Les travaux parlementaires

Journal des débats

Commission permanente de l'administration publique

Le mercredi 3 novembre 2004 • Vol. 38 N° 13

Audition de la sous-ministre du Revenu et du président-directeur général de la Société de l'assurance automobile du Québec la gestion de la sécurité informatique

Table des matières

Autres intervenants

Mme Rita Dionne-Marsolais, présidente
M. Henri-François Gautrin
M. Raymond Bernier
M. Guy Lelièvre
Mme Solange Charest
M. Serge Deslières
*** M. Pierre Boisvert, ministère du Revenu**
*** M. Michel Leblanc, idem**
*** M. Michel Léveillé, Société de l'assurance automobile du Québec**
*** M. Claude Gélinas, idem**
*** M. Mario Trudel, idem**
*** Témoins interrogés par les membres de la commission**

(Quinze heures trente-neuf minutes)

La Présidente (Mme Dionne-Marsolais): Comme le temps nous est compté, si vous voulez bien, chers collègues, je vais donc constater ce quorum et vous aviser que notre commission est réunie pour entendre le sous-ministre... la sous-ministre du ministère du Revenu et le président-directeur général de la Société de l'assurance automobile du Québec concernant la gestion de la sécurité informatique.

Alors, Mme la secrétaire, est-ce que nous avons des remplacements?

La Secrétaire: Oui, Mme la Présidente. Alors, Mme Thériault (Anjou) remplace M. Paquet (Laval-des-Rapides); et il y a deux membres temporaires: M. Lelièvre (Gaspé), le porte-parole en matière de revenu, et M. Deslières (Beauharnois), le porte-parole en matière de transports.

n *(15 h 40)* n

La Présidente (Mme Dionne-Marsolais): C'est très bien. Alors, je veux donc vous souhaiter, Mme la sous-ministre et tous vos collaborateurs, dont je reconnais quelques-uns, bienvenue. Souhaiter aussi la bienvenue à l'équipe du Vérificateur général, avec laquelle on a travaillé ce matin pour essayer d'accélérer les discussions d'aujourd'hui.

Et, avant de passer la parole au Vérificateur général, je voudrais vous dire que nous avons fait une très bonne revue du rapport du Vérificateur général, et j'espère qu'on aura une bonne discussion pour rassurer les citoyens quant à la qualité de la gestion informatique dans l'ensemble des ministères. Alors, sans plus tarder, M. le Vérificateur général, je vous passe la parole.

Exposé du Vérificateur général du Québec, M. Renaud Lachance

M. Lachance (Renaud): Mme la Présidente, Mme la vice-présidente, Mmes et MM. les membres de la commission, Mme la sous-ministre du Revenu, M. le président de la Société de l'assurance automobile du Québec. L'application de mesures de sécurité informatique adéquates est essentielle à la mise en oeuvre des programmes gouvernementaux. En effet, les atteintes à la sécurité peuvent avoir d'importantes répercussions sur le respect de la vie privée. Elles risquent aussi d'influer sur le maintien des services essentiels, la conduite des activités courantes et la productivité du personnel.

Cette vérification visait à nous assurer que la sécurité informatique bénéficie d'un encadrement approprié à l'échelle gouvernementale. Nous cherchions, entre autres, à évaluer si les ministères et les organismes ont mis en place les composantes majeures en vue de protéger leur actif informationnel. Pour ce faire, nos travaux ont porté sur les composantes qui contribuent le plus à l'atteinte des résultats escomptés et dont l'absence ou la défaillance sont susceptibles d'entraîner la multiplication des incidents. Nos travaux ont été menés principalement auprès du Secrétariat du Conseil du trésor, à qui des responsabilités particulières ont été confiées en matière de sécurité informatique.

En ce qui a trait aux moyens de protection déployés, nous avons vérifié les activités menées à cet égard par le ministère du Revenu, la Société de l'assurance automobile et la Régie de l'assurance maladie du Québec ainsi que par deux directions spécialisées du Secrétariat du Conseil du trésor. La présente vérification s'est terminée en mars 2004.

L'information numérique et les échanges électroniques du ministère du Revenu, de la Société de l'assurance automobile du Québec et la Régie de l'assurance maladie du Québec sont généralement bien protégés contre les menaces les plus courantes. Nous avons cependant détecté des failles, car le niveau de protection obtenu repose beaucoup plus sur l'expertise et l'implication des employés ainsi que sur la technologie que sur des processus bien établis.

Concernant l'action propre aux entités, nous avons relevé quelques lacunes par rapport à l'encadrement qu'elles doivent assurer, en particulier le manque d'attention à l'égard du suivi de la performance de leur programme de sécurité. En outre, des processus consacrés à la protection des ressources informationnelles requièrent des améliorations. C'est le cas notamment de ceux qui servent à déterminer la vulnérabilité de l'entité, à planifier l'ensemble des activités en fonction des orientations et des risques, à baliser la sensibilisation et la formation des utilisateurs et des gestionnaires ainsi qu'à gérer adéquatement les mots de passe nécessaires à l'authentification des utilisateurs.

Malgré ces lacunes, notre rapport fait état de certaines bonnes pratiques. D'abord, le ministère du Revenu effectue périodiquement une révision des droits d'accès depuis 1999. Soulignons aussi les efforts marqués de celui-ci pour sensibiliser son personnel à la

nécessité de préserver la confidentialité de l'information. Finalement, mentionnons que la Société de l'assurance automobile du Québec s'est dotée d'un outil spécialisé conçu pour favoriser la robustesse des mots de passe.

Par ailleurs, nous avons réalisé des tests d'intrusion dans quatre entités pour sonder l'efficacité de leurs dispositifs de sécurité. Pour des raisons évidentes, le nom de ces entités, la nature exacte des tests ainsi que les résultats détaillés ne sont pas présentés dans un rapport. Précisons que nous avons fait appel à des techniques ou à des outils facilement disponibles, en cherchant avant tout à simuler des scénarios selon lesquels une personne tentait d'accomplir une action répréhensible.

Nos travaux révèlent que la protection des actifs informationnels des quatre entités est adéquate par rapport aux flux d'information qui proviennent du réseau Internet. Par contre, elle est moins efficace sur d'autres plans, soit la résistance des mécanismes de sécurité, la robustesse des mots de passe, la pertinence des droits d'accès, la configuration des postes de travail et l'aménagement des lieux. Les lacunes détectées pourraient permettre de mener, dans certaines conditions, diverses activités inappropriées. Il est important que les entités du gouvernement du Québec évitent qu'un intrus soit capable d'accéder de façon illégitime à des systèmes informatiques ou à des données sensibles, de modifier des données ou des programmes, d'installer des programmes malveillants et d'empêcher le bon fonctionnement de plusieurs équipements.

Enfin, je veux rappeler que notre vérification fait ressortir que les entités vérifiées s'appliquent à assurer la sécurité de leurs ressources informationnelles. Elle indique aussi que des gestes concrets devront être accomplis pour que leurs actions soient conformes aux meilleures pratiques en vigueur. Cela est d'autant plus important dans le contexte où l'État s'engage à se rapprocher des citoyens en misant sur une utilisation plus intensive des technologies de l'information et des communications. Je vous remercie.

La Présidente (Mme Dionne-Marsolais): Merci, M. le Vérificateur général. Alors, maintenant nous allons entendre Mme la sous-ministre du Revenu. Merci pour votre texte, d'ailleurs.

Exposé de la sous-ministre du Revenu, Mme Diane Jean

Mme Jean (Diane): Alors, Mme la Présidente, Mmes, MM. les députés membres de la commission, M. le Vérificateur général, bonjour et merci de votre invitation.

J'aimerais en commençant vous présenter les personnes qui m'accompagnent aujourd'hui. Alors, à ma droite, M. Pierre Boisvert, sous-ministre adjoint responsable des technologies de l'information; à ma gauche, M. Michel Leblanc, chef du service de la sécurité informatique. M'accompagnent également, de mon bureau, le secrétaire général, M. Norbert Boudreau, et un conseiller, M. Michel Hébert; le directeur de la vérification interne et le chef de service, MM. Claude Gauthier et Pierre Gagné; de la direction centrale de l'accès à l'information et de la protection des renseignements confidentiels, le directeur par intérim, M. Marcel Carbonneau, et Mme Carmen Gauthier, conseillère; et M. Yves St-Jacques, directeur du traitement informatique.

Alors, d'entrée de jeu, Mme la Présidente, j'aimerais préciser que, bien que la présente audition se concentre sur la gestion de la sécurité informatique à Revenu Québec, je joindrai à mes propos des considérations générales rattachées à l'un des principaux enjeux de Revenu Québec, soit la protection des renseignements confidentiels, puisque la sécurité informatique constitue l'un des principaux champs d'intervention pour assurer efficacement cette protection des renseignements confidentiels.

J'aimerais souligner également que les commentaires formulés par le Vérificateur général sont appréciés et nous aident à améliorer nos processus et à devenir plus performants.

Globalement, le rapport du Vérificateur général dénote que Revenu Québec s'applique à assurer la sécurité de ses ressources informationnelles. Cependant, certaines actions doivent être accomplies pour assurer une conformité aux meilleures pratiques en vigueur.

Nos préoccupations de gestion efficace de la sécurité informatique et d'amélioration de la protection des renseignements personnels ne sont pas nouvelles. En novembre 1997, Revenu Québec se dotait d'un premier plan d'action ministériel pour améliorer la sécurité des informations. Au cours de l'année qui a suivi l'adoption de ce plan d'action, Tolérance zéro, plusieurs actions ont été réalisées.

C'est ainsi que les droits d'accès aux transactions interactives et aux fichiers informatiques ont été révisés afin de s'assurer que le personnel n'ait accès qu'aux renseignements nécessaires à la réalisation de ses fonctions. De plus, un mécanisme a été mis en place afin de suspendre sur le champ les accès des employés au moment où ils quittent l'organisation ou s'absentent pour une période prolongée. Également, des programmes informatiques ont été développés afin de détecter les accès non permis aux renseignements

confidentiels. Enfin, plusieurs activités de sensibilisation du personnel ont été réalisées, dont l'instauration d'une campagne annuelle de signature de la déclaration de discrétion.

Au cours de l'année 1998, un diagnostic de l'état de vulnérabilité de notre dispositif de sécurité informatique a été effectué à l'aide de la méthode MARION. Pour y donner suite, la politique ministérielle en matière de sécurité informatique a été révisée en décembre 1999 et une table ministérielle de concertation a été mise en place. De plus, un mécanisme de chiffrement des données conservées sur les ordinateurs portatifs et des communications avec le réseau informatique ministériel a été implanté.

Un suivi de la mise en oeuvre des mesures identifiées effectué par la Direction de la vérification interne et des enquêtes en 2002 indiquait que 90 % des mesures avaient été appliquées ou étaient en voie de l'être, permettant de réduire la vulnérabilité à un niveau acceptable.

n *(15 h 50)* n

En décembre 1999, le rapport Moisan nous recommandait, en matière de protection des renseignements confidentiels, de poursuivre l'amélioration des mesures de sécurité entourant les dossiers fiscaux de tous les contribuables et d'identifier les vérifications, analyses et contrôles notamment par des routines informatiques de vérification des journaux d'accès aux dossiers.

Afin de donner suite à ces recommandations, une nouvelle révision massive des droits d'accès aux transactions interactives a été réalisée en juin 2000. Cet exercice est maintenant répété aux 18 mois. Un bilan de gestion de sécurité informatique a également été réalisé, dans les suites de ce même rapport. Ce bilan a couvert l'ensemble des domaines de gestion de la sécurité aux plans administratif, organisationnel et technique.

Les informations recueillies lors de la réalisation de ce bilan sont à l'origine de l'actuel Plan triennal de gestion de la sécurité informatique 2002-2005. Ce plan, issu d'une démarche bien organisée, comme le mentionne le Vérificateur général dans son rapport, constitue un plan d'ensemble que s'est donné Revenu Québec pour se rendre conforme aux politiques et directives du Secrétariat du Conseil du trésor ainsi qu'aux meilleures pratiques du marché dans le domaine de la sécurité informatique.

Les travaux prévus au plan triennal répondront en quasi totalité aux recommandations formulées par le Vérificateur général. Ce projet sera complété en décembre 2005.

Ainsi, la classification des actifs informationnels fait partie des priorités d'action de Revenu Québec, notamment pour améliorer le registre d'autorité. Les résultats de cette activité seront aussi à la base de l'analyse de risques prévue en 2006. Cette analyse de risques permettra de nous assurer que les mesures de sécurité prennent en compte les principaux risques informatiques auxquels nous sommes exposés et que les déficiences détectées soient prises en charge et corrigées rapidement. De plus, la classification des actifs informationnels nous permettra de nous assurer que l'attribution des droits d'accès s'appuie sur une catégorisation appropriée de l'information.

Également Revenu Québec poursuivra l'exploitation et le renforcement du processus de gestion des vulnérabilités pour assurer une prise en charge et une correction rapides des failles détectées. Ainsi, il prévoit acquérir au cours des prochaines semaines un produit qui lui permettra d'améliorer ce processus.

Par ailleurs, depuis le passage du Vérificateur général, des indicateurs de performance ont été définis pour plusieurs processus développés et mis en place dans le cadre du plan triennal. À titre d'exemple, mentionnons les nombres mensuels et cumulatifs des vulnérabilités ouvertes et fermées et leur statut qui peut être en analyse, en attente d'approbation ou encore en correction.

Le Vérificateur général a constaté que Revenu Québec menait plusieurs activités de sensibilisation et de formation mais que ces dernières n'ont pas été encadrées par un programme global. Il reconnaît cependant les efforts marqués pour sensibiliser le personnel à la nécessité de préserver la confidentialité de l'information.

Afin de répondre à ce constat et dans un souci d'aborder les différents aspects de la sécurité et de la sensibilisation, Revenu Québec a arrimé des activités de formation et de sensibilisation dans un programme consolidé pour la sécurité informatique ainsi que pour la protection des renseignements confidentiels. Cet exercice a été réalisé pour le plan d'action 2004-2005 portant sur la formation et la sensibilisation à la confidentialité. En ce qui concerne la reprise sur sinistre, Revenu Québec a revu et adapté sa stratégie. Il est aussi à compléter la documentation de son plan de reprise, pour lequel des tests sont effectués à intervalles de six mois.

En outre, Revenu Québec entend améliorer le contrôle d'accès à ses ressources informationnelles notamment en resserrant la gestion des mots de passe. Il poursuit ses travaux pour réviser son processus d'attribution des droits d'accès au regard des profils de

fonction. De plus, il vise à améliorer son exercice de révision massive périodique des accès à ses ressources informationnelles.

En termes de suivi de l'activité dans ses systèmes, le Vérificateur général mentionne que Revenu Québec s'emploie à surveiller les consultations de renseignements personnels. J'ajouterais que Revenu Québec est également très sensible à protéger l'intégrité et la disponibilité des données. Nos systèmes comportent des mécanismes de contrôle qui permettent de s'assurer de la fiabilité et de l'exactitude des renseignements fiscaux.

En ce qui a trait au danger d'intrusion, par le réseau Internet ou autrement, Revenu Québec améliore de façon continue ses façons de faire dans l'utilisation des équipements en place et par l'acquisition de nouveaux outils.

En termes de gestion, notre politique sur la sécurité informatique définit les rôles et les responsabilités relatifs à la sécurité. À cet effet, un détenteur des ressources informatiques est nommé pour s'assurer que les mesures de sécurité informatique sont mises en place et appliquées • c'est M. Yves St-Jacques, qui est derrière moi • ainsi qu'un responsable du support à la gestion de la sécurité • M. Michel Leblanc • pour coordonner, normaliser et contrôler l'ensemble des activités reliées à la sécurité informatique. Le détenteur est appuyé par la table ministérielle de concertation de la gestion du contrôle de la sécurité d'accès aux ressources informatiques.

Quant au responsable du support à la gestion de la sécurité, il est également chef du service de la sécurité informatique, qui regroupe 23 personnes. Également, les activités du plan triennal sont sous la supervision d'un comité directeur de projets.

Enfin, le comité ministériel de la protection des renseignements confidentiels, que je préside, coordonne les activités relatives à la confidentialité.

La présence du responsable du support à la gestion de la sécurité dans chacun de ces comités permet d'avoir une vue d'ensemble des travaux réalisés en matière de sécurité informatique.

Pour compléter cette énumération des actions prises par Revenu Québec en matière de gestion de la sécurité informatique et de protection des renseignements confidentiels, je m'en voudrais de ne pas mentionner un élément qui à mes yeux est essentiel, soit l'implication et l'engagement du personnel. Un programme d'accueil a été élaboré pour faciliter l'intégration des nouveaux employés. Ce programme prévoit notamment la signature d'une déclaration de discrétion qui rappelle les obligations auxquelles sont assujettis les employés. De plus, les employés sont informés des pratiques en matière de sécurité et de protection des renseignements confidentiels.

J'aimerais préciser en terminant, Mme la Présidente, que Revenu Québec a investi de façon appréciable en matière de sécurité informatique, en plus de son budget régulier, au cours des deux dernières années • au 31 août 2004, un investissement de 7,2 millions sur un total de 12,8 millions prévus au plan triennal • et qu'il continuera de le faire pour protéger adéquatement ses actifs informationnels et conserver ainsi la confiance de ses diverses clientèles et partenaires.

Revenu Québec est déjà bien positionné en matière de gestion de la sécurité informatique. Les améliorations déjà apportées et celles qui le seront dans le cadre du plan triennal et du plan d'action visant à donner suite au rapport du Vérificateur général, que je dépose aujourd'hui, viendront consolider cette position. Merci, Mme la Présidente.

Discussion générale

La Présidente (Mme Dionne-Marsolais): Je vous remercie beaucoup, Mme la sous-ministre. L'avantage des rapports du Vérificateur général, c'est que, quand on vous reçoit, on voit le progrès. C'est concret, c'est bien écrit, mais néanmoins on a quand même quelques questions. Et je pense que l'enjeu de la confiance, que vous exprimiez à la fin, la confiance de vos clientèles et de vos partenaires, c'est vraiment crucial.

Je tiens à rappeler les conclusions de la vérification, à savoir que le Vérificateur a constaté que l'information numérique et les échanges électroniques étaient généralement bien protégés. Je pense que c'est important de le dire d'entrée de jeu pour ne pas laisser entendre de craintes ou initier des craintes inutiles.

Par contre, la protection, comme il le dit lui-même, repose plus sur des dimensions humaines et technologiques que sur la dimension organisationnelle, et on aura l'occasion d'en discuter puisque vous y avez fait allusion vous-mêmes dans vos remarques.

Vous nous déposez un plan et un certain nombre de documents qui font état des correctifs que votre administration entend

apporter, et on va les regarder. Et les membres de la commission aussi ont certaines préoccupations très spécifiques. Je vais donc commencer... procéder de la façon suivante: 10 minutes, 10 minutes chaque côté, à peu près deux fois. Et on va commencer par le député de Verdun.

M. Gautrin: Je vous remercie, Mme la présidente. Je veux aussi vous signaler et signaler pour les gens qui enregistrent nos débats qu'il y a peu de craintes de notre côté quant à la sécurité de l'information, une sécurité informatique au ministère du Revenu. Donc, le questionnement que nous avons n'est pas un questionnement qu'il faudrait mal interpréter et penser qu'il y a problématique au ministère du Revenu. Je pense que... je tenais à le préciser dès le départ.

n *(16 heures)* n

Vous avez en partie répondu, dans votre document, à mes deux interrogations, mais je vais néanmoins les reformuler. Ma première interrogation touchait l'article 4.62 du rapport du Vérificateur général, que, vous, vous avez répondu, parce que vous l'avez identifié en 4.63, c'est un peu la même chose, c'est-à-dire, c'était la classification des actifs informationnels. Et, bon, le Vérificateur général était un peu dur à cet effet-là, il disait • je vais vous lire 4.62: «Même si les entités vérifiées ont mis en place diverses mesures en ce sens, principalement en ce qui a trait à la reprise des activités après un incident, elles n'ont pas de vue d'ensemble des risques associés aux éléments à sécuriser ni des précautions qui ont été prises. Elles ignorent donc si les principaux risques ont été recensés et si les mesures adoptées sont cohérentes avec la menace réelle.» Vous nous avez, dans votre déclaration, signalé que vous êtes conscients de ce problème-là et que vous êtes en train d'y remédier, que dès octobre 2005, ça veut dire à peu près dans un an, vous serez en mesure d'avoir révisé complètement la classification. Et, en décembre... en janvier 2006... prévoit... dans le cas de l'analyse des risques déjà mentionnée.

Peut-être, pour le bien des membres de cette commission et des gens qui nous écoutent, préciser qu'est-ce que ça veut dire, la classification des actifs informationnels, et quel effet votre plan, que vous mettez de l'avant, va avoir quant à l'inquiétude qu'on aurait pu avoir sur ce qui arriverait en cas de sinistre et en cas de... et les précautions que vous avez mises de l'avant.

La Présidente (Mme Dionne-Marsolais): Mme la sous-ministre.

Mme Jean (Diane): Merci. Alors, oui, ce sont des concepts qui sont complexes. Alors, la solution passe par la classification des actifs informationnels. Qu'est-ce que c'est, la classification des actifs informationnels? C'est un recensement à la fois des infrastructures mais de tous les types de transactions que nous effectuons au ministère.

Et quand on parle de classification, on les classe comment? On les classe par rapport à la confidentialité, donc il s'agit... par divers niveaux de confidentialité, par rapport à l'intégrité et les risques par rapport à l'intégrité, et par rapport à la disponibilité. Certains systèmes doivent être disponibles en tout temps parce que... par exemple, pensons au système des pensions alimentaires, parce qu'ils garantissent le versement des pensions alimentaires de façon régulière.

Ensuite, quand cette classification est faite, elle nous permettra de réviser les droits d'accès, donc les autorisations qui sont données à chaque personnel par rapport à certaines transactions, par rapport à certains fichiers. Elle vont nous permettre aussi d'évaluer les mesures de sécurité à mettre en place, les mesures étant adaptées au niveau de confidentialité requis, au niveau d'intégrité requis, au niveau de disponibilité requis.

Alors, le tout, et vous comprendrez, compte tenu de l'ampleur du travail, c'est en cours de transaction et d'opération, ça demande un grand déploiement. Donc, c'est en cours. Ça va être terminé d'ici environ un an, et ensuite on pourra procéder à une analyse de risques et à l'ajustement du registre d'autorité, du suivi de la sécurité, des tests sur la vulnérabilité, les tests... donc raffiner nos tests d'intrusion, revoir le statut de nos infrastructures pour voir lesquelles sont les plus critiques. Donc, c'est le document de base, cette classification des actifs informationnels, c'est la base pour avoir une action structurée et concrète pour...

M. Gautrin: Et une stratégie de continuité.

Mme Jean (Diane): ...et une stratégie, c'est ça, et pour avoir un nouveau plan triennal à l'issue de celui-ci, là, qui se termine en 2005.

M. Gautrin: Mme la Présidente.

La Présidente (Mme Dionne-Marsolais): Oui, M. le député de Verdun.

M. Gautrin: Je comprends donc que le travail est en cours?

Mme Jean (Diane): Oui.

M. Gautrin: Est-ce que vous auriez l'amabilité d'informer la commission lorsque le travail sera terminé, de manière à nous...

Mme Jean (Diane): Bien sûr.

M. Gautrin: ...sans nécessairement revenir témoigner devant nous...

Mme Jean (Diane): Ça me fera plaisir.

M. Gautrin: ...mais nous informer que vous avez maintenant fait la classification des actifs informationnels, que c'est terminé?

Mme Jean (Diane): Bien sûr.

M. Gautrin: Alors, je vous remercie. Et je crois que mon collègue de Montmorency avait voulu intervenir.

La Présidente (Mme Dionne-Marsolais): Oui. M. le député de Montmorency.

M. Gautrin: J'aurai d'autres questions après...

M. Bernier: Merci, Mme la Présidente. Donc, bienvenue, Mme la sous-ministre, bienvenue aux gens de Revenu Québec. Vous comprendrez que c'est toujours un plaisir de vous recevoir ici et de discuter des éléments concernant la sécurité informatique. Au niveau de Revenu Québec, on sait que c'est quand même un ministère qui a au-delà de 10 000 employés, hein? Une mission quand même assez complexe: l'application de lois fiscales, l'application de lois sociales. C'est un organisme également où on parle de principe d'autocotisation et ces choses-là, donc il y a beaucoup d'éléments et beaucoup d'informations qui sont cumulés au ministère du Revenu. O.K.?

Et, tout à l'heure, vous avez mentionné divers points en ce qui regarde la sécurité justement au niveau de la protection des renseignements confidentiels, vous êtes même la présidente d'un comité sur ça. Je pense que, pour les contribuables du Québec, cet élément-là de protection des renseignements confidentiels en ce qui concerne les personnes, les équipements aussi, l'introduction à l'intérieur des systèmes, ces choses-là, moi, j'aimerais vous entendre, là, sur les mesures qui ont été prises, qui sont prises au ministère pour assurer cette confidentialité en ce qui regarde les renseignements confidentiels.

Je pense que les gens... Comme la présidente l'a mentionné, la vérification au niveau du Vérificateur général, c'est quand même très pointu. On parle de structures, on parle d'éléments qui sont quand même beaucoup plus avancés sur le plan technologique, sur le plan de mise en place. Mais, pour les Québécois et les Québécoises, je pense qu'on doit s'assurer que les mesures prises au ministère pour protéger les renseignements confidentiels sont fort importantes, surtout avec, aujourd'hui, les transactions en ligne, qui sont de plus en plus en force au ministère, présentement et au cours des prochaines années. Donc, j'aimerais vous entendre sur ça.

La Présidente (Mme Dionne-Marsolais): Mme la sous-ministre.

Mme Jean (Diane): D'accord. Oui. Alors, je vais rappeler d'abord pour la commission que j'ai déposé un document sur la protection des renseignements confidentiels à Revenu Québec, alors qui vous permettra de faire le tour de la question, si vous le jugez intéressant. C'est un document qui vient d'être terminé chez nous; il a encore une forme administrative, mais on lui prévoit une plus large diffusion éventuellement, dans un format qui sera rendu un peu plus facile de lecture.

Mais allons-y maintenant plutôt en termes généraux: qu'est-ce qu'on fait, à Revenu Québec, pour s'assurer de la protection des renseignements confidentiels? Parlons prévention d'abord, détection, contrôle, concernant les personnes. D'abord, dès que quelqu'un entre à l'emploi de Revenu Québec: enquête pré-emploi pour s'assurer de l'absence de conflits d'intérêt puis vérifier l'intégrité des personnes avant d'embaucher. Donc, une enquête pré-embauche. Lors de l'entrée en fonction: rencontre avec le gestionnaire pour sensibiliser le nouvel employé; documentation; session d'accueil • je vous en ai parlé tout à l'heure; signature de la première déclaration de confidentialité, de discrétion. Alors, lors de l'accueil de la personne: sensibilisation personnalisée, signature, émission d'une carte d'identité avec photo que la personne doit avoir en sa possession en tout temps pour circuler dans l'établissement, dans tout l'établissement.

L'accès aux locaux. Ceux qui sont déjà venus chez nous, c'est parce qu'ils y travaillaient, parce qu'autrement ils ont dû rester à l'accueil, où sont sortis les employés du ministère du Revenu pour aller les rencontrer. Alors, les accès aux secteurs de travail sont contrôlés; il y a surveillance de secteurs névralgiques au moyen de systèmes de caméras; un système de signature pour le soir ainsi que les jours non ouvrables; surveillance à distance des bureaux régionaux; émission de laisser-passer pour les visiteurs et accompagnement. Là, on est juste... Ça, c'est pour l'entrée en fonction et l'entrée dans la bâtisse.

L'accès aux données informatiques: un code d'identification, un mot de passe, un mot de passe qui doit être gardé secret, qui doit être remplacé tous les 30 jours, qui doit ne pas avoir été utilisé dans les 10 derniers mois et qui comporte aussi d'autres critères. Je sais que vous avez peut-être... que le Vérificateur général et vous avez peut-être des questions sur ça, la question des mots de passe. On travaille à avoir plus de robustesse dans la définition des mots de passe...

M. Bernier: C'est ça, je veux juste vous arrêter sur ce plan-là. Effectivement, le Vérificateur général fait certaines mentions en ce qui regarde la sécurité en ce qui regarde les mots de passe, surtout au niveau des éléments répétitifs, à savoir le nombre de fois qu'on peut présenter un mot de passe avant que l'ordinateur se ferme ou que l'accès se ferme.

Mme Jean (Diane): Nombre d'essais.

M. Bernier: Donc, est-ce qu'il y a des mesures qui vont être prises pour corriger? Parce que c'est un élément qui est souligné dans le rapport du Vérificateur.

Mme Jean (Diane): O.K. Actuellement, c'est trois fois, puis ensuite il tombe.

M. Bernier: Actuellement, c'est trois fois?

Mme Jean (Diane): Trois fois. O.K.? Ce qu'on est à travailler, nous, c'est le choix des mots de passe. Le choix des mots de passe, actuellement, on reconnaît qu'il y aurait peut-être des resserrements à faire, sans tomber dans une trop grande complexité, parce que, si le mot de passe doit être absolument complexe, il est difficile de l'avoir en mémoire, puis les gens ont tendance à l'écrire puis à le mettre en note en dessous du coin du clavier. Donc, on ne veut pas en venir là, mais on veut augmenter la robustesse de nos mots de passe, pour dépasser le simple mot du dictionnaire. Mais donc on envisage une formule alphanumérique, qui est à être évaluée actuellement. Donc, robustesse des mots de passe, on y travaille à ce moment-ci.

n *(16 h 10)* n

Peut-être qu'il faudrait que je couvre un autre aspect, rapidement: l'accès aux services électroniques. On offre certains services électroniques. Mentionner que diverses mesures sont appliquées aussi pour vérifier l'identité de la personne qui communique avec le ministère du Revenu, pour assurer la sécurité des transactions électroniques et des échanges d'informations confidentielles. Il y a l'exigence de procuration électronique ou écrite du contribuable ou de son représentant; chiffrement de l'information échangée avec les personnes; journalisation de l'utilisation par la clientèle des services Internet, et ce, à des fins de contrôle a posteriori. Alors, ça fait un survol.

La Présidente (Mme Dionne-Marsolais): C'est bien. Alors, je vais maintenant passer la parole au député de Gaspé, qui est le porte-parole de l'opposition officielle en matière de revenu.

M. Lelièvre: Merci, Mme la Présidente. Mme Jean, bonjour, ainsi qu'à tous les collaborateurs et collaboratrices, s'il y en a ici, parce que je les cherche...

Une voix: ...

M. Lelièvre: Oui, ils sont derrière, on ne les voit pas tous, hein?

Mme Jean (Diane): Toutes les personnes ici ne sont pas mes collaborateurs, quand même.

M. Lelièvre: Ah non? Bon.

Mme Jean (Diane): Ce sont tous des collègues, mais pas tous mes collaborateurs de Revenu Québec.

M. Lelièvre: Écoutez, je vais continuer sur la... ce qu'on parle, on parle des droits d'accès. Dans le rapport du Vérificateur, à la page 92, à l'élément 4.84, on dit, concernant les droits d'accès, que les droits seraient trop permissifs. J'aimerais ça vous entendre là-dessus, parce que c'est quand même une affirmation qu'il faut... très sérieuse ou...

Mme Jean (Diane): En fait, si je me souviens bien, il s'agissait d'un petit groupe de personnes, des gens qui se situaient dans une unité centrale, qui avaient des fonctions de révision, donc un accès large. Des corrections ont été apportées.

Et par ailleurs, à travers notre processus de révision des droits d'accès, dont je vous ai parlé tout à l'heure, et notre meilleure classification des fonctions, nous croyons avoir pris le moyen que ça ne se reproduise plus.

Mais je voudrais surtout mentionner que le phénomène dont il était question, c'était le fait d'un petit groupe de personnes qui faisaient les fonctions de soutien au système. Alors, on parle de personnes qui avaient un large spectre de droits d'accès compte tenu de leurs fonctions, mais ce sera quand même resserré.

La Présidente (Mme Dionne-Marsolais): M. le député.

M. Lelièvre: Oui. Merci, Mme la Présidente. J'aimerais revenir au début, au point 4.44 du rapport, concernant l'architecture de sécurité. Vous en avez parlé brièvement dans votre introduction, dans votre présentation. On y dit, bon, que les devoirs de chacun ne sont pas spécifiés dans un registre d'autorité; le comité de sécurité informatique ne rend pas compte à la bonne autorité ou ne joue pas pleinement son rôle stratégique; le MRQ n'exerce pas la fonction ou le suivi avec rigueur. Comment on peut améliorer la situation?

Mme Jean (Diane): Bon, O.K. Écoutez, je voudrais dire que nous avons un registre d'autorité. Peut-être qu'il a besoin d'être amélioré, j'en conviens. Mais il existe un registre d'autorité, en sécurité informatique, il y a une structure. Et d'ailleurs vous pouvez voir la structure, là, dans les documents que je...

M. Lelièvre: C'est dommage qu'on ne les ait pas reçus avant.

Mme Jean (Diane): Non. Bien, écoutez, ils sont tout neufs.

La Présidente (Mme Dionne-Marsolais): Mme la sous-ministre, à quelle page que vous vous référez...

Mme Jean (Diane): Si vous prenez la page 47 et l'annexe VI, vous avez la gestion de la sécurité de l'information numérique, la structure de gestion.

La Présidente (Mme Dionne-Marsolais): Ce document-là, si je comprends bien, n'était pas disponible au moment de la vérification, c'est ça?

Mme Jean (Diane): Non, il...

La Présidente (Mme Dionne-Marsolais): Ce n'était pas celui-là, en tout cas.

Mme Jean (Diane): Ce n'était pas celui-là.

La Présidente (Mme Dionne-Marsolais): D'accord.

Mme Jean (Diane): C'était la politique Tolérance zéro...

La Présidente (Mme Dionne-Marsolais): À l'époque, O.K.

Mme Jean (Diane): ...et qui ne contenait pas... qui contenait les mêmes principes et orientations, mais qui ne contenait pas les processus de gestion et la structure associée à la protection de la confidentialité, ce que ce document-là intègre donc.

La Présidente (Mme Dionne-Marsolais): Très bien.

Mme Jean (Diane): Mais vous me demandez comment va-t-on l'améliorer. D'abord, je veux vous montrer que la gestion de la sécurité est structurée autour de moi puis des personnes, là, responsables. Vous avez donc... Je suis propriétaire des ressources

informatiques • c'est un titre, ce n'est pas un fait; la direction de la vérification interne, qui est mon second regard sur tous les processus qui se réalisent à la vérification interne. Le comité stratégique en matière de technologies de l'information, il existe. On nous dit: Il n'est peut-être pas... Il ne se réunit peut-être pas assez fréquemment ou... Bon, alors on va travailler à ça. Il est présidé par le sous-ministre adjoint, ici. Le détenteur des ressources informatiques, directeur du traitement de l'information, M. St-Jacques, derrière moi, s'assure du fonctionnement de la table ministérielle de concertation; il est le supérieur du responsable du soutien à la gestion de la sécurité informatique et de l'équipe de 23 personnes qui s'occupe de sécurité informatique.

Et il faut dire qu'il y a ensuite un réseau de répondants en sécurité informatique, dans l'ensemble des directions générales. Alors, vous voyez, là, l'organigramme nous mène au responsable de la sécurité, par direction générale, qui doit être un cadre supérieur, un administrateur local, utilisateur et gestionnaire. Donc, nous avons... et nous progressons.

Toutefois, je vais revenir à notre classification des actifs informationnels, dont nous avons parlé tout à l'heure. Cette classification va nous permettre de revoir notre registre d'autorité, qui de l'avis du Vérificateur général est incomplet parce qu'il ne couvre que principalement la confidentialité. Donc, on va s'assurer qu'il couvre aussi l'intégrité et la disponibilité. Ça devrait être complété en janvier 2005, et ça va couvrir l'ensemble de ces fonctions-là et ce qui gravite autour donc de la propriété des actifs, du traitement de l'information et de la sécurité de l'informatique. Ça va se greffer autour de cette organisation que vous trouvez dans le document.

La Présidente (Mme Dionne-Marsolais): M. le député de Gaspé, pour une autre question.

M. Lelièvre: Oui. Merci, Mme la Présidente. Si on revenait au processus d'évaluation de la vulnérabilité et de l'efficacité. Bien, lorsqu'on a fait l'étude du rapport, on note que le ministère du Revenu ne dispose pas d'une stratégie assurant l'évaluation périodique complète et indépendante. On retrouve ça à la page 86, au point 4.51. Donc, l'efficacité du dispositif de sécurité et la prise en charge des failles détectées.

Nous, on est des parlementaires, on n'est pas familiers avec toutes vos... on n'a pas toutes vos connaissances, mais ce serait pertinent, je pense, là, que nous soyons éclairés sur ce point-là.

La Présidente (Mme Dionne-Marsolais): Mme la sous-ministre.

Mme Jean (Diane): D'accord. Alors, peut-être que je vais me permettre une définition, hein? On parle de vulnérabilité: de quoi parle-t-on quand on parle de vulnérabilité? On parle des faiblesses d'un système qui pourraient se traduire par une incapacité partielle ou totale • partielle, on l'espère • à faire face aux menaces informatiques qui le guettent, donc aux menaces externes ou internes à l'organisation.

Vous me parlez... On parle donc de tests d'intrusion. Et vous me parlez d'avoir une expertise interne. D'abord vous dire que nous effectuons certains tests d'intrusion, puis nous en ferons. Au cours de la dernière année, Pierre, l'embauche... On en a effectué, mais on a embauché cinq spécialistes de la sécurité informatique, qui sont de l'équipe, pour nous aider à concevoir de tels tests et puis réagir à de tels tests, à des tentatives d'intrusion.

Les faiblesses, il y en a, il y en aura toujours puis des nouvelles stratégies peuvent se développer en tout temps. Ce que je peux vous dire, c'est qu'il nous semble que l'opération que nous menons, de faire le recensement de toutes nos transactions, de revoir le registre d'autorité, le maintien d'une équipe de spécialistes, le fait d'effectuer nous-mêmes des tests d'intrusion régulièrement, et on suit aussi le marché des équipements puis des logiciels qui peuvent être utiles, il me semble que nous nous protégeons. Mais c'est un processus constant. Nous pensons que l'analyse de risques qu'on va réaliser à la suite du présent plan triennal va nous guider aussi pour savoir s'il faut faire d'autres évaluations.

La Présidente (Mme Dionne-Marsolais): M. le député de Gaspé.

M. Lelièvre: Oui. Mais le VG... le Vérificateur dit aussi que le ministère «ne consigne pas l'information avec diligence dans [un] registre», à 4.52 Est-ce que vous avez un tel registre?

Mme Jean (Diane): Oui. Oui, il y en a un.

M. Lelièvre: Un nouveau?

La Présidente (Mme Dionne-Marsolais): ...depuis combien de temps?

Mme Jean (Diane): Ah, ce n'est pas récent. Non, c'est un registre virtuel. Il n'est habituellement pas sur papier, là, c'est un registre électronique qui... Depuis combien de temps?

M. Boisvert (Pierre): Bien, voyez-vous, ici, c'est une copie qu'on a eue...

M. Lelièvre: On parle de la diligence à inscrire des données.

M. Boisvert (Pierre): Oui. Et j'ai un dossier ici, qui est en haut, il a été ouvert le... 2003, février, le 3. Donc, c'est une copie du registre qui a été...

Mme Jean (Diane): Il était au moins à date, lui.

M. Boisvert (Pierre): Il était au moins en 2003.

Mme Jean (Diane): Puis ça indique le statut de chacune des vulnérabilités.

n *(16 h 20)* n

M. Boisvert (Pierre): Il y a l'ouverture, il y a la résolution, il y a la description. Et nous avons ici... on en a sorti quelques-uns, vous avez des pages... Vous comprendrez qu'on ne puisse pas le rendre public, mais nous avons un tel registre, depuis 2003, que nous suivons de façon importante.

Mme Jean (Diane): C'est ça. On va l'améliorer, couvrir plus de volets, mais il y en a un.

La Présidente (Mme Dionne-Marsolais): Moi, j'aurais une petite question avant de passer la parole à mes collègues, à mon collègue de Verdun, c'est concernant la formation. Vous en avez fait allusion lors de vos notes d'introduction...

Mme Jean (Diane): De l'intégration de la formation sur la confidentialité et la sécurité.

La Présidente (Mme Dionne-Marsolais): Oui, voilà, toute cette notion-là, là, de formation à la sécurité. Les commentaires du Vérificateur général...

Une voix: ...

La Présidente (Mme Dionne-Marsolais): Merci. Non, ce n'est pas là. Je vais le trouver, là.

Une voix: Page 90.

La Présidente (Mme Dionne-Marsolais): Page 90, oui, justement. J'aimerais ça... Bon, on a vu, dans vos commentaires, que vous aviez un plan à cet effet-là et que c'était une dynamique... Pouvez-vous nous dire combien vous investissez, au ministère du Revenu, en formation, et quelle est la part de cette formation-là qui est faite en informatique, la partie informatique, là, et la part pour la sécurité, si c'est possible de nous fournir ça? Ce n'est pas nécessaire de me le dire tout de suite, là, mais...

Mme Jean (Diane): Moi, je ne l'ai pas, là, je peux vous dire, dans toute la documentation que j'ai apportée aujourd'hui, je ne l'ai pas. Peut-être que c'est dans la mémoire d'un de mes collaborateurs?

La Présidente (Mme Dionne-Marsolais): On va lui demander. Alors, il s'agit de monsieur...

M. Jean (Diane): M. Michel Leblanc...

La Présidente (Mme Dionne-Marsolais): M. Leblanc.

M. Jean (Diane): ...responsable de la sécurité informatique.

M. Leblanc (Michel): C'est approximativement 20 000 $.

La Présidente (Mme Dionne-Marsolais): Par année?

M. Leblanc (Michel): Par année.

La Présidente (Mme Dionne-Marsolais): Pour tout?

M. Leblanc (Michel): Pour les spécialistes en sécurité.

La Présidente (Mme Dionne-Marsolais): Par personne?

M. Leblanc (Michel): Non, non, au total. Regardez, j'ai 23 personnes, qu'on a dit tout à l'heure, en sécurité informatique, dans le service de la sécurité informatique, puis, en termes de formation, donc de cours...

Mme Jean (Diane): Écoutez, je pense qu'on parle d'une formation très spécialisée. Je vais vous revenir sur l'ensemble de la formation, parce que c'est...

La Présidente (Mme Dionne-Marsolais): O.K. Alors, ce qu'on voudrait, là, je vais vous le dire, c'est: l'enveloppe formation, l'enveloppe formation informatique puis, en dessous, l'enveloppe formation informatique-sécurité. C'est ça que je veux.

Mme Jean (Diane): Le ministère a investi en formation l'équivalent de 15,7 millions en 2002-2003.

La Présidente (Mme Dionne-Marsolais): Ça, ça a du bon sens. Vous avez beaucoup de choses à apprendre dans ce ministère-là. C'est compliqué, la loi de l'impôt!

Mme Jean (Diane): Bon, alors, je l'ai par diverses catégories, là, mais...

La Présidente (Mme Dionne-Marsolais): Alors, pourriez-vous nous le faire parvenir?

Mme Jean (Diane): C'est ça, alors...

La Présidente (Mme Dionne-Marsolais): Donnez-nous le, là, mais vous nous l'enverrez formellement, s'il vous plaît.

Mme Jean (Diane): Il y a 5 % en informatique, 13 % en bureautique, 24 % en fiscalité. Je n'ai pas l'item «confidentialité», dans cette liste-là, mais j'ai «méthodes de travail». Il faudrait que je... Oui.

La Présidente (Mme Dionne-Marsolais): Regardez-le comme il faut, là. Parce que je pense que le point que je veux faire ou que j'essaie de faire, c'est: dans quelle mesure les engagements et le plan d'action dont vous parlez se traduisent par des investissements ou des dépenses financières • moi, je prétends que c'est des investissements, quand c'est de la formation, là • pour assurer cette sensibilisation continue du personnel à la sécurité?

Et je vous pose cette question-là parce qu'il y a de plus en plus de moyens faciles sur le marché, «over the counter», comme on dit, qui peuvent être utilisés. Et, moi, je vais beaucoup au cinéma, donc je me laisse un peu influencer, mais peut-être que je fais un peu... Il y a des choses qui ne sont pas vraies, là, mais... Alors, ça semble très facile finalement de se procurer des trucs pour faire du piratage, et tout ça. Alors, c'est pour ça que je voudrais savoir quel effort est fait là-dedans, en termes d'investissement, pour que les gens soient au moins au courant de ce qui peut être fait, qu'ils soient vigilants. À la limite, là, c'est ça, l'objectif: qu'ils soient vigilants.

Mme Jean (Diane): ...sommes importantes qui sont consacrées à la formation. Puis je vous dirais que le changement... Là, je ne peux pas l'identifier immédiatement dans le rapport, on va vous le transmettre...

La Présidente (Mme Dionne-Marsolais): Non, non, il n'y a pas de problème.

Mme Jean (Diane): ...mais je vous dirais que le changement aussi qu'on instaure, puis à la suggestion du Vérificateur général, c'est de consolider la formation qui concerne la confidentialité et la sécurité informatique. Et ça, je pense que ça va être un plus, de pouvoir intégrer les deux volets de la formation.

La Présidente (Mme Dionne-Marsolais): M. le député de Verdun.

M. Gautrin: Merci, Mme la Présidente. Je voudrais commencer mon intervention en rappelant ce qui est probablement le plus préoccupant pour nos concitoyens, qui est la question de la gestion des incidents, de la part du Vérificateur général, dans l'article 4.41. Et je vous lis cette phrase: «Les pages suivantes présentent [les fruits de] travaux que nous avons réalisés auprès de trois d'entre eux. Elles traitent de tous les critères d'évaluation, à l'exception de celui qui porte sur la gestion des incidents. À ce sujet, nous avons en effet observé que les entités vérifiées disposent dans l'ensemble d'une bonne capacité d'intervention.» Il me semblait important de le rappeler, Mme la Présidente, puisqu'on n'en parle pas. Et donc on parle évidemment de choses sur la périphérie, mais ce qui est la gestion des incidents est considéré à ce moment-là comme une bonne capacité d'intervention.

Je veux revenir, si vous me permettez, sur une autre question, qui est la gestion des risques résiduels. Alors, c'était... j'avais des paragraphes, si vous voulez, 4.54 à 4.58, et dans lesquels on s'inquiétait en quelque sorte de la non-identification du concept des risques résiduels. Je me permets de vous lire 4.58: «Ces lacunes ne favorisent pas l'équilibre qu'il faut maintenir entre les différentes dimensions de la sécurité, équilibre [...] à réaliser en raison de la propension des organisations à intervenir surtout au regard de la dimension technologique. Il s'ensuit que des éléments d'ordre organisationnel aussi fondamentaux que la classification de l'information et la gestion des risques sont encore peu développés.» Et, à cet effet-là, le Vérificateur général vous faisait une recommandation en 4.60.

Dans votre document, actuellement, vous dites que vous avez pris actuellement le taureau par les cornes • si cette expression a un sens • et vous êtes en train d'intégrer dans le processus de gestion des vulnérabilités l'évaluation des risques résiduels de manière à faciliter et à formaliser la communication des informations relatives à ces risques. Et vous avez actuellement, après, modifié le processus de gestion adapté à la forme du registre des vulnérabilités pour y intégrer les informations sur les risques résiduels, et puis, après, pour les vulnérabilités identifiées dans le registre des vulnérabilités, fait une évaluation des risques résiduels et un échéancier: janvier 2005 pour le début des travaux sur le premier élément; novembre 2004, c'est-à-dire maintenant, sur le registre des vulnérabilités; et octobre 2004 sur identifier les...

Alors, moi, ma question est un peu plus pédagogique qu'autre chose: Pourriez-vous expliquer ce qu'est exactement les vulnérabilités liées aux risques résiduels? Et qu'est-ce que le travail que vous êtes en train de faire va permettre de corriger? Et, en sous-question, pour éviter de la poser à la fin, c'est: Quand vous aurez terminé ce travail, est-ce que vous pourriez communiquer l'information à la commission?

La Présidente (Mme Dionne-Marsolais): Mme la sous-ministre, le contrat est gros. Allez.

Mme Jean (Diane): Oui. Est-ce que vous me permettriez de céder la parole à mon sous-ministre adjoint, responsable des technologies de l'information, pour le concept des risques résiduels?

La Présidente (Mme Dionne-Marsolais): M. Boisvert, nous vous écoutons.

M. Boisvert (Pierre): Vous allez voir, c'est très simple.

M. Gautrin: Oui, je le sais.

Des voix: Ha, ha, ha!

M. Boisvert (Pierre): Merci, M. Gautrin. Vous savez, le risque résiduel en fait, c'est le risque qui subsiste une fois que toutes les mesures de protection ont été faites et appliquées au niveau d'une organisation. On vous a, je pense... et le Mme la sous-ministre l'a dit, au ministère, on a une gestion de la sécurité qui est relativement importante et intéressante, donc le résiduel est vraiment, on pourrait dire, très résiduel. Évidemment, notre processus devrait faire en sorte d'éliminer presque entièrement ces risques que l'on dit résiduels, sauf qu'il faut comprendre qu'une élimination complète d'un risque est pratiquement impossible et que les investissements requis pour réduire un risque résiduel, des fois minime, peuvent s'avérer aussi très, très importants.

Une voix: ...

M. Boisvert (Pierre): C'est ça. Donc, il restera... Je pense que ce serait utopique de penser qu'une organisation peut avoir un système de sécurité où il n'y a aucun risque résiduel. Il s'agit juste de voir de s'assurer, et surtout par le registre de vulnérabilité, les tests d'intrusion, à l'effet que ces risques résiduels là ne deviennent pas... demeurent un risque résiduel.

Et lorsqu'il est connu, exemple, lorsque des fois vous avez ce qu'on appelle plus communément des hackers qui essaient de jouer

dans nos choses, bien évidemment, quand eux... Un élément de notre infrastructure peut paraître résiduel, mais, dès que cet élément d'infrastructure là est sujet à une attaque, il ne devient plus résiduel, il est corrigé. Mais on y va au fur et à mesure, et c'est un risque que l'organisation et, je pense, que toute organisation doit prendre.

n *(16 h 30)* n

La Présidente (Mme Dionne-Marsolais): Je voulais savoir sur ça, là... Parce qu'à 4.58, si je lis la dernière... si vous lisez ce paragraphe-là comme il faut... «Ces lacunes ne favorisent pas l'équilibre qu'il faut maintenir entre les différentes dimensions de la sécurité • dont vous avez parlé • équilibre difficile à réaliser en raison de la propension des organisations à intervenir, surtout au regard de la dimension technologique.» Ça va. «Il s'ensuit que des éléments d'ordre organisationnel aussi fondamentaux que la classification de l'information et la gestion des risques sont encore peu développés.» Bon.

Vous avez parlé du risque résiduel, résiduel, là. C'est des beaux mots, mais on comprend que vous faites un choix entre jusqu'où on doit aller pour se prémunir au maximum... Mais est-ce qu'on est en mesure d'évaluer qu'est-ce que c'est, le risque résiduel, résiduel? Est-ce que ça existe, ça? Ou peut-être que le Vérificateur pourrait nous venir en aide, là-dessus, et nous expliquer ce qu'il voulait dire et par rapport à ce que vous pouvez faire.

Une voix: ...

La Présidente (Mme Dionne-Marsolais): Oui. Ce serait peut-être bien qu'on...

Mme Jean (Diane): ...une analyse de risques. On pourra ensuite parler de l'analyse de risques.

La Présidente (Mme Dionne-Marsolais): Ou si les propos... C'est ça. Ou si les propos que vous avez... Oui. M. le député de Verdun, peut-être?

M. Gautrin: Non, non, mais je comprends ce que vous avez. Là, à l'heure actuelle, vous allez être en mesure de faire une analyse, de faire une classification complètement. Et ensuite vous êtes quand même en mesure de dire: On ne peut pas tout couvrir actuellement. Parce que vous ne couvrirez jamais toute la possibilité des risques. Mais il faut savoir qu'il y a encore un certain nombre de choses et qu'il faut que vous en soyez conscients. Et c'est ça que vous identifiez comme risques résiduels. Les connaître et savoir qu'ils existent... Bon, ils sont mineurs, ils sont contrôlés, etc., et, à ce moment-là, vous ne remettez pas du tout toute la structure de protection en cause dans ce sens-là.

Mme Jean (Diane): On identifie l'ensemble des risques...

M. Gautrin: Je m'excuse. Ce n'était pas une question, mais enfin...

Mme Jean (Diane): Non. Ça va. On identifie l'ensemble des risques et puis on les classifie, puis ensuite on agit sur les risques majeurs, et il peut rester des risques qu'on choisit de ne pas couvrir, notamment à cause des coûts et de la fréquence...

M. Gautrin: ...

Mme Jean (Diane): ...et aussi de la qualité, si je peux dire, du risque. Est-ce que c'est un risque à la confidentialité, à l'intégrité ou à la disponibilité? Selon le type de risque, on peut choisir aussi.

M. Gautrin: Est-ce que vous pourriez nous transmettre votre... votre truc, là?

Mme Jean (Diane): Bien sûr.

La Présidente (Mme Dionne-Marsolais): ...

Mme Charest (Rimouski): ...la gestion comment, là, en termes de suivi? Vous dites, bon, vous avez évalué que c'était plus ou moins important, dépendamment du niveau de sécurité exigé, mais, une fois que vous avez fait ça une fois dans le temps, je veux dire...

Mme Jean (Diane): Il faut que ce soit fait en continu, vous avez raison. Il doit aussi se faire un suivi de la sécurité.

La Présidente (Mme Dionne-Marsolais): M. Boisvert...

Mme Jean (Diane): Oui, M. Boisvert va compléter.

M. Boisvert (Pierre): Notre principal outil est le registre de vulnérabilité. Lorsque...

Une voix: ...

M. Boisvert (Pierre): Le registre de vulnérabilité que je vous ai...

Mme Charest (Rimouski): C'est le registre des faiblesses détectées.

M. Boisvert (Pierre): ...des faiblesses qui sont détectées. Et là on regarde et, dépendant de la classification de l'actif, est-ce qu'on va investir ou pas là-dedans? Parce que des fois, vous savez, il est résiduel, mais, comme M. Gautrin disait, un jour, à un moment donné, on ne sait pas pourquoi, il devient plus important. Donc, on a pas mal tous les éléments à l'intérieur du registre de vulnérabilité.

La Présidente (Mme Dionne-Marsolais): D'accord.

Mme Charest (Rimouski): ...le registre de vulnérabilité vous informe à quel rythme? Quotidiennement, hebdomadairement, mensuellement?

M. Boisvert (Pierre): Du moment...

Mme Jean (Diane): C'est toujours ouvert.

M. Boisvert (Pierre): C'est toujours, toujours ouvert. On a des outils qui balaient l'ensemble de notre infrastructure, et il y a des gens qui sont aussi aux aguets. Les personnes que Mme Jean vous signalait sont aux aguets continuellement au niveau de tout ce qui concerne notre réseau informatique.

Mme Charest (Rimouski): Et pour pallier le fait qu'une personne s'absente... Parce que là vous nous parlez des personnes, de l'implication de votre personnel. Ça, c'est une chose puis ça va, il y a pas de problème...

M. Boisvert (Pierre): La fonction est permanente.

Mme Jean (Diane): La fonction est permanente.

Mme Charest (Rimouski): La fonction est permanente.

M. Boisvert (Pierre): On a... Il y a des outils qui balaient complètement... Exemple, pour tout ce qui concerne les échanges électroniques, du moment qu'il y a un test d'intrusion ou que c'est quelqu'un qui vient cogner à la porte, il se fait identifier et, s'il cogne une autre fois, habituellement il est identifié. On ne sait pas c'est qui, mais il y a un autre pare-feu qui s'installe.

La Présidente (Mme Dionne-Marsolais): Merci. M. le député de Montmorency.

M. Bernier: Peut-être un peu, pas nécessairement sur les risques résiduels, mais... Justement, dans le cadre de vos opérations, maintenant on sait que... Vous nous avez parlé au niveau des éléments de sécurité à l'interne, à l'intérieur du ministère, que ce soit à Québec, Montréal ou région, mais il y a également les vérificateurs qui vont à l'extérieur, hein? Nos vérificateurs, aujourd'hui, on sait que les méthodologies de travail ont énormément changé. Les gens du ministère partent avec leurs «computers», leurs mini-ordinateurs, ils doivent faire un chargement d'informations en regard de l'établissement là où ils s'en vont vérifier, ils doivent procéder également à des consultations, probablement en cours de vérification, là où ils se trouvent, hein, et par la suite ils doivent revenir avec de l'information qu'ils possèdent pour alimenter les banques de données et les informations pour en arriver à terminer le travail de vérification qu'ils ont effectué.

Donc, tout ce processus-là, on voit, là, qu'il y a quand même des mesures de sécurité, j'imagine, qui doivent être importantes pour s'assurer, premièrement, qu'il n'y a pas d'intrusion. Parce que, à ce moment-là, que vous le vouliez ou pas, l'individu se trouve à l'extérieur et il a accès au X fichiers du ministère à l'extérieur du ministère et... De quelle façon on s'assure aussi que l'information

qu'il va recueillir va être transmise au ministère avec toute la sécurité qu'il faut?

Donc, j'aimerais, moi, vous entendre sur ça. Je pense que ça a une implication pratico-pratique, là, puis c'est ce qu'on aimerait connaître, parce que les gens... toute entreprise est susceptible de recevoir la visite de vos vérificateurs.

Mme Jean (Diane): Oui. Écoutez, avant de vous répondre, j'avais prévu que peut-être on s'intéresserait au travail des vérificateurs, puis j'ai amené une petite brochure qui décrit la vérification fiscale, qui présente le travail des vérificateurs, comment ils se présentent chez l'employeur, comment ils procèdent, et c'est une brochure qui est utilisée pour informer ceux que nous vérifions sur notre travail. Alors, si ça vous intéresse... Bon.

Mais revenons-en à votre propos. Disons que Revenu Québec en effet fournit des micro-ordinateurs portatifs aux vérificateurs. C'est normal. Avant de quitter le bureau, l'employé charge les renseignements relatifs aux dossiers sur son ordinateur. Le chargement se fait par le biais d'une application, là, qui s'appelle Système intégré de vérification. Les renseignements sont chargés ainsi, de même que toutes les feuilles de travail, puis ils sont chiffrés par l'application, donc ils sont codés... le dossier qui part, avec lequel le vérificateur part.

Les renseignements sous forme de fichiers électroniques sont également fournis souvent par l'entreprise au vérificateur. Ces fichiers sont protégés par des mécanismes de sécurité installés sur les micro-ordinateurs. Donc, les données qu'on collecte puis qu'on insère sont également protégées. Pour avoir accès à son micro-ordinateur, l'employé doit s'authentifier à l'aide de son code d'identité, de son mot de passe, et ainsi une seule personne autorisée peut se servir de l'appareil. Alors, une seule personne. Les appareils sont munis d'un logiciel antivirus, d'un écran de veille puis d'une fonction qui permet de chiffrer automatiquement les fichiers sauvegardés sur le disque rigide.

Puis, il y a aussi une fonction de chiffrement pour les communications. Il y a une fonction de chiffrement aussi sur les supports amovibles, si c'est des disquettes ou des disques. Puis en plus il y a des câbles de sécurité qui sont fournis au vérificateur pour les branchements sur place. Il y a un mécanisme dit d'authentification forte, puisque le vérificateur dispose d'une carte qu'on appelle «jeton» qui fournit un mot de passe valide pour une minute seulement qui, joint au numéro d'identification, lui permet d'établir la communication avec le réseau informatique. Ensuite, on vérifie, au retour, si les mécanismes de contrôle ont fonctionné puis s'ils ont été appliqués, avec du personnel de support informatique.

Donc, l'équipement est protégé avant de partir, les données qu'on y chiffre, les communications. Donc, il y a des rappels périodiques qui sont faits aux personnels qui utilisent ces appareils-là pour les protéger également contre tout vol, perte ou autres.

M. Bernier: J'imagine que les tests de sécurité sont faits pour s'assurer, là, qu'effectivement ces mesures de sécurité là sont mises en place ou sont...

Mme Jean (Diane): Oui, il y a des rappels périodiques puis en plus, peut-être un changement qui s'est fait récemment, il y a beaucoup de ces chiffrements-là qui se font maintenant automatiquement. Alors qu'auparavant on comptait sur le vérificateur pour actionner les logiciels de chiffrement, maintenant, dans plusieurs sinon la totalité des situations, il n'a pas à les demander, ils sont automatiques. Donc, on n'a plus ce risque. Parce que ça avait un effet de ralentissement • sans doute que vous connaissez la chose • sur la saisie, ce qui fait que les vérificateurs avaient tendance à ne pas l'utiliser. Mais c'est fini parce que maintenant le chiffrement est automatique.

M. Bernier: C'est bien. Merci.

La Présidente (Mme Dionne-Marsolais): Alors, M. le député de Gaspé.

n *(16 h 40)* n

M. Lelièvre: Oui. Merci, Mme la Présidente. J'aimerais revenir sur les mots de passe.

Mme Jean (Diane): Oui.

M. Lelièvre: On en a parlé un peu au début, tout à l'heure. Vous disiez que, bon, il ne faut pas que ce soit trop compliqué, il ne faut pas que ce soient des mots que les gens vont oublier, ça prend une procédure spéciale par après pour se donner un autre mot de passe, donc ça prend du temps, ça prend du service... le service... Et, dans son rapport, à la page 92, il en parle des... Excusez-moi, pas à la page... oui, le mot de passe, c'est à la page 92, au point 4.83, que «les règles en vigueur donnent lieu à des mots de passe

trop simples». Et, de ce côté-là, il serait peut-être important d'agir rapidement parce que...

Je vais vous présenter la situation suivante. Vos bureaux ferment, hein? Certainement que vos bureaux ferment. J'imagine qu'il y a des gens qui font l'entretien ménager, il y a des gens qui font le ménage partout. Si, par malheur, quelqu'un qui est bien informé, qui a une formation en informatique mais qui par hasard se retrouve sans emploi et qu'il travaille au ministère du Revenu à faire l'entretien ménager, il peut avoir accès à des mots de passe. Ce matin, on nous a fait la démonstration qu'avec un petit bidule qu'on peut brancher facilement entre deux fils, bon, etc. • je n'en dirai pas plus pour donner plus d'idées à d'autres personnes • on peut aller chercher des informations importantes, hein? Donc, j'aimerais savoir: À partir du moment qu'on ouvre une porte, la première porte, disons, êtes-vous en mesure de pouvoir contrôler l'ouverture des autres portes?

Une voix: ...

M. Lelièvre: Bien, dans quelle mesure, on ne le sait pas, parce que ça dépend qu'est-ce qu'on obtient, qu'on peut retrouver comme informations. Si on met les mots de passe en dessous du cartable, ou du sous-main, ou dans le dictionnaire, tu sais...

La Présidente (Mme Dionne-Marsolais): D'où l'importance de la sensibilisation. Mme la sous-ministre.

Mme Jean (Diane): Bien, d'abord, une chose pour vous rassurer au départ: le personnel de l'entretien ménager y compris fait l'objet d'enquêtes de sécurité et est soumis... Tout personnel qui travaille régulièrement de l'autre côté des guichets est soumis à ces processus-là. Donc, il y a une enquête de sécurité sur les personnes puis il y a un enregistrement des personnes. Donc, on sait exactement qui va où, même s'il s'agit de faire l'entretien ménager ou l'arrosage des plantes. Et plusieurs... certaines personnes, quand ce sont des remplacements, sont accompagnées. Par exemple, la personne qui vient dans mon bureau arroser la plante, elle est accompagnée si elle n'est pas à nos registres. Alors, d'abord, il y a... Première sécurité, les personnes ne circulent pas librement dans les locaux. Mais, vous avez raison, on doit les renforcer, les rendre plus robustes.

Je vous ai parlé tout à l'heure de mots de passe plus robustes, d'une formule alphanumérique. En effet, actuellement, on a déjà des dispositifs de sécurité sur le renouvellement, sur la durée. C'est en cours actuellement. Mais il faut penser qu'on a plusieurs environnements informatiques, et il faut harmoniser les règles puis les rendre opérationnelles. On ne veut pas implanter non plus une règle de mots de passe trop complexes, pour les raisons dont on a parlé, parce que les gens ont tendance à les écrire. Donc, on est à... Et je ne vous la donnerai pas aujourd'hui, vous comprenez pourquoi. Alors, on va donner prochainement de nouvelles règles pour les mots de passe sous une formule alphanumérique, donc mots et lettres, qui vont permettre d'améliorer la robustesse.

Une voix: Chiffres et lettres.

Mme Jean (Diane): Oui, c'est vrai. Je m'excuse. Bon. Et puis M. Boisvert, si vous permettez, va vous parler du petit bidule dont vous parlez.

La Présidente (Mme Dionne-Marsolais): M. Boisvert.

M. Boisvert (Pierre): Oui, effectivement, c'est un petit bidule, mais ce n'est pas tout le monde qui pourrait s'en servir. Ça peut paraître facile d'installer un petit bidule sur un poste de travail. C'est comme un logiciel: vous l'installez, théoriquement ça marche. Et ça, si vous le mettez sur le fil, ça prend une certaine expertise pour être capable d'aller chercher les mots de passe dans l'ordinateur. Il ne faut jamais oublier qu'il n'a accès qu'au mot de passe de la personne qui est là. Donc, ça veut dire que, s'il veut avoir une information particulière sur quelque chose, il faut qu'il sache que ce poste-là qui appartient à telle personne lui donne accès à tels fichiers.

La Présidente (Mme Dionne-Marsolais): Oui, mais, M. Boisvert, en toute honnêteté, là, quelqu'un qui est malveillant et qui a des intentions malveillantes sait comment s'en servir puis il sait comment l'utiliser au maximum, hein? Bon.

M. Boisvert (Pierre): Effectivement.

La Présidente (Mme Dionne-Marsolais): Bon. Cela étant dit...

M. Boisvert (Pierre): Et ça fait partie des risques résiduels.

La Présidente (Mme Dionne-Marsolais): Ah, ça fait partie des risques résiduels! D'accord. O.K.

M. Boisvert (Pierre): ...c'est que le fameux petit bidule, le fameux petit bidule, ce n'est pas, vous savez, là, une prise de courant, là.

La Présidente (Mme Dionne-Marsolais): Ce n'est pas simple, je suis d'accord.

M. Boisvert (Pierre): Ce n'est pas simple. Il est facile à se procurer, et tout, mais il n'est pas facile à utiliser.

La Présidente (Mme Dionne-Marsolais): Je ne crois pas que les pirates dont on s'inquiète non plus soient des gens simples. C'est des gens qui voient dans cet exercice un défi. Puis-je vous demander, moi... Vous avez dit, au début, qu'il y avait 23 personnes dédiées à la sécurité informatique. Pourriez-vous nous dire ce qu'elles font, ces 23 personnes-là?

Mme Jean (Diane): Comme j'ai à ma gauche le chef du service, le responsable de la sécurité informatique, si vous permettez, on va...

La Présidente (Mme Dionne-Marsolais): ...le 23 personnes?

Mme Jean (Diane): M. Leblanc.

M. Leblanc (Michel): Le 23 personnes, ça fait environ deux ans.

La Présidente (Mme Dionne-Marsolais): D'accord.

M. Leblanc (Michel): Parce que le service a été mis en place en mars 1999, et au départ nous étions 10 personnes, et au fil du temps, avec les besoins qui se sont accrus, avec le support qu'on devait fournir au niveau de la refonte des systèmes au ministère du Revenu, l'équipe s'est accrue. Donc, on est passé, en l'espace de quatre ans, de 10 personnes à 23 personnes.

Et ce que font ces gens-là? On couvre vraiment tout le spectre des responsabilités associées à la sécurité informatique. Donc, on parle autant de politiques de sécurité, de directives de sécurité, on parle d'architecture de sécurité, de cadre de gestion de la sécurité. Par «cadre de gestion» j'entends les différentes fonctions de gestion que nous avons à assurer, que ce soient la gestion des droits d'accès, la gestion de la journalisation, la gestion des intrusions, des vulnérabilités, donc tout ça. On a un plan de travail actuellement où on est en train de parfaire, de peaufiner nos façons de faire à l'égard de la sécurité informatique.

Et on couvre également tous les aspects opérationnels. Donc, par «aspects opérationnels», bien sûr, il y a la gestion des vulnérabilités, il y a la gestion des droits d'accès, on fournit le support aussi aux différents utilisateurs de Revenu Québec. Donc, en gros, là, c'est autant des aspects administratifs, organisationnels.

La Présidente (Mme Dionne-Marsolais): Merci. En terminant, est-ce que vous pouvez nous dire, en 2003-2004, combien de cas d'intrusion est-ce que vous avez constatés au ministère du Revenu?

Mme Jean (Diane): On ne peut vous dire ça.

La Présidente (Mme Dionne-Marsolais): Ah, vous ne pouvez pas nous dire ça?

Mme Jean (Diane): Non.

La Présidente (Mme Dionne-Marsolais): Ah bon!

Mme Jean (Diane): Pour des raisons...

La Présidente (Mme Dionne-Marsolais): Des raisons de confidentialité?

Mme Jean (Diane): ...de sécurité. De sécurité.

La Présidente (Mme Dionne-Marsolais): O.K. D'accord. Alors... Oui, M. le député de Gaspé? Il vous reste 1 minute et demie.

M. Lelièvre: Ah bien, une minute... Je ne sais pas s'il en a parlé tout à l'heure, mais...

Une voix: On ne peut peut-être pas nous le dire verbalement, mais on peut peut-être nous le transmettre par écrit, par exemple?

Mme Jean (Diane): Non.

M. Lelièvre: Bon, écoutez, je ne sais si on en a parlé, mais la question de la continuité de service... Je ne sais pas si le député de Vaudreuil... Verdun l'avait abordée tout à l'heure. Moi, j'aimerais savoir... Parce que, dans le rapport du Vérificateur, on dit que la documentation des procédures est incomplète au MRQ.

Mme Jean (Diane): Pour la reprise en cas de sinistre?

M. Lelièvre: Oui. *Continuité de service*, point 4.78, dernière ligne, quoi, et on dit que «la portée des tests qui visent à éprouver l'efficacité de leurs plans respectifs est trop restreinte». Donc...

Mme Jean (Diane): En fait...

M. Lelièvre: Page 91 du rapport du Vérificateur.

Mme Jean (Diane): Bon, écoutez, de mémoire, là, je vous dis, il s'agit donc de la reprise en cas de... après un sinistre. Il se fait des opérations annuelles. Ça fait partie des choses qui doivent faire l'objet d'un suivi périodique, qui fait l'objet de notre plan d'action.

M. Lelièvre: On parle d'un sinistre informatique, là?

Mme Jean (Diane): Oui, oui, on parle d'un sinistre informatique, donc un événement... Donc, deux fois par année, le ministère effectue des tests de son plan de reprise sur sinistre, autant sur la plateforme centrale que sur les applications de la plateforme départementale. Les derniers tests ont été réalisés en septembre 2004. Donc, c'est récent. Les éléments du plan de reprise attestés sont identifiés lors de chaque essai en fonction des objectifs visés. On réfère principalement ici aux composantes d'infrastructure technologique, aux applications, aux procédures. La stratégie de reprise a été revue et adaptée aux besoins actuels. Puis, au cours des prochains mois, le nouveau processus de reprise sur sinistre sera mis en oeuvre puis la documentation des procédures sera complétée.

Donc, c'est identifié à notre plan de travail de compléter cette stratégie-là et de la documenter après chaque événement.

M. Lelièvre: Et, s'il arrivait un sinistre majeur, un incendie, par exemple, au ministère? S'il arrive un sinistre majeur?

Mme Jean (Diane): Un sinistre...

M. Lelièvre: Majeur. J'imagine qu'il y a un back-up à quelque part?

Une voix: Oui, oui, oui.

Mme Jean (Diane): On a... Oui, oui, oui. Ça, là-dessus...

Une voix: En dehors du ministère.

Mme Jean (Diane): À l'extérieur. On a un contrat à l'externe pour une relève. Ça, c'est ce qu'on appelle la relève. On a une relève informatique, oui.

n *(16 h 50)* n

La Présidente (Mme Dionne-Marsolais): Bon. Alors, en terminant, je comprends que vous ne puissiez pas nous dire si vous avez eu des intrusions, parce que cette commission est publique, mais pourriez-vous nous dire à qui vous rendez cette information-là accessible? Qui est-ce qui est juge de votre... Parce que... En fait ce n'est pas une colle, là.

Mme Jean (Diane): Non, non.

La Présidente (Mme Dionne-Marsolais): Qui est-ce... Est-ce que c'est possible... Est-ce qu'on peut faire une session non publique

où vous pourriez nous communiquer ça ou... À qui répondez-vous quant à cette force-là? Parce que, quand même, dans le tableau II du rapport du Vérificateur, il y a des cas, là, où il y a eu des cas d'intrusion. Évidemment, ils ont... Pour les mêmes raisons, ils ne les ont pas mentionnés, puis on comprend ça, mais ça pourrait être chez vous.

Mme Jean (Diane): Ce que je disais, c'est qu'en fait je vais vérifier avec mes conseillers juridiques. Je peux vous dire que le Vérificateur général... C'est des informations donc que nous échangeons avec le Vérificateur général. Il nous fournit les indications requises et il a accès à toutes ces informations-là, puis on prend les actions. Ça, je peux vous dire ça. Donc, il y a des échanges avec le Vérificateur général. Et les gens qui détectent les choses doivent me faire rapport.

La Présidente (Mme Dionne-Marsolais): Donc, le Vérificateur général pourrait être garant des correctifs?

Mme Jean (Diane): Oui. Tout à fait. Exact.

La Présidente (Mme Dionne-Marsolais): Si on lui demandait, à la fin de cette réunion, de nous faire un rapport quant à la mise en place...

Mme Jean (Diane): Il n'y aurait pas de problème.

M. Lachance (Renaud): ...le paragraphe 43, sur la gestion des incidents, est correct.

La Présidente (Mme Dionne-Marsolais): 4.43?

M. Lachance (Renaud): 4.43.

Mme Jean (Diane): Parce qu'il a eu accès... le Vérificateur général a eu accès...

M. Lachance (Renaud): 41, excusez-moi. 41.

Mme Jean (Diane): Le Vérificateur général a accès à ces informations-là et il donne son point de vue, oui.

La Présidente (Mme Dionne-Marsolais): Oui, mais, à 4.43, on dit bien: «Les trois entités vérifiées ont accompli une bonne partie des gestes attendus [...] néanmoins...»

M. Lachance (Renaud): Non, 4.41.

La Présidente (Mme Dionne-Marsolais): 4.41, les actions propres aux entités. «Elles traitent de tous les critères [...] sur la gestion des incidents.»

Mme Jean (Diane): C'est ça. C'est de ça dont il est question.

La Présidente (Mme Dionne-Marsolais): «...disposent dans l'ensemble d'une bonne capacité d'intervention.»

Mme Jean (Diane): Et ils ont... Donc, l'information est disponible au Vérificateur général, qui nous fait ce rapport.

La Présidente (Mme Dionne-Marsolais): D'accord. Alors, je vous remercie beaucoup, messieurs, Mme la sous-ministre.

Une voix: C'est terminé?

La Présidente (Mme Dionne-Marsolais): Oui. Nous allons maintenant entendre la Société...

Une voix: ...

La Présidente (Mme Dionne-Marsolais): Attendez un instant. Le Vérificateur général veut répondre à une préoccupation que nous avions tout à l'heure. Oui, M. le Vérificateur général.

M. Lachance (Renaud): Oui. C'est justement une chose pour souligner l'excellente collaboration du ministère du Revenu lors de

nos vérifications et vous dire que nous sommes très heureux du dépôt du plan d'action parce que, pour nous, ça signifie la pertinence d'une recommandation mais surtout la mise en oeuvre, la volonté de la mise en oeuvre de ces recommandations à l'entité.

Des voix: Merci.

La Présidente (Mme Dionne-Marsolais): Nous sommes aussi très heureux, puisque la confiance au ministère du Revenu est très importante pour l'avenir de notre société, n'est-ce pas? Alors, merci. Bonne fin de journée.

(Suspension de la séance à 16 h 53)

(Reprise à 16 h 58)

La Présidente (Mme Dionne-Marsolais): ...travaux de la commission et nous allons entendre les représentants de la Société de l'assurance automobile du Québec, notamment son président-directeur général. Bienvenue, M. Brind'Amour et votre équipe, que vous allez nous présenter, j'imagine, dans quelques minutes. Je vous indique que nous sommes tous membres de la commission et que le porte-parole de l'opposition officielle, le député de Beauharnois, est également membre de la commission pour aujourd'hui. Et donc la façon dont nous fonctionnons • petit rappel, bien que vous le savez sans doute • le Vérificateur général a déposé son rapport, on a fait une session de travail avec lui, il a déjà fait ses remarques au début de cette session-ci, certains de vos collaborateurs vous les ont sans doute transmises, et donc, là, maintenant, il s'agit de voir comment vous avez répondu ou vous allez répondre, dans certains cas, aux préoccupations qu'il a soulevées. Et donc je vous passe la parole, M. Brind'Amour.

Exposé du président-directeur général
de la Société de l'assurance automobile du Québec,
M. Jacques Brind'Amour

M. Brind'Amour (Jacques): Merci, Mme la Présidente. D'abord, merci de nous recevoir. On est très heureux d'être ici. Peut-être effectivement que je pourrais vous présenter brièvement les gens qui m'accompagnent. Alors, à ma droite, Michel Léveillé, qui est le directeur général des technologies de l'information, et Mario Trudel, qui est le responsable, le coordonnateur, si vous voulez, de la sécurité de l'information numérique à la société. Je vais peut-être vous présenter aussi les personnes qui sont à l'arrière.

La Présidente (Mme Dionne-Marsolais): Pourraient-elles se lever à l'appel de leur nom?

n *(17 heures)* n

M. Brind'Amour (Jacques): Oui, bien sûr. Alors, Me Claude Gélinas, qui est le directeur du Secrétariat des affaires juridiques et qui est responsable évidemment, là, de la protection des renseignements personnels, accès à l'information, etc.; Alain Collerette, qui est le directeur général du registre de l'expertise et du pilotage, donc c'est le registraire de la société; Mme Renée Martineau Beaulieu, qui est la directrice des ressources matérielles et immobilières.

La Présidente (Mme Dionne-Marsolais): Bonjour, Madame.

M. Brind'Amour (Jacques): Martine Boucher, qui est la chef du Service de gestion et de sécurité informatique, Direction générale des technologies de l'information. Mme Boucher. On a également M. Crépin, Raynald Crépin, qui est vérificateur, qui est de notre Direction de la vérification et des enquêtes; Jean-Guy Bordeleau, qui est le responsable du plan de sécurité à la Direction des ressources matérielles; et Daniel Fortin • il est ici? Oui • qui est architecte en sécurité informatique et de la Direction des... technologies, pardon, de l'information.

La Présidente (Mme Dionne-Marsolais): Alors, la liste n'est pas tout à fait la même, hein?

M. Brind'Amour (Jacques): Pardon? Ah, non, ce que vous avez, c'est la liste des membres du Comité de sécurité de l'information.

La Présidente (Mme Dionne-Marsolais): Ah, d'accord, d'accord.

Une voix: ...

La Présidente (Mme Dionne-Marsolais): Ah, c'est parce qu'on ne l'a pas. O.K. On les a notés, là. Ça va, là. Parce qu'on n'avait pas les noms...

M. Brind'Amour (Jacques): Si vous le souhaitez, je peux vous la déposer la...

La Présidente (Mme Dionne-Marsolais): Ah, vous l'avez?

M. Brind'Amour (Jacques): Oui, oui.

La Présidente (Mme Dionne-Marsolais): Bon, parfait. Peut-être que vous pouvez... On va la déposer. On en fera des copies pour tout le monde. Merci, M. Brind'Amour. Alors, on vous écoute.

M. Brind'Amour (Jacques): Alors donc, merci de nous accueillir pour un sujet, là, qui pour nous, à la Société de l'assurance automobile, est évidemment une question primordiale. Nous avons consacré au cours des dernières années des efforts importants et soutenus en sécurité informatique. Ainsi, à titre administratif simplement, au cours des quatre dernières années, des investissements de plus de 8,4 millions de dollars ont été réalisés pour améliorer notre sécurité, à la fois notre sécurité informatique, à la fois sécuriser l'émission des permis de conduire et améliorer la sécurité des biens et des bâtiments.

Je voudrais simplement ajouter, pour vous donner une idée de ce que ça représente chez nous: Sur une base récurrente annuelle, nous investissons, en termes de personnes et d'équipements pour assurer la gestion au jour le jour, environ 3,3 millions de dollars de coûts.

Alors, permettez-moi peut-être de rappeler brièvement les actions que nous avons entreprises, à la société, concernant la gestion de la sécurité informatique de ses installations, de ses biens et de ses dossiers. En 1992, la société s'est dotée d'une politique de sécurité informatique, et un coordonnateur a été chargé de la faire appliquer.

En 1998, la société a participé à l'étude Marion, que vous connaissez bien, sur l'état de la sécurité informatique. Initiée par la Commission d'accès à l'information, cette démarche est en effet à l'origine de la révision de la directive gouvernementale qui s'applique à l'ensemble des ministères et organismes.

En 1999, dès l'adoption de la Directive sur la sécurité de l'information numérique et des échanges électroniques, nous avons nommé un responsable de la sécurité de l'information numérique et évidemment participé aux travaux du Comité d'orientation stratégique de la sécurité. Et en 1999 le président-directeur général d'alors a regroupé en un seul comité le Comité sur la sécurité informatique et celui sur la protection des renseignements personnels, et c'est devenu le Comité sur la sécurité de l'information.

En l'an 2000, à la suite d'événements médiatisés entourant des fuites de renseignements dont les journaux avaient abondamment parlé à l'époque, la Commission d'accès à l'information avait examiné les mesures de sécurité informatique en place à la société. Pour tenir compte du rapport de la commission, nous avions alors renforcé la gestion des mots de passe et révisé les accès informatiques que nous consentons à 5 010 codes d'utilisateurs. Donc, c'est 5 000 personnes environ, là, qui ont accès à nos systèmes. Cet exercice avait permis d'ajuster déjà 36 % des règles d'accès. Nous avons également modifié à cette période notre approche en matière d'investigation des gestes, donc tous les gestes qui font l'objet de consultations ou de modifications sur nos systèmes, ce que le Vérificateur désigne dans son rapport sous le thème de *Suivi de l'activité des systèmes*.

Depuis 2001, certaines mesures de sécurité mises de l'avant, particulièrement en matière de sécurité de l'information, dépassent en ce sens les exigences gouvernementales. Ainsi, nous avons mis en place un système de portillons, à titre d'exemple, pour contrôler chaque entrée et sortie du personnel, fournisseurs et visiteurs, ce qui a complété d'autres mesures qui visent à protéger l'accès au siège social où se trouve le centre de traitement informatique de la société.

La protection des personnes est également au centre de nos préoccupations. Nous avons donc voulu assurer davantage la sécurité de nos lieux de travail. Les accès physiques ont été resserrés. La surveillance a été accrue à la fois au siège social et dans l'ensemble de nos lieux de travail. L'ensemble de nos lieux de travail, évidemment, c'est nos 45 centres de services notamment, plus les locaux que nous louons un peu partout sur le territoire. Des plans et des guides d'intervention illustrent aussi comment on doit faire face à des situations d'urgence, et nous avons mis à jour notre plan de mesures d'urgence, et l'ensemble du personnel en a reçu une copie.

Comme vous le savez sans doute, on remarque • le Vérificateur pourrait vous le confirmer, je crois; on remarque • que la plupart des incidents dans le domaine de la sécurité informatique proviennent de l'intérieur des organisations. Pour diminuer ce type de risques, nous avons évalué, ces dernières années, les employés contractuels les plus exposés et nous avons exigé que plus de

500 employés qui agissent, qui travaillent chez nos mandataires en permis et «immat» ainsi que 32 de nos contractuels en technologies de l'information soient accrédités, donc qu'ils fassent l'objet d'une enquête, pour accéder à nos systèmes et à nos installations. On a également une habilitation de sécurité, là, pour les personnes qui font des tâches d'entretien ménager et pour les agents de sécurité. Nous avons débuté, il y a quelques mois, des travaux pour identifier parmi les postes occupés par notre personnel les postes qui sont les plus sensibles et qui devraient faire l'objet de vérifications similaires avant l'engagement des personnes, notamment pour le personnel de la société qui pourrait être engagé en recrutement.

Afin d'assurer la protection des renseignements personnels et la sécurité informatique, nous avons aussi multiplié les activités de sensibilisation et de formation auprès de notre personnel. En 2002, la très grande majorité des employés de la société assistaient à des séances de sensibilisation portant à la fois sur la protection des renseignements... personnels, pardon, et la sécurité informatique. Suite à ces séances, 95,7 % des employés ont signé volontairement une déclaration de discrétion qui représente, par rapport au serment d'office qu'ils font à la fonction publique, donc un nouvel engagement au respect des règles de confidentialité et d'utilisation des accès informatiques. Je vous signale qu'on a gagné un prix pour notre action en ce sens.

La protection des personnes s'accompagne évidemment d'une protection des biens et des outils stratégiques. À la suite de 27 vols d'équipements et de fournitures reliés à la production des permis de conduire, vols qui se sont réalisés en 2001 et 2002, et afin de sauvegarder l'information qu'ils contiennent et de contrer la fraude, ces équipements ont été retirés de nos points de service, et c'est maintenant à l'intérieur du centre de traitement informatique de la société que sont produits les permis depuis septembre 2002.

Également, depuis 1999, des coupe-feux protègent le réseau informatique des réseaux potentiellement hostiles, tel Internet. Des logiciels spécialisés installés en 2001 surveillent en permanence notre réseau et signalent tout comportement inhabituel. Des vérifications continues nous assurent du bon fonctionnement de l'ensemble de ces contrôles en se basant sur les vulnérabilités et les possibilités d'attaques connues. Même, depuis 1999, on peut dire que la configuration des postes de travail limite les risques d'attaques par ces milieux hostiles.

En cas de sinistre au siège social, la société dispose depuis 1996 d'un plan de reprise informatique. Nous pourrions donc, s'il y avait un désastre ou s'il y avait quelque chose de majeur, reprendre les activités essentielles dans un délai de 72 heures, avec des ententes qu'on a avec des partenaires. Je n'insiste pas, là, ça semble évident. On planifie, également, des tests deux fois par année et, depuis peu, là, on a des tests d'escalade fortuits pour vérifier notre capacité à mobiliser notre personnel si de telles nécessités empêchaient le siège social, et donc les systèmes informatiques, de fonctionner.

Le rapport du Vérificateur général mentionne que l'information numérique et les échanges électroniques sont bien protégés par la Société de l'assurance automobile du Québec contre les menaces les plus répandues. Le Vérificateur reconnaît l'expertise et l'implication des employés de la société ainsi que la qualité des technologies en place. Il remarque que la société dispose, je reprends ses termes, «d'une bonne capacité d'intervention» et «d'une bonne partie des gestes attendus». On a bien compris que ce n'étaient pas tous les gestes attendus, mais une bonne partie des gestes attendus.

Bien que nous fassions tout ce qui est nécessaire pour respecter les règles de l'art en sécurité informatique, le présent rapport du VG fait état de certaines lacunes. Je précise que la majorité d'entre elles nous étaient connues et que, dans la plupart des cas, des mesures étaient déjà entreprises pour remédier à la situation.

La démarche de vérification entourant l'application du rapport a amené la révision de l'ordonnancement de nos priorités. Dès le 21 juin, soit moins de deux semaines après le dépôt du rapport, la direction de la société a approuvé un plan d'action qui recense les interventions requises et les délais de réalisation. Ainsi, la mise en oeuvre du registre d'autorité de la sécurité de l'information sera l'occasion pour nous de préciser notre gouvernance en ce domaine et d'assigner les responsabilités en matière de sécurité informatique. Je vous informe d'ailleurs, comme je vous le disais tout à l'heure, que nous avons créé une fonction de registraire unique pour assurer l'intégrité et la confidentialité de l'information concernant notre clientèle. Nous avons également nommé les trois principaux détenteurs d'actifs et procédé à une catégorisation sommaire. Donc, nous avons, à ce stade-ci, déterminé la valeur de leurs attributs de sécurité... que chacun de ces détenteurs détient pour nos principaux systèmes d'information.

La sécurité est un domaine, vous le savez, qui exige de demeurer à l'affût des nouveaux risques et des nouvelles vulnérabilités ainsi que des opportunités pour revoir nos façons de faire. C'est pourquoi nous sommes d'accord avec le Vérificateur général pour doter la société d'une stratégie d'évaluation périodique de la menace et des risques, et non pas seulement aveugle. Nous avons donc entrepris des travaux pour dresser un nouveau diagnostic dans notre sécurité informatique et pour intégrer la méthode gouvernementale MEHARI à nos pratiques de gestion. Cette approche est déjà utilisée pour apprécier les risques associés à l'introduction de nouveaux services ou de nouvelles technologies.

Une révision de la démarche de planification et d'établissement des priorités pour les interventions en sécurité est également

prévue en 2005. Cette démarche tiendra compte des recommandations du Vérificateur général et des résultats de l'évaluation de la menace et des risques.

Toujours dans le domaine de la gestion des risques, nous procéderons à une catégorisation des infrastructures critiques de manière à nous assurer que toutes les mesures soient prises pour sécuriser adéquatement les équipements sensibles.

n *(17 h 10)* n

En ce qui a trait au maintien de la sécurité au sein de notre personnel, nous comptons agir sur deux fronts. D'abord, les accès informatiques consentis aux utilisateurs de nos systèmes d'information, accès qui ont tous été requestionnés en 2003, seront dorénavant vérifiés sur une base continue. Et, sous réserve des lois et des conventions collectives, ce dont je vous parlais tout à l'heure, nous adopterons les mesures nécessaires pour vérifier l'intégrité des personnes qui postulent certains postes, une pratique donc qui est déjà en vigueur pour d'autres types d'intervenants qui ont accès à nos systèmes.

En matière de sensibilisation et de formation, nous prévoyons consigner dès la fin de cette année l'ensemble des interventions à l'intérieur d'un plan spécifique qui sera évidemment évalué.

En 2005, nous compléterons notre stratégie en matière de continuité du service en cas de sinistre par l'ajout de mécanismes de reprise à la plateforme intermédiaire; jusqu'à maintenant, c'était uniquement à la plateforme centrale. Cette démarche était entreprise au moment d'ailleurs où le Vérificateur est passé.

Enfin, je peux vous annoncer que nous avons déjà effectué cet automne des correctifs mineurs nécessaires pour mieux gérer l'utilisation des mots de passe. Ces changements s'appliquent à notre personnel ainsi qu'à l'ensemble des utilisateurs du système d'information.

Alors, voilà, Mme la Présidente, pour l'essentiel, en guise d'introduction, ce que j'avais à vous dire.

La Présidente (Mme Dionne-Marsolais): Bien, je vous remercie beaucoup de ces commentaires, et on a aussi reçu le sommaire de votre plan d'action, qui a été transmis aux membres de la commission. Et, comme vous l'avez bien indiqué, je crois que le Vérificateur général concluait que l'information numérique et les échanges électroniques étaient généralement bien protégés, et donc c'est rassurant. En contre-partie, il soulignait que la protection reposait beaucoup plus sur des dimensions humaines et technologiques que sur la dimension organisationnelle et qu'il y avait des lacunes à combler. Vous en avez soulevé quelques-unes, avec les correctifs que vous avez proposés, mais néanmoins nous avons certaines préoccupations, au fur et à mesure évidemment où les ambitions du gouvernement du Québec sont de servir mieux les citoyens en ligne.

Je vais donc procéder de la façon suivante. On va avoir une discussion avec vous, 10 minutes chaque côté, du côté du gouvernement, du côté de l'opposition, deux fois. Et je vais commencer par le député de Verdun.

Discussion générale (suite)

M. Gautrin: Je vous remercie, Mme la Présidente. Encore là, comprenez-moi bien, les questions qu'on vous pose, ce n'est pas pour contester la sécurité qui existe globalement. Donc, on est rendus réellement dans des questions un peu plus pointues et qui viennent tâcher ici de s'assurer que vous corrigez certaines inefficacités au niveau de la sécurité, mais nous ne remettons pas en cause globalement la sécurité informatique à la SAAQ.

J'ai des questions sur lesquelles j'ai un peu de difficultés à comprendre dans votre rapport. Je vais revenir donc sur la continuité des services. À la page 8 de votre rapport, vous dites: En cas de sinistre au siège social, depuis 1996, un plan de reprise informatique • je comprends bien que c'était sur la plateforme centrale, c'est bien ça? • vous permettait de reprendre les activités en 72 heures. Vous nous dites aussi, en page 13, deuxième paragraphe: «Au cours de l'année 2005, nous compléterons notre stratégie en matière de continuité du service en cas de sinistre par l'ajout de mécanismes de reprise sur la plateforme... [sur les plateformes intermédiaires].» Mais vous dites: «Cette démarche était [déjà] entreprise au moment du passage du Vérificateur général.» Alors, le Vérificateur général est passé chez vous à quelle date à peu près? En 2004?

La Présidente (Mme Dionne-Marsolais): M. le Vérificateur général, en 2004?

M. Gautrin: Alors, moi, ce que... Ma question, c'est un peu une question de temps. Je m'étonne que ça vous prenne tant de temps pour corriger quelque chose que vous avez déjà commencé à corriger. Et dans le document que vous nous déposez ici, l'ajustement

Gestion de la continuité • Reprise des activités essentielles, la mise en place de la reprise informatique, pour les nouvelles technologies et l'ajustement des ... vous aviez un objectif, décembre 2005, ce qui à mon sens me semble très long, si vous avez déjà commencé au début 2004. Alors, ma question, c'est: Pouvez-vous nous expliquer pourquoi, si vous aviez déjà commencé à faire les corrections sur les plateformes intermédiaires, ça prend tant de temps pour en arriver à la correction en ce qui a trait à la continuité du service?

M. Brind'Amour (Jacques): Écoutez, peut-être que...

La Présidente (Mme Dionne-Marsolais): M. le président-directeur général. Excusez-moi.

M. Brind'Amour (Jacques): Excusez-moi, madame. Peut-être que ma façon de présenter les choses était inadéquate. Ce que nous avions amorcé, au moment du passage, c'est les études. Bon, maintenant, vous savez, c'est une question de priorité. C'est important, une plateforme intermédiaire, mais ce n'est pas aussi important que la plateforme centrale.

M. Gautrin: Oui, mais la plateforme centrale, elle n'était pas à corriger...

M. Brind'Amour (Jacques): Non.

M. Gautrin: ...puisque depuis 1996 la plateforme centrale était opérationnelle en cas de sinistre.

M. Brind'Amour (Jacques): Oui. Ce que je veux dire, c'est qu'en cas de reprise, en cas de sinistre, là, ce qui est important pour nous, c'est de protéger la plateforme centrale. Je vais vous donner peut-être un exemple...

M. Gautrin: Quelle est la fonction de la plateforme centrale par rapport aux plateformes intermédiaires, peut-être, pour qu'on comprenne mieux?

M. Brind'Amour (Jacques): Oui, c'est ça. Bien, je vais vous expliquer, tiens. Disons que les bases de données sensibles sont toutes sur la plateforme centrale. Elles sont protégées dans un environnement, là, c'est quasiment inattaquable, je crois. La plateforme intermédiaire, pour donner un exemple, c'est pour les données... Exemple, en prestation électronique de services, tiens, nous avons des ententes avec des concessionnaires automobiles, qui peuvent depuis peu, à partir de leur lieu, faire une transaction avec la SAAQ. La transaction qu'ils font, ce n'est pas un accès à un fichier. Ce qu'ils font, c'est qu'ils vont rentrer la donnée qui permet à la personne sur place, au lieu d'aller ailleurs... Donc, elle rentre la donnée, et cette donnée-là va être entrée sur une plateforme intermédiaire, un serveur, oui, plateforme intermédiaire qui, elle, va répercuter à la plateforme centrale: Pourriez-vous changer les informations que ce monsieur vient de me transmettre? La plateforme centrale va retourner à la plateforme intermédiaire pour dire: C'est fait. Et lui, il va recevoir de la plateforme intermédiaire le O.K.

S'il y avait un sinistre, les données centrales sont protégées. Les autres données, c'est des données qui peuvent être récupérées autrement. Exemple, si la transaction de l'individu ne se fait pas, bien elle va se faire le lendemain ou autrement. C'est ça un peu, là, qui fait que, en termes de priorités qu'on a à réaliser, là, par rapport à ça et d'autres, bien ça nous a donné jusqu'à décembre 2005, parce que ça ne remet pas en question, là, si vous voulez, l'essentiel de ce qu'on fait.

M. Gautrin: Deuxième question. Vous avez été, dans le rapport du Vérificateur général, aussi interpellés quant à la classification des actifs informationnels. À moins que je ne voie pas bien et que ce soit inscrit sur un élément différent, dans la gestion de la sécurité informatique, je ne vois pas d'élément pour corriger ce qui a été perçu comme une lacune actuellement par le Vérificateur général. Je ne vous lirai pas actuellement 4.62, je l'ai lu tout à l'heure, et la recommandation qui s'ensuivait: Nous avons recommandé au ministère du Revenu ainsi qu'à l'assurance automobile et à la Régie de l'assurance maladie «de s'assurer que les mesures de sécurité relatives aux systèmes et aux infrastructures [...] prennent en compte les principaux risques informatiques auxquels ils sont exposés.» Et on faisait appel évidemment à la classification des actifs informationnels. Et, dans le document que vous nous avez remis ce matin, je n'ai pas vu, à moins que ce soit indiqué à un autre endroit, une volonté de votre part de corriger cet élément-là.

La Présidente (Mme Dionne-Marsolais): Oui, M. le président-directeur général.

M. Brind'Amour (Jacques): Alors, oui, sous le volet registre d'autorité. Alors, vous...

M. Gautrin: Alors, sous le volet registre d'autorité, c'est là que ça se trouvait? Ah bon.

M. Brind'Amour (Jacques): Exact. Alors, vous voyez que... Vous savez, comme le signalait le Vérificateur général, nous avons une classification qui existe déjà pour nos systèmes informatiques, mais elle n'existe pas pour nos bases de données, pour nos à faire, d'ici février 2005, c'est la phase I, et ensuite infrastructures informatiques. Donc, ce qu'on s'est engagé, voyez-vous, là, juin 2005, décembre 2005, donc l'ensemble des quatre phases qui vont nous permettre d'avoir un registre d'autorité complet qui à ce moment-là, je pense, va répondre aux préoccupations du Vérificateur non seulement au niveau des inventaires des actifs les plus critiques, qui doivent être protégés, mais aussi qui sont les responsables d'actifs, comment se fait l'attribution des droits d'accès, est-ce qu'ils devront être révisés, etc.

M. Gautrin: Donc, dans le registre d'autorité, tel que vous le voyez, la classification des actifs informationnels, tel qu'il est écrit actuellement, et vous voyez qu'est-ce que ça veut dire, la classification...

M. Brind'Amour (Jacques): Oui, bien sûr.

M. Gautrin: ...question de sécurité, effectivement.

M. Brind'Amour (Jacques): Oui, modéré...

M. Gautrin: Ceci est inclus, et on devrait le voir en phase II. Est-ce que c'est ça que ça voulait dire?

M. Brind'Amour (Jacques): Phase I: l'inventaire. Phase II: l'évaluation. Oui.

M. Gautrin: O.K. Est-ce que ça répond à votre questionnement?

La Présidente (Mme Dionne-Marsolais): M. le Vérificateur général, est-ce que vous êtes satisfait de cette réponse-là? D'accord. M. le député de Verdun.

M. Gautrin: Alors, est-ce que vous pourriez... Si je comprends bien, ce sera terminé en février 2005, cet élément-là?

M. Brind'Amour (Jacques): L'inventaire, oui.

M. Gautrin: Alors, je me permets de faire la même demande que j'ai demandée au ministère du Revenu: pouvoir nous informer lorsque vous aurez terminé cet élément de classification.

M. Brind'Amour (Jacques): Avec plaisir.

M. Gautrin: Je crois que mon collègue de Montmorency voulait parler.

La Présidente (Mme Dionne-Marsolais): M. le député de Montmorency.

M. Gautrin: Oui, une question, quitte à ce que je puisse revenir après...

M. Bernier: Alors, bonjour, M. Brind'Amour. M. Léveillé, M. Trudel, bienvenue. Alors, comme mon collègue l'a mentionné, le but n'est pas de mettre en doute les aspects sécuritaires de la société mais davantage de s'assurer que les recommandations du Vérificateur ont été ou sont en processus de mise en fonction.

En ce qui regarde la société, vous comprenez que les questions vont porter dans un premier temps au niveau de vos ressources humaines et l'intégrité des personnes. C'est que, bon, il y a eu une problématique en ce qui regarde ces différentes personnes à un moment donné. Donc, ça a été mentionné dans le cadre de la vérification que, en ce qui regarde la prudence, au niveau de l'évaluation et de l'intégrité du personnel qui doivent être mises en place au niveau de la société ou de d'autres organismes, il n'y a pas de règles précises au niveau de la fonction publique. C'est l'organisme ou le ministère qui doit déterminer quelles sont les mesures qu'ils doivent mettre en place.

n *(17 h 20)* n

Donc, si je regarde, au niveau des plans d'action que vous nous avez déposés suite au rapport du Vérificateur, on parle, au niveau habilitation des personnes, d'un projet pilote pour le contrôle d'intégrité des employés, qui est en cours de réalisation, on parle de novembre 2004, de mise en oeuvre du contrôle de l'intégrité des employés • une application graduelle • donc dans le but de

sécuriser les gens qui transigent avec la Société d'assurance automobile. J'aimerais vous entendre sur le sujet en ce qui regarde votre plan, vos processus, votre mise en fonction pour assurer l'intégrité du personnel de la société.

La Présidente (Mme Dionne-Marsolais): M. Brind'Amour.

M. Brind'Amour (Jacques): Oui. D'abord peut-être de dire, là, que, lorsqu'on accueille un nouvel employé à la société, on prend un certain nombre de mesures, là, dans ce qu'on appelle la journée d'accueil. Donc, dès qu'il est accueilli, il doit signer une déclaration de discrétion. Donc, il s'engage à ne pas divulguer l'information dont il pourrait avoir la possession. À cette même journée d'accueil, évidemment, là, on lui donne une formation sur la Loi d'accès, sur la protection des renseignements personnels, et on insiste, avec des exemples, sur l'importance de la protection des renseignements personnels et des sanctions qui pourraient en résulter. Et d'ailleurs on l'incite même à faire appel au service d'aide au personnel quand il a des problèmes.

On a constaté souvent qu'un employé qui a un comportement qui est non conforme, c'est souvent lié à deux choses. Soit la curiosité: il se sert des fichiers auxquels il a accès pour vérifier, des fois, qui habite dans sa rue, etc., des choses comme ça. On a constaté des choses comme ça. L'autre chose qu'on a constatée souvent • et là c'est dans le cas de gens qui vont vouloir le faire contre une rémunération ou contre un avantage pécuniaire • c'est des gens qui ont des difficultés personnelles, soit eux, soit leur entourage, et tout ça, et, là encore, ce qu'on fait, c'est qu'on leur dit: Écoutez, avant d'arriver là puis de perdre votre emploi ou d'être sanctionné de façon où vous ne trouverez plus d'emploi, on a des services qui peuvent vous aider. Bon. Alors ça, c'est des choses qu'on leur explique dès le départ.

Ensuite, on détermine quels sont leurs droits d'accès. Tout le monde n'a pas accès aux mêmes choses. On donne des droits d'accès qui sont limités à ce à quoi les gens auront besoin pour exercer leurs tâches. C'est le supérieur immédiat qui détermine la nature des droits. La plupart du temps, évidemment, dans une boîte donnée, on va retrouver à peu près sensiblement les mêmes droits lorsque les gens sont dans des tâches d'opération. Et l'employé, lui aussi, doit, si vous voulez, signer un formulaire où il s'engage à ne pas diffuser ou à faire utiliser par d'autres son droit d'accès. C'est à peu près ce qu'on a avec l'ensemble du personnel.

On a une particularité pour le contrôle routier. Vous savez que les contrôleurs routiers, ce sont des gens qui sont des agents de la paix. Alors, on a une procédure d'enquête qui est sensiblement la même que pour les policiers, donc c'est une enquête de sécurité. Ce n'est pas seulement de vérifier l'antécédent judiciaire, c'est aussi de vérifier dans son environnement, pendant le questionnaire, etc.

Une voix: ...

M. Brind'Amour (Jacques): Pardon?

La Présidente (Mme Dionne-Marsolais): Oui, monsieur...

M. Bernier: ...au niveau antécédents, justement, au point de vue du personnel de l'ensemble de la SAAQ, est-ce qu'il y a des validations qui sont faites au niveau des antécédents?

M. Brind'Amour (Jacques): On n'a pas ça. On ne le fait pas. On le fait pour le personnel qui travaille chez les mandataires. C'est nous qui faisons cette validation. On leur donne aussi la formation. On le fait pour des personnes contractuelles qui ont accès à des systèmes sensibles. Mais ce qu'on est en train de faire, comme on le disait peut-être un peu trop rapidement tout à l'heure, c'est de définir quels sont nos emplois sensibles dans la société et comment à l'avenir nous allons procéder pour que ces emplois sensibles là soient vérifiés. Et, quand je faisais référence à des conventions collectives, rapidement, ce que je voulais dire, c'est qu'on a mis nos syndicats dans le coup de ça pour leur expliquer les raisons. Ils comprennent très bien les raisons, et ce qu'ils nous disent, c'est: Bien, écoutez, si vous voulez le faire pour toute nouvelle personne que l'on recrute qui n'est pas au gouvernement, nous, on n'a pas de problème, mais, si c'est pour des personnels qui sont déjà engagés dans la fonction publique du Québec depuis x années et qui donc ont fait une preuve qu'ils avaient un comportement acceptable et correct, on aurait peut-être un petit problème. Voyez-vous?

M. Bernier: ...sur ce plan, il reste qu'au moment où vous embauchez une personne qui provient de la fonction publique vous avez quand même le dossier qui provient de l'autre ministère ou d'autres organisations qui vous est transmis, puis à ce moment-là ça vous permet de valider quand même certains points en ce qui a...

M. Brind'Amour (Jacques): ...des questions liées à la sécurité ou à l'antécédent, et tout ça, là, ce n'est pas...

Une voix: ...

M. Brind'Amour (Jacques): Non.

M. Bernier: O.K.

M. Brind'Amour (Jacques): Donc, c'est ce qu'on fait actuellement, et notre objectif est, comme je vous le disais, au cours de l'année, d'arriver avec une politique pour au moins le personnel que nous aurons recruté.

Une voix: D'accord.

La Présidente (Mme Dionne-Marsolais): Alors, M. le député de Beauharnois.

M. Lelièvre: ...juste vérifier si M. Brind'Amour peut prendre 30 secondes pour nous dire...

La Présidente (Mme Dionne-Marsolais): Bien là j'ai donné la parole au député de Beauharnois.

Des voix: Ah, bien allez-y, madame...

La Présidente (Mme Dionne-Marsolais): Voulez-vous passer votre droit de parole, M. le député de Beauharnois?

M. Deslières: Bien, est-ce qu'on peut permettre à mon collègue...

La Présidente (Mme Dionne-Marsolais): Bien sûr. M. le député de Gaspé.

M. Deslières: ...le sujet, peut-être.

La Présidente (Mme Dionne-Marsolais): D'accord. M. le député de Gaspé.

M. Deslières: Oui, on va régler ça.

M. Lelièvre: Est-ce que la société fait des vérifications aux plumitifs des palais de justice pour s'assurer qu'il n'y a pas de dossier judiciaire?

M. Brind'Amour (Jacques): Bien, comme je le disais, on le fait pour le personnel qui travaille chez nos mandataires. Il y en a à peu près 500, personnes, là. Il y a un certain roulement. Alors ça, on le fait pour ce personnel-là. On le fait évidemment pour le contrôle routier, mais pas pour les employés de la société.

Une voix: Le personnel d'entretien.

M. Brind'Amour (Jacques): Oui, mais pas pour les employés de la société. Ah, bien, on le fait...

La Présidente (Mme Dionne-Marsolais): Ah, pour le personnel d'entretien.

M. Brind'Amour (Jacques): ...pour nos agents de sécurité, notre personnel d'entretien, oui, mais pas pour nos employés qui ont accès à des fichiers sensibles, pour le moment.

La Présidente (Mme Dionne-Marsolais): D'accord. Alors, M. le député de Beauharnois.

M. Deslières: Merci, Mme la Présidente. M. Brind'Amour, mesdames, messieurs, c'est toujours un plaisir de vous revoir. Je sais qu'on va se voir toute la journée demain aussi. C'est toujours un plaisir.

Une voix: ...

M. Deslières: Oui, mais je pense qu'on va avoir l'occasion d'en profiter longuement au cours des prochains jours.

Alors, ma question, M. Brind'Amour, une question d'ordre général et global. Le Vérificateur général débarque chez vous, fait une vérification, dépose son rapport. À part les moyens et les compétences, je pense que c'est une question d'attitude face à cet élément

de sécurité informatique. Quelle a été chez vous la réaction de votre personnel face à l'ensemble des éléments constatés et des recommandations? Quelle attitude qu'on a eue, là, face à l'ensemble du rapport concernant la société, à date, chez vous?

La Présidente (Mme Dionne-Marsolais): M. Brind'Amour.

M. Brind'Amour (Jacques): Vous savez, nous, depuis plusieurs années, on accueille, plusieurs mois par année, les gens du Vérificateur. Et, avec nos états financiers, avec tout ce qu'ils vérifient, on est souvent une organisation qui est vérifiée quand il y a des mandats...

Une voix: D'envergure.

M. Brind'Amour (Jacques): ...des mandats d'envergure. Donc, on est habitués de les recevoir. On les reçoit toujours bien, je crois, je pense.

Non, je pense que les gens n'étaient pas fermés à ça du tout, au contraire. Vous savez, même si nous sommes une organisation qui opère un nombre assez impressionnant de transactions annuelles... On parle de 17 millions de transactions annuelles, là, qui touchent 4,7 à 5 millions de personnes. C'est beaucoup, là. Probablement qu'on est, avec le ministère du Revenu, les deux organismes qui ont le plus de contacts avec les individus sur une base annuelle. Même à ça, ça ne veut pas dire qu'il y a une culture de sécurité qui est implantée depuis des années dans des organisations comme ça. Les organismes publics au Québec n'ont pas une culture de sécurité implantée. Les employés, là, qui sont engagés, qui viennent travailler, des fois ils sont un peu surpris quand au départ on les met en garde puis on... Ils n'ont pas ce réflexe de dire: Oui, c'est vrai, c'est important, là, les renseignements personnels des individus, etc.

Donc, je pense qu'on a été bien reçus. Et puis, moi, je vous dis, je le disais tout à l'heure, il y a beaucoup de problèmes qu'on avait déjà identifiés. Le problème de la sécurité informatique, on le sait, tout le monde dit que c'est un bon investissement, mais c'est coûteux comme investissement. Il n'y a pas de doute, là, que très rapidement on fait un rapport d'affaires, on est à 500 000 $, 600 000 $, puis là on ajoute quelque chose, on est rendus à deux, trois, quatre millions. Ça s'ajoute à d'autres priorités. Donc, c'est évident que le rythme d'implantation d'un certain nombre de mesures peut des fois être un petit peu attaqué par ça.

La Présidente (Mme Dionne-Marsolais): M. le député de Beauharnois.

M. Deslières: ...vous donner votre note de passage tout à l'heure, là, ils l'ont fait tantôt.

Sans vouloir remettre la sécurité des systèmes informatiques en jeu... Parce que je pense que des deux côtés on l'a mentionné, mon collègue de Verdun l'a mentionné... Mais il reste que, dans le rapport du Vérificateur, on parle de lacunes, on parle de faiblesses, on parle de failles, on parle d'imprudences dans certains éléments. Puis je vais y venir, là.

Je regardais globalement le rapport, qui nous a été présenté, du Vérificateur et, au niveau de l'encadrement, trois éléments sur quatre où on a constaté des lacunes, des faiblesses, des failles. Concernant le dispositif de sécurité, 13 éléments sur 18 ont été constatés en faiblesse, lacune, tout ça. Et là vous nous dites que c'est quand même priorité puis que... Je veux bien camper ma question, là, hein. Je ne veux pas alarmer, rien, mais il reste que, quand même, un élément pris au hasard ou comme ça, c'est une chose. On va dire: Bon, bien, écoute, on va le corriger, ce n'est pas majeur. Mais, quand on regarde l'ensemble de ces éléments-là, ça commence à être imposant, ça commence à être questionnable, là, je veux dire. On dit: Woup, là, attends un peu, là! Sans aller, encore une fois, là, remettre en cause la sécurité des systèmes informatiques à la SAAQ... Mais sauf que, là, il y a, je trouve, beaucoup d'éléments qui demandent des corrections et de le faire assez rapidement. Et je reviendrai sur une autre question. Je vous laisse...

La Présidente (Mme Dionne-Marsolais): M. Brind'Amour.

n *(17 h 30)* n

M. Brind'Amour (Jacques): Oui. Vous avez raison. Évidemment, il faut voir sur quoi portaient les recommandations du Vérificateur. Je crois aussi que le Vérificateur a dit que peut-être qu'on n'a pas un registre unique, centralisé, peut-être qu'on n'a pas ci, peut-être qu'on n'a pas ça. Peut-être donc qu'au niveau de certains processus, de certaines façons de travailler, ce n'est pas parfait. Et je pense qu'il a aussi dit: Ce que j'ai constaté à la fin, c'est qu'ils ont agi.

Exemple, on a trois détenteurs d'actif. Les trois ont la responsabilité, dans chacun de leur domaine, d'agir et de corriger les lacunes.

Oui, c'est vrai, on n'a pas un registre qui est actuellement centralisé. Il va l'être en 2005, là, mais il ne l'est pas. Mais ça ne veut pas dire que, dans ces domaines-là, ils n'ont pas agi, voyez-vous?

On dit, par exemple... Le comité de sécurité de l'information, on dit: Il s'est penché sur beaucoup trop d'aspects opérationnels et pas assez stratégiques. Moi, je peux vous dire, quand je suis rentré là, ce qui m'a frappé, c'est qu'il fallait se pencher sur des aspects opérationnels pour faire des aspects stratégiques. Donc, on s'est penché sur ce qu'on a constaté comme problèmes qu'il fallait corriger, voyez-vous?

Alors, moi, je pense que, oui, c'est vrai qu'on a des lacunes, si on regarde les recommandations au niveau... on n'a pas toujours bien identifié ça, on n'a peut-être pas bien catégorisé tout ça, mais je pense qu'on a fait la preuve par nos actions qu'on s'est assurés en tout temps, en tout temps, de préserver nos actifs sensibles, et c'est ce que j'ai retenu aussi.

La Présidente (Mme Dionne-Marsolais): M. le député de Beauharnois.

M. Deslières: Je vous entends, M. le président, puis je vous écoute, là, mais je vais vous apporter sur un point... je vais revenir sur un point bien précis, au niveau de l'habilitation des personnes. Dans le rapport du Vérificateur, à 4.66, on nous dit: «D'abord, la SAAQ et la RAMQ ne font pas preuve d'assez de prudence relativement à l'intégrité des employés qu'ils embauchent», «qu'ils» au pluriel. Deuxième élément: «Ensuite, l'attribution des droits d'accès ne s'appuie pas sur une classification adéquate de l'ensemble des informations», on parle que c'est trop primaire, tout ça.

Alors, c'est des éléments importants, quand on fait référence, et vous en avez fait... vous avez fait vous-même référence dans votre présentation aux événements de 2000. Alors ça... Il y avait eu 2000, puis il vient d'y avoir le Vérificateur. Là, qu'est-ce qui s'est passé entre ça? Et là, même là, on le signale que, sur ça, il y a des lacunes. Sur cet élément-là, moi, je vais vous dire bien franchement, entre parenthèses, je suis très surpris de voir ça dans le rapport du Vérificateur.

La Présidente (Mme Dionne-Marsolais): M. Brind'Amour.

M. Brind'Amour (Jacques): Écoutez, tout ce que je peux vous répondre, c'est: effectivement, nous avons des lacunes et nous tentons de les corriger, c'est vrai. Depuis maintenant deux ans, un peu moins de deux ans, nous faisons aussi de la journalisation de nos activités. L'ensemble des gestes qui sont posés sont journalisés, c'est-à-dire qu'ils sont intégrés, ils sont connus, puis on a des enquêteurs qui font une analyse de ça à partir d'un certain nombre de critères pour juger si, oui ou non, certains de nos employés posent des gestes qui seraient répréhensibles.

Je vais vous donner un exemple. Si, M. Deslières, on constate que, sur son dossier de permis, il y a des gens qui vont interroger, mais il n'y a pas de transactions, bien, avant, on ne le savait pas; maintenant, on le sait. Bien, on a des critères qui font que, si quelqu'un fait ça à deux, trois reprises, ou même à une reprise, bien... On a aussi des listes de gens... je ne sais pas si je dois révéler ça, mais, en tout cas, on a une liste de gens sensibles pour lesquels on surveille un certain nombre de... tous les gens qui sont dans l'appareil judiciaire, mettons, procureurs, juges. On suit ça régulièrement, s'il y a des gens qui vont sur leur dossier.

Une voix: ....les députés.

M. Brind'Amour (Jacques): Non, pas les députés, à moins qu'ils nous le demandent. S'ils nous le demandent, on va le faire. Mais il faudrait qu'ils nous le demandent.

Si vous êtes dans...

Une voix: ...

M. Brind'Amour (Jacques): Bien, M. Gautrin, tiens. Si vous êtes dans l'actualité, mettons que vous seriez dans l'actualité pendant deux, trois semaines, pour diverses raisons et sur un sujet qui est sensible, je prends pour acquis que nos enquêteurs se mettraient un petit point... pendant un certain temps, ils vont vérifier si quelqu'un a les... Pourquoi? Bien, parce que • on parle évidemment de sujets sensibles qui ne sont pas des sujets qui ont trait probablement au système de lois, etc., là, au système judiciaire • parce que c'est des gens qui pourraient faire l'objet de menaces ou être influencés, etc.

La Présidente (Mme Dionne-Marsolais): ...vulnérables sur cette question-là.

M. Brind'Amour (Jacques): Vulnérables, voilà. Alors, c'est des choses que nous faisons. C'est des choses que nous faisons, mais

vous avez raison de dire que, au départ, on n'a pas identifié l'ensemble de nos postes sensibles... On doit en avoir à peu près 2 200, là, pour être sérieux, là. Tout le monde qui a accès à nos fichiers, dans l'intérieur, on en a 2 000, 2 200 personnes à peu près, là. Tous les gens qui sont à un comptoir et qui font du permis, «immat», là, ils ont accès à tous les fichiers. Alors, identifier et effectivement, par rapport à l'ensemble de ces personnes-là, s'assurer qu'elles ont, au moins à l'entrée, un comportement correct.

Ce que je vous dirais pour terminer • je m'excuse, deux secondes encore • c'est de vous dire que, même si vous faites des vérifications... même si vous faites une enquête de sécurité, moi, je vous le dis tout de suite, là, sur 99,9 % du monde, vous ne trouverez rien. Le problème, c'est quand la personne, une fois qu'elle est dans un système où elle a accès à des choses qui lui permettent de, c'est là que le problème se pose, et la seule façon de le vérifier, c'est qu'on demande à nos gestionnaires d'être vigilants. Les gens manipulent l'argent, il y a toutes sortes de choses, là, dans nos systèmes, bon. Alors, d'être vigilants. On demande aussi, avec la journalisation, de vérifier des choses. Puis, aussitôt qu'on constate qu'il y a une chose qui est... Quelqu'un qui irait, là, sur certains dossiers sans faire de transactions, le lendemain matin, son gestionnaire va le rencontrer et va lui dire: Pourquoi? Explique-moi ça. On a des cas de bris de confidentialité. On en a eu...

Une voix: 47.

M. Brind'Amour (Jacques): 47. Depuis?

Une voix: Depuis 2001.

M. Brind'Amour (Jacques): 2001. On en a eu 47. Alors, à chaque cas de bris de confidentialité, bien il y a une rencontre, et tout ça, il peut y avoir des sanctions. Si ça va plus loin, il y a une enquête, on a notre service des enquêtes qui va fouiller non seulement autour de la personne, mais il va aller chercher les transactions qu'elle a faites. Et, si ça va plus loin, il y a des accusations, bien le système policier va embarquer. Alors, on a quand même des systèmes...

Une voix: C'est partout dans votre système...

M. Brind'Amour (Jacques): Oui, oui.

Une voix: ...on parle de services...

M. Brind'Amour (Jacques): Exact, oui.

La Présidente (Mme Dionne-Marsolais): Sur ce point-là, dans votre plan d'action, vous mentionnez un projet pilote pour le contrôle d'intégrité des employés, qui est en cours et qui doit être échu en novembre 2004. Nous sommes en novembre 2004. Est-ce que vous pourriez • il me reste peut-être deux minutes • nous dire ce que c'est que ce projet pilote là, s'il vous plaît, pour le bénéfice des membres?

M. Brind'Amour (Jacques): Oui. Il s'agit des employés du contrôle routier qui ne sont pas agents de la paix. Alors, comme on avait déjà là des enquêtes sécurité assez grandes, on s'est dit: On va compléter au contrôle routier avec les personnels qui ne sont pas agents de la paix. C'est ce qu'on fait actuellement. Et on est en discussion avec le ministère de la Sécurité publique pour trouver un mécanisme, là, pour l'ensemble de nos employés.

La Présidente (Mme Dionne-Marsolais): D'accord. Alors maintenant je vais passer à... le député de Verdun.

Une voix: Les personnes, là?

La Présidente (Mme Dionne-Marsolais): Excusez, là, il y a une question: Combien d'employés à la...

Une voix: 3 500.

La Présidente (Mme Dionne-Marsolais): 3 500 employés au total. Alors, M. le député de Verdun.

M. Gautrin: Je vous remercie, Mme la Présidente. Je reviens donc au rapport sur la sécurité informatique et je veux juste poser une question sur les risques résiduels. Les risques résiduels, c'est, une fois que vous avez fait votre analyse de risques, c'est la gestion des risques que vous ne pouvez pas couvrir ou que vous pensez qu'il est trop coûteux de devoir couvrir. De fait, le Vérificateur général a soulevé un certain nombre de questions sur les lacunes par rapport aux risques résiduels dans les trois

organismes qu'il a vérifiés.

Ma question est encore reliée aux dates. J'ai vu que vous avez donc une gestion des risques, au troisième élément de votre correction que vous faites, vous faites une étude des menaces et des risques, résultats concrets progressivement. Mais ce qui m'interpelle, c'est que votre objectif est de juin 2006; c'est-à-dire, vous ne corrigez pas à court terme, ce qui à mon sens est assez... une vision générale de la gestion des risques, vous ne corrigez que très lentement et vous n'arrivez qu'à échéance en 2006, ce qui est malgré tout, dans un certain temps, dans plus de deux ans... bien, un peu moins de deux ans, mais presque, ici.

Alors, ma question, c'est non pas que vous n'êtes pas conscient de l'existence d'une... de la nécessité d'une gestion des risques, non pas que vous sachiez qu'il est important d'avoir une gestion des risques résiduels, je comprends que vous l'avez, mais pourquoi l'échéance est en juin 2006, de devoir corriger cette lacune qui a été identifiée par le Vérificateur général?

La Présidente (Mme Dionne-Marsolais): M. Brind'Amour. Vous pouvez passer la parole à un collègue, si vous voulez, hein?

M. Brind'Amour (Jacques): Bien sûr, c'est ce que je vais faire, d'ailleurs. Peut-être de dire simplement en commençant qu'il y a des risques qui touchent à la fois nos actifs et qui touchent les mesures de sécurité qui entourent les actifs. Alors, on fait déjà des choses, on fait déjà des choses pour protéger nos actifs. Je parlais tout à l'heure du contrôle des accès au siège social, les contrôles d'accès aux salles d'informatique. Vous vous en doutez, personne ne peut arriver chez nous, là, puis rentrer dans une salle informatique, là, salle des traitements. Il y a deux ... il y a des caméras, il y a des trucs d'accès, il n'y a pas grand monde qui rentre là, là, à moins d'être complètement autorisé. Bon. Alors, je vous ai parlé de ce qu'on fait...

Une voix: ...

M. Brind'Amour (Jacques): Bien oui, c'est ça, j'imagine. Alors, concernant l'information, je vous ai parlé de la journalisation, l'analyse des journaux qu'on fait, on a un registre des bris de confidentialité, on fait des enquêtes.

M. Gautrin: ...ma question. Ma question... J'ai compris que vous faites actuellement des choses. Ma question, c'est: Est-ce que vous avez une connaissance des risques résiduels? Et est-ce que vous avez accepté, est-ce que vous en avez... Les inquiétudes que j'ai, c'est juin 2006. C'est l'échéance très tardive que vous mettez actuellement pour corriger une faiblesse... qui est mineure. Je ne veux pas non plus majorer, non plus, l'importance de ça, mais, juin 2006, ça me semble très loin.

La Présidente (Mme Dionne-Marsolais): M. Brind'Amour.

M. Brind'Amour (Jacques): Si vous permettez, Mme la Présidente, simplement dire... Je vais faire rien qu'un commentaire puis je vais demander à M. Léveillé de vous expliquer. C'est l'ampleur de la tâche qui fait qu'on est en 2006. Peut-être M. Léveillé pourrait vous expliquer un peu ce qu'il y a à faire.

La Présidente (Mme Dionne-Marsolais): M. Léveillé, peut-être éclairer notre collègue de Verdun et tous les autres.

n *(17 h 40)* n

M. Léveillé (Michel): Oui. Il faut voir qu'actuellement on ne part pas de rien. Il y a eu des études d'évaluation de menaces et de risques; on en a eu une en 1994, une en 1998 et on en a démarré une en 2004. Donc, actuellement, on a déjà des risques qui sont pris en compte, parce qu'on a déjà eu des études et qu'on a pris des actions appropriées.

Maintenant, l'étude qu'on entreprend, c'est suivant une méthode recommandée par le Secrétariat du Conseil du trésor, la méthode MEHARI. Cette méthode-là, elle, elle nous permet de passer l'ensemble de nos actifs. Je vous rappelle qu'on a des travaux actuellement qu'on a amorcés sur le registre d'autorité pour faire un inventaire exhaustif de nos actifs, donc avoir ces actifs-là pour, après ça, qu'on puisse prendre l'étude des menaces et risques et l'appliquer à chacun de nos actifs. C'est une étude qui demande beaucoup de travail, c'est beaucoup de tâches à réaliser. L'approche qu'on a prise, c'est de faire un premier projet avec deux systèmes, puis on va avoir des résultats en février 2005, et, à partir de cette date-là, on va se doter d'une stratégie pour faire l'étude MEHARI graduellement sur chacun de nos actifs suivant leur caractère critique, de sorte qu'on va avoir des résultats continuellement jusqu'à juin 2006.

Ce qu'il faut comprendre, c'est qu'on n'aura pas les résultats dans 18 mois, mais on va avoir des résultats tout au long du processus, de sorte qu'on va pouvoir ajuster les mécanismes de sécurité au fur et à mesure qu'il y a des points à améliorer qui vont être détectés. Mais, comme je vous dis, c'est beaucoup d'actifs, il faut voir que c'est toutes nos banques de données, tous nos systèmes

informatiques, toutes nos pièces d'infrastructures, matérielles et logicielles. Donc, je crois que, pour faire une étude sérieuse, il faut se donner le temps. Et, comme je vous dis, le registre d'autorité, lui...

M. Gautrin: ...

M. Léveillé (Michel): Oui.

M. Gautrin: Même si vous dites que vous avez déjà un certain nombre de choses, une étude complète actuellement sur l'analyse de la gestion des risques par...

M. Léveillé (Michel): Oui, on considère que c'est une mesure de suivi et qu'à un intervalle de quatre ou cinq ans il faut refaire ces études-là pour avoir un portrait général.

M. Gautrin: Donc, à ce moment-là, vous avez fait un projet pilote qui va donner des résultats à ce moment-là, d'ici février 2005, et, à partir de là, vous aurez donc validé la méthode sur un certain nombre de vos actifs informationnels et vous allez donc l'appliquer petit à petit dans chacun de vos actifs. Est-ce que je comprends?

M. Léveillé (Michel): C'est exactement ça, oui.

M. Gautrin: Alors, est-ce que vous pourriez informer la commission, au fur et à mesure de l'évolution, de ce qui se passe?

M. Léveillé (Michel): Certainement.

M. Gautrin: Vous avez terminé le premier élément d'évaluation, vous avez terminé... Je comprends, à ce moment-là, que, si vous faites une réévaluation globale de toute la gestion des risques, ça peut vous prendre un certain temps, mais, si je comprends bien, ça va se faire sur un phénomène, un temps continu. C'est bien ce que je comprends?

M. Léveillé (Michel): C'est ça.

M. Gautrin: Très bien. O.K. Bien, écoutez, ça répond à ma question, Mme la Présidente.

M. Bernier: C'est un peu en complémentarité, ma question, de mon collègue de Verdun. Justement, au niveau des... quand on parle des tests d'intrusion, de plus en plus, on regarde au niveau des transactions, c'est très ouvert, public: on parle d'Internet, on parle également de postes que vous avez à l'extérieur de vos bureaux, qui sont dans d'autres ministères, je pense au Revenu qui a des postes de la Société d'assurance automobile aux fins de consultation, ainsi de suite. Donc, est-ce que présentement vous avez des tests? J'imagine, des tests d'intrusion que vous faites... et vous apportez des corrections. J'aimerais vous entendre sur ça, là: Quels sont les tests que vous procédez et quelles sont les mesures, les correctifs qui sont apportés? Ou de quelle façon ils sont documentés, ces éléments également qui vont supporter ces tests-là, pour apporter les correctifs?

La Présidente (Mme Dionne-Marsolais): Puis, en complément, la stratégie d'audits et de tests d'intrusion périodiques dont vous parlez, là, dans votre plan qui est dû pour décembre 2005, peut-être vous pourriez couvrir les deux en même temps. C'est ce que ça couvre...

Une voix: ...

La Présidente (Mme Dionne-Marsolais): Ça va répondre. Alors, oui, M. Léveillé. C'est ça?

M. Léveillé (Michel): Notre stratégie actuelle pour les tests d'intrusion, c'est qu'on se concentre sur les actifs qu'on estime qui sont les plus à risque. Donc, ce sont les actifs qui sont associés à la prestation électronique des services. À toutes les fois qu'on a une modification à un de ces actifs-là, on fait ce qu'on appelle un audit, on vérifie si... dans la façon qu'on a eue de développer le service, est-ce qu'on a suivi les règles de l'art en matière de sécurité? Par la suite, via des firmes externes à la société, on procède à des tests d'intrusion pour s'assurer que les différents mécanismes qu'on a mis en place résistent aux tentatives d'intrusion. C'est notre approche actuelle.

Une voix: ...

M. Léveillé (Michel): Oui, O.K. Bon. Maintenant, ce qu'on prévoit faire, notre nouvelle approche qu'on prévoit instaurer, elle est

en trois volets. La première sur... Les tests d'intrusion sont basés sur la menace et les risques. Une fois qu'on va avoir complété notre registre d'autorité, qu'on va savoir lesquels sont le plus sensibles; ce qu'on se propose de faire, c'est justement des audits et des tests d'intrusion périodiques. Ce qu'on va regarder, c'est: Est-ce que, à part la prestation électronique des services, il y a d'autres actifs à la société qui devraient faire l'objet de tests d'intrusion ou d'audits spécialisés? Ça, c'est via la révision du registre d'autorité et via l'étude de menaces et risques, qui va se terminer en juin 2006, qu'on va déterminer les actifs sensibles. Et, à ce moment-là, on va établir • c'est pour ça que la date est décembre 2005 • on va établir une stratégie d'audits et de tests d'intrusion périodiques pour les actifs qu'on considère sensibles. Ça ne nous empêchera pas de continuer à faire des tests d'audits et d'intrusion de façon ad hoc. Lorsqu'il va y avoir des modifications, entre autres sur les actifs de la prestation électronique des services, c'est certain qu'on va continuer à faire les tests qu'on fait actuellement.

La Présidente (Mme Dionne-Marsolais): Oui, M. le député de Verdun.

M. Gautrin: Je vais vous poser une question qui n'est pas tellement en lien avec le rapport actuellement mais qui me préoccupe, moi, personnellement. Vous, comme spécialiste de la sécurité dans un organisme comme la SAAQ, comment vous réagiriez à l'idée d'avoir une certification de sécurité régulière par un organisme externe? Est-ce que c'est quelque chose...

Des voix: Genre ISO...

M. Gautrin: Du genre ISO 2000, ou qui serait donnée par un organisme externe, un peu comme vous pouvez avoir ça régulièrement.

M. Léveillé (Michel): Parce qu'a priori on ne peut pas être contre une mesure comme celle-là qui viserait d'avoir une certification externe. Il faudrait regarder, à ce moment-là, ça consiste en quoi, parce que c'est quand même... Pour avoir une certification, il y a certains travaux qu'il faut effectuer. O.K.? Ça suppose que, ces gens-là, on leur donne accès à de l'information confidentielle. Ça prenait une organisation qui est vraiment reconnue dans le domaine.

M. Gautrin: Non, mais je fais référence très spécifiquement au projet du CRIM, que vous devez connaître, un projet du CRIM actuellement d'avoir un élément de certification et... le CRIM, le Centre de recherche informatique de Montréal, sur lequel ils pourraient certifier, à ce moment-là, en termes de sécurité, chacun des organismes. Donc, ce n'est pas complètement inutile.

La Présidente (Mme Dionne-Marsolais): M. Brind'Amour, vous voulez ajouter quelque chose?

M. Brind'Amour (Jacques): Non, j'allais dire effectivement que, si c'est une mesure qui s'appliquait à plusieurs organismes qui sont de même nature, c'est une bonne idée.

M. Gautrin: Merci.

La Présidente (Mme Dionne-Marsolais): Alors, moi, j'ai des petites questions de détails, surtout de compréhension. Vous avez dit dans vos remarques préliminaires que 95 % de vos employés avaient signé... vous avez ajouté «volontairement»...

Une voix: Page 6.

La Présidente (Mme Dionne-Marsolais): Merci, une déclaration de discrétion. Pourquoi les 4,3 % autres n'ont pas signé, et quels moyens avons-nous pour assurer... Ça me préoccupe, moi, ça.

M. Brind'Amour (Jacques): Oui, il y a deux raisons. La première, c'est que, lorsqu'on a fait l'opération, là, parce qu'on l'a regardée dans un temps donné... les nouveaux employés le signent automatiquement, mais on parle des employés existants... bien, c'est simplement qu'il y en a qui étaient absents, il y en a qui étaient malades de longue durée, etc. Il y a un premier phénomène qui est lié à l'absence simplement des gens au moment des séances de sensibilisation. Lorsqu'ils sont revenus, ils n'ont pas eu leur séance de sensibilisation, donc elle est programmée, puis, lorsqu'ils l'auront, bien peut-être que nos chiffres vont continuer de s'améliorer.

La Présidente (Mme Dionne-Marsolais): Alors donc, les 100 % n'ont pas été disponibles ou assujettis à cette formation-là.

M. Brind'Amour (Jacques): Oui, du 4 % qui restent, il y en a une partie que c'est ça. L'autre partie, effectivement, il y a des gens qui n'ont pas voulu signer, mais... J'aurais pu vous donner un autre chiffre, qui est de 98 % à peu près, même si les gens n'ont pas signé, ils ont assisté à la séance...

La Présidente (Mme Dionne-Marsolais): Mais quelle est la raison qu'ils donnent et quel pouvoir avez-vous pour les...

M. Brind'Amour (Jacques): Bien, la raison qu'ils donnent, c'est simplement qu'ils ont déjà signé, en entrant dans la fonction publique, un serment d'allégeance • comment on appelle ça? • une déclaration de...

La Présidente (Mme Dionne-Marsolais): Bien, c'est quoi, la réponse?

M. Brind'Amour (Jacques): Bien, c'est-à-dire qu'ils ont déjà...

La Présidente (Mme Dionne-Marsolais): C'est quoi, la réponse?

M. Brind'Amour (Jacques): Ils ont déjà pris un engagement éthique. Dans le fond, c'est ce qu'ils disent.

La Présidente (Mme Dionne-Marsolais): D'accord.

M. Brind'Amour (Jacques): Mais là, vous savez, entre nous, on parle de gens qui... c'est en dizaines de personnes, là.

La Présidente (Mme Dionne-Marsolais): Oui, d'accord, d'accord. Mais on comprend, mais...

Une voix: Ça prend une personne...

La Présidente (Mme Dionne-Marsolais): Mettez-vous à notre place, on trouve ça curieux, parce que ce sont quand même des employés. Ils iraient dans une entreprise, quelle qu'elle soit, et puis on leur...

L'autre question que j'ai, parce que, moi, je suis très préoccupée par la formation puis les ressources humaines, parce que je crois que c'est 80 % de la réussite et de l'échec, ça, même plus... Vous dites, et vous l'avez mentionné tantôt, certaines restrictions de vos conventions collectives, hein, «sous réserve des lois et des conventions collectives en vigueur», on va adopter des mesures, etc., «pour vérifier l'intégrité des personnes qui postulent certains postes». Je comprends qu'il y a des contraintes... il peut y avoir des contraintes.

n *(17 h 50)* n

Ma question, c'est: Est-ce que vous avez transmis au Conseil du trésor ces réserves-là, et les recommandations ont-elles été faites pour que les corrections soient apportées et que la négociation s'entame avec les représentants syndicaux pour que ces correctifs-là soient mis en place, considérant le fait que de plus en plus... que l'exercice du travail va requérir de plus en plus l'utilisation de ces réseaux informatiques, et on doit exiger ces choses-là?

M. Brind'Amour (Jacques): La réponse, c'est oui. Effectivement, nous avons discuté de cette question avec le Conseil du trésor et nous leur avons suggéré effectivement d'établir pour l'ensemble de la fonction publique une norme, une façon de procéder, ce qu'ils sont en train de faire de toute façon, là. Je ne sais pas où ils en sont exactement, mais ils sont en train de le faire, ils sont en train d'étudier ça.

La Présidente (Mme Dionne-Marsolais): On pourrait questionner le Trésor là-dessus.

M. Brind'Amour (Jacques): Exact, possiblement, oui.

La Présidente (Mme Dionne-Marsolais): À votre connaissance, est-ce qu'il y a d'autres organismes ou ministères qui ont soulevé ce point-là, dans le processus de la sécurité informatique et de l'embauche des employés de l'État? Parce que, si la réponse qui vous est servie, c'est: Quand j'ai été embauché, j'ai déjà signé mon engagement à l'éthique, il faudrait qu'à l'embauche partout ce soient les mêmes...

Une voix: ...

La Présidente (Mme Dionne-Marsolais): Oui, exact, c'est ça. La vice-présidente me fait penser que, au moment où la RAMQ est passée ici, j'avais fait état de ce même constat aussi.

M. Brind'Amour (Jacques): M. Gélinas me signale qu'on a discuté, nous, avec Emploi et Solidarité. Eux aussi sont également dans la même... Et, eux, je pense qu'ils le font, hein? Peut-être je vais donner la parole à M. Gélinas. Il pourra vous l'expliquer en deux minutes.

La Présidente (Mme Dionne-Marsolais): D'accord. M. Gélinas, nous vous écoutons.

M. Gélinas (Claude): Essentiellement, sur cette question-là, pour faire le travail au niveau des antécédents judiciaires, et tout le reste, on est allé voir ce qui se faisait dans d'autres ministères, en particulier Emploi et Solidarité et de la Famille. Eux ont fait un exercice en profondeur pour identifier, dans un premier temps, les emplois à risque et, une fois qu'il avaient identifié les emplois à risque, mais de savoir comment, maintenant, est-ce qu'on va traiter les gens qui sont assignés à ces emplois-là, au niveau des antécédents judiciaires, et tout le reste. Et c'est une opération qui a duré, à ma connaissance, au-delà de deux ans chez eux. Ils l'ont fait également, je pense, si mes souvenirs sont bons, de concert avec les représentants syndicaux pour que le tout se fasse harmonieusement. Et, chez nous, on s'apprête à faire une opération qui va dans le même sens. Et aussi, avant de procéder à ce niveau-là, au niveau des affaires juridiques, on a vérifié avec le Conseil du trésor quels étaient les empêchements, au niveau des conventions collectives et tout le reste, qui pouvaient exister à ce niveau-là. Et eux nous ont fourni, à ce moment-là, une opinion juridique qui traitait de l'ensemble de la question. Et il est évident que ce dossier-là est un dossier qui intéresse aussi le Conseil du trésor, parce que je pense qu'on a soulevé une question d'intérêt lorsqu'on avait fait cette demande-là.

La Présidente (Mme Dionne-Marsolais): Une autre question, toujours sur les ressources humaines. Le Vérificateur, à 4.72, dans son rapport, a été très précis sur les activités de sensibilisation et de formation du personnel de gestion informatique en disant que ces activités-là n'étaient pas encadrées par un programme formel et qui font en sorte que certaines... que les interventions qui sont destinées aux utilisateurs et aux gestionnaires sont organisées à la pièce, et notamment chez vous. Donc, j'aimerais ça savoir de quelle façon vous avez l'intention de compenser cela. Vous avez, dans votre plan, là, soumis, vous avez l'élaboration d'un plan et des mesures d'évaluation pour décembre 2004, donc dans un mois, et la réalisation du plan l'année prochaine.

Ma question: Vous avez donné des montants, tout à l'heure, sur l'investissement que vous faisiez en informatique. Dans la formation, à la Société d'assurance automobile, vous investissez combien d'argent en formation de vos ressources humaines? Et plus spécifiquement, en informatique, pour la formation tout court, vous investissez combien? Et, pour la sécurité informatique, vous investissez combien? Ça fait trois questions, c'est pas gros. Vous êtes habitué à pire que ça, M. Brind'Amour.

M. Brind'Amour (Jacques): Oui.

La Présidente (Mme Dionne-Marsolais): On vous écoute.

M. Brind'Amour (Jacques): ... un peu les règles parlementaires, mais est-ce qu'on peut prendre la question en délibéré?

La Présidente (Mme Dionne-Marsolais): Oui, vous pouvez.

Des voix: Ha, ha, ha!

Une voix: On peut revenir demain.

La Présidente (Mme Dionne-Marsolais): M. Brind'Amour, vous pouvez très bien nous revenir... nous faire parvenir ces questions-là. Et nous ne nous attendions pas à une réponse détaillée, là. Je ne sais pas si vous voulez donner une envergure, mais, quant au processus d'activité, vous pourriez peut-être commenter?

M. Brind'Amour (Jacques): Je vais demander à M. Trudel, qui est coordonnateur, de vous expliquer ce qu'il en est.

La Présidente (Mme Dionne-Marsolais): M. Trudel, on vous écoute.

M. Trudel (Mario): Oui. On fait effectivement beaucoup d'activités de formation et de sensibilisation à la sécurité informatique. Je pense qu'on...

La Présidente (Mme Dionne-Marsolais): Mais encore?

M. Trudel (Mario): On l'a assez bien démontré au Vérificateur, on a montré l'ensemble des actes qu'on a posés dans ce domaine-là, entre autres pour tous les groupes d'employés qui ont une formation à la tâche. Donc, dès qu'il y a un grand nombre d'employés

qui font le même travail, un agent d'indemnisation, un préposé... tous ces gens-là ont une formation de départ, d'accueil, à laquelle on a toujours intégré un volet sécurité informatique et un volet protection des renseignements personnels. Donc, pour tous nos grands groupes d'employés, il y a une formation structurée, c'est pris en compte en même temps que les autres éléments de formation. Donc, comment réaliser mes tâches, mais comment réaliser mes tâches de manière sécuritaire. Donc, c'est une bonne façon de l'aborder.

Et on a fait aussi des grandes campagnes de sensibilisation. On en a fait une en 2002 à l'interne, où la très grande majorité des employés ont été rencontrés pendant une séance de deux à trois heures: présentation d'un vidéo, échange avec les personnes présentes sur les enjeux, remise d'un matériel, aussi, promotionnel, qu'on peut garder sur son bureau, qui rappelle les règles de sécurité. Donc, on fait énormément d'actions dans ce sens-là.

Ce que le Vérificateur a noté, c'est l'absence d'un plan d'ensemble de ces mesures-là, pour s'assurer que tous les besoins sont pris en compte, notamment ceux des gestionnaires. C'est vrai, et on va prendre le temps de le faire, de recenser à nouveau l'ensemble des besoins. On l'a fait dans le passé, on va le faire maintenant, quels sont les besoins actuellement, et on va intégrer ça dans une démarche plus structurée. Mais le nombre d'actions va être le même, notre travail de sensibilisation va se poursuivre, c'est juste qu'il va être mieux encadré par un plan.

La Présidente (Mme Dionne-Marsolais): D'accord. Et donc, vous allez... continuer. Mme la députée de Rimouski, là-dessus.

Mme Charest (Rimouski): Sur ça, j'avais des précisions à vous demander. Quand vous parlez de vos employés, est-ce que vous parlez de tous ceux qui sont les mandataires, les contractuels, en fait, ou si c'est juste les employés considérés comme faisant partie de la SAAQ, de la Société de l'assurance automobile?

M. Trudel (Mario): Dans le cas particulier des mandataires...

Mme Charest (Rimouski): Par rapport à la formation.

M. Trudel (Mario): ...en permis, immatriculation, les 500 employés de nos mandataires, ceux-là ont une formation à la tâche, dont je vais vous parler tantôt. Donc, à l'intérieur de la formation à la tâche, il y a un volet sécurité informatique et il y a un volet protection des renseignements. Donc, oui, ces gens-là ont le message. Et on a fait une tournée de rappel effectivement, on le fait à chaque année, au moment, je pense, du renouvellement des contrats, où on rencontre les responsables des mandataires pour leur rappeler les règles dans le domaine.

Mme Charest (Rimouski): Et, là-dessus, quand vous dites que vous allez le faire et que vous le faites, vous avez des échéanciers?

M. Trudel (Mario): Dans le cas de la formation à la tâche, c'est lui qui accueille les nouveaux employés des mandataires. Donc, c'est une activité continue de formation. Et, dans le cas des rappels annuels, je n'ai pas les dates avec moi, mais on pourrait vous les transmettre.

Mme Charest (Rimouski): ...habituellement et...

M. Trudel (Mario): Oui, c'est au rythme des renouvellements des ententes avec nos mandataires.

Mme Charest (Rimouski): Et je ferai juste un commentaire en terminant. Je pense que, bon, 95,7 % des employés qui signent des déclarations de confidentialité, c'est bien, c'est très bien, mais il ne faut jamais abandonner son droit de gérance. Et je pense que, là-dessus, le Conseil du trésor devrait vous appuyer pour que 100 % des employés signent leur contrat de confidentialité. C'est la même remarque qu'on a déjà faite dans le passé à la RAMQ, à Emploi-Québec et à d'autres, là. Je pense que, là-dessus, c'est important, surtout avec... Bon, il y a la confidentialité puis il y a la sécurité informatique, qui sont deux choses mais qui se rejoignent étroitement.

M. Trudel (Mario): Oui, et je peux apporter une nuance là-dessus.

La Présidente (Mme Dionne-Marsolais): Oui, je vous en prie.

M. Trudel (Mario): Sur le 95 %. Pour obtenir un accès à nos systèmes d'information, la règle de départ s'applique à 100 % des utilisateurs de nos systèmes, c'est de signer un engagement à respecter des règles, dont une des règles est d'utiliser son code uniquement pour accomplir ses tâches. Et les sanctions sont rappelées. Donc, on a 100 % d'adhésion sur ce formulaire-là. La

déclaration de discrétion est un rappel de cet engagement-là. Donc, on a 100 % d'adhésion aux règles de base de sécurité informatique.

La Présidente (Mme Dionne-Marsolais): M. le député de Beauharnois.

M. Deslières: Merci, Mme la Présidente. Je vais profiter du passage du président de la société pour lui poser une question un peu en aparté avec cette question de la sécurité informatique.

n *(18 heures)* n

On sait que le gouvernement a l'intention de mettre sur pied une fiducie par le truchement du projet de loi n° 55, que vous connaissez bien. Est-ce que cette fiducie va être assujettie aux mêmes règles qui nous gouvernent, qui gouvernent l'ensemble des organismes? Parce que je n'ai rien vu... Je regardais dans le projet de loi n° 55, je n'ai rien vu à cet effet, concernant comment va se gouverner cette fiducie face aux règles de sécurité informatique.

La Présidente (Mme Dionne-Marsolais): M. le président, êtes-vous en mesure de répondre?

M. Brind'Amour (Jacques): Oui, bien sûr. Bien, il n'y aura pas de différence, effectivement. Les mêmes règles vont s'appliquer, c'est certain.

La Présidente (Mme Dionne-Marsolais): M. le député de Verdun, on finit sur vous.

M. Gautrin: J'ai une question qui n'a rien à voir, mais je voudrais quand même vous la poser, puisque j'ai la chance. Vos mandataires, vous avez des contrats avec vos mandataires. Est-ce que vous pouvez les briser facilement, premièrement?

Deuxième question. Vous savez qu'il y a un projet de loi qui est actuellement déposé sur ce que j'appelle Services Québec, et est-ce qu'éventuellement il serait possible, compte tenu des règles de cette... qu'une même personne puisse • un employé de Services Québec • traiter avec la SAAQ et traiter ensuite avec un autre organisme gouvernemental • vous voyez, toute la théorie du guichet unique • ou est-ce qu'il y a des règles qui empêcheraient... des règles de sécurité qui empêcheraient ça actuellement?

La Présidente (Mme Dionne-Marsolais): M. Brind'Amour.

M. Brind'Amour (Jacques): Oui. Sur votre première question, effectivement, nous avons des contrats qui sont très, très liants, et ça va aussi loin que, si un employé est pris à faire un bris de confidentialité • curiosité, etc. • chez un mandataire, nous pouvons mettre fin au contrat. Ça va jusque-là.

M. Gautrin: ...

M. Brind'Amour (Jacques): Pour ce qui est du guichet unique, ça poserait sûrement des problèmes, compte tenu des accès qu'on a à des fichiers, là. Ça ne veut pas dire que ce mandataire-là ne pourrait pas... Mais le même employé qui pourrait faire à la fois un travail pour nous comme mandaté et qui pourrait en même temps faire un autre travail, ce serait... ce n'est pas...

M. Gautrin: ...c'est le cas, hein, c'est comme ça que ça fonctionne?

M. Brind'Amour (Jacques): Oui. Alors, à ce moment-là, ce qu'il faudrait, c'est que les employés qui sont chez nous deviennent des employés de Services Québec, avec une autre règle du jeu.

M. Gautrin: O.K.

La Présidente (Mme Dionne-Marsolais): Bon. Alors, merci beaucoup, messieurs, mesdames. Merci, M. le Vérificateur général et votre équipe. Je vous suis très reconnaissante de la rigueur de nos échanges. Et puis, si vous pouviez... Nous avons encore une petite session à faire entre nous, alors si vous pouviez quitter doucement, doucement mais efficacement, ça nous aiderait.

(Fin de la séance à 18 h 2)