CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent des ressources humaines, du développement des compétences, du développement social et de la condition des personnes handicapées

HUMA • NUMÉRO 067 • 1re SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 14 février 2013

Président

M. Ed Komarnicki

Comité permanent des ressources humaines, du développement des compétences, du développement social et de la condition des personnes handicapées

Le jeudi 14 février 2013

● (1105)

[*Traduction*]

Le président (M. Ed Komarnicki (Souris—Moose Mountain, PCC)): La séance est ouverte.

Bonjour à tous. Nous allons commencer.

J'ai quelques observations générales à faire, et le sous-ministre nous parlera ensuite des questions à l'étude.

Vous aurez des écouteurs pour entendre la traduction de la séance. Bien entendu, nous savons tous que la protection des renseignements personnels est une question très importante pour tous les Canadiens, en particulier ceux dont les données ont disparu.

Notre comité se réunit pour se pencher sur la motion de M. Cleary, dans sa version modifiée par d'autres députés. Voici essentiellement de quoi il s'agit.

La motion porte sur une atteinte à la vie privée, ce qui suscite évidemment de graves inquiétudes pour tous les Canadiens, en particulier ceux qui en sont victimes. Nous sommes ici pour que vous nous expliquiez comment l'atteinte a eu lieu et pour que vous nous parliez des mesures prises pour assurer la protection des renseignements personnels dans l'ensemble du ministère et des solutions à long terme mises en place pour protéger l'identité des Canadiens touchés.

Il s'agit des principaux sujets. Vous devez donc vous attendre à ce que chaque parti vous pose des questions qui s'y rapportent après votre exposé.

Je ne fais évidemment pas abstraction du fait que la commissaire à la protection de la vie privée enquête sur les incidents. Le dossier a été confié à la GRC, et il est possible qu'il y ait des recours collectifs. Il y en a peut-être même déjà un de déposé. Il s'agit là d'éléments dont je tiens également compte.

J'ai l'intention d'accorder à chaque parti sept minutes plutôt que cinq pour les questions et réponses. Je demanderais à mes collègues de généralement respecter le temps qui leur est imparti pour que nous puissions faire deux tours. Je sais que nous avons un autre point à l'ordre du jour prévu à la fin de la séance, mais, dans la mesure du possible, j'espère pouvoir compléter les deux tours. Si nous manquons de temps, je proposerai au comité de reporter ce point; autrement, nous pourrons nous en occuper aujourd'hui.

Voilà qui termine ma déclaration préliminaire.

Vous avez la parole, monsieur Shugart.

M. Ian Shugart (sous-ministre, ministère des Ressources humaines et du Développement des compétences): Merci, monsieur le président.

Mesdames et messieurs les membres du comité, je m'appelle Ian Shugart. Je suis sous-ministre de RHDCC. Je suis accompagné du sous-ministre délégué de la Direction générale de l'apprentissage, M. Ron Parker; du directeur de nos services juridiques, M. Al Sutherland, qui est ici pour discuter des enjeux liés aux lois régissant notre travail; et du dirigeant principal de l'information du ministère, M. Charles Nixon.

Je tiens à dire que compte tenu de la gravité des incidents et de la question examinée par votre comité aujourd'hui et par le ministère au cours des dernières semaines, j'ai demandé à M. Parker, en sa qualité de sous-ministre délégué, de s'occuper personnellement des mesures correctrices ainsi que du suivi et de la surveillance de tout ce qui touche à ces incidents. Pendant de nombreuses journées au cours des derniers mois, ce dossier l'a occupé pratiquement à temps plein.

Mesdames et messieurs les membres du comité, comme le président l'a mentionné, nous comparaissons devant vous relativement à deux incidents touchant la sécurité qui se sont produits au sein de notre ministère et qui concernent la disparition d'appareils de stockage électroniques contenant des renseignements personnels.

Comme la ministre l'a dit, et je le répète au nom des gestionnaires du ministère, de tels incidents sont inacceptables. Des renseignements personnels de nature délicate ont été stockés sans être chiffrés sur des appareils portatifs, et ils n'ont pas été adéquatement protégés. Cela n'aurait pas dû se produire.

La ministre a aussi annoncé les mesures que nous sommes en train de prendre pour empêcher que des incidents de ce genre ne se reproduisent.

Au nom de Ressources humaines et Développement des compétences Canada, je voudrais m'excuser devant votre comité de ce qui s'est passé.

[*Français*]

J'aimerais profiter de l'occasion qui m'est offerte aujourd'hui pour présenter au comité un compte rendu détaillé de ce qui s'est passé dans les deux cas, pour décrire les mesures que nous avons prises en réaction à ce qui s'est produit, et pour expliquer les mesures que nous avons mises en oeuvre depuis pour atténuer les répercussions de ces incidents et empêcher que des incidents de ce genre ne se produisent de nouveau.

[*Traduction*]

Permettez-moi d'abord de faire la chronologie des deux événements. Dans les deux cas, les activités qui ont été menées avaient trait à la confirmation des incidents, à l'enquête sur ceux-ci, au renforcement des pratiques, ainsi qu'à l'information des Canadiens.

J'aimerais d'abord vous parler du disque dur manquant. Le 5 novembre 2012, un employé de l'administration centrale de RHDCC à Gatineau a découvert qu'un disque dur externe avait disparu et en a parlé à son gestionnaire, qui était la seule autre personne sachant exactement où se trouvait l'appareil. Le gestionnaire a déclaré qu'il n'avait pas pris le disque dur. On a demandé à d'autres employés de l'étage s'ils avaient vu ou emprunté un disque dur. Ils ont répondu que non.

Le disque dur externe se trouvait dans un immeuble d'accès restreint, dans un secteur également d'accès restreint, et il était dans une armoire avec cadenas.

L'équipe a déployé de multiples efforts sur de nombreux jours pour essayer de retrouver le disque dur manquant: on a parlé avec tous les membres de l'équipe ainsi que procédé à plusieurs fouilles du bureau de l'employé, de l'étage de l'employé et d'autres étages de l'édifice.

Le 22 novembre, la disparition du disque dur a été portée à l'attention du directeur, qui a demandé à tous les gestionnaires et les employés de la division de procéder à de nouvelles fouilles. Encore une fois, des efforts ont été déployés pour retrouver le bien manquant.

● (1110)

[*Français*]

D'anciens employés ainsi qu'un ancien gestionnaire du même groupe que les employés en question ont aussi été interrogés. On a également communiqué avec les commissionnaires et le technicien chargé du réseau local pour leur demander si un disque dur leur avait été remis ou si quelqu'un en avait trouvé un. Aucun n'avait été retrouvé.

Le 26 novembre, le directeur général a été avisé du fait que le disque dur disparu était utilisé pour faire des copies de sauvegarde des fichiers d'un lecteur réseau dans le cadre du processus de transmission des fichiers d'un secteur à l'autre du serveur. Des renseignements personnels concernant les clients et les employés étaient stockés sur le lecteur réseau, et la disparition du disque dur a donc été signalée immédiatement à la haute direction des programmes.

[*Traduction*]

Les employés de la direction générale ont continué de chercher, et l'agent de sécurité ministériel a été avisé le 28 novembre de la disparition du disque. De plus, les services de sécurité ministériels ont alors lancé plusieurs activités de recherche, dont des fouilles complètes des locaux et des entrevues avec les employés actuels et passés du secteur d'où provenait le disque dur manquant. Ils n'ont trouvé aucune preuve de méfait et ont jugé fort probable que le disque dur se trouvait quelque part dans les locaux de l'immeuble.

À ce moment-là, la haute direction a demandé une analyse de tous les fichiers stockés sur le disque dur, afin de déterminer quels renseignements avaient été perdus. L'analyse a été terminée Ie 6 décembre, et elle a permis de constater que Ie disque dur externe contenait des renseignements personnels sur environ 583 000 emprunteurs du Programme canadien de prêts aux étudiants, dont leur nom, leur date de naissance, leur numéro d'assurance sociale, leur numéro de téléphone, leur adresse et Ie solde de leur prêt. Le disque dur contenait également les coordonnées de 250 employés du ministère. II n'était pas protégé par mot de passe, et les fichiers qu'il contenait n'étaient pas chiffrés.

Les recherches approfondies dans l'immeuble où Ie disque dur aurait dû se trouver se sont poursuivies du 8 au 14 décembre, et il y a eu notamment d'autres fouilles complètes du rez-de-chaussée de l'immeuble effectuées par le bureau de sécurité régional ainsi qu'une analyse du contenu de tous Ies disques durs de la Direction générale de l'apprentissage. Toutes ces recherches ont été vaines et, le 14 décembre, Ie ministère a informé Ie Commissariat à la protection de la vie privée qu'un disque dur externe contenant des renseignements personnels avait disparu.

Au cours de la deuxième moitié du mois de décembre, la direction a procédé à de nouvelles entrevues avec les employés et la direction de l'immeuble, et d'autres disques durs similaires ont été recueillis à des fins d'analyse.

[*Français*]

Au cours de la première semaine de janvier, une enquête interne officielle a été lancée. Simultanément, des mesures correctives ont été mises au point, et les Canadiens ont été informés de la disparition du disque dur le 11 janvier.

Jusqu'à maintenant, il n'y a toujours pas de preuve qu'un méfait a été commis ou que les renseignements personnels que contenait le disque dur ont été consultés ou utilisés à des fins frauduleuses.

Un autre incident, sans lien avec le premier, s'est produit: une clé USB contenant des renseignements personnels a elle aussi disparu.

Le 14 novembre 2012, de l'information personnelle a été transférée sur la clé USB et livrée à un employé situé à un étage sécurisé à RHDCC.

● (1115)

[*Traduction*]

La clé USB a été utilisée Ie 15 novembre, mais Ie 16 novembre l'employé ne la retrouvait pas et en a avisé la direction. Le même jour, les agents de sécurité ministériels ont été avisés de sa disparition. À partir du 16 novembre, des agents de sécurité ministériels et des commissionnaires ont procédé à des fouilles complètes du bureau de l'employé et de l'étage sur lequel il est situé. L'employé a cherché la clé USB chez lui, et on a communiqué avec le chauffeur de taxi qui l'avait reconduit chez lui le 15 novembre; le taxi a été fouillé. Une équipe d'employés a également fait des recherches partout dans les dossiers, les classeurs, les salles de bain, les meubles et les bureaux de l'étage où la clé USB avait disparu. Les employés des services de nettoyage qui travaillaient sur cet étage ont été interrogés.

La clé USB contenait des renseignements sur 5 045 personnes, elle n'était pas protégée par mot de passe et les données qu'elle contenait n'étaient pas chiffrées. Elle contenait le type de renseignements suivants sur chacune des personnes en question: le numéro d'assurance sociale, le nom de famille, des codes d'affection génériques provenant de la Classification internationale des maladies, la date de naissance, les autres payeurs, par exemple la commission des accidents de travail, le degré de scolarité, la profession et le centre de traitement de Service Canada.

Le 22 novembre, le ministère a informé le Commissariat à la protection de la vie privée de la disparition de la clé USB contenant des renseignements personnels et des recherches qui avaient été menées pour la retrouver.

[*Français*]

Les recherches se sont poursuivies depuis cet incident, et une fouille approfondie du bureau de l'employé a de nouveau eu lieu le 7 décembre, menée par un cadre et une équipe d'employés.

Des lettres d'avis ont été envoyées aux 5 000 personnes touchées ou à leur tuteur légal le 19 décembre.

J'aimerais maintenant souligner toutes les mesures que nous prenons depuis ces deux incidents, et les mesures que nous mettons en vigueur pour empêcher que des incidents de ce genre ne se produisent de nouveau.

[*Traduction*]

Le ministère a renforcé ses politiques sur la protection et l'entreposage des renseignements personnels. Les mesures prises portent principalement sur le matériel, sur l'aspect logiciel et sur la culture que nous avons relativement au traitement des renseignements personnels.

Pour ce qui est du matériel, nous avons de nouveaux protocoles qui sont plus rigoureux. Les disques durs portables sont désormais proscrits. Les clés USB non approuvées ne peuvent être branchées au réseau.

De plus, tous les dispositifs de sécurité portables utilisés dans les locaux du ministère ont été évalués en fonction des risques afin d'assurer que des mesures de précaution appropriées soient mises en place. Ces évaluations se poursuivront sur une base régulière.

En ce qui a trait à l'aspect logiciel, nous procéderons à la mise en oeuvre d'une nouvelle technologie pour prévenir la perte de données, technologie qui pourra être programmée pour contrôler le transfert des renseignements névralgiques ou en empêcher la divulgation. Quant à la culture présidant au traitement de l'information, nous veillerons à renforcer l'importance primordiale de manipuler correctement les renseignements personnels de nature délicate grâce à une formation annuelle obligatoire qui sera offerte à tous les employés.

Nous travaillons à conscientiser notre effectif. Des événements de communication seront organisés à l'intention du personnel, et des mesures disciplinaires seront mises en oeuvre — lesquelles pourraient aller jusqu'à la cessation d'emploi — au cas où les codes stricts encadrant la protection des renseignements personnels et la sécurité n'étaient pas respectés. Nous avons aussi pris des mesures pour atténuer les répercussions pour les Canadiens touchés.

[*Français*]

Nous avons alerté les clients touchés pour qu'ils puissent prendre les mesures nécessaires pour protéger leurs renseignements personnels. Nous l'avons fait en diffusant des annonces publiques, en fournissant de l'information spéciale sur nos pages Web portant sur le sujet, en envoyant des lettres aux personnes touchées et en créant une ligne d'information sans frais pour répondre aux questions concernant les deux incidents, à savoir la clé USB et le disque dur manquants.

● (1120)

[*Traduction*]

Les dossiers des numéros d'assurance sociale touchés ont été annotés dans le registre de l'assurance sociale pour indiquer qu'ils ont été impliqués dans un incident et pour assurer que toute demande de modification soit soumise à un processus d'identification amélioré. Le ministère avertira aussi les personnes dont nous avons des coordonnées à jour s'il constate que leur dossier de numéro d'assurance sociale fait l'objet d'activités suspectes, quelles qu'elles soient. Comme précaution supplémentaire, le ministère a acheté d'Equifax Canada une trousse adaptée à ses besoins, qui est une solution unique en son genre faite sur mesure pour cet incident et qui sera disponible à toute personne qui aurait pu être touchée. Cette protection du crédit est une stratégie fiable et appropriée qui aidera à prévenir l'utilisation inappropriée des renseignements personnels et de l'information sur le crédit.

[*Français*]

Grâce à l'entente conclue avec Equifax, le ministère est en mesure d'offrir gratuitement la trousse personnalisée aux personnes touchées qui consentent à recevoir le service.

La note demeurera au dossier de crédit pendant six ans, à moins que la personne touchée ne décide de la faire enlever. Elle indiquera aux organismes de crédit que les données peuvent avoir été faussées, et les prêteurs prendront des mesures supplémentaires pour vérifier l'identité de la personne avant de lui faire crédit ou de lui ouvrir un compte ou lui permettre de l'utiliser.

[*Traduction*]

Monsieur le président, la protection et la sécurité des renseignements personnels sont des pierres angulaires de la mission du ministère. Nous sommes sûrs d'avoir pris les mesures adaptées à la situation, et nous veillons à faire en sorte que ces mesures soient observées afin d'assurer la sécurité des renseignements personnels qui nous sont confiés.

Merci.

Le président: Merci pour votre exposé.

Je n'ai qu'une question à vous poser. Vous avez indiqué que le disque dur était entreposé dans une armoire munie d'un cadenas et qu'il n'y avait que deux personnes qui pouvaient y accéder. Est-ce exact?

M. Ian Shugart: Oui, je le confirme.

Le président: D'accord.

Je vais lancer la ronde de questions. Commençons avec Mme Borg.

Allez-y.

[*Français*]

Mme Charmaine Borg (Terrebonne—Blainville, NPD): Merci, monsieur le président.

La perte des renseignements d'un demi-million de Canadiens nous préoccupe tous. Quand on calcule vraiment l'ampleur de cette perte, on se rend compte que c'est énorme.

[*Traduction*]

Pour moi, la situation illustre encore bien le manque total de respect de ce gouvernement à l'égard de nos renseignements personnels. Nous avons vu que le gouvernement n'a pas procédé aux mises à jour attendues des lois de base en la matière. Le rapport présenté l'an dernier au Parlement par la commissaire à la protection de la vie privée indique une hausse de 300 p. 100 des atteintes à la vie privée. Il s'agit de toute évidence du total pour l'ensemble des ministères. L'an dernier, dans son rapport de 2011-2012, la commissaire rapportait 80 atteintes à la protection des données dans les ministères, ce qui constitue un record. Lorsque je regarde ces chiffres, je vois qu'il y a un problème récurrent bien réel.

Maintenant, j'aimerais savoir si vous pouvez répondre à cette question: parmi ces 80 atteintes à la protection des données rapportées, combien sont survenues à RHDCC?

M. Ian Shugart: Je crois, sous réserve de confirmation, qu'il y en a eu 19, ce qui est un modeste recul — mais tout de même important pour nous — de deux par rapport à l'année précédente.

Mme Charmaine Borg: En ce qui me concerne, je crois que 19 atteintes de ce genre est un nombre assez élevé pour une seule année.

M. Ian Shugart: Nous avons l'intention de ramener ce chiffre à zéro et de le maintenir là, pour peu que cela soit possible.

Mme Charmaine Borg: Je suis très heureuse de l'entendre.

En fait, selon la Loi sur la protection des renseignements personnels, les ministères ne sont pas tenus de rapporter ces atteintes à la commissaire à la protection de la vie privée. Vous dites que 19 brèches ont été rapportées. Combien ne l'ont pas été?

M. Ian Shugart: Nous avons bel et bien un seuil qui tient compte de la nature et de la gravité d'une atteinte, ainsi que de la capacité à contenir très rapidement tous les types d'intrusion possibles. Il y a de temps en temps des incidents de cette nature, et nous intervenons aussitôt que nous en sommes informés, mais le seuil qui détermine un signalement à la commissaire n'est pas très élevé. Nous sommes souvent en rapport avec elle.

Quant à nos pratiques, nous recevons des conseils de la commissaire. Dans le cas qui nous intéresse, nous sommes restés en contact avec le Commissariat à la protection de la vie privée pendant tout le temps qu'a duré l'incident et nous avons été conseillés par lui, soit d'une façon officielle conforme à son mandat, soit par le biais d'un conseiller juridique ou sous forme d'une orientation pratique. Si un incident se produit qui soit de petite envergure et qui puisse être circonscrit facilement, il se peut que nous n'en informions pas la commissaire.

● (1125)

Mme Charmaine Borg: Êtes-vous en train de dire qu'il y a eu des atteintes à la protection des données qui n'ont pas été rapportées? En avez-vous un registre? Cette information peut-elle être transmise au comité?

Le président: Madame Borg, si je peux me le permettre, je sais que vous êtes à échafauder votre argumentaire, mais ce comité s'intéresse à trois choses: comment l'atteinte à la vie privée s'est-elle produite, quelles démarches ont été entreprises suite à cela, et quelle marche à suivre sera adoptée comme solution à long terme pour ceux qui ont été particulièrement touchés par cet incident.

Je sais que vous faites référence à des choses qui ont pu se produire dans le passé. Bien qu'elles puissent avoir de façon générale une certaine pertinence, il importe de traiter de cet incident en lui-même. Comment l'incident s'est produit, quelles mesures ont été prises par la suite et qu'est-ce qui sera fait pour ceux qui ont été touchés sont les sujets dont nous devons traiter.

Je vous ai laissé pas mal de latitude jusqu'ici, mais je vous demande de rester plus près du sujet, faute de quoi je devrai déclarer votre intervention irrecevable.

Mme Charmaine Borg: Merci pour cette clarification, monsieur le président, mais je pense que les Canadiens sont très préoccupés par le nombre d'intrusions subies par le gouvernement.

Le président: Nous parlons de celle-là en particulier.

Mme Charmaine Borg: Je comprends. Merci.

La commissaire à la protection de la vie privée a ni plus ni moins supplié le gouvernement d'agir et d'inciter les ministères à se doter d'exigences obligatoires en matière d'intrusion et d'exigences relatives aux atteintes à la sécurité des données. Comme cet incident concerne une atteinte à la sécurité des données et compte tenu de ce qui s'est produit, recommanderiez-vous que tous les ministères soient tenus d'informer la commissaire lorsque la sécurité des données est attaquée?

Le président: Si c'est ce que vous souhaitez faire, vous pouvez répondre à la question, mais votre rôle n'est pas d'indiquer quelles politiques le gouvernement pourrait adopter à l'égard des autres ministères. Dans le cas qui nous intéresse, votre responsabilité concerne ce qui s'est produit sur le plan administratif. La présente audience ne porte pas sur ce qui pourrait arriver relativement aux politiques du gouvernement et sur ce que le gouvernement pourrait choisir de faire ou de ne pas faire par rapport aux autres ministères.

Mme Charmaine Borg: Mais ils ont subi une brèche de données. Ils ont vécu quelque chose et ils peuvent... Je crois que nous souhaitons tous voir régler les problèmes systémiques.

Le président: Ils peuvent aborder la question, oui, mais je ne veux pas que nous nous attardions à ce que devraient être les politiques du gouvernement ou à ce que les autres ministères devraient faire. Nous traitons d'une atteinte à la protection des renseignements personnels au sein d'un ministère, et les questions devraient porter sur cet événement. Toutes les autres seront jugées irrecevables.

Mme Chris Charlton (Hamilton Mountain, NPD): Sauf votre respect, monsieur le président, je comprends les limites de la tâche qui nous est confiée, mais nous devons également étudier les systèmes mis en place par le gouvernement du Canada pour protéger les renseignements personnels des Canadiens. Il est donc opportun de s'informer à leur sujet. C'est ce que fait ma collègue. Je crois que vous devez lui accorder une certaine latitude.

Le président: Je n'en dirai pas plus et jugerai irrecevables toutes les questions sur les autres ministères.

Vous pouvez répondre de façon générale si vous le souhaitez, mais vous devez uniquement faire référence à votre ministère.

M. Ian Shugart: Merci, monsieur le président. J'irai aussi loin qu'il m'est possible d'aller, étant donné que les conseils que je donne au gouvernement sont transmis par le truchement de la ministre.

Je ne peux pas parler au nom des autres, mais je sais que le Conseil du Trésor a élaboré des politiques et directives qui s'appliquent à l'ensemble des ministères, dont RHDCC. Il incombe aux ministères de les appliquer en fonction de leur mission. C'est ce que nous tentons de faire.

Je peux vous dire que les cadres supérieurs ont recours à des mécanismes pour rester au courant des dossiers, de même que pour tirer les leçons des incidents en vue d'adopter les pratiques exemplaires et de veiller à ce que la culture d'entreprise de tous les ministères soit sensible à la protection des renseignements personnels et à la sécurité des TI. Le Conseil du Trésor est responsable de mettre régulièrement à jour ses politiques et directives en la matière. Voilà, en des termes généraux, le système qui régit notre travail.

Mme Charmaine Borg: Merci.

Vous dites avoir réformé vos politiques et la culture relative au traitement des renseignements personnels. Je me réjouis de l'entendre. J'ai très hâte de voir ce qui émanera de cette réforme, et de voir si le nombre d'atteintes à la protection des données chutera jusqu'à zéro, ce qui serait idéal.

Je me demande quels protocoles étaient déjà en place, et pourquoi certaines données n'étaient pas chiffrées. Vous dites que cela n'aurait pas dû arriver. Quelle était la politique à ce moment-là?

● (1130)

M. Ian Shugart: Je pourrais peut-être commencer par affirmer, et on le fera sans doute à d'autres reprises au cours de cette audience, que la culture revêt un caractère individuel. Donc, pour que les politiques et les directives fonctionnent au sein d'une grande organisation, tous les gestionnaires et les employés doivent les connaître et les respecter.

Mme Charmaine Borg: Puis-je vous demander comment vous faites pour vous en assurer?

M. Ian Shugart: Principalement par la formation. Comme je l'ai déjà dit, nous nous sommes engagés à mettre à jour notre formation dans ce domaine. Toutefois, au-delà de la formation, les employés doivent s'imprégner de ces politiques et directives.

Mme Charmaine Borg: Qu'est-ce qui n'a pas fonctionné?

M. Ian Shugart: Dans ces cas particuliers, les employés n'avaient pas suffisamment assimilé les réflexes à avoir. C'est ce qu'on appelle une culture d'entreprise, et nous sommes tenus de faciliter la protection des renseignements par l'entremise des logiciels, de l'équipement, des politiques et de la formation.

J'invite M. Parker à poursuivre.

M. Ron Parker (sous-ministre délégué, ministère des Ressources humaines et du Développement des compétences): Deux politiques particulières sont pertinentes dans ce cas: en premier lieu, les employés sont responsables de déclarer les incidents; en deuxième lieu, les données sensibles doivent être chiffrées avant d'être stockées sur un appareil portatif.

Mme Charmaine Borg: Pourquoi cet ensemble de données en particulier n'était-il pas chiffré?

M. Ron Parker: Comme l'a dit le sous-ministre, il semble que les employés n'aient pas chiffré les données comme ils auraient dû le faire.

Le président: Votre temps est écoulé. Vous avez pris un peu plus de temps pour répondre, et c'est très bien.

La parole est maintenant à Mme Leitch.

Allez-y.

Mme Kellie Leitch (Simcoe—Grey, PCC): Merci beaucoup d'avoir pris le temps de témoigner.

Comme vous l'avez dit, monsieur le sous-ministre, nous prenons tous la question au sérieux, tant les membres du gouvernement que les membres de l'opposition. Il s'agit également d'un enjeu très important pour les Canadiens, qui se préoccupent de la protection de leur vie privée et de la façon dont elle est assurée.

Vous avez dit que la ministre avait pris certaines mesures, notamment la mise à niveau du réseau à des fins sécuritaires et la prestation d'une formation obligatoire. Je crois que nous reconnaissons — du moins je reconnais — votre sensibilité envers cette question et la façon dont vous et vos collègues l'abordez.

J'aimerais poser quelques questions. Vous ou vos collègues pourrez répondre; je crois que cela nous conviendra, puisque mes collègues de l'opposition et nous visons le même objectif, soit comprendre ce qui s'est passé et traiter de la gravité de la question.

Quelles ont été les mesures immédiates prises par le ministère lorsque le disque dur a été perdu? Après avoir lu vos notes et suivi votre dialogue, je réalise qu'il y a eu un certain délai entre le moment ou la perte a été signalée et votre intervention.

Quelle a été votre réaction immédiate? Quelle formation est offerte au personnel en la matière? Vous avez dit qu'elle faisait partie de la culture. Bien sûr, nous devons tous prendre une part de responsabilité pour les gestes que nous posons; mais est-ce que cette question était abordée dans la formation? Quelles étaient les procédures en place? Les membres du personnel reconnaissent-ils maintenant la gravité de la situation?

M. Ian Shugart: Monsieur le président, je peux peut-être répondre à la dernière question de la députée, puis Ron et Al pourront répondre aux premières.

À mon avis, le personnel est maintenant bien informé. Je crois qu'au sein d'une organisation aussi vaste que la nôtre, on peut s'attendre à ce que certains employés soient mieux informés que d'autres quant à l'importance de la question. La formation obligatoire pour tous les employés vise à éliminer, autant que faire se peut, les écarts entre les employés, de sorte que personne ne puisse affirmer ne pas connaître la norme. Nous voulons sensibiliser tous les employés.

De façon générale, nous avons été heureux d'obtenir l'entière collaboration des employés, notamment pour l'évaluation des appareils de l'organisation. Nous voulions que les membres du personnel soient suffisamment préoccupés par la question pour faire tout ce qui était nécessaire pour respecter nos directives, sans toutefois leur faire peur. À en juger par leurs réactions lors des réunions et des séances d'information, je crois que nous avons réussi.

Je cède la parole à mes collègues.

● (1135)

M. Ron Parker: Pour ce qui est des actions immédiates, comme le sous-ministre adjoint l'a expliqué, l'incident a initialement été traité comme un cas où un bien est manquant — quelque chose qu'il faut trouver —, en croyant qu'il était sur les lieux, qu'il était toujours dans l'immeuble.

Lorsque cela est devenu moins probable, cela a mis en évidence que la probabilité de retrouver le disque dur était moindre. La Division de la sécurité ministérielle et les agents de sécurité régionaux ont été informés, ce qui est le protocole normalisé. Ils ont alors entrepris une série de recherches professionnelles pour retrouver le disque dur, et des entrevues se sont poursuivies tout au long du mois de décembre jusqu'au début janvier, lorsque la probabilité de retrouver le bien semblait être très faible. À ce moment, nous avons entrepris une enquête officielle pour laquelle on a eu recours à des enquêteurs professionnels. Au début du mois de janvier, nous avons pris des mesures pour commencer à informer les Canadiens.

Le président: C'est tout?

D'accord.

Mme Kellie Leitch: Comme ce qu'a dit le sous-ministre plus tôt, nous trouvons aussi que c'est totalement inacceptable. Il faut s'assurer de protéger les renseignements personnels des Canadiens.

Je pense que nous savons tous quel est le partage des responsabilités: la Chambre est chargée de l'aspect des politiques et la ministre, des mesures à prendre. Je sais que vous y participez et que vous avez reçu des directives pour vous assurer que ces choses sont mises en place.

Avec le ministère, nous avons aussi pris des mesures, et il a aussi un certain degré de responsabilité pour s'assurer que ces choses sont mises en oeuvre à l'avenir de façon à garantir un environnement sécuritaire.

Un des points qui a été soulevé — et nous en avons entendu parler et avons eu des discussions à ce sujet —, c'est l'intervention de la Commissaire à la protection de la vie privée et le délai accordé pour une intervention dans ce dossier, mais aussi la participation de la GRC en raison de la gravité de cette affaire.

Pourriez-vous nous dire à quel moment et par qui ont été prises les décisions de demander l'intervention de la Commissaire à la protection de la vie privée et de la GRC pour s'assurer que les Canadiens étaient protégés?

M. Ian Shugart: M. Parker a parlé de nos protocoles, et j'ai mentionné auparavant nos normes, notre approche, en ce qui a trait au Commissariat à la protection de la vie privée.

Dès que nous avons appris qu'il était probable que ces renseignements étaient perdus et qu'il était peu probable qu'ils soient retrouvés, nous savions, sans l'ombre d'un doute, que le Commissariat à la protection de la vie privée devait intervenir, et c'est à ce moment-là que nous avons pris cette décision.

C'est au cabinet de la ministre que la décision de faire appel à la GRC et de la saisir de cette affaire a été prise.

Au ministère, je dirais simplement que cela ne nous pose absolument pas problème. La décision a été prise en fonction de la gravité de la situation dans laquelle nous sommes. Bien entendu, il reviendra à la GRC de décider de quelle façon elle souhaite répondre à cette demande.

Nous travaillerons de manière appropriée avec le Commissariat à la protection de la vie privée dans le cadre de l'enquête qu'il a entreprise. Nous ferons de même pour toute mesure que la GRC décidera d'entreprendre et pour nos propres enquêtes internes. Nous voulons assurer la transparence, l'ouverture et la conformité de ces enquêtes et aussi garantir la pertinence de l'information de façon à ce que l'intégrité de toute enquête qui sera entreprise ne soit pas compromise.

● (1140)

Mme Kellie Leitch: Merci beaucoup.

Le président: Nous passons à Mme Charlton.

Allez-y

Mme Chris Charlton: Merci beaucoup, monsieur le président.

Messieurs, je vous remercie d'être venus témoigner au comité ce matin. Je sais que ce n'est probablement pas l'endroit où vous souhaitiez être le jour de la Saint-Valentin, mais je vous remercie de passer cette partie de la journée avec nous.

Permettez-moi de poser d'abord cette question, monsieur Shugart. Pouvez-vous dire au comité ce que vous entendez par « responsabilité ministérielle »?

M. Ian Shugart: Monsieur le président, les ministres doivent rendre des comptes au Parlement pour toutes les questions qui relèvent de leur compétence, en fin de compte, y compris les politiques du gouvernement et le comportement approprié des fonctionnaires de leur ministère. Par convention, et souvent en raison d'un instrument de délégation officiel, ces autorités sont déléguées aux fonctionnaires des ministères. Dans bien des cas, cela est prévu dans la réglementation prise en vertu des lois, et parfois dans les lois elles-mêmes.

Par convention, les ministres sont responsables de la politique et les fonctionnaires conseillent les ministres au sujet des politiques. Les fonctionnaires sont responsables de l'administration des ministères.

Mme Chris Charlton: Merci beaucoup, monsieur. Vous avez entendu le président rappeler à ma collègue que l'on ne devrait pas vous poser de questions au sujet des politiques aujourd'hui, et c'est pour cette raison que notre demande initiale était que la ministre comparaisse au comité.

Vous avez plutôt raison: vous devez répondre aux questions dans le contexte de l'administration de votre ministère. Dans ce contexte, permettez-moi d'essayer de vous poser des questions auxquelles vous pourrez répondre.

Pouvez-vous me dire à quel moment, selon l'interprétation de votre ministère, une atteinte est considérée comme « totalement inacceptable »? Ce sont les mots employés par votre ministre en réponse aux questions que nous avons soulevées lors de la période des questions: que cette atteinte est « totalement inacceptable ».

Le président: Vous pouvez indiquer ce que vous jugez comme totalement inacceptable, mais vous ne pouvez pas parler de ce que quelqu'un d'autre pourrait penser, manifestement.

Mme Chris Charlton: Non, mais comme ma collègue l'a souligné, le fait que cette atteinte était inacceptable est aussi indiqué dans les notes.

Monsieur le président, sérieusement, nous n'avons que sept minutes.

Le président: Je le sais. Ce que j'essaie de vous dire, c'est que nous voulons nous concentrer sur les trois questions dont nous sommes saisis. Si la question que vous lui posez consiste à savoir pourquoi il trouve que c'est totalement inacceptable, il a le droit de répondre, mais il ne peut pas parler de ce que quelqu'un d'autre aurait dit, ni de ce qu'il pense qu'on a voulu dire par là.

Sur ce, vous pouvez répondre à ces questions. Vous comprenez ce que je veux dire.

Mme Chris Charlton: Monsieur le président, sauf votre respect, cela découle de l'exposé que nous avons entendu. Le sous-ministre a dit que c'était inacceptable, alors permettez-moi de faire un suivi.

Le président: Je vous dis qu'il peut répondre à cela en fonction de son utilisation de ces mots.

Allez-y.

Mme Chris Charlton: Merci, monsieur le président.

Pouvez-vous s'il vous plaît...

Le président: Eh bien, laissez-le répondre.

Mme Chris Charlton: Pouvez-vous me dire, selon le point de vue du ministère, ce qui est considéré comme une « atteinte inacceptable »?

M. Ian Shugart: Monsieur le président, je dirais que tout incident où des renseignements personnels sont compromis n'est pas acceptable. Après avoir été informé d'une situation où, ne serait-ce que pour un seul Canadien, les renseignements personnels n'auraient pas été manipulés selon les règles de l'art ou auraient été compromis, je ne peux pas m'imaginer dire que c'est acceptable.

Mme Chris Charlton: Merci. Nous sommes certainement d'accord sur ce point.

Cependant, nous savons, d'après votre témoignage, qu'il y a eu 19 atteintes à la protection des données au sein de votre ministère, et ce, pour l'an dernier seulement. Nous savons qu'il n'y a aucune exigence pour le signalement des atteintes à la protection des données. Par conséquent, il y a de toute évidence un certain nombre d'atteintes qui n'entraient pas dans la même catégorie que celle-ci, parce que ce n'est que maintenant que votre ministère renforce ses politiques en matière de sécurité et de stockage des renseignements personnels, selon le témoignage que vous venez de nous donner.

Cela me surprend quelque peu. Dans nos bureaux locaux, lorsque nous avons des renseignements personnels sur des électeurs relativement à toutes sortes de questions liées à la santé ou des renseignements sur les passeports, nous avons mis en place des protocoles.

Ce n'est pas la première atteinte au sein du ministère, ni au sein du gouvernement. Or, ce n'est que maintenant que vous élaborez un nouveau protocole. Pouvez-vous nous expliquer pourquoi?

M. Ian Shugart: Monsieur le président, je ne crois pas avoir utilisé les mots « que maintenant ». J'ai expliqué ce que nous avons fait en réponse à cet incident. Selon ce que nous avons appris de cet incident, nous avons renforcé ces politiques, procédures et pratiques.

Respectueusement, je rejette toute description selon laquelle aucune politique n'était en place au préalable. Manifestement, il y en a; il y a des directives et elles étaient en place auparavant. Voici ce que nous avons fait: nous avons renforcé les protocoles et renforcé les règles et les dispositions du système relatives au matériel et aux logiciels de façon à mieux protéger les renseignements personnels des Canadiens.

● (1145)

Mme Chris Charlton: Permettez-moi de vous rappeler une autre chose que vous avez dite dans votre témoignage. Vous avez dit qu'on a demandé aux employés s'ils avaient « emprunté un disque dur ». Il me semble que si les employés ont la possibilité d'emprunter un disque dur contenant les renseignements personnels de plus d'un demi-million de Canadiens, ce n'est pas un protocole très strict.

Êtes-vous d'accord?

M. Ian Shugart: Monsieur le président, les questions que nous avons posées aux employés visaient à couvrir toutes les possibilités quant à ce qui a pu se produire. Parmi ces possibilités, il y avait la manipulation inappropriée du disque dur.

Nous n'avions aucunement l'intention de laisser entendre que nous trouverions ce comportement acceptable. En effet, les questions ne visaient pas à présumer de quoi que ce soit au sujet de ce qui s'était produit. Nous cherchions simplement à poser une série de questions exhaustives aux employés afin d'obtenir des renseignements sur ce qui s'était produit.

Dans cette situation, les priorités étaient de retrouver le bien et les informations qu'il contenait. C'était la raison d'être des questions. Cela ne sous-entend en aucun cas que nous considérerions un tel comportement comme acceptable.

Mme Chris Charlton: À l'ère de la technologie, si quelqu'un a accès à ces renseignements, il peut en faire un usage frauduleux en quelques secondes, par voie électronique.

Une des choses dont vous avez parlé, c'est que la Commissaire à la protection de la vie privée a été contactée une semaine après la découverte de l'atteinte concernant la clé USB. Quel est votre protocole concernant le temps que vous attendez pour savoir si elle réapparaîtra miraculeusement quelque part, avant de penser que vous devez aviser quelqu'un qu'une atteinte est survenue?

M. Ian Shugart: De toute évidence, nous ne comptons pas sur des miracles. Pour ce qui est de la recherche, nous avons fait preuve de diligence, et lorsque nous avons conclu que le matériel ne serait fort probablement pas retrouvé, vous vous souviendrez que j'ai indiqué que nous avons tout de même poursuivi des recherches exhaustives. C'est à ce moment-là que nous avons informé la Commissaire à la protection de la vie privée.

Mme Chris Charlton: Qui informez-vous en premier, la ministre ou la commissaire?

Le président: Votre temps est écoulé, mais je vous permets de terminer.

M. Ian Shugart: J'ai informé la ministre assez tôt que nous avions entrepris cette recherche, et nous l'avons tenue informée de la participation de la Commissaire à la protection de la vie privée, de toutes les étapes cruciales de notre enquête et de ce que nous apprenions pendant l'enquête.

Pourrais-je demander à mon collègue s'il souhaite ajouter quelque chose à ces faits?

Le président: Comme je l'ai indiqué, le temps est écoulé, mais allez-y et répondez à cette question. Ensuite, nous passerons au prochain intervenant.

M. Ron Parker: Pour ce qui est de la Commissaire à la protection de la vie privée, nous avons informé le Commissariat à la protection de la vie privée le 14 décembre, ce qui a été suivi d'une communication écrite le lundi suivant. Nous avons consulté le Commissariat à la protection de la vie privée tout au long du processus pour trouver la façon adéquate de gérer l'incident et d'informer les Canadiens.

Le président: Merci.

Nous passons à M. Mayes.

Allez-y. Vous avez sept minutes.

M. Colin Mayes (Okanagan—Shuswap, PCC): Merci, monsieur le président.

Merci aux représentants du ministère d'être ici aujourd'hui. Je vous remercie d'avoir déclaré dans votre exposé que la perte de ces renseignements n'est pas acceptable et que votre ministère le reconnaît. Nous sommes tout à fait d'accord sur ce point.

Un des éléments qui me pose problème, c'est que vous avez pris la décision d'informer la GRC que le ministère avait perdu ces données. Après avoir fait des recherches, avez-vous conclu que vous étiez passé d'une situation où un bien était égaré à celle d'un bien manquant puis, en fait, au vol possible d'un bien? Si oui, qui a pris la décision de faire appel à la GRC?

M. Ian Shugart: Nous n'avons pas formulé d'hypothèse — et nous ne le faisons toujours pas — sur ce qui s'est produit précisément. C'est pourquoi des enquêtes ont été entreprises, y compris notre propre enquête interne.

Nous pouvons affirmer — et le comité conviendra qu'il n'est pas possible de prouver un élément négatif — que nous n'avons trouvé aucune preuve de méfait et la surveillance que nous avons exercée depuis ce temps ne nous a donné aucune raison de croire que des activités malveillantes ont eu lieu, mais en soi, cela ne règle pas la question de la gravité de l'incident. Étant donné le nombre de personnes en cause, il a été décidé — ce qui n'est pas déraisonnable, à mon avis — que la GRC devrait être informée et qu'on devrait lui demander d'intervenir.

● (1150)

M. Colin Mayes: Merci.

Pour ce qui est de ce genre d'infractions à la sécurité et aux procédures par des employés, le ministère a-t-il une politique sur les conséquences associées à toute infraction aux procédures de sécurité du ministère?

M. Ian Shugart: Oui. Monsieur le président, les obligations des employés relatives à la manipulation des renseignements personnels sont établies dans le code d'éthique. Il y a un code d'éthique normalisé pour l'ensemble de la fonction publique, qui relève du Conseil du Trésor; ensuite, chaque ministère applique ce code fondamental en fonction de son propre mandat et de sa propre situation, puis y apporte des précisions.

Dans notre cas, comme je l'ai indiqué, la protection des renseignements personnels est si essentielle à notre mandat qu'elle est inscrite dans notre code. Les employés sont notamment tenus de respecter le code pour tous les aspects liés aux renseignements. Les infractions au code d'éthique sont étudiées au cas par cas, et toute infraction entraîne des mesures disciplinaires pouvant inclure la cessation d'emploi. En cas d'incident comportant des éléments criminels, des sanctions autres que les mesures disciplinaires de la fonction publique qui relèvent du ministère entreraient en jeu, selon le principe de l'application régulière de la loi, etc.

M. Colin Mayes: Le ministère a agi rapidement pour s'assurer de la protection du crédit et des renseignements des personnes dont les renseignements personnels étaient compromis. Pouvez-vous nous fournir une mise à jour? Y a-t-il eu des problèmes? Avez-vous eu des indications selon lesquelles quelqu'un aurait utilisé ces renseignements? Quel genre de commentaires recevez-vous de ceux qui ont des préoccupations? Avez-vous mis en place un système quelconque pour recevoir les appels et rassurer les gens dont les renseignements ont été compromis?

M. Ron Parker: La principale mesure que nous avons prise pour régler cette question, c'est le contrat que nous avons conclu avec Equifax.

Près de 50 000 anciens étudiants touchés se sont inscrits à ce service. À ce jour, nous n'avons aucune preuve qu'il y ait eu des fraudes ou d'autres activités illicites. Une ligne 1-800 spéciale a été créée pour les clients touchés. Nous n'avons reçu aucun appel indiquant qu'on avait constaté une fraude.

De plus, nous avons mis en place des annotations dans le Registre d'assurance sociale de façon à ce que chaque numéro d'assurance sociale soit accompagné d'une annotation spéciale indiquant que le client a possiblement été touché par l'incident. Si le centre du Registre national d'identité reçoit une demande pour le changement des renseignements liés à l'assurance sociale ou une demande de carte, il y aura un signalement spécial et on demandera au client de fournir les pièces d'identité appropriées et une pièce d'identité avec photo.

Nous avons étudié les activités liées au registre d'assurance sociale avant et après la perte des renseignements et il n'y a eu aucun changement pour ce qui est des tendances ou de la nature des demandes qui sont présentées.

● (1155)

M. Colin Mayes: Vous gérez beaucoup de renseignements. Avez-vous des chiffres sur le volume? C'est horrible et c'est un défi énorme, et surtout en raison de la communication aujourd'hui, ces défis... Nous nous y adaptons. Je siège au comité sur l'éthique et la protection des renseignements personnels. Nous menons actuellement une étude à ce sujet et nous comprenons certains des défis auxquels nous sommes confrontés par rapport à l'atteinte à la protection des renseignements personnels, pas seulement au sein du gouvernement, mais aussi dans la société. C'est assez difficile.

Au ministère, avez-vous un programme permanent pour l'examen des procédures et des renseignements — les pare-feux et ce genre de choses — pour vous tenir à jour?

Le président: Si vous pouviez faire court, nous en reparlerons peut-être un peu plus tard. Allez-y.

M. Ron Parker: Merci, monsieur le président.

Dans l'ensemble des principaux programmes que gère RHDCC, quelque 28 millions de clients se trouvent dans nos bases de données chaque année. Nous traitons environ 84 millions de transactions par année entre ces principaux groupes, dont le Programme canadien de prêts aux étudiants, le Programme canadien pour l'épargne-études, le Régime de pensions du Canada, la sécurité de la vieillesse et l'assurance-emploi. Nous traitons beaucoup de transactions et nous avons beaucoup de Canadiens comme clients. Pour ce qui est de leur...

Une voix: Passons.

M. Ron Parker: D'accord. Nous y reviendrons.

Le président: Vous y reviendrez? D'accord.

Souhaitiez-vous formuler un bref commentaire, monsieur Shugart? Non. Nous y reviendrons.

La parole est maintenant à M. Cuzner.

M. Rodger Cuzner (Cape Breton—Canso, Lib.): Merci beaucoup, monsieur le président, et je remercie aussi ce monsieur d'être venu aujourd'hui.

Je n'ai que sept minutes, alors je ferai de mon mieux pour poser toutes mes questions. Vous avez été très directs et je vous en sais gré. Si vous pouvez, continuez de l'être, et si je vous interromps, ce n'est pas par impolitesse, mais parce que je tiens vraiment à poser mes questions.

Mes questions vont d'abord porter sur les personnes qui ont été touchées, celles qui avaient des prêts. Pouvez-vous garantir que les seules personnes touchées ont été celles qui ont reçu des prêts entre 2000 et 2006? En êtes-vous certain?

M. Ron Parker: Nous avons examiné les données avec soin. Il y a environ 2 800 anciens étudiants qui n'ont pas reçu de prêts pendant cette période, mais plutôt en 2007 pour la plupart. Il y en a environ 2 600 en 2007, et après...

M. Rodger Cuzner: Je comprends. Nous les comptons à partir de 2007. Merci beaucoup.

Pour ce qui est des renseignements relatifs aux parents, détient-on des renseignements relatifs aux parents ou aux conjoints ainsi qu'aux étudiants?

M. Ron Parker: Non, on ne détient aucun renseignement relatif aux parents.

M. Rodger Cuzner: Vous estimez qu'on ne détient aucun renseignement relatif aux parents ou aux conjoints. Génial.

Savez-vous combien de Canadiens se sont dits préoccupés de la perte d'identité ou de renseignements?

M. Ron Parker: Nous avons répondu à 200 000 appels au total; 65 p. 100 d'entre eux provenaient de clients touchés. Avant que les lettres d'avis soient envoyées, environ la moitié des étudiants étaient touchés, et depuis que les lettres ont été reçues, les contacts ont été...

M. Rodger Cuzner: Si je puis vous donner un conseil, certains des étudiants qui ont téléphoné ont dit que les agents d'Equifax n'ont pas vraiment confiance en l'information qu'ils transmettent, alors je vous recommanderais de faire en sorte qu'on les informe ou qu'on leur donne continuellement les meilleurs renseignements possibles.

Un exemple dans le monde des affaires est celui de Sony International, qui a dû composer avec pareille atteinte à la sécurité il y a un certain nombre d'années. Pour les millions de personnes touchées, Sony a payé la note pour ce qui est des alertes, de la surveillance et de l'assurance. Sony a prévu des mécanismes d'alerte à la fraude, de surveillance de crédit et d'assurance de 1 million de dollars pour chaque personne. Si leur identité avait été volée, chacune d'entre elles aurait été assurée pour ce montant par Sony.

Disons que cela se passe de notre côté. La réponse du ministère se situerait quelque part entre l'inertie et le modèle de Sony. Selon vous, où s'est située votre réponse dans ce continuum?

● (1200)

M. Ron Parker: Nous estimons qu'il s'agit d'une réponse appropriée et énergique en deux volets dans le cadre du contrat avec Equifax. Le contrat sur mesure spécialisé que nous avons conclu permettra de cerner toute tentative d'accroître le crédit ou de changer les renseignements de solvabilité, et de concert avec la surveillance du Registre d'assurance sociale...

M. Rodger Cuzner: Je suis préoccupé lorsque je regarde le site Web de l'Agence de la consommation en matière financière du Canada et celui du Commissaire à la protection de la vie privée.

Ils disent sur le site Web que si un organisme a recueilli vos renseignements personnels et qu'ils vous avertissent que ceux-ci pourraient être utilisés par des usurpateurs d'identité parce qu'il y a eu atteinte à la sécurité des données, protégez-vous. Ils vous disent de prendre contact avec les services des fraudes des deux principales agences de vérification de la solvabilité, de leur demander de placer une alerte à la fraude dans vos dossiers, de demander des copies de votre dossier de crédit et de le refaire tous les six mois.

Vous avez utilisé Equifax. Pourquoi n'avez-vous pas aussi fait appel à TransUnion?

M. Ron Parker: Monsieur le président, nous envisageons de prendre des arrangements avec d'autres agences de vérification de la solvabilité et institutions financières.

M. Rodger Cuzner: Dans le contrat que nous avons signé avec Equifax, ces services sont offerts gratuitement dans huit provinces. Je crois comprendre qu'ils le sont. Offrez-vous un service spécial au-delà de ce qui est normalement offert gratuitement dans huit provinces? Pourriez-vous nous dire ce que vous offrez au-delà de cela?

M. Allen Sutherland (sous-ministre adjoint, Direction générale de l'apprentissage, ministère des Ressources humaines et du Développement des compétences): Je serais ravi de le faire, car cette question a créé beaucoup de confusion.

Certaines personnes ont confondu le service Perdre son portefeuille avec la trousse sur mesure Alerte crédit préparée pour le ministère par Equifax. Il y a des différences importantes entre les deux. Premièrement, le service Perdre son portefeuille n'est pas offert à la grandeur du pays, mais en plus, il est moins efficace que l'autre. Par exemple, il n'est disponible que pendant trois mois. Le service que nous avons acheté d'Equifax est pour six ans, comme c'est la norme dans l'industrie.

La deuxième chose est que le service Perdre son portefeuille n'offre pas aux clients un mécanisme de prévention ou d'atténuation de la fraude comme le fait le système Alerte crédit. Ce système avertit le fournisseur de crédit que l'identité de la personne a peut-être été...

M. Rodger Cuzner: Désolé de vous interrompre, mais Equifax nous a dit que ce service est, en fait, offert gratuitement à tous les consommateurs.

Le président: Monsieur Cuzner, vos sept minutes sont écoulées. Posez une question brève s'il vous plaît ou nous allons passer à la personne suivante.

M. Rodger Cuzner: Quel est le coût total du forfait d'Equifax pour couvrir les 600 000 personnes?

M. Ron Parker: Le contrat avec Equifax et sa valeur sont des renseignements commerciaux de nature confidentielle, sinon les concurrents seraient capables de le réduire au coût unitaire. Nous avons donc convenu de garder l'information confidentielle.

Le président: Votre temps est écoulé.

Nous passerons maintenant à M. Daniel avant de prendre une courte pause et d'entamer la deuxième ronde de questions.

● (1205)

M. Joe Daniel (Don Valley-Est, PCC): Merci, monsieur le président. Merci aux témoins d'être venus.

Encore une fois, je dois dire que la perte de données vous place manifestement en situation difficile, alors je peux compatir à la situation des gens dont les données ont été perdues.

Il est important de comprendre la source du problème, car j'estime qu'elle vous aidera à trouver la meilleure solution.

Ma question est la suivante: pourquoi a-t-on permis que ces renseignements soient copiés dans un dispositif externe à partir d'un serveur, et quelle était la politique ministérielle de l'époque en ce qui concerne les dispositifs portatifs comme celui-là?

M. Ron Parker: Selon la politique, les données auraient dû être encodées avant d'être copiées dans un appareil portatif, et il est clair qu'elles ne l'ont pas été. La politique existe. L'enquête déterminera pourquoi les données n'ont pas été encodées et tentera de trouver les causes.

M. Joe Daniel: Cette perte de données a-t-elle entraîné d'autres changements stratégiques importants sur la façon dont le ministère gère les renseignements canadiens? Si tel est le cas, comment ces changements feront-ils en sorte que pareille situation ne se reproduise pas?

M. Ron Parker: Les changements que nous avons mis en place sont cruciaux. Côté niveau de protection, ce sera le jour et la nuit.

Premièrement, en ce qui concerne le matériel d'information, toutes les clés USB que nous avons...

Le président: Allez-y, madame Borg.

Mme Charmaine Borg: Monsieur le président, vous m'avez gentiment rappelé pendant mon témoignage que je devais m'en tenir précisément aux trois points contenus dans la motion concernant cette atteinte à la sécurité des données en particulier, et sa question ne s'y rapportait pas. Si vous appliquez cette règle, je crois que vous devriez l'appliquer à tous les membres du comité

Merci.

Le président: Très bien. J'ai accepté cette question pour établir un rapprochement avec les mesures que vous avez prises après cette atteinte à la sécurité. Si nous faisons erreur, c'est une autre histoire, mais il y a certainement lieu de parler de certaines de ces solutions à long terme et des mesures que vous avez prises.

Mme Charmaine Borg: Alors, il y a lieu de parler de la situation en général? Je pense que si.

M. Joe Daniel: Non, cela se rapporte spécifiquement à la politique ministérielle. Voilà la question. Elle se rapporte directement à ce dont nous parlons.

Le président: Allez-y.

M. Ian Shugart: Je pense, monsieur le président, que nous avions compris que cette question portait sur les mesures que nous avons prises en réponse à ces incidents et que, si j'ai bien saisi, elle faisait partie de l'ordonnance.

Le président: C'est l'idée, mais répondez dans ce contexte. Si les membres trouvent toujours cela choquant, soulevez votre objection.

Allez-y.

M. Ron Parker: On n'autorisera l'utilisation que des clés USB approuvées, et le ministère fait l'acquisition d'un grand nombre de clés USB encodées. En conséquence, il n'est plus permis de brancher des disques durs portables dans le réseau, ni les dispositifs personnels qui utilisent une connection USB. Nous surveillons le réseau et y accédons régulièrement, et nous prenons des mesures pour veiller à ce qu'aucun de ces dispositifs ne soit branché, ce qui est une démarche importante pour empêcher que des données sortent du réseau, qui est encodé.

L'autre mesure importante est la mise en oeuvre de logiciels de protection contre la perte de données. Cela nous dira exactement quels renseignements de nature délicate se trouvent sur le réseau, à quel endroit ils se trouvent et comment ils sont stockés, et cela nous permettra de prendre les mesures qui s'imposent pour veiller à ce qu'ils soient sécuritaires.

Je le répète, le réseau est encodé. Cela nous permettra aussi de suivre le mouvement des données. Nous pouvons contrôler ou prévenir ce mouvement une fois que ce logiciel est installé. Il s'agit de mesures très importantes que nous prenons à la suite de cet incident.

M. Joe Daniel: Prenez-vous des mesures particulières pour limiter la quantité de données que l'on peut stocker à la fois sur une clé USB, ou quelque chose du genre?

M. Ron Parker: Nous ne nous sommes pas encore penchés sur cette question en particulier.

● (1210)

M. Joe Daniel: D'accord.

Quelles garanties pouvez-vous offrir à mes électeurs que ces données ne seront pas utilisées de manière frauduleuse à cause de cette erreur?

M. Ian Shugart: Monsieur le président, je ne crois pas que nous puissions jamais offrir de garanties. Nous pouvons toutefois vous assurer que, comme M. Parker l'a mentionné, nous suivons les choses de très très près, tant par le truchement de notre arrangement avec Equifax que par celui des annotations dans le Registre de l'assurance-sociale, pour repérer toute activité pouvant susciter des doutes. Ces doutes en eux seuls motiveraient la personne concernée et RHDCC à prendre les mesures qui s'imposent.

Encore une fois, nous sommes manifestement très heureux de ne voir aucun signe de méfait ou d'usage abusif d'un quelconque de ces renseignements par un tiers.

M. Joe Daniel: Pour mes collègues de l'autre côté, nous avons parlé tout à l'heure de faire appel à TransUnion et à Equifax, mais vous avez choisi de n'utiliser qu'Equifax. Pouvez-vous m'aider encore une fois à comprendre pourquoi vous n'avez fait appel qu'à une seule agence de vérification de la solvabilité?

M. Ron Parker: Je crains que la réponse ne soit très similaire. Nous envisageons la possibilité de faire appel à d'autres agences de vérification de la solvabilité et institutions financières pour obtenir des services supplémentaires. À ce stade, c'est tout ce que nous pouvons dire concernant notre position.

M. Joe Daniel: Mais la grande majorité des clients seront desservis par Equifax.

M. Ron Parker: Oui, en ce moment, le contrat est avec Equifax.

M. Joe Daniel: Merci beaucoup.

Le président: Merci.

Sur ce, nous avons terminé la première ronde de questions. Nous allons suspendre les travaux pendant cinq petites minutes et nous passerons ensuite à la deuxième ronde.

● (1210)

(Pause)

● (1215)

Le président: Je demanderais aux membres de regagner leur siège et aux fonctionnaires, aux sous-ministres et aux sous-ministres délégués de retourner à leurs tables pour que nous puissions commencer. Si vous pouviez retourner à votre table, ce serait bien. Nous aimerions faire une deuxième ronde complète, si possible.

Nous allons entamer notre deuxième ronde de questions. Je crois que nous allons commencer avec Mme Boutin-Sweet.

[*Français*]

Mme Marjolaine Boutin-Sweet (Hochelaga, NPD): Merci, monsieur le président.

Merci, messieurs.

Nous n'avons pas beaucoup parlé de la protection offerte aux gens que vous avez désignés sous le nom de « clients ». Pour ma part, je vais utiliser les mots « anciens étudiants ». Il y a même 250 employés, qu'on a souvent tendance à oublier.

La ministre a dit que vous aviez communiqué avec les personnes impliquées sur lesquelles vous aviez de l'information à jour. On parle ici d'un demi- million d'étudiants ou d'anciens étudiants, soit de gens très mobiles.

Quelle proportion de ce demi-million de personnes avez-vous été en mesure de joindre?

M. Allen Sutherland: Nous sommes entrés en contact avec 320 000 personnes environ.

● (1220)

Mme Marjolaine Boutin-Sweet: Autrement dit, 200 000 personnes ne savent toujours pas qu'elles pourraient avoir des problèmes. Si ces personnes ont été victimes d'un vol d'identité ou d'un problème quelconque, ça pourrait encore faire surface, surtout si ça s'est passé en décembre, par exemple, avant que toute cette situation ne soit divulguée dans les journaux.

M. Ron Parker: C'est pourquoi nous avons diffusé des annonces, affiché des documents sur notre site Web et fait des efforts sur le plan médiatique en vue d'entrer en contact avec les étudiants sur lesquels nous n'avions pas d'information à jour.

Mme Marjolaine Boutin-Sweet: Vous avez dit également qu'il y avait eu 300 000 appels. C'est donc dire que 200 000 personnes n'ont peut-être ni appelé ni vu ces annonces et qu'elles ne savent pas que leur protection personnelle pourrait être menacée.

M. Ron Parker: Il y a eu 200 000 appels jusqu'à maintenant. Comme l'a dit Al, nous avons envoyé 326 000 lettres. Parmi les gens à qui nous avons envoyé des lettres, il en reste probablement qui peuvent encore nous joindre.

Mme Marjolaine Boutin-Sweet: J'aimerais avoir un peu plus de détails sur Equifax. Comme l'a dit M. Sutherland, c'est compliqué. J'aimerais que vous nous disiez très clairement ce qui est offert aux gens. Premièrement, faut-il que les étudiants fassent une demande? Qu'est-ce qu'on leur offre? Qui paie quoi? De quelle sorte de services parle-t-on, ici? S'agit-il simplement d'une note au dossier de crédit ou offrez-vous une surveillance ou une vérification? J'aimerais que ce soit très clair, autant pour moi que pour tout le monde ici présent.

M. Ron Parker: Les étudiants doivent appeler au centre d'appels pour avoir accès au programme. C'est un processus à option d'adhésion afin de conserver des informations privées. C'est le seul moyen de faire cela de manière sécuritaire.

En fait de services, nous avons un forfait personnalisé pour nos clients. Il y a une annotation dans le dossier d'Equifax qui indique aux institutions financières qu'on a peut-être atteint à la vie privée de ces gens. Dans ce cas, l'institution financière va demander des preuves d'identité additionnelles aux clients qui demandent une augmentation de crédit ou une nouvelle carte de crédit, ou d'autres transactions de ce genre.

De plus, comme on l'a mentionné, il y a un centre d'appels spécialisé pour nos clients à Equifax. Ces services seront offerts pendant six ans. Après six ans, on devra réexaminer la situation de près.

Également, nous avons fait des annotations relativement aux numéros d'assurance sociale qui auraient pu être en cause. Pour toute demande de changement à cet égard, des preuves d'identité additionnelles seront demandées.

● (1225)

Mme Marjolaine Boutin-Sweet: Selon la terminologie, il s'agit d'une note au dossier de crédit, à proprement parler, et non pas d'une surveillance qui serait faite. Autrement dit, personne ne va aller vérifier pour s'assurer qu'un numéro d'assurance sociale n'a pas été choisi par quelqu'un quelque part pour faire des emprunts ou demander des cartes de crédit. En fait, aucune surveillance ne sera offerte par le gouvernement ou par Equifax.

M. Ron Parker: Pas exactement. En fait, les deux sont indépendants.

Les gens en cause sont des clients des institutions financières. Quand ils vont faire une demande pour obtenir du crédit additionnel ou une hypothèque, ou encore pour faire augmenter la limite de leur carte de crédit, l'institution va voir une note à leur dossier d'Equifax indiquant que ces gens pourraient avoir été impliqués dans un incident. Selon leur protocole, les institutions financières pourront alors demander des preuves d'identité additionnelles.

Mme Marjolaine Boutin-Sweet: Je n'ai pas eu de réponse à ma question qui demandait s'il y avait des coûts...

[*Traduction*]

Le président: Merci, madame Boutin-Sweet...

Mme Marjolaine Boutin-Sweet: J'ai déjà posé cette question.

Le président: ... votre temps est largement écoulé. Parfois vous n'obtenez pas la réponse que vous voulez ou vous n'aimez pas la façon dont elle est formulée, mais votre temps est écoulé. Si M. Parker souhaite donner d'autres précisions en cours de route, il peut le faire, mais nous allons maintenant donner la parole à M. McColeman.

M. Phil McColeman (Brant, PCC): Merci d'être venus aujourd'hui pour parler d'un incident très difficile et — le mot a peut-être été utilisé à outrance, mais je le répète — inadmissible.

Cela me rappelle le risque. M. Shugart a affirmé qu'il est impossible de donner des garanties absolues. Il y aura toujours des risques. Il y avait un certain niveau de risque avant que cet incident se produise, et peut-être qu'après le fait, il y en a un deuxième en raison des nouveaux protocoles qui ont été mis en place pour régler cette situation. Cela me rappelle les attentats du 11 septembre et l'incidence qu'ils ont eu sur notre sentiment de sécurité. Le monde a changé. Nous avons dû prendre beaucoup plus de mesures de sécurité.

Cela étant dit, j'aimerais connaître les protocoles qui étaient en place lorsque les dispositifs contenant des données personnelles importantes sont disparus. Suivait-on les protocoles de manutention et d'entreposage de cette information?

M. Ian Shugart: Mes collègues peuvent donner des précisions, mais sous réserve de ce que l'enquête nous révélera, il nous paraît évident que la politique n'a pas été suivie, compte tenu des exigences d'encodage et du fait que l'information transférée n'était pas encodée.

La politique et l'exigence étaient en place, mais tout porte à croire que la politique n'a pas été respectée.

M. Phil McColeman: Est-ce que cela comprend votre politique concernant l'entreposage et l'endroit où ils étaient entreposés? On nous a dit qu'ils se trouvaient dans une armoire verrouillée. Était-ce le bon protocole à suivre pour entreposer les disques durs sauvegardés?

M. Ron Parker: Les dispositifs doivent être entreposés dans une armoire verrouillée sécurisée. L'enquête se penchera sur ce qu'étaient les circonstances lorsque le dispositif, le disque dur en particulier, ne s'est pas retrouvé dans une armoire verrouillée.

À un moment donné, nous savions qu'il s'y trouvait, n'est-ce pas? Les preuves portent à croire qu'il se trouvait dans l'armoire. Ce que l'on sait, c'est qu'on ne le trouve plus, et nous cherchons à comprendre comment cela a pu se produire.

● (1230)

M. Phil McColeman: Vous avez mentionné dans vos remarques liminaires, et ce point a été soulevé dans nos questions, que les sanctions imposées pour manquement au protocole peuvent aller jusqu'au congédiement.

Quelles mesures prenez-vous?

M. Ian Shugart: Monsieur le président, je dois d'abord préciser que nous ne connaissons pas les résultats de l'enquête, alors nous ne connaissons ni les circonstances exactes ni l'identité des personnes impliquées. En conséquence, je ne pourrais qu'avancer des hypothèses. M. McColeman comprendra que je ne le ferai pas.

Je peux cependant dire que l'on tiendrait compte d'un certain nombre de facteurs en pareilles situations pour déterminer les mesures disciplinaires qu'il convient d'imposer, par exemple celle de savoir si l'employé concerné était bien conscient de la situation. On s'attendrait, par exemple, à ce que le gestionnaire ait une plus grande responsabilité dans l'affaire qu'un employé, et on s'attendrait à ce qu'un employé qui manipule constamment ces données suive mieux le protocole qu'un autre qui n'en a pas l'habitude. C'est ce qu'on entend par « être bien conscient » de la situation.

La motivation — l'intention de la personne — est clairement un facteur à prendre en compte pour imposer des mesures disciplinaires. Encore une fois, je n'avancerai pas d'hypothèses dans ce cas, mais l'intention est manifestement un facteur. La gravité de la situation est un facteur, de même que la mesure dans laquelle une personne regrette son geste et la volonté de respecter les protocoles. Nous tiendrons compte de tous ces facteurs pour décider de chaque cas, en fonction de ce que nous savons.

Bien entendu, avant de prendre des mesures disciplinaires, il faut bien connaître la situation. Nous prendrons tous ces facteurs en compte pour décider des mesures qu'il convient d'imposer.

M. Phil McColeman: Je vous sais gré d'indiquer clairement dans votre présentation du processus le fait qu'il tient compte d'un vaste éventail de circonstances, ainsi que d'influences culturelles, j'imagine.

Je pense que nous, les députés des deux côtés de l'échiquier politique, reconnaissons tous que la situation est grave. Il a été mentionné, par le ministre, je pense, qu'en raison de la gravité de la situation, les conséquences qu'entraînera à l'avenir le non-respect des nouveaux protocoles et des nouvelles procédures établis seront plus dures, si je peux m'exprimer ainsi.

M. Ian Shugart: Encore une fois, monsieur le président, je ne tiens pas à me perdre trop en conjectures, mais j'estime pouvoir dire qu'à la suite de l'enrichissement de notre culture, de notre formation et de notre sensibilisation à ces enjeux, on devrait pouvoir s'attendre à ce qu'à l'avenir, une norme plus élevée soit respectée.

Comme je l'ai indiqué auparavant, le code d'éthique décrit l'éventail de mesures disciplinaires qui peuvent être prises ainsi que l'obligation de protéger les renseignements personnels. Dans la mesure où nous développons la sensibilisation culturelle ainsi que la rigueur et l'étendue de la formation, etc., nous serons en mesure d'accroître la sensibilisation et l'engagement des employées, en particulier en ce qui concerne cet enjeu. Je dois dire bien entendu que nos fonctionnaires doivent suivre des cours de formation obligatoires dans de nombreux domaines, ce qui est approprié. Comme notre DPI ne le sait que trop bien et comme nous le savons tous en tant que gestionnaires, le domaine de la sécurité des technologies de l'information et de la gestion de l'information devient lui-même de plus en plus vaste, compliqué et inextricable et, pour atteindre l'état de culture auquel j'ai fait allusion, nous devons faire mieux en matière de sensibilisation et d'engagement des employés.

Dans ce contexte, je pense que les employés devraient s'attendre à ce que nous menions ce projet d'une manière stricte.

● (1235)

Le président: Merci, monsieur Shugart.

Nous allons maintenant passer à M. Cleary qui dispose de sept minutes.

M. Ryan Cleary (St. John's-Sud—Mount Pearl, NPD): Merci, monsieur le président.

Monsieur Shugart, j'ai passé en revue vos notes d'allocution et la date des deux incidents, et la première question que je souhaite vous poser concerne ces dates.

Dans le cas du premier incident qui a eu lieu le 5 novembre, un disque dur renfermant des renseignements sur 583 000 Canadiens, des renseignements sur des prêts aux étudiants, est disparu. Cette disparition a été signalée à la commissaire à la protection de la vie privée le 14 décembre, soit plus de cinq semaines après l'incident. Dans le deuxième cas, une clé USB a disparu le 16 novembre, et la commissaire à la protection de la vie privée en a été avertie six jours plus tard.

Pourquoi avez-vous mis cinq semaines dans le premier cas — le cas que je décrirais comme le plus grave et celui ayant des répercussions sur un nombre plus élevé de Canadiens — et six jours dans le deuxième cas?

M. Ron Parker: Selon moi, c'est parce qu'au début — du 5 novembre à la fin du mois environ —, nous cherchions un bien manquant. Nous ne saisissions pas bien ce qu'il contenait. Le 6 décembre, nous avons compris clairement l'importance des renseignements enregistrés sur celui-ci. À partir de ce moment-là, nous avons commencé à prendre rapidement des mesures. Les recherches se sont intensifiées et, comme je l'ai mentionné, la commissaire à la protection de la vie privée a été informée de l'incident le 14 décembre.

M. Ryan Cleary: Monsieur Parker, je vais vous interrompre ici. Je dois vous poser la question suivante.

Vous avez utilisé le mot « rapide » pour décrire vos actions. Vous avez dit que vous aviez agi rapidement. Cependant, le disque dur a disparu le 5 novembre, et aucune enquête officieuse n'a été lancée avant la première semaine de janvier. Comment pouvez-vous qualifier votre intervention de « rapide »?

M. Ron Parker: Lorsqu'on recherche un disque dur, le protocole à observer en cas d'incidents de sécurité exige l'intervention des services de sécurité ministériels. Cela a eu lieu le 28 novembre, après avoir avisé la direction du ministère. C'est à ce moment-là que le processus s'enclenche, que les échelons supérieurs sont informés de l'incident et que, par conséquent, nous avons pris conscience du problème.

Jusqu'à cette date, les employés cherchaient un disque dur. En ce qui concerne la rapidité de notre réaction, peu de temps s'est écoulé entre le 6 décembre, date à laquelle nous avons compris clairement que nous avions perdu 583 000 dossiers d'étudiants et les renseignements de 250 employés, et le moment où la commissaire à la protection de la vie privée en a été informée. Nous avons intensifié la recherche et, une fois que cela a été fait et que nous sommes parvenus à la conclusion qu'il était peu probable que nous le retrouvions, nous avons avisé la commissaire à la protection de la vie privée

M. Ryan Cleary: Monsieur Parker, je suis désolé de vous interrompre, mais je tiens à vous poser rapidement quelques questions supplémentaires.

Je sais que la ministre et les représentants officiels du ministère qui sont présents aujourd'hui ont qualifié d'inacceptable cette atteinte potentielle à la sécurité mais, en ce qui concerne la réaction du ministère relativement à la disparition du disque dur et de la clé USB ainsi que les délais que cette réaction a entraînés, diriez-vous qu'ils sont également inacceptables

M. Ian Shugart: Non, et je ne veux en aucun cas qu'on se méprenne sur mes paroles et qu'on pense que je suis en train de dire que ce qui s'est produit est acceptable. Ce n'est pas le cas mais, compte tenu des renseignements dont nous disposions et du moment où ils nous ont été communiqués, nous croyons avoir agi d'une manière appropriée et conforme à nos protocoles concernant la commissaire à la vie privée.

Nous cherchions continuellement les biens. Aussitôt que nous avons pris conscience de leur contenu, nous avons immédiatement entamé le processus visant à informer les gens et à mettre en oeuvre, pendant toute cette période, les mesures supplémentaires — le matériel, les logiciels, etc. — nécessaires pour prévenir de tels événements à l'avenir. À ces trois égards, nous croyons avoir agi de manière appropriée, compte tenu de la gravité de la situation, gravité que nous ne remettons nullement en question.

● (1240)

M. Ryan Cleary: J'ai également deux requêtes à vous faire. Le comité pourrait-il recevoir une copie papier de vos nouvelles politiques et de vos nouvelles procédures en matière de manipulation des données personnelles — vous ne voudrez probablement pas nous la présenter sur une clé USB ou sur un autre support de ce genre?

De plus, êtes-vous prêt à remettre au comité une copie du rapport qui traite de la façon dont vous avez enquêté sur ces deux incidents?

M. Ian Shugart: Monsieur le président, en ce qui concerne la première demande, je vais m'efforcer de fournir au comité tous les renseignements qu'il désire.

En ce qui concerne la deuxième demande, je vais vous faire parvenir tous les renseignements que je peux vous fournir sans enfreindre les lois canadiennes.

M. Ryan Cleary: À quel moment…

Le président: Monsieur Shugart…

M. Ryan Cleary: J'ai une brève question à vous poser.

Le président: D'accord, mais avant que nous passions à cette question, nous devrions probablement clarifier ce que vous demandez.

En ce qui concerne la première des deux requêtes, vous dites qu'il ne tient qu'au comité de décider des renseignements qui seront fournis. En ce qui concerne la deuxième requête, vous fournirez les renseignements. Ai-je bien compris?

M. Ian Shugart: Je suis désolé, monsieur le président. J'ai un peu de mal à comprendre ces réparties.

Le président: D'accord. Monsieur Cleary, vous avez demandé deux choses...

M. Ryan Cleary: Oui, j'ai demandé qu'une copie des nouvelles politiques et des nouvelles procédures en matière de manipulation des données personnelles soit présentée au comité…

Le président: Monsieur Shugart, vous avez répondu....?

M. Ian Shugart: J'ai dit que je fournirais au comité tous les renseignements qu'il demanderait.

En ce qui concerne la deuxième requête — le rapport d'enquête, pour être précis —, je m'attends à ce que certaines parties du rapport traitent de certaines personnes et qu'en raison des restrictions juridiques qui s'appliquent, je ne sois peut-être pas en mesure de vous les communiquer. Toutefois, je serai aussi communicatif que je le peux.

Le président: Voici ce que nous ferons. Si vous souhaitez proposer ces deux éléments précis sous forme de motion, le comité s'en occupera après votre départ et prendra une décision à cet égard. Toutefois, nous n'interromprons pas le déroulement des témoignages.

Souhaitez-vous proposer cela sous forme de motion?

M. Ryan Cleary: D'accord

Le président: D'accord. Alors, nous nous en occuperons après votre départ mais, en attendant, nous continuerons d'entendre vos questions.

Nous avions effectivement stoppé l'horloge. Par conséquent, allez-y.

M. Ryan Cleary: Merci, monsieur le président.

Pour m'assurer que j'ai bien compris la situation concernant la disparition du disque dur et de la clé USB, j'aimerais savoir si les deux biens ont disparu du même immeuble de Gatineau.

M. Ian Shugart: Non.

M. Ryan Cleary: Il s'agissait d'immeubles différents.

M. Ian Shugart: Oui.

M. Ryan Cleary: À quel moment avez-vous appelé la GRC afin qu'elle enquête?

M. Ron Parker: Avez-vous la date?

M. Ryan Cleary: Je vais passer à une autre question, et vous pourrez me donner votre réponse dans une minute.

Dans votre déclaration préliminaire, monsieur Shugart, vous avez signalé, entre autres, la façon dont les personnes seraient protégées pendant six ans contre les atteintes à la vie privée potentielles. Puis, au cours d'une autre intervention, M. Daniel, je crois, vous a demandé s'il était possible de garantir à quelqu'un que ses renseignements personnels ne seraient jamais utilisés malicieusement, et vous avez répondu qu'il était impossible d'offrir ce genre de garantie. Ma question est la suivante: que se passera-t-il après les six années que vous avez signalées? Qu'arrivera-t-il après cela?

Selon moi, il se peut que les 583 000 Canadiens du premier incident ainsi que les 5 000 du deuxième passent le restant de leurs jours à regarder par-dessus leur épaule, alors que se passera-t-il après six ans?

M. Ian Shugart: Nous n'excluons pas, monsieur le président, la possibilité de prolonger cette période. Nous allons surveiller la situation, et nous évaluerons à ce moment-là ce qui est advenu pendant cette période. Toutefois, selon l'évaluation des risques qui aura été effectuée à ce moment-là, nous n'excluons pas non plus la possibilité qu'elle ne soit pas prolongée.

Le président: Le temps qui vous était imparti est écoulé, monsieur Cleary. Merci beaucoup. En ce qui concerne votre intervention, nous ne l'avons pas interrompu pour discuter des motions.

Nous allons maintenant passer à M. Butt. Mais avant de le faire, vous pouvez prendre la parole, si vous avez trouvé la réponse à sa question précédente.

● (1245)

M. Ron Parker: Le bureau du ministre a avisé la GRC le 7 janvier.

Une voix: Cela s'applique-t-il aux deux cas?

M. Ron Parker: Non, c'est seulement dans l'un d'eux.

Le président: Fort bien. Est-ce clair?

Alors, nous allons maintenant passer à M. Butt.

Allez-y.

M. Brad Butt (Mississauga—Streetsville, PCC): Merci, monsieur le président.

Messieurs, je vous remercie tous d'être venus aujourd'hui. J'ai beaucoup apprécié votre franchise dans cette affaire, votre manière candide de répondre aux questions et la façon très saine dont vous abordez ce problème qui, nous en convenons tous, est inacceptable. Toutes les personnes présentes dans la salle croient que ces deux incidents étaient complètement inacceptables.

Je reconnais la valeur de l'approche que le ministère a adoptée pour gérer cette situation. Mais je fais partie des gens qui croient qu'il faut également transcender un incident ou des incidents comme ceux-ci et nous demander ce que nous allons faire pour nous assurer qu'ils ne se répètent pas.

Qu'allons-nous faire pour améliorer nos mesures de protection, nos processus et nos procédures? Voilà le genre de questions que je vais vous poser. Que faisons-nous à partir de maintenant — comment pouvons-nous éliminer complètement ces incidents, étant donné que nous soutenons viser cet objectif?

Je veux vous céder la parole rapidement afin que vous puissiez formuler des observations et réitérer les directives que la ministre vous a données. Je crois comprendre qu'elles consistent à examiner la façon dont les employés manipulent les données des Canadiens, à combler toutes les failles qui ont permis que de tels incidents se produisent, à actualiser les pratiques en matière de sécurité des réseaux afin d'interdire l'utilisation de disques durs externes et à faire suivre à tous les employés un plus grand nombre de cours de formation obligatoires portant sur la façon appropriée de manipuler des renseignements de nature personnelle ou délicate et sur les nouvelles politiques de sécurité.

Monsieur Shugart, est-ce les directives que vous recevez de la ministre, en ce qui concerne ce que vous devez faire à partir de maintenant?

M. Ian Shugart: Oui, en effet.

Je mentionne également que nous sommes prêts à écouter tous les conseils que le personnel du Commissariat à la protection de la vie privée pourrait vouloir nous donner ainsi que les mesures qu'il pourrait nous recommander de prendre. De même, nous avons consulté des experts externes de l'industrie. Nous sommes prêts à suivre les conseils et à mettre en oeuvre les pratiques exemplaires de qui que ce soit qui peut nous aider à respecter la norme que nous cherchons à instaurer. Mais, oui, ce sont les directives que nous avons reçues.

Permettez-moi de vous indiquer deux domaines particuliers. Si j'ai bien compris — et mon collègue, le dirigeant principal de l'information, me corrigera si je me fourvoie —, le logiciel de protection contre la perte de données que nous emploierons sera déployé partout dans notre réseau, ce qui nous permettra de surveiller tous les transferts de données et de déterminer ceux qui sont inappropriés. Cette fonctionnalité est intégrée dans le logiciel. Le système a été conçu de manière à ce que les gens qui surveillent ces activités sachent que, quand un témoin s'allume et clignote, cela indique que des données ont été transférées d'une façon inappropriée et que le protocole ou la norme n'a pas été respecté. Nous serons ensuite en mesure de demander aux gens qui travaillent dans un secteur très précis la raison pour laquelle les données ont été transférées de cette façon.

Il s'agit là d'une solution technologique, mais nous cherchons avant tout à prévenir en premier lieu tout transfert ou manipulation de données inapproprié. La valeur même de notre institution est fondée sur la dignité humaine — c'est la raison pour laquelle nous protégeons les renseignements des particuliers — et sur un souci à l'égard des êtres humains — c'est la raison pour laquelle nos programmes sont tels qu'ils sont.

L'envers du décor, c'est que des êtres humains font tourner le système et qu'aucun système ne peut être absolument infaillible. Toutefois, en ce qui concerne la culture humaine, nous souhaitons que notre organisation excelle dans tout ce qu'elle fait, que ses employés sachent le rôle qu'ils jouent dans le contexte global et que ces derniers manipulent les renseignements des Canadiens prudemment et conformément aux règles.

Voilà ce que nous recherchons et la direction que nous suivons.

● (1250)

M. Brad Butt: Souhaitiez-vous ajouter quelque chose, monsieur Parker? Allez-y.

M. Ron Parker: Permettez-moi de reprendre l'un des premiers arguments que vous avez fait valoir en ce qui concerne l'examen des pratiques actuelles.

Avec l'aide de ses employés, chaque sous-ministre adjoint examine en ce moment les pratiques en vigueur dans son secteur, au chapitre du transfert et du stockage des données. Je crois que les employés prennent ces incidents aussi au sérieux que nous, et nous examinons jusque dans ses moindres détails la façon exacte dont les renseignements sont stockés et transférés d'une direction générale du ministère à l'autre.

Ce processus est très intensif. Nous rencontrons chaque unité du ministère et nous examinons ce qu'elle fait pour vérifier ses données ou ses inventaires ainsi que la façon dont elle stocke ces renseignements.

M. Brad Butt: Pourriez-vous nous fournir des précisions supplémentaires sur les mesures qui seront prises pour accroître la sévérité des conséquences que les employés devront subir à l'avenir, s'ils ne respectent pas les nouvelles politiques, mesures sur lesquelles la ministre a formulé des observations? Quels sont quelques-uns des scénarios qui risquent de prendre place, si ce genre d'atteinte au protocole se répète dans les mois ou les années à venir?

Je présume qu'une partie de votre plan consistera à faire suivre une formation intensive à tous les employés de RHDCC et à leur rappeler la teneur des règles et des protocoles à respecter. Toutefois, il se peut que vous mettiez de nouveau au jour une situation dans laquelle la protection de la vie privée a été compromise. Nous espérons tous que ce ne sera pas le cas, mais si cela se produit, quelles sont certaines des conséquences qui risquent d'en découler?

M. Ian Shugart: Monsieur le président, M. Butt sait que je n'émettrai pas d'hypothèse, mais l'une des conséquences pourrait être, à la limite, le licenciement; c'est clairement indiqué dans la politique et dans le code d'éthique à l'intention des employés. Il s'agit évidemment d'une mesure d'une extrême sévérité qui doit être justifiée en concomitance d'un comportement grave.

Par ailleurs, s'il y a eu méfait de la part de l'employé — et malheureusement, il nous est déjà arrivé de voir, dans la fonction publique, des comportements criminels —, dans cette situation, la loi sera appliquée dans toute sa rigueur.

Le président: Merci. Vous pouvez faire un dernier commentaire, après quoi nous donnerons la parole à M. Cuzner.

M. Ian Shugart: Je dirais que dans l'ensemble du spectre, pour les personnes qui sont visées par le système de rémunération conditionnelle, cet élément serait utilisé. Le comportement sur ce plan pourrait avoir une incidence sur les décisions relatives aux promotions et à l'avancement, et certaines mesures, comme la suspension, peuvent faire partie de cet arsenal de moyens disciplinaires.

Le président: C'est au tour de M. Cuzner, pour sept minutes.

M. Rodger Cuzner: Merci.

Je tiens simplement à répéter ce que j'ai dit lors de ma dernière question au sujet d'Equifax; si vous pouviez faire preuve de vigilance et vous assurer de tenir Equifax au courant, je sais que les personnes concernées vous en seraient reconnaissantes.

En ce qui concerne le recours à TransUnion, vous avez indiqué que vous envisagiez cette possibilité. C'est ce que recommandent la commissaire fédérale à la protection de la vie privée et l'Agence de la consommation en matière financière du Canada. Sachez que je vous recommande fortement de vous assurer de cette protection, pour au moins... Nous tentons actuellement d'apaiser les craintes des 600 000 personnes qui sont touchées.

Monsieur Shugart, vous avez indiqué dans votre exposé que 250 employés ont été touchés. A-t-on offert à ces employés la même protection que celle offerte aux 600 000 personnes?

● (1255)

M. Ron Parker: Oui. Nous avons communiqué officiellement avec les employés par lettre et leur avons offert les mêmes services.

M. Rodger Cuzner: Merci beaucoup.

J'ai donné l'exemple de la société Sony, qui a pris une police d'assurance pour les personnes touchées par l'atteinte à la sécurité. À la question de savoir si vous avez une assurance, je pense que la réponse est que le gouvernement du Canada est son propre assureur. En l'occurrence, si quelqu'un se fait voler ses renseignements personnels et est aux prises avec des pertes financières, le gouvernement sera-t-il disposé à assumer le coût de ces pertes, s'il peut être prouvé qu'il y a eu atteinte à la sécurité ou que ces pertes découlent de cette atteinte? En sommes-nous là?

Le président: Encore une fois, vous êtes libre de répondre ou non à cette question. Il est clair que les mesures que prendra le gouvernement ne sont pas de votre ressort, et que la question est hypothétique. En fait, c'est...

Si vous avez un commentaire, allez-y. Je veux seulement vous prévenir.

M. Rodger Cuzner: Puis-je demander si le ministère va le faire, monsieur le président?

M. Ian Shugart: J'allais dire, monsieur le président, que je ne veux pas être évasif, mais je dois considérer cela comme hypothétique. Je ne me sentirais pas à l'aise de m'aventurer sur ce terrain à ce moment-ci.

Dans votre question, vous avez utilisé le conditionnel. Permettez-moi simplement de dire que notre plan d'action comprend une surveillance très étroite de notre part et par l'entremise du service fourni par Equifax, et que nous allons suivre la situation de très près.

M. Rodger Cuzner: Donc, le ministère ne participerait pas au processus.

M. Ian Shugart: Je ne suis pas en mesure d'émettre d'hypothèses relativement à ce que le gouvernement ferait ou ne ferait pas dans une situation...

M. Rodger Cuzner: Vous ne prépareriez pas de plan d'urgence en ce sens?

M. Ian Shugart: Eh bien, les circonstances sont elles-mêmes hypothétiques, et je ne suis pas en mesure de faire de commentaires à ce chapitre. Je ne veux tout simplement pas m'aventurer dans le domaine des hypothèses à ce stade-ci.

M. Rodger Cuzner: Monsieur Sutherland, nous sommes en contact avec Equifax depuis la dernière séance. Un membre très haut placé de la compagnie nous a assurés que les étudiants obtiennent exactement la même chose que les autres, c'est-à-dire des services offerts gratuitement dans huit provinces sur dix.

Faites-moi deux colonnes et expliquez-moi ce qui distingue les deux types de protection, soit la protection gratuite et la protection spéciale que vous avez.

M. Allen Sutherland: Mes renseignements proviennent aussi d'Equifax. C'est peut-être une chose que vous devrez examiner avec eux. Nous avons eu des discussions très franches, avec les hauts dirigeants également. Le service pour perte de portefeuille n'est pas offert à l'échelle nationale. Il n'est pas offert...

M. Rodger Cuzner: Je l'ai déjà indiqué — il est offert dans huit provinces sur dix —, mais il s'étend sur six ans.

M. Allen Sutherland: D'après ce que j'ai compris et ce qu'ils m'ont dit, il dure trois mois.

M. Rodger Cuzner: C'est six ans, mais ce n'est pas grave.

Le président: Poursuivez.

M. Rodger Cuzner: Quelles sont les autres différences?

M. Allen Sutherland: Le service pour perte de portefeuille est différent de l'alerte crédit, laquelle exige que le fournisseur de crédit pose des questions additionnelles nécessitant un processus d'identification amélioré. C'est différent du service pour perte de portefeuille, qui n'a pas les mêmes exigences et obligations.

M. Rodger Cuzner: Je suis sûr qu'on ne demande qu'une pièce d'identité supplémentaire pour la perte du portefeuille.

M. Allen Sutherland: D'après Equifax, les exigences sont supérieures. De plus, il y a les services personnalisés que nous obtenons des services à la clientèle; ils prennent le temps d'expliquer comment fonctionnent le service et les options, y compris la mise en place du service et les améliorations possibles. C'est une trousse de services que nous avons acquise.

Nous avons posé la question à Equifax à quelques reprises, car nous avons entendu les commentaires que vous avez entendus vous aussi, et on nous a assuré que l'ensemble des services que nous offrons n'est pas négligeable. Il y a un coût qui y est rattaché, et ce n'est pas la même chose que le service pour perte de portefeuille.

● (1300)

M. Rodger Cuzner: Je dirais que le coût...

Me reste-t-il quelques minutes, monsieur le président?

Le président: Il vous reste environ 30 secondes.

M. Rodger Cuzner: Pourriez-vous nous en parler plus en détail? Je pense que la trousse comprend les renseignements additionnels, mais je ne vois aucune protection supplémentaire pour les gens. Je ne suis pas certain que c'est ce qui se passe. Je pense que des coûts sont rattachés à l'interaction additionnelle avec le client sur laquelle nous pourrions mettre l'accent et que nous pourrions peut-être tenter d'améliorer. Pourriez-vous nous fournir des données comparatives sur les services?

Le président: Merci, monsieur Cuzner.

Je pense que si vous voulez voir la comparaison entre les deux, vous pourriez en faire une motion. Nous en avons une qui traite de la communication d'autres renseignements et nous pouvons nous en occuper après le départ de ces messieurs. Voulez-vous en faire une motion pour que nous en discutions, monsieur Cuzner?

M. Rodger Cuzner: Certainement.

Le président: Je vois que Mme Leitch souhaitait poser des questions, mais il ne nous reste malheureusement plus de temps, et nous avons une motion à traiter.

Messieurs, je tiens à vous remercier d'être venus et de nous avoir fourni des renseignements clairs et francs. Vous pouvez partir, mais nous voulons encore discuter des motions avant que je lève la séance.

Merci beaucoup.

Je propose que nous discutions des motions au début de la prochaine réunion. De plus, si les membres du comité sont d'accord, je reporterais les travaux du comité que nous devions examiner aujourd'hui à la fin de la prochaine séance. Nous pourrons en discuter à ce moment-là, si cela vous convient.

La séance est levée.