en 2004 seulement; une ébauche était disponible à la fin de 2003. Lorsqu'on évalue les ministères, on constate inévitablement qu'ils ne respectent pas entièrement la norme. L'étude que nous avons menée a révélé qu'un seul ministère respectait les exigences de base. La norme de GSTI expose les exigences de base, c'est-à-dire le niveau minimal de sécurité que nous voulons qu'il existe dans tous les ministères et organismes.

M. Brian Fitzpatrick: C'est ce que je dis, les ministères doivent réussir le test. C'est la première épreuve à subir, et seulement un sur 46 l'a réussit.

Ma question est la suivante : Ces résultats portent sur 2004, mais pensez-vous que, aujourd'hui, si nous refaisions une évaluation, nous constaterions que ces ministères se sont réellement améliorés?

● (1625)

Mme Helen McDonald: J'estime que nous observerions des améliorations, mais les ministères ont jusqu'en 2006 pour se conformer entièrement à la norme de GSTI. Lorsque nous avons mis en oeuvre la norme, nous savions que la plupart des ministères ne s'y conformaient pas entièrement et qu'il faudrait un certain temps pour qu'ils y arrivent.

M. Brian Fitzpatrick: Monsieur Timmins, partagez-vous son enthousiasme ou sa confiance à propos des progrès réalisés?

M. Douglas Timmins: Nous sommes tout à fait en faveur de l'idée de fixer une échéance et d'établir des objectifs à atteindre. Nous ne savons pas si des progrès ont été réalisés jusqu'à maintenant, car nous n'avons pas effectué d'évaluation.

Ce qui posait particulièrement des problèmes, c'étaient les exigences de base. Il est vrai que la norme a été établie en 2004, mais certaines des exigences qu'elle comporte existent ailleurs depuis une dizaine d'années déjà. L'état de la situation nous préoccupe, mais nous sommes encouragés par le fait qu'une échéance a été fixée et que quelqu'un...

M. Brian Fitzpatrick: Cela soulève un autre point. S'il est un domaine qui est beaucoup plus avancé que le secteur public et le gouvernement, c'est celui de la technologie. Nous accusons un retard d'une dizaine d'années à certains égards, si je comprends bien. Je n'ai jamais vu le gouvernement prendre la tête du peloton; il suit toujours derrière.

Ce que je me demande, c'est si le gouvernement entretient des rapports avec certains chefs de file mondiaux du secteur privé du milieu de la technologie, ceux qui sont à la fine pointe dans le domaine de la sécurité, ou s'en remet-il à ses fonctionnaires pour déterminer les normes et la façon de faire face à ce type de menaces?

Selon moi, il s'agit d'un domaine où le gouvernement devrait aller voir à l'extérieur, dans le secteur privé, afin de trouver les meilleures personnes qui oeuvrent dans le milieu et faire en sorte d'être à l'avant-garde pour ne pas accuser un retard d'une dizaine d'années. Estimez-vous que c'est ce que fait le gouvernement?

Mme Helen McDonald: Oui. Nous essayons non seulement de nous renseigner auprès des meilleures entreprises, comme Microsoft —nous utilisons largement ses produits—pour nous tenir au courant des problèmes qui existent en matière de sécurité, mais nous essayons aussi de faire en sorte que le secteur privé, dans l'ensemble du Canada, partage davantage avec le gouvernement l'information qu'il détient à propos des risques. Si nous sommes une cible, le secteur privé en est une également, alors nous pouvons apprendre l'un de l'autre à propos des nouvelles menaces ou des mesures qui ont fonctionné.

Nous essayons aussi d'adopter, lorsque possible, des normes internationales. Nous ne les inventons pas. Nous essayons de suivre des normes internationales parce que beaucoup d'efforts sont déployés à l'échelle internationale sur le plan des architectures et des logiciels.

Enfin, nous recevons au Canada, par l'entremise d'échanges, des sommités du secteur privé dans le domaine de la sécurité de façon à détenir une expertise au sein du gouvernement.

M. Brian Fitzpatrick: Il me reste peu de temps, mais je veux vraiment poser une autre question.

S'il arrivait que les systèmes d'un ministère tombent en panne ou qu'un grave problème survienne, existe-t-il un plan pour faire face à une telle situation? Je pose cette question parce que seulement 45 p. 100 des ministères ont effectué une évaluation de la menace et du risque. Je doute fort que les ministères qui n'ont pas fait une telle évaluation disposent d'un plan d'urgence au cas où surviendrait une panne de leurs systèmes. C'est ce que je voudrais savoir.

Mme Helen McDonald: Des plans de cette nature ont été élaborés en prévision du passage à l'an 2000. Plus récemment, nous avons exigé que les ministères établissent des plans de poursuite des activités au cas où une telle situation survenait.

Le président: Avez-vous un commentaire à formuler, monsieur Timmins?

M. Douglas Timmins: Je veux seulement ajouter quelque chose. Au paragraphe 1.65 de notre rapport, nous parlons des plans de poursuite des activités. Nous écrivons que 53 ministères, c'est-à-dire 65 p. 100, détiennent un plan de poursuite des activités, mais seulement 24 d'entre eux, soit 29 p. 100, les ont mis à l'épreuve au cours des deux dernières années. Nous avons constaté des progrès, mais nous estimons qu'il y a un peu de travail à faire quant à la mise à l'épreuve des plans.

● (1630)

Le président: Je vous remercie beaucoup, monsieur Fitzpatrick.

[*Français*]

Monsieur Sauvageau, vous disposez de huit minutes.

M. Benoît Sauvageau (Repentigny, BQ): Madame et messieurs, je vous souhaite la bienvenue.

J'aimerais vous poser quelques questions. Tout d'abord, j'aimerais que vous éclairiez ma lanterne en ce qui a trait aux menaces. Il semble que si le système n'est pas sécuritaire, on est vulnérable face à des menaces. Sans donner de trucs à qui que ce soit, pouvez-vous, autant au Conseil du Trésor qu'au Bureau de la vérificatrice générale, nous dire quelles sont les menaces qui pèsent sur la population canadienne si le système n'est pas sécurisé? Pouvez-vous être bref? J'aimerais poser plusieurs questions.

M. Simon Gauthier (dirigeant principal associé de l'information, Secrétariat du Conseil du Trésor du Canada): Je peux répondre brièvement.

Elles sont nombreuses. Typiquement, elles sont le résultat de faiblesses sur le plan de la conception ou de la mise en oeuvre du code ou du logiciel.

M. Benoît Sauvageau: Pouvez-vous nous donner un exemple de menace? Je sais ce qu'est une menace. Par exemple, est-il possible d'effacer toutes nos dettes envers Revenu Canada?

M. Simon Gauthier: Non.

M. Benoît Sauvageau: C'est bien. C'est de cela qu'il s'agit. J'aimerais connaître un exemple de menace.

M. Simon Gauthier: Un exemple de menace...

M. Benoît Sauvageau: Mon exemple n'est peut-être pas bon, mais je vais vous en donner un. Le Comité permanent des opérations gouvernementales a reçu un témoin. Il travaillait au consulat à Hong-Kong. Il a déclaré que, parce que le système informatique n'était pas sécuritaire, il pourrait y avoir de la fraude au niveau des passeports et des visas. Le gars a perdu son travail. La GRC a fait enquête pour voir si ce que le type disait était vrai. L'enquêteur de la GRC responsable de l'enquête a prouvé que le gars avait raison. Il a perdu également son travail. La Loi sur la protection des fonctionnaires-dénonciateurs d'actes répréhensibles n'était pas en vigueur et ne l'est toujours pas. Le témoin a dit au Comité permanent des opérations gouvernementales que, puisque le système n'était pas sécurisé dans la très grande majorité des ambassades et des consulats, on pourrait se faire jouer des tours sur le plan des passeports et des visas. Est-ce un exemple concret de menace?

M. Simon Gauthier: Je ne peux pas vous le dire.

M. Benoît Sauvageau: Ma question est peut-être plus précise.

M. Simon Gauthier: Je ne peux pas le dire, monsieur. Je ne la sais pas, je ne suis pas courant. Cependant, c'est un exemple de menace potentielle. Cela étant dit, je crois que dans la plupart des systèmes qui sont directement reliés à Internet—qui est en fait la source de ces menaces—, des mesures ont été prises au cours des deux dernières années pour réduire la vulnérabilité ou les marques de faiblesse. Je n'irais pas jusqu'à dire qu'elles ont été éliminées totalement, mais au moins, elles ont été réduites.

M. Benoît Sauvageau: Si vous receviez des rapports de façon plus régulière, vous pourriez affirmer, et non pas seulement croire, que cela a été corrigé. Par exemple, on dit, au Bureau du vérificateur général, que vous ne recevez pas de rapports assez fréquemment. Cela vous fait dire que vous croyez que tout, ou une partie des choses, a été corrigé, mais si le rapport vous était remis, vous pourriez dire que vous le savez.

Si vous me le permettez, j'aimerais demander à Mme McDonald si le manque d'encadrement ou le manque de surveillance, lorsque environ 20 ministères sur environ 80 ministères ont de tels plans, peut faire en sorte que de graves menaces pèsent sur le système de passeports et de visas. Cela veut-il plutôt dire qu'on pourrait jouer dans le système informatique sans qu'il y ait trop de conséquences?

[*Traduction*]

Mme Helen McDonald: Je ne peux répondre directement en ce qui a trait au système des passeports. Quant à la déclaration des incidents, il est plus important que ce soient les coordonnateurs en matière de sécurité des TI, plutôt que le Secrétariat du Conseil du Trésor, qui soient immédiatement mis au courant d'un incident ou bien de l'apparition d'un nouveau virus ou d'une menace informatique de la sorte, et que des mesures correctives soient prises.

Je crois que la vérificatrice générale souhaite que le Secrétariat du Conseil du Trésor suive de façon plus efficace les progrès relatifs à la mise en oeuvre de la Politique du gouvernement sur la sécurité et de la norme de gestion de la sécurité des technologies de l'information. C'est le genre de choses que nous allons améliorer grâce aux rapports des ministères sur leurs plans d'action visant à corriger les lacunes en matière de sécurité des TI qu'ils ont relevées au sein de leur entité.

[*Français*]

M. Benoît Sauvageau: Ce n'est pas une attaque personnelle, madame. Je vais donc utiliser un autre nom: je vais parler du ministère de l'Optimisme. J'ai aussi siégé au Comité permanent des langues officielles. Le Secrétariat du Conseil du Trésor, qui est censé vérifier, est optimiste. Il a bon espoir que les choses vont s'améliorer à l'avenir. Vous êtes, vous aussi, optimistes. Vous croyez que les choses vont s'améliorer à l'avenir. Dans ce cas, pourquoi les plans d'action qui devaient être mis en application ne l'ont-ils pas été dans le passé? Cela aurait peut-être réduit votre optimisme, mais cela aurait peut-être aussi rendu les choses plus efficaces.

J'ai préparé beaucoup de questions. J'en avais d'autres, mais celle-là a été préparée avec beaucoup de soin.

Le paragraphe 12 de la présentation de M. Timmins contient quatre questions. Si on vous les posait, que répondriez-vous? Avez-vous le libellé de ces questions?

● (1635)

[*Traduction*]

Mme Helen McDonald: Oui je l'ai lu.

Comment s'assurerait-on que les normes de sécurité informatique nécessaires sont préparées en temps opportun? Nous proposons que toutes les normes soient terminées au plus tard en décembre 2006. Nous avons élaboré un plan qui établit, mois par mois, quelle est la situation concernant les 12 normes qui sont nécessaires et qui ne sont pas terminées. Trois d'entre elles ont été rédigées et distribuées, et nous sommes au courant du temps qu'il faudra.

Comment s'assure-t-on que les ministères mettent en place un niveau raisonnable de sécurité informatique? Dernièrement, nous nous sommes employés à nous assurer que les normes que nous mettons en oeuvre s'accompagnent des lignes de conduite pertinentes pour les ministères. Il ne suffit pas simplement de les afficher sur votre site Web. Vous voulez collaborer avec les gens pour vous assurer qu'ils sont au courant de ces exigences et qu'ils les comprennent. Vous essayez de trouver les outils nécessaires pour aider les fonctionnaires à être efficaces.

Aux niveaux supérieurs, nous voulons promouvoir l'importance des TI. Je suis optimiste peut-être parce que je pense que chaque sous-ministre se préoccupe du maintien des opérations et sait que nous mettons beaucoup l'accent sur les systèmes informatiques. À leurs yeux, il ne s'agit peut-être pas de sécurité mais bien d'intégrité, d'intégrité de leurs opérations, mais je pense qu'ils s'en préoccupent beaucoup. Nous demandons donc que les sous-ministres approuvent ces plans d'action à l'automne—et je ne fais pas allusion aux responsables ministériels de la sécurité mais bien aux sous-ministres —, afin qu'ils soient conscients des points forts et des lacunes de la sécurité informatique, des mesures qu'ils prendront et des délais qu'ils respecteront en matière d'amélioration.

Quant au rôle de surveillant de la sécurité informatique, nous avons demandé que les plans d'action soient reçus au plus tard en août, et nous nous assurons que les ministères en sont au courant. Ils ont commencé à prendre les mesures, et nous examinerons leurs plans d'action pour transmettre un rapport au secrétaire à la fin de l'année civile. Au cours de la prochaine année, soit 2006, nous envisageons de demander aux ministères de procéder encore une fois à une auto-évaluation de la sécurité informatique afin que nous pussions vérifier non seulement les modifications apportées mais aussi les mises à jour aux plans d'action. Nous pourrons ainsi évaluer les progrès réalisés et ce qu'il reste à accomplir. Nous examinerons ces renseignements et tiendrons compte également d'autres sources d'information comme les évaluations de la vulnérabilité, un peu comme l'a fait la vérificatrice générale, et nous transmettrons notre rapport au Conseil du Trésor au début de 2007.

Vous n'êtes pas sans savoir que la politique en matière de sécurité doit faire l'objet d'un examen tous les cinq ans. Entre deux examens, il faut établir l'efficacité de la mise en oeuvre. De plus, il y a l'examen à mi-parcours, en mai.

Le président: Merci, monsieur Sauvageau.

Monsieur Lastewka, vous disposez de huit minutes.

L'hon. Walt Lastewka: Merci, monsieur le président. Je remercie également les témoins de comparaître devant le comité aujourd'hui.

Je procéderai en trois étapes.

Madame McDonald, depuis combien de temps êtes-vous dirigeante principale de l'information par intérim?

Mme Helen McDonald: Depuis mai.

L'hon. Walt Lastewka: Qui occupait votre poste avant vous?

Mme Helen McDonald: Michelle d'Auray.

L'hon. Walt Lastewka: Je cherche à savoir pourquoi. Pourquoi n'y a-t-il qu'un seul ministère qui a satisfait aux exigences de base? Je veux revenir aux propos de M. Fitzpatrick. Pourquoi n'y a-t-il qu'un seul ministère? Était-ce imputable à un manque d'intérêt, à une absence de compréhension ou à un manque de communication? Répondez à mes pourquoi—pourquoi n'y avait-il qu'un seul ministère?

Mme Helen McDonald: La norme sur la gestion de la sécurité des technologies de l'information impose les exigences minimales auxquelles doivent satisfaire tous les ministères et organismes. Parce qu'il a fallu, comme nous l'avions pensé, presque 44 normes différentes, il en découle un ensemble assez complexe d'exigences régissant la sécurité matérielle, la sécurité personnelle—pardon, je parle de la norme de GSTI. Elle est axés sur la sécurité des technologies de l'information, mais traite également de ce qui s'impose en matière d'accès aux systèmes, de protection de l'information, d'utilisation des technologies spécialisées, etc.

La norme n'a été établie que l'an dernier. Elle a été approuvée en mai 2004. Je crois que la vérification était sur le point de commencer à ce moment-là. Les ministères ont donc eu accès à ces précisions—et c'est exactement ce que nous visions—à peu près en même temps que les vérificateurs ont entamé leurs travaux.

Lorsque la norme a été approuvée, nous avons indiqué aux ministères qu'ils avaient jusqu'en 2006 pour la mettre en oeuvre. Sur les 46 ministères qui nous ont transmis de l'information, vous en décelez un qui signale avoir observé tous les aspects de norme de GSTI. Ce n'est pas parce qu'ils n'attachent pas d'importance ou d'intérêt à cette question. C'est plutôt que nous avons une nouvelle norme avec laquelle les gens cherchent à se familiariser.

● (1640)

L'hon. Walt Lastewka: Très bien, je ne suis pas sûr d'être convaincu. Je suis vraiment inquiet. À titre de parlementaires, nous considérons que le Secrétariat du Conseil du Trésor doit donner l'exemple aux autres ministères, et je suis vraiment inquiet lorsque je lis qu'il « ne joue pas pleinement son rôle de surveillant, tel que le prévoit la Politique ».

Lorsqu'on lit dans le rapport que « le Secrétariat n'a pas présenté au Conseil du Trésor un rapport à mi-terme sur l'efficacité de la Politique du gouvernement à renforcer la sécurité », doit-on en conclure premièrement que le Conseil du Trésor a fait preuve de laxisme en ne l'exigeant pas du Secrétariat, et deuxièmement que ce rapport, qui devait être transmis à l'été 2004, ne l'a jamais été?

Mme Helen McDonald: Initialement, ce rapport à mi-parcours auquel on fait allusion devait être transmis au plus tard à l'été 2004. C'est le rapport dont je parle qui sera terminé au plus tard en mai 2005.

Effectivement, nous accusons du retard. Nous voulions nous assurer que nous avions mis en oeuvre les normes nécessaires, que nous avions aidé les ministères à comprendre comment les instaurer et que ceux-ci nous avaient transmis l'information sur le respect des exigences minimales. Par conséquent, les exigences minimales que nous avons sont en quelque sorte un point de départ pour la norme sur la gestion de la sécurité des technologies de l'information.

L'hon. Walt Lastewka: Dans votre rapport, vous indiquez que ce rapport sera achevé au plus tard à l'été 2005, est-ce exact? Nous avons des ministères imposants, des petits ministères, etc. Combien de ministères ont déjà terminé leur rapport et obtenu l'approbation de leur sous-ministre pour celui-ci.

Mme Helen McDonald: Je ne m'attends pas à ce que les sous-ministres l'aient fait. Nous visons plutôt à obtenir des plans d'action pour le mois d'août. Nous ne nous entendons pas à les recevoir avant le mois d'août.

L'hon. Walt Lastewka: Par conséquent, si nous vous demandons de comparaître de nouveau en septembre ou octobre, vous direz-nous qu'ils les ont pas encore approuvés? Je constate que nous avons reporté le délai. Nous n'avons pas fait respecter notre règle en matière de surveillance. Nous leur avons donné jusqu'en août. Cela signifie-t-il que tout sera signé et approuvé en août?

Mme Helen McDonald: Je mettrai la dernière main au rapport de mi-parcours sans égard aux plans d'action. Je ne veux pas le reporter. Je voudrais produire le rapport. Les plans d'action seront diffusés au cours de l'été, et nous proposons comme délai le mois d'août. La lettre d'appel officielle n'a pas encore été envoyée.

Je veux obtenir ces plans d'action parce qu'ils constituent notre meilleure façon de savoir comment on s'y pendra pour satisfaire aux exigences. Nous travaillons en étroite collaboration avec les autres ministères et organismes hiérarchiques pour nous assurer qu'ils comprennent les exigences relatives aux plans d'action et qu'ils sont mesure de produire ceux-ci. Nous aurons recours à la fois à mon bureau et au Secrétariat du Conseil du Trésor pour faire ressortir qu'il est important d'établir ces plans d'action.

L'hon. Walt Lastewka: J'ai de plus en plus l'impression que le Secrétariat du Conseil du Trésor doit convaincre les sous-ministres qu'ils doivent comprendre les risques et effectuer leur travail. De quel moyen contraignant disposez-vous pour vous assurer que ce travail sera effectué? L'heure n'est pas à la persuasion, cette question étant trop grave. Quel mécanisme employez-vous pour vous assurer que le tout sera terminé d'ici octobre?

● (1645)

Mme Helen McDonald: Si un ministère ou un organisme souhaite recourir aux services offerts par la Voie de communication protégée, il doit obtenir la certification et l'accréditation garantissant que ses systèmes sont conformes aux pratiques exemplaires en matière de sécurité des TI. Cela couvre donc un aspect de la question. Nous comptons certes sur les pressions exercées par les sous-ministres entre eux, si l'on veut. Afin de tenter d'amener peut-être les plus retardataires à prendre plus rapidement les mesures qui s'imposent, nous avons envisagé d'utiliser une carte de pointage pour indiquer aux sous-ministres où ils se classent par rapport à leurs homologues des autres ministères.

Plutôt que de simplement les punir, nous pourrions aussi les aider en continuant de mettre l'accent sur le fait qu'un niveau de sécurité beaucoup plus élevé que celui que les organisations auraient les moyens de s'offrir permettrait de fournir collectivement des services en matière de technologie de l'information, particulièrement aux petits organismes. Le niveau de sécurité sera certes accru grâce à la protection des réseaux, à la protection périmétrique et à la détection des intrusions pour l'ensemble de l'administration fédérale.

Le président: Merci infiniment, monsieur Lastewka.

Monsieur Christopherson, vous disposez de huit minutes.

M. David Christopherson (Hamilton-Centre, NPD): Merci, monsieur le président. Je remercie également tous nos témoins de comparaître.

Madame McDonald, vos commentaires empreints d'optimisme m'étonnent également, surtout compte tenu des termes utilisés par la vérificatrice générale. Il existe réellement un écart entre les mesures prises qui nous ont été signalées et votre attitude positive.

Mettons donc les choses en perspective. L'enjeu est énorme. Je suis surpris que les mesures prises jusqu'à présent aient été aussi timides. C'est extrêmement crucial pour à peu près tous les aspects de la gouvernance, sans aucune exception.

J'aimerais citer un paragraphe du rapport de la vérificatrice générale :

> 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 coure 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.

Ce qui est pire qu'une atteinte à la sécurité des systèmes, c'est qu'elle ait lieu sans même que nous le sachions. Une telle atteinte pourrait durer Dieu seul sait combien de temps. Il convient de souligner que c'est de la plus haute importance. Il est décevant que le gouvernement ne semble pas avoir accordé à cette question la priorité nécessaire.

Je vous cite encore un extrait du rapport de la vérificatrice générale. Ce passage se trouve à la page 5 et couvre quelques paragraphes. Je commencerai par celui-ci, qui est en contradiction avec l'optimisme que vous manifestez, madame McDonald. Je vous le lis :

> Dans l'ensemble, le gouvernement n'a pas fait de progrès satisfaisants dans le renforcement de la sécurité des TI. Deux ans et demi après avoir révisé sa politique sur la sécurité, il a encore beaucoup à faire pour concrétiser ses politiques et ses normes en pratiques cohérentes et rentables, propres à assurer un environnement informatique plus sécuritaire.

Les systèmes informatiques des ministères et organismes continuent d'être vulnérables sur le plan de la sécurité. Je crois que c'est assez alarmant et accablant, à moins qu'un des témoins représentant l'un des ministères ne veuille formuler une réfutation.

> 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.

Il faut se rappeler que cet avertissement n'est pas le premier. Ce n'est pas comme si vous pouviez prétexter qu'il s'agit de quelque chose de nouveau qui nécessitera un certain temps. Nous en sommes au courant depuis quelque temps.

Le dernier paragraphe de la page 5 est ainsi libellé :

> Nous nous inquiétons du fait que 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.

Je passe directement à la page 12, où nous retrouvons le passage suivant dans l'encadré au bas de la page :

> 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.

Je passe au deuxième paragraphe :

> Cependant, la sécurité des TI n'est pas toujours prise en compte au début du projet.

Je crois comprendre qu'on veut parler de l'examen du modèle.

> 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.

Malgré cela, vous continuez à être très optimiste, madame McDonald.

Je vous lis la dernière phrase :

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

Je m'inscris en faux, ces propos ne cadrent pas avec l'optimisme affiché par le gouvernement et n'indiquent pas que ce dernier prend cette question au sérieux.

Pourriez-vous préciser si la haute direction prend cette question au sérieux? Selon la vérificatrice générale—et elle le dit noir sur blanc dans ce document—, elle ne la prend pas au sérieux.

● (1650)

Mme Helen McDonald: Je ne voudrais pas qu'on confonde mon optimisme avec... Soyons réalistes. Nous sommes d'accord avec la vérificatrice générale. Nous convenons que nous ne respectons pas les normes comme nous le devrions. Je suis optimiste, car même la vérificatrice générale décèle certains signes de progrès. Je suis optimiste, car ce que j'ai dit aujourd'hui sur la mise en oeuvre des plans d'action et l'examen par le Conseil du Trésor contribuera à mettre davantage l'accent sur cet aspect. Je dois cependant admettre que nous devons redoubler d'ardeur pour amener la haute direction à comprendre cet enjeu et à s'y intéresser. C'est pourquoi j'ai fait un peu allusion à ce que nous avons réussi à fournir aux cadres supérieurs, les sous-ministres, des explications qu'ils comprendront. Je pense qu'ils considèrent que la sécurité est un élément qui s'ajoute a posteriori.

Nous essayons de leur faire comprendre qu'ils doivent songer à la sécurité des TI et en intégrer les principes dès le départ, lorsqu'ils commencent à concevoir un système. C'est pourquoi nous avons une architecture de programme pour aider les ministères à comprendre comment assurer une sécurité pertinente lorsqu'ils configurent ou conçoivent un système et à saisir qu'ils ne doivent pas le faire a posteriori. Nous ne voulons pas qu'il y ait des atteintes à la sécurité.

M. David Christopherson: Je vous dirai cependant que c'est très bien que vous espériez, que vous souhaitiez et que vous priez, que tous jouent de la baguette comme vous pour que leurs voeux se réalisent, mais dans la réalité, rien ne se produira si personne ne prend les mesures nécessaires. Je regrette, mais cela n'est pas suffisant. Cela aurait peut-être été acceptable, il y a quelque temps, mais ce ne l'est pas à l'heure actuelle, pas avec ce qui se passe dans le monde, ni pas avec un tel rapport accablant. Il est précisé dans ce rapport que la haute direction ne prend pas suffisamment cette question au sérieux, et vous venez me dire que vous espérez et que vous voulez les convaincre.

Vous aviez presque commencé, je pense, à me retourner la question sur les mesures que nous devrions prendre à cet égard. C'est la question que nous vous avons posée.

Je veux donner un autre exemple. Il s'agit d'un passage qui se trouve à la page 18 et qui porte le titre « Pratiques de surveillance des programmes de sécurité dans les organisations ». Et ça recommence : « Dans les quatre organisations examinées, les pratiques de surveillance des programmes de sécurité allaient d'insatisfaisantes »—c'était le meilleur résultat—« à inexistantes.»

Il faudrait commencer à recevoir des rapports qui ne mettent pas en colère les membres du comité comme c'est le cas actuellement, car malgré nos rires et nos sourires, il s'agit d'une question très grave. C'est le deuxième rapport dans lequel la vérificatrice générale signale qu'il y a des retards. C'est inacceptable. Dans vos propos, Mme McDonald, et dans ceux des autres témoins, rien ne me convainc que le gouvernement prend cette question au sérieux ou que vous êtes même dans une position pour prendre les mesures qui s'imposent à cet égard.

Si, après votre comparution, vous étiez résolument déterminée à faire bouger les choses parce qu'il est clair dorénavant que le Parlement prend cette question au sérieux, que changeriez-vous aux mesures que vous prenez actuellement?

Mme Helen McDonald: Je ne sais pas si je ferais les choses différemment, et je suis déterminée et résolue à régler le problème. Il faut reconnaître que ce n'est pas seulement le Secrétariat du Conseil du Trésor qui assure la sécurité informatique; chaque ministère a un rôle à jouer et chaque sous-ministre doit être convaincu de l'importance de la sécurité.

Ce qui est encourageant, c'est que des progrès sont faits. Les choses sont claires. Nous avons des données de référence qui nous permettent d'évaluer la situation actuelle, ce que nous n'avions pas il y a quelques années. Les vérificateurs n'ont pas tenu compte de certains autres aspects comme le rôle de la voie de communication protégée ou la prestation de services communs. Ils n'ont pas tenu compte de la facilité accrue avec laquelle on pouvait partager l'information sur les incidents dans l'ensemble de l'administration fédérale.

Il n'y a pas eu d'intrusion grave dans les systèmes du gouvernement du Canada. Oui, nous saurions...

● (1655)

M. David Christopherson: À votre connaissance.

Mme Helen McDonald: Je crois que nous le saurions s'il y en avait eu.

M. David Christopherson: Eh bien, la vérificatrice générale s'inquiétait justement du fait que vous ne le sauriez pas.

Le président: Merci beaucoup.

J'aimerais simplement rappeler ce qu'on disait en 1997 ou 1998, peut-être même en 1996, lorsqu'on se préparait au passage à l'an 2000. Le problème que nous avions cerné à l'époque, c'était que le Conseil du Trésor, qui devait veiller à ce que le passage à l'an 2000 ne soit pas une catastrophe, ne pouvait obtenir la collaboration des ministères parce qu'il n'exigeait rien d'eux.

J'entends la même chose aujourd'hui. Vous avez les rôles, les mécanismes de surveillance, de contrôle, etc., mais les sous-ministres semblent être maîtres de leur destin. Ils ne subissent aucune pénalité, même s'ils ne suivent pas les lignes de conduite. Six, sept ou huit ans se sont maintenant écoulés, et nous retrouvons le même problème dans un autre contexte : le Conseil du Trésor, le gestionnaire central du gouvernement, n'oblige pas les ministères à faire le travail même si, comme M. Christopherson l'a souligné, de graves problèmes pourraient s'ensuivre.

Monsieur Allison, vous avez huit minutes.

M. Dean Allison (Niagara-Ouest—Glanbrook, PCC): Merci, monsieur le président, et merci aux témoins de comparaître.

David a déjà lu le paragraphe que je voulais lire, alors je ne vais pas le refaire. Toutefois, il y a deux questions que j'aimerais aborder. Il y a d'abord l'usurpation d'identité, puis toute la question de la responsabilité au sein des ministères : qui, en bout de ligne, est responsable ou est tenu de rendre des comptes?

Concernant l'usurpation d'identité, comme nous le savons, il est très facile maintenant aux États-Unis et en Amérique du Nord d'avoir accès à des renseignements personnels. Nous comprenons aussi que les torts causés aux individus sont irréparables, que ce soit sur le plan financier ou encore lorsque la réputation est en jeu, peu importe.

En tant que gouvernement, vous détenez les plus grandes banques de données et vous possédez les renseignements les plus personnels sur chaque membre de chaque organisation, de chaque organisme et de chaque entreprise au Canada, et je dirais même en Amérique du Nord. Compte tenu que des effractions sont commises et que nous ne sommes pas certains si des gens ont accès à nos données, comment pouvez-vous nous garantir que les données personnelles des Canadiens sont protégées, notamment lorsqu'ils communiquent avec vous par Internet, ce qui est de plus en plus fréquent? Quelles garanties pouvez-vous donner aux Canadiens?

Mme Helen McDonald: C'est que nous savons qui vous êtes, que c'est bel et bien avec vous que nous communiquons; nous sommes en mesure d'établir, sans l'ombre d'un doute, votre identité. C'est pour cette raison que nous avons beaucoup réfléchi à la façon dont nous pouvions interagir efficacement avec les Canadiens et les entreprises qui communiquent avec nous par Internet, qui veulent traiter avec nous en ligne.

Comment savoir qui est vraiment Helen McDonald@hotmail? Il nous faut un ensemble de secrets qui sont échangés entre vous et le ministère, d'après les antécédents que vous avez eus avec ce dernier. Dans ce cas, notre système d'évaluation des menaces et des risques nous dit que nous pouvons établir votre identité à notre satisfaction, selon cet ensemble de secrets que nous partageons.

Dans d'autres cas, il est possible que vous n'ayez pas de relation préétablie avec un ministère. C'est là où la situation devient un peu plus délicate, où nous aurions besoin d'une rencontre en personne et où nous pourrions vous demander d'apporter des documents originaux, pour que nous puissions établir qui vous êtes.

Comme vous le savez sans doute, l'identité est comme une chaîne formée de divers maillons : un NAS, un permis de conduire, telle ou telle chose. Le gouvernement fédéral, de concert avec les provinces et les territoires, s'est penché sur cette chaîne de confiance. Est-ce que nous émettons, sur la foi d'une carte de bibliothèque, un document de portée plus grave? Comment pouvons-nous être certains que les documents de base qui établissent l'identité d'une personne sont soumis à un processus rigoureux à tous les paliers de gouvernement et qu'ils sont dignes de confiance? Comment pouvons-nous être certains que lorsqu'une personne naît dans une province et meurt dans une autre, nous comprenons que cette personne est décédée et que son identité ne peut être réutilisée?

C'est un effort réel que nous poursuivons depuis quelques années afin de réduire le risque d'usurpation d'identité lors de nos interactions avec les citoyens ou les entreprises. Il y a beaucoup de zones tampons entre les programmes et les ministères. Ces zones tampons protègent vos renseignements, parce que vous pouvez empêcher les autres de les voir. Vous pouvez en contrôler l'accès. Toutefois, nous essayons aussi de trouver un équilibre entre ces mesures et l'optimisation des ressources financières. Est-ce possible d'avoir des opérations gouvernementales plus efficaces et plus efficientes en partageant l'information qui se trouve dans les zones tampons des programmes?

C'est moins coûteux. C'est peut-être aussi plus facile pour le client qui n'a pas à répéter la même information. Toutefois, vous voulez aussi un système qui respecte les droits à la vie privée des Canadiens et qui n'augmente pas les risques pour la sécurité que pose la circulation de ces renseignements. C'est pourquoi nous utilisons des mécanismes comme l'infrastructure à clés publiques pour protéger l'information lorsqu'elle transite et nous cherchons des moyens de garantir que chaque donnée, ou presque, est adéquatement protégée, peu importe où elle est dirigée.

● (1700)

M. Dean Allison: Très bien. Ce qui m'inquiète davantage, c'est la protection des réseaux.

Je lis le paragraphe 1.55 du rapport de la vérificatrice générale, qui dit ceci :

> 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... non autorisé

C'est ce qui m'inquiète, l'accès non autorisé et non l'accès ponctuel normal.

> ... 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.

À mon sens, la protection des réseaux est fondamentale. On dit ici que les réseaux ne sont pas protégés et que les contrôles d'accès aux réseaux sont inadéquats. Il n'est pas question ici des manipulations normales d'une personne qui cherche des données, mais bien des intrusions par la porte de derrière, et c'est ce qui m'inquiète. Ce ne sont pas les systèmes que vous mettez en place devant la façade, qui me paraissent logiques; ce sont les approches par derrière et les solutions rapides.

En 1999, un projet a permis de tester le niveau de cybermenace auquel était exposé l'espace Internet du gouvernement fédéral. L'expérience a duré trois mois et a donné lieu à plus de 80 000 alarmes et plus de 500 tentatives d'intrusion dans les systèmes des ministères. Est-ce que d'autres tests ont été effectués?

Mme Helen McDonald: Est-ce que d'autres tests ont été effectués pour...?

M. Dean Allison: Est-ce que d'autres tests ont été effectués pour voir quel type de cybermenace guettait notre espace Internet?

Mme Helen McDonald: Nous effectuons des tests constamment et nous en faisons rapport. M. Gauthier peut probablement donner plus de précisions à ce sujet.

La protection des portes arrières, puisque votre question partait de là, est aussi absolument essentielle. Nous ne devons pas seulement parer aux menaces de l'extérieur, mais aussi aux menaces de l'intérieur; il faut empêcher les employés de voir des renseignements ou d'accéder à une banque de données s'ils n'en ont pas le droit, et nous avons des pistes de vérification qui nous permettent de dire qui s'est introduit ou ne s'est pas introduit dans un système.

Nous devons veiller à ce que l'information ne soit pas modifiée par un employé malicieux ou une attaque malveillante, parce que nous devons faire en sorte que notre système de transactions inspire la confiance, de part et d'autre, que nos pistes de vérifications sont telles que personne ne peut nier qu'une transaction a eu lieu. C'est pour cette raison que nous utilisons de plus en plus des technologies comme l'infrastructure à clés publiques, parce qu'elles donnent ces garanties. À ces mesures s'ajoutent l'enquête de sécurité sur le personnel, l'utilisation physique de mots de passe, l'encryptage des données, etc.

Toutes ces mesures doivent absolument aller de pair. Notre système est-il parfait? Non.

Le président: Il vous reste une minute, monsieur Allison.

M. Dean Allison: D'accord.

J'aurais peut-être dû parler d'abord—comme M. Christopherson et M. Lastewka l'ont fait—de toute la question de responsabilité. Au bout du compte, je n'ai pas l'impression que vous avez la poigne nécessaire pour faire bouger les choses dans votre ministère. Nous avons évidemment le Secrétariat du Conseil du Trésor qui y voit, et d'autres organismes.

Que peut-on faire? Quelles mesures recommandez-vous pour que quelqu'un soit responsable en bout de ligne, pour que nous puissions demander à quelqu'un pourquoi ces ministères ne suivent pas la cadence et pourquoi les rapports ne sont pas remplis? Qui doit faire face à la musique lorsque ces choses ne sont pas faites correctement? Ce que je redoute, c'est qu'il y aura une catastrophe et que chacun se mettra à montrer l'autre du doigt et à dire, comme nous l'avons entendu auparavant, « ce n'est pas ma faute ».

Que suggérez-vous?

Mme Helen McDonald: J'ai deux suggestions. En 2002, la politique du gouvernement sur la sécurité exigeait que les systèmes de TI soient certifiés comme étant conformes aux normes de sécurité informatique. Quelqu'un au sein du ministère doit donc passer en revue cette liste de vérification et dire voici comment nous pouvons prouver que nous suivons de saines pratiques en matière de sécurité informatique. Le propriétaire d'entreprise doit donner son approbation et accepter tous les risques résiduels. Il s'agit d'un document qui doit être signé et qui confère une certaine responsabilité.

À titre de DPI, je fais la même chose; je certifie toute l'infrastructure commune, les systèmes informatiques communs, qui touchent l'ensemble des ministères. Voilà un autre document que je signe. J'accepte les risques résiduels. Et je ne le fais que si j'ai la certitude que le système est conforme aux meilleures pratiques de sécurité informatique.

Je crois que c'est une façon d'y arriver. Je ne peux pas dire que tous les systèmes ont été certifiés—c'est un processus qui vient d'être mis en branle—, mais tous les nouveaux systèmes le sont.

Je songe à l'idée d'un système de pointage—et vous avez peut-être des conseils à nous donner à ce sujet—, si nous pouvons en arriver aux dimensions que nous recherchons dans les ministères, vaudrait-il la peine d'avoir un genre de tableau de bord qui dirait aux cadres supérieurs « Voici où vous en êtes et vos résultats laissent à désirer »? Je crois qu'il faut être en mesure d'indiquer où vous en êtes et où vous devez vous rendre.

● (1705)

Le président: Monsieur Timmins, voulez-vous ajouter quelque chose?

M. Douglas Timmins: Oui, monsieur le président.

Mme McDonald a dit un peu plus tôt, je crois, que les sous-ministres étaient les personnes qui étaient responsables au bout du compte. Si on les amène à reconnaître les risques que comportent les systèmes informatiques et la vulnérabilité de leur ministère, entre autres choses... parce qu'ils ont d'autres priorités. Les efforts faits dans ce sens, notamment en les amenant à signer des plans d'action, sont toutes des mesures positives qui nous permettront, je crois, d'assurer cette responsabilité.

C'est tout ce que je voulais ajouter.

Le président: Merci beaucoup.

Monsieur Murphy, vous avez huit minutes.

L'hon. Shawn Murphy (Charlottetown, Lib.): Merci beaucoup, monsieur le président, et merci aux témoins de comparaître aujourd'hui.

J'aimerais simplement poursuivre dans cette lignée, madame McDonald. Dans un ministère responsable normal, quelle personne—et je sais qu'on pourrait répondre que le sous-ministre est ultimement responsable—serait responsable de cette fonction au sein du ministère? Serait-ce un sous-ministre adjoint ou serait-ce le directeur des finances?

Mme Helen McDonald: C'est l'agent de sécurité du ministère.

L'hon. Shawn Murphy: Chaque ministère aurait donc un agent de sécurité. Cette personne relèverait-elle directement du sous-ministre ou du sous-ministre adjoint?

M. Simon Gauthier: Je peux peut-être répondre à cette question.

La situation est différente d'un ministère à l'autre, mais tous les ministères ont un ASM. Ils ont aussi un coordonnateur de la sécurité de la technologie de l'information. Oui, ces personnes font rapport au sous-ministre, mais ça varie d'un ministère à l'autre.

L'hon. Shawn Murphy: Concernant toute la question de responsabilité, supposons qu'il y ait—et c'est certainement le cas—un ministère qui refuse de se conformer ou dont les systèmes ne sont pas dans un état qui vous semble satisfaisant. Quels moyens d'action avez-vous dans ce cas? J'espère que ce n'est pas seulement votre pouvoir de persuasion.

Mme Helen McDonald: Nous pouvons leur interdire de se connecter à la voie de communication protégée.

L'hon. Shawn Murphy: L'avez-vous déjà fait?

Mme Helen McDonald: Non. Et je dis non... La voie de communication protégée est en place depuis peu de temps. Les ministères commencent à y migrer. C'est peut-être une question de maturité.

Je ne veux pas perdre de vue la certification. Je présume également que nous pourrions arrêter de financer un projet de TI si nous croyons que la sécurité... ou plutôt, je ne présume pas; nous pouvons effectivement arrêter de financer un projet de TI lorsque les questions de sécurité ne sont pas dûment intégrées dans sa conception, parce que les projets d'envergure doivent être approuvés par le Conseil du Trésor. Ce ne sont pas tous les projets que réalise un ministère, mais les projets d'envergure qui doivent être approuvés à un niveau supérieur.

L'hon. Shawn Murphy: Tous les organismes sont donc assujettis au même cadre fondamental?

Mme Helen McDonald: La plupart d'entre eux, je crois, mais les niveaux d'autorisation peuvent être différents.

L'hon. Shawn Murphy: Ce que je veux dire, madame McDonald, c'est que ce système vous impose tout un fardeau, à vous, à votre ministère et à votre personnel. Ne serait-il pas préférable d'avoir un système semblable à ce qu'on voit dans plusieurs autres sphères d'activités? Vous élaborez la liste de vérification, les normes et les exigences, et ce sont les ministères qui doivent certifier, sur une base trimestrielle ou semestrielle, de façon claire et sans équivoque, qu'ils respectent toutes les normes que vous avez fixées. C'est comme pour un avion. Tous les six mois ou dans un intervalle quelconque, chaque avion doit subir une inspection; s'il n'est pas soumis à cette inspection ou s'il échoue, alors l'avion est cloué au sol. C'est aussi simple que cela.

N'aurions-nous pas une meilleure architecture si le système était... D'une certaine façon, votre tâche serait allégée si un ministère ou un organisme ne se soumettait pas à ce processus ou s'il ne vous remettait pas le certificat signé par l'agent du ministère et le sous-ministre qui atteste le respect de toutes les normes. À défaut de se soumettre à cet exercice, il cesserait ses activités, et la décision viendrait d'en haut, du greffier du Conseil privé.

Vous voyez où je veux en venir. Vous enlevez cette responsabilité de votre ministère et de votre personnel et vous la confiez à ces 130 organismes et ministères. S'ils ne se plient pas aux exigences, ils cessent alors leurs activités.

● (1710)

Mme Helen McDonald: C'est justement ce que vise le processus de certification et d'accréditation. Dans chaque ministère, pour les projets qui lui sont propre ou qui sont en collaboration avec un ou deux autres ministères, il faut certifier que tout est correct et quelqu'un doit les approuver. Dans les cas où on voudrait voir jusqu'où va le processus, on pourrait alors envisager d'avoir davantage recours aux outils de vérification.

Comme je l'ai dit, ça touche manifestement les nouveaux projets, mais on devrait pouvoir revenir en arrière, ce qui n'est pas le cas. C'est un élément que nous allons devoir suivre de près; nous ne mettons pas uniquement l'accent sur les nouveaux projets car nous savons que les systèmes déjà en place sont dotés de certains bons outils technologiques.

Pour ce qui est de l'autorisation des plans d'action par les sous-ministres, c'est une façon pour ces derniers de reconnaître qu'ils sont tenus d'améliorer le niveau de sécurité informatique ou de s'assurer que ce niveau est adéquat.

L'hon. Shawn Murphy: Vous reconnaissez toutefois qu'il est possible que l'année prochaine, lorsque vous reviendrez devant ce comité, vous en serez encore à supplier certains ministères et organismes à amener leurs normes au niveau requis à la fois par la vérificatrice générale et par vous aussi, n'est-ce pas?

Mme Helen McDonald: Je crois que la majorité des grands ministères font actuellement de bons progrès. D'après les évaluations et les visites, tout semble indiquer que les principaux ministères ont une plus grande capacité d'amener leurs systèmes à niveau. Ces ministères s'inquiètent toutefois des systèmes de traitement des données fiscales et des autres grandes bases de données car ils tiennent énormément à protéger les renseignements personnels, la sécurité informatique et leur réputation. Les gens ne soumettront pas électroniquement leurs déclarations d'impôt sur le revenu s'il y a des risques.

Je crois que le problème se situe davantage au niveau des ministères et des organismes de moins grande envergure. Si on considère une approche commune... Pourquoi laisser les petits ministères élaborer ou fournir leurs propres outils de sécurité informatique au lieu de leur offrir une approche plus centralisée pour leur éviter d'avoir à développer cette capacité? Ça peut se faire de façon centrale, ce qui permettrait d'améliorer globalement le niveau de sécurité. Je pense qu'il faut non seulement envisager des solutions quelque peu différentes, selon la nature du problème, mais aussi une approche à facettes multiples; on ne peut pas avoir uniquement recours à la persuasion.

L'hon. Shawn Murphy: Merci, monsieur le président.

Le président: Merci, monsieur Murphy.

Monsieur Kramp, allez-y. Nous sommes rendus au deuxième tour de table; nous aurons donc cinq minutes.

M. Daryl Kramp: Merci.

Merci d'être ici aujourd'hui. Mon principal commentaire, c'est qu'on ne peut pas régler un problème si on n'en connaît pas la cause, comme on dit.

Bien entendu, si je regarde le rapport de la vérificatrice générale sur les évaluations de la vulnérabilité, qu'a mentionnées M. Fitzpatrick plus tôt, 46 des 82 ministères ont déclaré avoir effectué un type ou autre d'évaluation de la vulnérabilité. Cela signifie que près de la moitié des ministères ne savent même pas s'ils ont des failles. Il y a peut-être un problème, mais ils ne le savent pas. Ce qui m'amène à me demander comment on peut trouver des solutions si on n'a pas cerné le problème.

Comment expliquer ça? Pourquoi n'ont-ils pas évalué leur capacité de réagir à une situation imprévue? S'ils ne l'ont pas fait, c'est pour l'une des trois raisons suivantes : le manque de ressources, le manque de main-d'oeuvre ou le manque de volonté. D'après vous, quelle est la raison? Qui faut-il blâmer?

● (1715)

Mme Helen McDonald: Pendant la période visée par le rapport, 46 des 82 ministères nous ont remis leur auto-évaluation. D'autres ont été soumises plus tard. Le Bureau du vérificateur général a contacté les 82 ministères et a obtenu 82 auto-évaluations en plus d'autres questions.

On peut donc dire que ces 82 ministères ont une bonne idée de ce qui ne va pas car ils ont tous effectué une auto-évaluation de la gestion de leurs normes de sécurité relatives aux technologies de l'information.

M. Daryl Kramp: Vous pensez donc qu'ils sont au courant qu'il y a peut-être un problème, n'est-ce pas?

Mme Helen McDonald: Ils savent d'où pourraient surgir les problèmes, et nous nous attendons à ce que ça se voie dans leurs plans d'action qui seront soumis à la fin de l'été.

M. Daryl Kramp: J'aimerais maintenant revenir à une autre situation...

Monsieur Timmins, vous aviez un commentaire?

M. Douglas Timmins: J'aimerais préciser qu'on parle de deux types d'évaluation différents. Je pense que Mme McDonald parlait des auto-évaluations alors que la question de M. Kramp portait sur le paragraphe 151 où il est dit que 46 ministères ont effectué une évaluation de la vulnérabilité, ce qui n'est pas la même chose qu'une auto-évaluation. Je tenais à m'assurer que la réponse était reliée à la bonne question.

Nous avons un tableau qui fait une répartition de ces 46 ministères. Les six principaux ministères ont effectué une évaluation de la vulnérabilité. Ce sont donc certains ministères de plus petite taille qui ne l'ont pas faite.

M. Daryl Kramp: D'accord.

J'aimerais parler d'une situation qui pourrait être catastrophique. Lorsque nous nous sommes préparés au passage à l'an 2000, tout le monde a mis la main à la pâte. L'ensemble du gouvernement était relativement prêt à la fin pour le passage à l'an 2000, mais tout d'un coup, on dirait que le besoin d'être à jour n'est plus une priorité.

Pour donner suite à la préoccupation soulevée par M. Christopherson, je dirais que beaucoup de Canadiens et Canadiennes dépendent de... Nous sommes maintenant une nation qui est dépendante de la technologie de l'information. Par exemple, si demain aucun chèque ne pouvait être émis pendant deux, trois ou quatre semaines en raison d'un pépin informatique, tous les gens qui dépendent du système social pour survivre ne recevraient pas d'argent. Ça ne suffirait pas de dire, « on va régler ça ». Ce n'est pas une réponse acceptable pour les nombreuses personnes qui luttent chaque jour pour leur survie et qui n'arrivent pas à joindre les deux bouts.

Avons-nous des mesures de rechange en cas d'urgence? De quels types de mécanismes de sécurité intégrée disposons-nous? Quelle garantie avons-nous qu'il y a un plan de rechange en cas de situation catastrophique?

Mme Helen McDonald: Je ne peux pas parler pour DRH ou un autre ministère, mais je sais qu'il y a des plans de secours non seulement en cas de panne de courant, d'actes malveillants ou de grève, mais aussi pour assurer la continuité des services essentiels lors de situations d'urgence.

M. Daryl Kramp: Ces ministères vous ont-ils soumis leur plan ou vous en ont-ils seulement parlé?

Mme Helen McDonald: Non, leurs plans ne m'ont pas été soumis. Nous exigeons toutefois qu'un plan soit élaboré.

M. Daryl Kramp: Je vous conseillerais fortement de trouver une façon d'obtenir une quelconque validation, si c'est possible. Les gens ne paient pas l'épicerie avec des promesses.

M. Simon Gauthier: Si vous me le permettez, monsieur, j'aimerais ajouter qu'en vertu de la Politique du gouvernement sur la sécurité, ou PGS, nous demandons aux ministères qu'ils soumettent leur plan à la SPPCC. Conformément à cette politique, la SPPCC est l'organisme responsable de la « vérification », si j'ose dire, de ces plans de secours.

Le président: Merci, monsieur Kramp.

Monsieur Holland, vous avez cinq minutes.

M. Mark Holland: Merci, monsieur le président.

Merci à vous, chers témoins.

J'aimerais parler de deux ou trois choses. D'abord, je crois qu'il y a un élément qui transpire de tout ça, c'est-à-dire la possibilité d'obliger les sous-ministres à se conformer au processus ou d'établir un mécanisme qui les inciterait à le faire. Manifestement, c'est une question très sérieuse, et je crois que nous devons regarder le contexte. J'ai besoin de comprendre certains des termes utilisés qui sont un peu obscurs. Par exemple, on parle de risque ou de risque important, mais c'est assez flou.

De toute évidence, la technologie est, de par sa nature, vulnérable. Quiconque dit qu'il a un système à toute épreuve n'a qu'à attendre un ou deux mois pour qu'un adolescent de 16 ans invente une façon de le déjouer. La vérité, c'est que la technologie change sans cesse, qu'elle est vulnérable et qu'elle aura toujours des failles. En ce qui a trait au processus et à sa mise en oeuvre d'ici 2006, d'après Mme McDonald, il ne fait aucun doute que ça exige des efforts continus puisqu'il s'agit d'un environnement qui change sans arrêt, ce qui rend la tâche ardue.

C'est difficile aussi pour les grandes organisations car elles ont des systèmes informatiques très complexes et diversifiés. On veut évidemment avoir la meilleure protection possible, mais la mise en place rapide et répandue de mesures de protection peut être tout un défi pour une grande et complexe organisation.

En réalité, je n'ai que deux questions. J'imagine qu'elles sont pour M. Timmins car j'ai besoin de comprendre certaines choses.

Il y a des règlements de référence. Nous avons aussi parlé de normes internationales. Est-ce la même chose? Qu'est-ce qu'un risque important? À quel point est-ce qu'un système devient vulnérable et faible? Où doit-on fixer la limite pour ne pas alarmer inutilement les gens sans pour autant ignorer une préoccupation légitime?

Mon autre question concerne le processus permanent d'examen et de mise à jour. Comment peut-on aborder ça?

● (1720)

M. Douglas Timmins: Merci.

Pour ce qui est des règlements de référence ou de la limite tolérée, nous utilisons les normes, comme l'a dit Mme McDonald, qui ont été établies par le gouvernement, plus précisément le Conseil du Trésor, dans la Politique du gouvernement sur la sécurité et les directives afférentes. J'imagine qu'on demande aux ministères d'effectuer des évaluations de la menace et du risque ou de la vulnérabilité, et ce périodiquement, pour savoir où ils en sont.

Nous ne préjugeons pas des risques. Nous savons que ces risques et menaces existent. Je suis d'accord pour dire que nous ne pouvons pas nous attendre à enrayer tous les risques. C'est impossible. C'est d'ailleurs ce que nous avons dit dans notre chapitre, mais n'empêche que nous avons l'obligation d'être à jour et de ne pas prendre de retard.

Voilà pourquoi nous croyons qu'il faut remettre cet enjeu dans les priorités des sous-ministres en l'intégrant au profil de risque de l'organisation pour assurer la continuité des opérations. Il n'est pas nécessaire que tous les ministères demeurent pleinement opérationnels pendant une catastrophe ou lors d'une attaque, comme l'ont illustré la planification du passage à l'an 2000 et la grande panne d'électricité, il y a deux ans.

Dans notre esprit, nous ne nous attendons pas à ce que tout soit parfait et protégé. Il s'agit plutôt d'avoir une procédure et un processus permettant que tout soit à jour.

M. Mark Holland: Effectivement. Nous savons que d'autres grandes organisations, particulièrement les grandes sociétés, ont les mêmes inquiétudes que nous et ont été victimes d'atteintes à la sécurité. D'ailleurs, lorsque nous avons abordé la question des banques, celles-ci avaient des inquiétudes dans divers domaines. Il y a un risque inhérent à toute technologie, et nous voulons que celle-ci soit le plus solide possible.

Monsieur Timmins, voici ma dernière question. Vu les commentaires que nous avons entendus, nous comprenons maintenant que le point de référence est la norme qui a été adaptée au contexte gouvernemental. Mme McDonald a dit que nous devrions avoir adhéré à cette norme d'ici 2006 et qu'il serait peut-être possible que les grands ministères, ceux dont les préoccupations en matière de sécurité sont les plus considérables, le fassent plus tôt. Seriez-vous satisfait de voir les choses progresser ainsi et, avec l'appui du comité et peut-être même à la suite de ce processus, d'obtenir d'autres moyens, si vous voulez, d'inciter les sous-ministres à s'assurer qu'ils mettent plus rapidement de l'avant ces changements?

M. Douglas Timmins: Nous encourageons évidemment la prise de mesures plus précoces. L'échéance visé est 2006, et si nous y arrivons, ce sera merveilleux. Si nous pouvions atteindre nos objectifs avant, ce serait encore mieux. Je pense que la bonne façon de procéder serait que les grands ministères s'y mettent plus rapidement pour déterminer leurs priorités, élaborer un plan d'action et s'y engager.

M. Mark Holland: Merci.

Le président: Merci beaucoup, monsieur Holland.

Avant de terminer, j'ai une observation à vous faire, madame McDonald. Dans le rapport, la vérificatrice générale a soulevé des préoccupations sérieuses en ce qui a trait au risque d'atteinte à la sécurité des technologies de l'information du gouvernement du Canada. Vous avez entendu les commentaires des députés qui s'inquiètent du manque d'attention qu'accordent les ministères et les sous-ministres à la nécessité d'assurer la meilleure sécurité possible aux systèmes.

À la lecture de votre déclaration, on croirait qu'il n'y a pratiquement pas de problèmes, si ce n'est lorsque vous dites que « le gouvernement du Canada souscrit entièrement aux recommandations de la vérificatrice générale » et que « les recommandations de la vérificatrice générale sont conformes aux résultats de l'évaluation de la sécurité des technologies de l'information que nous avons effectuée ». Vous ne mentionnez aucun problème en particulier et ne dites pas ce que vous comptez faire. Outre ces deux passages où vous êtes d'accord avec la vérificatrice générale, vous ne faites nullement allusion à la gravité des problèmes soulevés dans le rapport. Je trouve ça déconcertant car nous ne vous avons pas fait venir ici pour nous dire que tout va bien, mais bien pour parler des lacunes repérées par la vérificatrice générale.

Je ne vais pas vous exiger de commenter mes propos, mais je vais demander au greffier qu'il s'assure que lorsque nous inviterons des témoins à comparaître devant ce comité à l'avenir, nous pourrons nous attendre à ce que ces derniers reconnaissent dans leur déclaration les problèmes soulevés par la vérificatrice générale et qu'ils en parlent. Nous ne voulons pas d'une déclaration dans laquelle on nous dit que tout est beau. Nous voulons traiter des problèmes soulevés. Par conséquent, je vais demander au greffier de s'assurer que les témoins qui comparaîtront devant le comité à partir d'aujourd'hui sauront que nous nous attendons à ce qu'ils abordent les lacunes soulevées par la vérificatrice générale. Après tout, c'est le but de nos délibérations.

Monsieur Timmins, avez-vous quelque chose d'autre à ajouter pour terminer?

● (1725)

M. Douglas Timmins: Monsieur le président, j'aimerais seulement vous dire encore une fois que je suis très heureux que le comité se soit intéressé à ce chapitre. J'encourage d'ailleurs le comité à maintenir cet intérêt. Il y a des plans d'action qui visent la prochaine année environ. Le comité pourrait penser à une façon de s'assurer qu'ils sont effectivement mis en oeuvre.

Le président: Merci beaucoup, mesdames et messieurs.

La séance est levée.

Publié en conformité de l'autorité du Président de la Chambre des communes

Published under the authority of the Speaker of the House of Commons

Aussi disponible sur le réseau électronique « Parliamentary Internet Parlementaire » à l'adresse suivante :
Also available on the Parliamentary Internet Parlementaire at the following address:
http://www.parl.gc.ca

Le Président de la Chambre des communes accorde, par la présente, l'autorisation de reproduire la totalité ou une partie de ce document à des fins éducatives et à des fins d'étude privée, de recherche, de critique, de compte rendu ou en vue d'en préparer un résumé de journal. Toute reproduction de ce document à des fins commerciales ou autres nécessite l'obtention au préalable d'une autorisation écrite du Président.

The Speaker of the House hereby grants permission to reproduce this document, in whole or in part, for use in schools and for other purposes such as private study, research, criticism, review or newspaper summary. Any commercial or other use or reproduction of this publication requires the express prior written authorization of the Speaker of the House of Commons.