CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 171 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le lundi 15 juillet 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le lundi 15 juillet 2019

● (1330)

[*Traduction*]

Le président: Mesdames et messieurs, nous nous efforçons de respecter notre horaire. Nous attendons l'arrivée de nos autres témoins, mais, dans l'intervalle, nous allons entendre le témoignage du représentant de la GRC, le capitaine Mark Flynn.

Vous ferez votre exposé et, si les représentants du Centre de la sécurité des télécommunications viennent, nous prendrons des dispositions afin qu'ils s'expriment eux aussi.

Soit dit en passant, la séance est maintenant publique.

En ce qui concerne les personnes qui témoignent devant nous, le véritable problème, c'est que les membres du Comité souhaitent poser des questions. Par conséquent, il est préférable de limiter la durée des exposés.

Et maintenant, je vous prie de faire votre exposé, surintendant Flynn.

Surintendant principal Mark Flynn (directeur général, Criminalité financière et la cybercriminalité, Opérations criminelles de la police fédérale, Gendarmerie royale du Canada): Vous serez heureux d'apprendre que je ne ferai pas de déclaration préliminaire, et je crois comprendre que le Comité en a été informé. Je suis ici aujourd'hui simplement pour répondre à toutes les questions que vous pourriez avoir. Comme cet enjeu est, à première vue, lié à une enquête criminelle en cours, il serait toutefois inapproprié que je vous communique des détails relatifs à une enquête, en particulier une enquête qui n'est pas menée par la GRC.

Je suis disposé à répondre à toutes les questions. Je suis ici pour vous apporter toute l'aide que je suis autorisé à vous offrir.

Le président: Monsieur Graham.

M. David de Burgh Graham (Laurentides—Labelle, Lib.): Il est un peu plus difficile de poser des questions sans s'appuyer sur une déclaration préliminaire.

Ma première question est la suivante: si quelqu'un appelle la GRC pour déposer une plainte concernant un vol de données présumé, comment la GRC traite-t-elle cette plainte dès sa réception?

Surint. pr. Mark Flynn: Cela dépend de l'endroit où le vol présumé a eu lieu. Sur le territoire où nous nous trouvons, ces cas relèvent des services de police. Par conséquent, les services de police provinciaux et municipaux se partagent la responsabilité. La plainte serait transférée à notre processus de réception là-bas, que ce soit notre bureau des télécommunications, la réception du détachement ou une unité d'enquête particulière qui a été désignée à cet effet.

Dans les cas où nous ne sommes pas les policiers compétents, comme en Ontario et au Québec, où nous assumons le rôle d'agents de police fédéraux, nous prenons conscience de ces situations en collaborant avec nos partenaires provinciaux et municipaux. Nous examinons l'information, et nous déterminons si la situation est liée à d'autres enquêtes en cours. De plus, nous offrons aux services de police compétents notre appui s'ils en ont besoin, bien que, dans bon nombre de cas, ces types d'incidents soient très bien gérés. Nos forces de police provinciales et municipales sont fort compétentes et sont en mesure de gérer ces incidents par elles-mêmes.

M. David de Burgh Graham: À quel moment un incident devient-il de compétence fédérale? Si un problème relève des provinces, mais touche plusieurs provinces, les services de police provinciaux doivent-ils le gérer séparément? La GRC est-elle en mesure d'intervenir à ce moment-là?

Surint. pr. Mark Flynn: La GRC n'intervient pas automatiquement uniquement parce qu'un problème touche plusieurs provinces. Comme avec les crimes traditionnels, qu'il s'agisse d'un réseau de voleurs qui exerce ses activités près de la frontière entre deux provinces ou d'homicides, les corps policiers de ces administrations ont l'habitude de collaborer et ils le font très efficacement.

Lorsqu'un cyberincident survient, s'il aura des répercussions sur un système du gouvernement du Canada ou un exploitant d'infrastructures essentielles, que des facteurs liés à la sécurité nationale doivent être pris en compte ou que l'incident est lié à un groupe important de criminels qui opère à l'échelle nationale et qui fait déjà parti des enjeux prioritaires sur lesquels nous enquêtons, nous donnerons suite à cet incident.

Dans le domaine du cyberespace, nous entretenons des relations et communiquons régulièrement avec la plupart des provinces et des municipalités dotées de cybercapacités dans leurs secteurs d'enquête. Nous savons que bon nombre de ces incidents surviennent dans plusieurs administrations, que ce soit au pays ou à l'étranger. Par conséquent, la coordination et la collaboration sont vraiment importantes.

C'est pourquoi l'Unité nationale de coordination de la lutte contre la cybercriminalité agira comme le service de police national qui contribuera à cette collaboration. Toutefois, avant sa mise en œuvre, l'une des responsabilités de mon équipe au quartier général est de communiquer régulièrement, que ce soit en tenant régulièrement des conférences téléphoniques ou des rencontres officielles au cours desquelles nous discutons de ce qui se passe dans les diverses administrations pour assurer la collaboration et la déconfliction. De plus, de façon ponctuelle, lorsqu'un incident important survient, les employés des nombreux corps policiers communiquent entre eux par téléphone pour déterminer l'intervention appropriée et s'assurer qu'elle n'est pas réalisée en double.

M. David de Burgh Graham: Dans le cas de l'incident dont il est question aujourd'hui, qui est, de toute évidence, un incident majeur, la GRC est-elle tenue au courant de ce qui se passe même s'il ne s'agit pas de son enquête?

Surint. pr. Mark Flynn: Je tiens à éviter de parler de cette enquête, mais je peux vous dire que les enquêtes de ce genre feront assurément l'objet de discussions. Ces discussions ont lieu en raison des rencontres régulières que nous tenons, que ce soit au sujet des cybercrimes ou d'autres types de crimes qui sont commis dans les différentes administrations. Il est évident qu'un incident de cette ampleur fera l'objet de discussions.

Pour l'instant, je n'ai pris part à aucune de ces discussions. Je ne sais pas s'il y en a.

M. David de Burgh Graham: Je comprends.

D'accord.

Le président: Monsieur Drouin, bienvenue au Comité.

M. Francis Drouin (Glengarry—Prescott—Russell, Lib.): Merci, monsieur le président.

Monsieur Flynn, merci d'être venu. Je sais que vous ne ferez pas de commentaires sur l'enquête en cours, mais, en tant que député qui représente beaucoup de membres qui ont été touchés — je l'ai moi-même été —, je m'intéresse surtout aux répercussions possibles de la fraude.

Je sais que beaucoup de Canadiens reçoivent des appels frauduleux de gens qui se font passer pour des agents de l'Agence du revenu du Canada. J'ai moi-même rappelé une personne qui prétendait travailler pour la GRC. Elle voulait obtenir de l'argent pour une personne en particulier. Elle était très exigeante et insistante. Elle m'a donné un numéro où je pouvais rappeler, que j'ai transmis à la police. Est-ce quelque chose que vous conseillez aux Canadiens de faire où, de toute évidence, la GRC ou le service de police local est le premier point de contact?

● (1335)

Surint. pr. Mark Flynn: Absolument. En fait, le Centre antifraude du Canada dispose d'un programme à cet effet et il entretient une relation étroite avec les fournisseurs de services de télécommunications, qui ont beaucoup aidé à résoudre certains des problèmes entourant le télémarketing et les fraudes massives commises au téléphone. Lorsque nous découvrons et que nous validons les numéros utilisés pour commettre des fraudes, l'industrie des télécommunications bloque ces numéros pour réduire la victimisation. Nous avons adapté certaines de nos pratiques pour faire en sorte que cela se produise beaucoup plus rapidement qu'autrefois.

M. Francis Drouin: Selon votre expérience et ce qu'on a appris des cas de fraude, nous savons que certains fraudeurs ont peut-être mon numéro d'assurance sociale. Ils ont peut-être mon adresse de courriel ainsi que mon adresse municipale. Ils pourraient prétendre de façon très convaincante être un représentant du gouvernement ou d'une quelconque institution financière. À votre avis, quel est le meilleur moyen pour que les Canadiens se protègent?

Surint. pr. Mark Flynn: Dans toutes les campagnes de fraude massive, que ce soit un cas comme celui-ci ou en général, les gens doivent faire preuve d'un grand scepticisme et prendre des mesures pour se protéger. Le gouvernement du Canada offre de nombreuses ressources, comme le Centre antifraude du Canada et Pensez cybersécurité, qui fournissent une liste de conseils pour les Canadiens. Essentiellement, il faut protéger ses renseignements et émettre des doutes raisonnables quand quelqu'un nous appelle. Si une banque nous appelle, il faut composer le numéro de la succursale locale. Il ne faut pas répondre au numéro qu'on a fourni ni rappeler immédiatement à ce numéro. Il faut passer par des sources fiables pour valider les questions qu'on pose.

J'ai déjà reçu des appels semblables au vôtre. J'ai reçu un appel très convaincant de ma propre banque. J'ai communiqué avec cette dernière, qui m'a indiqué que l'appel était frauduleux. C'était intéressant parce que, au bout du compte, l'appel était réel, mais nous nous sommes tous sentis très en sécurité parce que nous avions pris les mesures appropriées. Je préfère risquer de ne pas obtenir un service plutôt que de compromettre mon identité ou mes renseignements financiers.

M. Francis Drouin: Bien, parfait.

Merci.

Le président: Monsieur Paul-Hus, vous disposez de sept minutes.

[*Français*]

M. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, PCC): Merci, monsieur le président.

Merci, monsieur Flynn. Je reviendrai à vous dans quelques instants.

Le chef du Parti conservateur du Canada, Andrew Scheer, m'a demandé d'appeler nos collègues afin d'organiser cette réunion, et j'aimerais lire quelques paragraphes d'une lettre ouverte qu'il a envoyée aux médias le 12 juillet:

> Comme la grande majorité des Québécois et de tous les Canadiens, je suis préoccupé par la sécurité des technologies de l'information, le vol d'identité et la protection des renseignements et informations personnels.
>
> La situation est très sérieuse et je comprends l'inquiétude et l'angoisse des victimes qui craignent les effets futurs de tels vols d'information personnelles, incluant les numéros d'assurance sociale, et qui doivent y consacrer temps et énergie pour y remédier.
>
> Il est rassurant de voir que les dirigeants du Mouvement Desjardins prennent la situation au sérieux en déployant beaucoup d'énergie à protéger et rassurer leurs membres. Le gouvernement fédéral a également la responsabilité et le devoir de soutenir toutes les victimes affectés par les vols d'identités, en travaillant avec tous les acteurs du secteur pour tirer des leçons et améliorer la sécurité informatique.
>
> [...] Je veux dire aux victimes de vol d'informations, ainsi qu'à tous les Canadiens, de notre solidarité et de la volonté d'un futur gouvernement conservateur de s'attaquer aux défis de la protection des renseignements et données personnelles des Canadiens.

[*Traduction*]

Le président: Eh bien, nous remercions M. Scheer pour ce merveilleux message.

[*Français*]

M. Pierre Paul-Hus: Nous tenons à démontrer l'importance que nous accordons à ce dossier. C'est pourquoi il est important pour nous d'être ici en cette belle journée ensoleillée du 15 juillet 2019.

Monsieur Flynn, vous avez répondu à mes collègues libéraux, mais je trouve un peu faible la réponse de la GRC concernant une telle situation. Je m'explique. Il y a 2,9 millions de Canadiens, dont 2,5 millions de Québécois et quelque 300 000 Canadiens de l'Ontario et d'ailleurs au pays, qui ont un compte auprès du Mouvement Desjardins, et ces gens sont très inquiets. Nos bureaux sont constamment interpellés depuis trois semaines et on n'a pas eu de réponse du gouvernement. C'est pourquoi nous tenons cette réunion d'urgence aujourd'hui afin de déterminer ce que peuvent faire les ministères fédéraux pour aider les Canadiens.

Vous nous dites que la GRC n'est pas vraiment impliquée, mais avec son agence de cybersécurité, ses liens avec des organisations comme INTERPOL et tous les autres moyens à sa disposition, n'est-elle pas en mesure d'intervenir? Nous ne voulons pas nous immiscer dans l'enquête policière, mais nous avons appris que des données auraient été vendues à l'étranger. Alors, n'y a-t-il pas des moyens technologiques ou techniques pouvant permettre à la GRC d'intercepter d'éventuelles fraudes?

● (1340)

[*Traduction*]

Surint. pr. Mark Flynn: Comme je l'ai expliqué tout à l'heure, dans bon nombre des situations de ce genre, le rôle de la GRC est de collaborer avec ses partenaires provinciaux et municipaux. Il est important de reconnaître que nos partenaires provinciaux et municipaux sont très habiles pour intervenir dans beaucoup de ces incidents. Il n'est pas toujours vrai que la GRC dispose de pouvoirs, d'autorisations ou de capacités supérieurs à ceux que nos partenaires ont pour faire face à un incident unique en son genre, où une personne est impliquée dans un événement unique, contrairement à un événement plus vaste.

Toutefois, si les partenaires provinciaux et municipaux de la GRC ont besoin d'assistance technique ou de conseils, cette dernière est toujours prête à les lui offrir. Il serait inapproprié que la GRC s'immisce dans la compétence d'un autre corps policier pour diriger l'enquête qu'il mène.

[*Français*]

M. Pierre Paul-Hus: Je comprends ce que vous nous dites au sujet de l'enquête qui est probablement menée par la Sûreté du Québec. Cependant, ce que les conservateurs et le NPD veulent savoir, c'est ce que peut faire la GRC en ce qui concerne les données de 2,9 millions de personnes qui ont été transmises à des criminels. Je ne veux pas parler de l'enquête, je veux savoir si vous avez des ressources. Si ce n'est pas le cas, nous voulons le savoir. C'est pour cela que nous sommes ici aujourd'hui. Si des données ont été vendues à l'étranger, ce n'est pas la Sûreté du Québec ni la police de Laval qui va s'en occuper. Je crois que cela relève de la GRC.

[*Traduction*]

Surint. pr. Mark Flynn: Au-delà de l'enquête, je peux dire que, dans la plupart des cas, les cybercriminels commettent leurs crimes pour avoir accès à des renseignements personnels ou financiers dans le but de mettre la main sur l'argent que détiennent les institutions financières. La GRC travaille constamment en étroite collaboration avec la communauté internationale pour trouver et poursuivre les personnes qui commettent une bonne partie de ces crimes.

En collaboration avec ses partenaires étrangers, de nombreuses grandes institutions financières du Canada et l'Association des banquiers canadiens, la GRC cible les personnes qui causent les dommages les plus importants. L'équipe du Programme de prévention et de mobilisation de la Police fédérale a organisé des rencontres avec les institutions financières et les intervenants du secteur de la cybersécurité. Nous avons un nouveau comité consultatif qui nous aide à cibler ces personnes.

Le savoir est entre les mains des institutions financières et des organismes de cybersécurité. Nous consacrons nos ressources d'enquête à cibler les personnes qui causent le plus de dommages.

Nous collaborons aussi avec les autres pays. Quand des cas se produisent, nous nous entretenons avec les forces de l'ordre des autres pays. Nous signalons les comportements que nous avons constatés dans nos dossiers ou dans ceux de nos partenaires canadiens. Si des liens peuvent être faits, ou si des personnes recherchées sont dans un de ces pays, nous invoquons le traité d'entraide juridique et nous collaborons entre services de police dans le but de concentrer tous les efforts internationaux vers un problème commun.

Comme je l'ai déjà dit, je ne peux pas parler de ce cas en particulier, et je m'en excuse. Je ne peux pas dire ce qui est fait et ce qui n'est pas fait dans ce cas-ci.

[*Français*]

M. Pierre Paul-Hus: Depuis qu'on est au fait de ce problème, est-ce qu'une cellule spéciale a été mise sur pied à la GRC pour aider à le résoudre?

[*Traduction*]

Surint. pr. Mark Flynn: Je ne peux pas parler de ce cas. Ce serait inapproprié.

Le président: Je vous remercie, monsieur Paul-Hus.

[*Français*]

Monsieur Dubé, vous avez sept minutes.

M. Matthew Dubé (Beloeil—Chambly, NPD): Merci, monsieur le président.

Je remercie M. Flynn d'être ici aujourd'hui.

Il est important de parler de cette situation, car les gens sont inquiets, comme mon collègue vient de le mentionner. Il est essentiel d'obtenir plus d'information sur les capacités du fédéral et les moyens dont nous disposons pour traiter cette question, d'autant plus que ce comité vient de terminer, juste avant la levée des travaux en juin, une étude sur la cybersécurité dans le secteur financier. Je reviendrai sur certains éléments auxquels nous avions touché et qui sont pertinents dans le cas qui nous concerne aujourd'hui.

J'aimerais revenir sur quelques éléments que vous avez mentionnés dans vos réponses. Tout d'abord, il y a des rumeurs selon lesquelles des données auraient été vendues à des organisations criminelles au-delà des frontières du Québec et du Canada. Je ne vais pas parler de ce cas précis, puisque vous ne pouvez pas le commenter, mais à quel moment la GRC s'active-t-elle pour venir en aide aux instances très compétentes comme la Sûreté du Québec quand il s'agit d'une organisation criminelle qu'elle surveille déjà et qui opère à l'étranger?

● (1345)

[*Traduction*]

Surint. pr. Mark Flynn: Nous avons régulièrement des rencontres officielles avec les autres services de police du pays. Dans le domaine de la cybercriminalité, ces rencontres ont lieu une fois par mois. Dans d'autres domaines, elles ont lieu toutes les deux semaines. Quoi qu'il en soit, lorsqu'un cas comme celui-ci se produit, des appels sont immédiatement faits, comme vous le décrivez, pour que la collaboration fonctionne et que les renseignements pertinents que détiennent nos partenaires étrangers puissent servir aux enquêtes.

[*Français*]

M. Matthew Dubé: Merci.

En parlant des pouvoirs et des capacités de la police municipale, de la Sûreté du Québec et de la police provinciale de l'Ontario, vous avez dit qu'elles avaient des compétences importantes en matière de cybersécurité. Est-ce que la GRC détient une certaine expertise unique ou des informations qui pourraient leur être utiles?

Je pose la question parce que c'est que le gouvernement s'est vanté de la consolidation des compétences du CST, de la GRC et de toutes les agences qui œuvrent dans le domaine de la cybersécurité en nous disant qu'il voulait assurer une mise en commun de l'information afin que tout le monde soit sur la même longueur d'onde. D'ailleurs, j'y reviendrai quand ce sera le tour de M. Boucher, du Centre canadien pour la cybersécurité.

Est-ce que vous fonctionnez de la même façon avec la police municipale ou provinciale, le cas échéant?

[*Traduction*]

Surint. pr. Mark Flynn: Oui, c'est ce que nous faisons. Comme je l'ai dit, nous travaillons en étroite collaboration avec les services de police provinciaux et municipaux. En fait, je peux vous dire — et j'en suis très fier — que pendant certaines de ces rencontres, où l'équipe du Programme de prévention et de mobilisation de la Police fédérale avait réuni des intervenants du secteur privé, du secteur de la cybersécurité et des institutions financières, quelqu'un dans la salle a tenu à prendre la parole pour remercier la GRC de cette collaboration dans le domaine de la cybersécurité, qui était beaucoup mieux que cette personne n'avait jamais pu constater dans sa carrière.

J'en suis très fier parce que la collaboration et le soutien entre les forces de l'ordre, et non la concurrence, c'est une priorité pour mon équipe, mes employés et moi-même. Nous ne nous substituons pas aux autres services de police, nous cherchons à les aider.

[*Français*]

M. Matthew Dubé: Merci. Je ne veux pas vous couper la parole, mais le temps file.

Dans le cadre de notre étude sur la cybersécurité dans le monde financier, nous avons parlé du fait qu'on a tendance à se faire une image des acteurs étatiques. Sans les nommer, je suis certain que tout le monde a une idée des différents pays qui pourraient porter atteinte à la cybersécurité au Canada.

Je comprends que vous ne pouvez pas en parler, mais dans le cas qui nous concerne, on parle d'un individu. Il pose néanmoins une menace, car les données en question peuvent être vendues et se retrouver entre les mains d'acteurs étatiques. Une des choses que nous avons entendues, c'est que les individus posent la plus grande menace. Est-ce que c'est toujours le cas? Est-ce qu'un criminel qui voudrait procéder à un vol de données pose une plus grande menace que certains pays qu'on pourrait soupçonner?

● (1350)

[*Traduction*]

Surint. pr. Mark Flynn: L'origine de la menace est multiple. Je ne peux pas dire laquelle des origines possibles est la pire parce que, selon mon expérience, il y a un nombre considérable de groupes organisés et de personnes qui commettent des crimes sur Internet. Internet est tout aussi bien un catalyseur qu'un outil permettant d'utiliser et de mettre à profit les extraordinaires services qui nous sont offerts.

[*Français*]

M. Matthew Dubé: Je vais vous interrompre parce que mon temps de parole tire à sa fin.

La présence de groupes organisés ou de pays avec de mauvaises intentions et qui voudraient acheter les renseignements a-t-elle créé une espèce de marché? Y a-t-il un mauvais incitatif, mais néanmoins un incitatif, pour un individu comme l'individu allégué en question, de voler des renseignements pour ensuite les vendre à des groupes intéressés? La présence de tels groupes incite-t-elle des individus ayant une expertise en la matière à poser des gestes qu'ils ne poseraient pas normalement?

[*Traduction*]

Surint. pr. Mark Flynn: Oui, tout à fait. Il y a des services de cybercriminalité qui aident d'autres acteurs moins compétents à commettre des crimes sur Internet, qu'il s'agisse de créer des logiciels malveillants, de faire fonctionner les infrastructures ou de créer les mécanismes par lesquels quelqu'un peut vendre de l'information volée. C'est l'une des cibles visées par la GRC dans le cadre de son mandat fédéral. Elle cible les principaux services qui facilitent les crimes afin de s'attaquer plus efficacement aux crimes commis au lieu de pourchasser individuellement les criminels.

[*Français*]

M. Matthew Dubé: Je vous remercie encore d'avoir pris le temps de nous rencontrer aujourd'hui.

[*Traduction*]

Le président: Je vous remercie, monsieur Dubé.

M. André Boucher, du Centre de la sécurité des télécommunications, vient de se joindre à nous. Je lui donne la parole pour qu'il puisse faire sa déclaration préliminaire.

Je vais redire ce que j'ai déjà dit au surintendant Flynn, c'est-à-dire que les déclarations courtes valent mieux que les longues, car les participants ont plus de temps pour poser des questions.

Monsieur Fortin, je vois que vous voulez...

[*Français*]

M. Rhéal Fortin (Rivière-du-Nord, BQ): Si vous me le permettez, monsieur le président, j'aimerais m'adresser aux témoins. Je ne sais pas si c'est prévu dans votre ordre du jour. Si oui, j'aimerais avoir quelques instants.

[*Traduction*]

Le président: Non, ce n'est pas prévu. Je regrette, mais vous ne pourrez pas vous adresser aux témoins.

[*Français*]

M. Rhéal Fortin: Non?

[*Traduction*]

Le président: Non, pas maintenant. Nous en sommes encore au premier groupe.

Monsieur Boucher, comme je le disais, plus ce sera court, mieux ce sera. Je vous remercie.

[*Français*]

M. André Boucher (sous-ministre adjoint, Opérations, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Merci, monsieur le président. Comme vous l'avez demandé, ma présentation sera plutôt courte.

Monsieur le président et distingués membres du Comité, je m'appelle André Boucher. Je suis sous-ministre délégué des opérations au Centre canadien pour la cybersécurité.

Tout d'abord, je vous remercie d'avoir accepté de nous recevoir et d'entendre mon témoignage cet après-midi.

En guise de préambule, permettez-moi de vous présenter brièvement l'organisme que je représente.

Le Centre canadien pour la cybersécurité a été institué le 1er octobre 2018 et relève du Centre de la sécurité des télécommunications. À titre d'autorité canadienne en matière de cybersécurité, l'organisme dirige les interventions du gouvernement suivant des événements liés à la cybersécurité.

Notre équipe nationale d'intervention travaille étroitement avec les ministères, les propriétaires et les exploitants d'infrastructures essentielles, les entreprises canadiennes et les partenaires internationaux pour intervenir en cas d'incidents de cybersécurité ou pour atténuer les conséquences qui découlent de ces incidents. Ce faisant, nous offrons des conseils et du soutien d'expert et coordonnons les communications d'information ainsi que les interventions en cas d'incident.

Les partenariats que le Centre canadien pour la cybersécurité établit avec les intervenants de l'industrie représentent un élément clé de notre mission. Nous avons pour objectif de promouvoir l'intégration de la cyberdéfense dans le modèle d'affaires de nos partenaires de l'industrie, ce qui aura pour effet d'accroître le niveau global de résilience du Canada à l'égard des cybermenaces. Or, malgré les efforts que l'industrie et le Centre ont à déployer, force est de constater que des cyberincidents ont tout de même lieu.

Cela m'amène à aborder le sujet dont j'aimerais vous entretenir cet après-midi. Il convient tout d'abord d'indiquer que le Centre canadien pour la cybersécurité n'est en mesure de fournir aucun détail concernant l'incident en question et qu'il n'émettra aucun commentaire quant aux pratiques de cybersécurité d'une entreprise particulière ou d'un individu. Au reste, toute forme d'atteinte à la cybersécurité peut être vue comme une occasion de réévaluer ses propres pratiques et de renforcer les systèmes, les processus ainsi que les mesures de protection.

Dans le cas présent, les articles de médias et les déclarations publiques indiquent qu'une divulgation de renseignements personnels a eu lieu suivant des actes commis par un individu œuvrant pour l'entreprise en cause, ce que l'on appelle communément une menace interne.

[*Traduction*]

Dans sa récente publication intitulée *Introduction à l'environnement de cybermenaces*, le Centre pour la cybersécurité décrit la menace interne comme étant ces individus qui travaillent dans un organisme, mais que l'on considère comme particulièrement dangereux, puisqu'ils ont accès à des réseaux internes qui sont protégés par des périmètres de sécurité. Pour tout intervenant malintentionné, l'accès est l'élément déterminant. Comme ils jouissent d'un accès privilégié aux données protégées par l'organisme qui les emploie, les auteurs de menace internes ne sont pas contraints de recourir aux méthodes que l'on doit normalement appliquer à distance, ce qui leur permet de collecter assez aisément de précieux renseignements. De fait, cet incident nous rappelle l'importance du facteur humain en matière de cybersécurité. Or, les menaces internes ne sont qu'un exemple de ce type de problème.

Les cybercriminels ont été particulièrement ingénieux lorsqu'il s'est agi d'exploiter le comportement humain à des fins de piratage psychologique et d'inciter les personnes à divulguer, bien qu'à leur insu, des renseignements sensibles. La sécurité de nos systèmes dépend essentiellement de la fiabilité des humains, c'est-à-dire les utilisateurs, les administrateurs et les équipes responsables de la sécurité.

Il convient donc de nous demander ce que nous pouvons faire dans un environnement où les cybermenaces se multiplient. Sur le plan de l'entreprise, il est capital d'adopter une approche globale qui se caractérise d'abord par la promotion d'une culture de sécurité et par la mise en place des politiques, des procédures et des pratiques nécessaires en matière de cybersécurité. Nous disposerons ainsi d'un plan d'intervention en cas de problèmes; et nous savons que des problèmes, il y en aura toujours.

Il faut investir pour que les personnes détiennent les moyens d'agir. La formation et la sensibilisation des personnes et des entreprises s'avèrent essentielles. Ce n'est que par la sensibilisation que nous pourrons continuer de développer et d'inculquer de bonnes pratiques de sécurité, une mesure essentielle pour protéger les systèmes informatiques du Canada.

Il faut également déterminer et protéger les actifs essentiels. Il importe de savoir où se trouvent les données clés. Assurez-vous donc de leur protection et surveillez les mesures de protection prises. Soyez prêts à intervenir.

Au Centre pour la cybersécurité, nous continuerons à travailler avec les intervenants de l'industrie ainsi qu'à fournir des conseils et des avis en matière de cybersécurité par l'intermédiaire de notre site Web. En l'occurrence, nous publions des alertes et des avis lorsque des cybermenaces, des vulnérabilités ou des incidents possibles, imminents ou réels touchent ou pourraient toucher les infrastructures essentielles du Canada.

Quoi qu'il advienne, il conviendra de poursuivre le dialogue que nous tenons présentement, de redoubler de vigilance et de porter une attention particulière aux enjeux de cybersécurité.

En dernière analyse, on constate qu'il n'existe aucun remède miracle lorsqu'il est question de cybersécurité. Il nous est donc interdit de baisser la garde. Les enjeux sont beaucoup trop importants. Certes, les prochaines avancées technologiques pourraient très bien nous faciliter la tâche, mais il n'en demeure pas moins que nous devrons toujours pouvoir compter sur un effectif compétent et fiable.

Je vous remercie, et je suis maintenant disposé à répondre à vos questions.

● (1355)

Le président: Je vous remercie, monsieur Boucher.

Nous passons maintenant à M. Picard, qui dispose de sept minutes.

[*Français*]

M. Michel Picard (Montarville, Lib.): En guise de préambule, je rappelle que l'incident dont nous parlons aujourd'hui s'inscrit tout à fait dans l'étude que nous faisons depuis le mois de janvier sur la cybersécurité et les crimes financiers.

J'ai déposé une motion pour que nous fassions une étude sur ce sujet, tel que suggéré par mes collègues libéraux. Cela démontre notre grande préoccupation au sujet de la cybersécurité dans les institutions financières. Je me réjouis que M. Scheer ait salué les efforts que nous avons faits dans le cadre de cette étude. Finalement, il est tout à fait d'accord sur mon initiative et je suis content qu'on contribue aux efforts du Parti libéral pour traiter des préoccupations liées à cybersécurité dans les institutions financières. Alors, merci.

Monsieur Flynn, je pense qu'il est important de s'adresser au public maintenant et de gérer ses attentes dans une situation aussi grave qu'un vol d'identité.

On souhaite que la police intervienne dans l'enquête criminelle. Pour la plupart, les gens veulent qu'on remédie à la perte de leurs données et que leur identité soit restaurée, sans crainte qu'on l'usurpe à nouveau dans 5, 10 ou 15 ans. Quelles sont les attentes du public relativement aux résultats de l'enquête criminelle?

[*Traduction*]

Surint. pr. Mark Flynn: Du point de vue des services de police, je crois que les gens s'attendent à ce qu'ils trouvent l'auteur du vol ou de la monétisation des données ainsi que tous ceux qui y ont participé de quelque façon, que ce soit par l'intermédiaire de cybermenaces, de cybercompromissions, de menaces internes, et j'en passe. Ils s'attendent à ce que ces personnes répondent de leurs actes devant la justice, à ce qu'il y ait des conséquences, puis à ce que l'on prenne des mesures pour éviter que de tels incidents se reproduisent.

[*Français*]

M. Michel Picard: Les gens ont beaucoup de mal à comprendre jusqu'à quel point c'est difficile de prouver qu'on est bien la personne qu'on prétend être. De quelle façon peut-on prouver sa propre identité? Ce sera un grand défi lorsque trois personnes se présenteront avec le même nom et le même numéro d'assurance sociale éventuellement.

● (1400)

[*Traduction*]

Surint. pr. Mark Flynn: En tant qu'agent de police, la confirmation de l'identité n'est pas mon domaine de compétence. Comme je l'ai dit plus tôt, je me tournerais vers les ressources locales, qu'il s'agisse d'institutions financières ou d'autres types de services. Si vous pouvez utiliser un service local pour confirmer votre identité, c'est la meilleure façon de gérer les demandes des entreprises à cet effet.

[*Français*]

M. Michel Picard: Dans une certaine mesure, l'enquête criminelle va rendre justice. Si on met la main au collet des criminels à la suite du dépôt de la preuve, on les poursuivra en justice et il y aura une conséquence judiciaire, essentiellement leur emprisonnement.

Cela dit, la donnée sur le marché représente un actif virtuel et ne se trouve pas dans un endroit physique donné; elle peut être à plusieurs endroits. Je ne veux pas alarmer les gens, mais il est important qu'ils réalisent que, bien qu'on ait arrêté les criminels, cela ne veut pas dire nécessairement que la donnée a été éliminée et que l'identité a été restaurée.

[*Traduction*]

Surint. pr. Mark Flynn: C'est exact. Il est important de souligner que les poursuites ne sont pas forcément le seul indicateur de réussite. En fait, dans le milieu du cyber, beaucoup de poursuites peuvent, au fil de nos collaborations, relever d'autres compétences.

Une des approches adoptées par la GRC, tout comme d'autres corps policiers d'ailleurs, est d'inclure des institutions financières et des experts en cybersécurité dans nos enquêtes criminelles, ce qui ne correspond pas à la façon dont nous procédons habituellement. Toutefois, nous en constatons déjà les résultats, puisque nous en tirons des avantages importants. Ces « partenaires », comme je les appelle, repèrent des renseignements qui ne paraissent pas forcément importants aux policiers. Sans leur aide, nous ne pourrions peut-être pas savoir que ces renseignements peuvent servir à protéger leurs clients. Je connais au moins un exemple dans le cadre d'une enquête majeure en cours où, grâce à une telle collaboration, plusieurs institutions financières ont pu repérer des comptes compromis et en atténuer les vulnérabilités.

Je crois donc que l'approche que nous avons adoptée engendre des avantages qui ne se quantifient pas seulement en arrestations et en poursuites.

[*Français*]

M. Michel Picard: Monsieur Boucher, vous avez une approche-conseil auprès des organismes. Comment une entreprise peut-elle se protéger de ses propres employés? Quels conseils peut-on lui donner à cette fin?

Comme on l'a vu cet hiver, il n'y a aucune raison de croire que les banques, les institutions financières et les entreprises de services financiers ne profitent pas de la meilleure technologie possible pour protéger leurs données des menaces extérieures. Ce qui nous préoccupe, ce sont les menaces qui viennent de l'intérieur. À mon avis, il n'y a pas de logiciel qui aide à contrer ce genre de risque. Quelle approche conseil avez-vous auprès des organismes pour couvrir le risque humain de fraude?

M. André Boucher: Je vous remercie de votre question.

Cela revient à mes commentaires d'ouverture. Il existe quelques outils, mais ce qui est le plus efficace, c'est de retourner aux principes de base et d'avoir une approche holistique et large en matière de sécurité.

Il faut d'abord avoir un programme de sécurité bien établi relativement au personnel à l'interne, bien comprendre où sont les choses qu'on veut protéger, connaître les individus avec qui on s'associe et avoir un programme toujours renouvelé. Ce n'est pas parce qu'on rencontre quelqu'un une fois dans une entrevue que sa situation de vie ne va pas changer. On renouvelle périodiquement ces conversations. Pour les individus, il y a un programme clair d'entraînement, de formation et de rafraîchissement des connaissances, lequel est soutenu par des processus clairs.

Les équipes de technologie de l'information ont accès à certains outils de prévention de la perte de données, notamment, qui peuvent contribuer à la détection d'une fraude. Cependant, par le temps qu'on détecte une fraude, il est souvent trop tard. Il est donc important d'investir le plus tôt possible dans l'édification d'une confiance et de s'entourer de gens fiables.

[*Traduction*]

Le président: Merci, monsieur Picard.

Monsieur Motz, vous avez cinq minutes.

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Merci, monsieur le président.

Je remercie tous les témoins de s'être déplacés.

Monsieur Boucher, vous avez déclaré dans vos commentaires d'ouverture que le Centre canadien pour la cybersécurité est l'autorité nationale en matière de cybersécurité et dirige la réponse du gouvernement en cas d'incident lié à la sécurité informatique, ce qui a attiré mon attention:

> Notre équipe nationale d'intervention travaille étroitement avec les ministères, les propriétaires et les exploitants d'infrastructures essentielles, les entreprises canadiennes et les partenaires internationaux pour intervenir en cas d'incidents de cybersécurité ou pour atténuer les conséquences qui découlent de ces incidents.

C'est fantastique. Et cela m'amène aussi à vous poser la question suivante: quelles sont les normes ou mesures appliquées à l'heure actuelle? Pour nous, le système bancaire canadien est une infrastructure essentielle de notre pays. Quelles sont les normes appliquées actuellement pour veiller à ce que ces attentes soient respectées? Y a-t-il des incitatifs? Y a-t-il des pénalités? Y a-t-il quoi que ce soit qui assure une approche uniforme au sein de ce secteur pour veiller à la sécurité des Canadiens? Nous sommes là pour servir les Canadiens. Je serais curieux de savoir s'il y a des exigences opérationnelles de base auxquelles tous les acteurs du secteur doivent se plier. S'il n'y en a pas, pouvez-vous me dire pourquoi? Et comment pouvons-nous en établir?

● (1405)

M. André Boucher: Je vous remercie pour votre question. Sa portée est très large. Je crois que, cet après-midi, vous entendrez des experts de ce secteur précis des institutions financières.

Je vous dirais que, du point de vue de la cybersécurité, le secteur financier est fort développé, puisqu'il comprend tant des organismes de réglementation que des pratiques exemplaires bien établis. En tant qu'experts de la cybersécurité, nous déployons des efforts considérables pour qu'une telle collaboration s'inscrive dans ces pratiques exemplaires. Nous laissons les organismes de réglementation du secteur établir les normes et lignes directrices de base, les revoir et assurer leur application. En fait, nous misons sur ce que chacun a de mieux à offrir et en tirons le maximum dans des secteurs en entier. Dans le cas présent, il s'agit du secteur financier. C'est l'un des secteurs très développés où la collaboration va de soi. C'est un secteur qui accorde sa véritable valeur aux risques pour la réputation. Des investissements majeurs sont faits à cet égard.

Sur le plan national, je crois que la présence de normes de base et d'organismes de réglementation qui veillent à leur application, sans compter des équipes qui s'emploient à aider les entreprises à offrir le meilleur rendement possible, est fort rassurante.

M. Glen Motz: Environ 2,9 millions de particuliers et d'entreprises au Canada sont touchés par cet incident, mais des millions d'autres au pays ont aussi été victimes d'un vol d'identité ou de renseignements relatifs à leur carte de crédit. Le fait d'apprendre que notre secteur bancaire est bien développé ne suffira peut-être pas à les réconforter, puisqu'ils continuent de subir les répercussions de ce méfait. Je serais curieux de savoir si nous sommes aussi énergiques que nous pourrions ou devrions l'être quant à la sécurité des institutions financières et des personnes qui leur accordent leur confiance.

M. André Boucher: Je vous assure que nous mettons énergiquement à profit toutes les mesures à notre disposition, qu'il s'agisse de pratiques exemplaires en matière de collaboration ou de mesures en place.

La triste réalité, comme je l'ai mentionné plus tôt, c'est que nous devons malheureusement tous vivre avec la perte de données et le fait que nous ne pourrons jamais les récupérer. Contrairement à un actif tangible, il n'est pas possible d'aller les chercher pour les ramener à la maison. C'est une nouvelle réalité, tant pour les clients que les entreprises.

Comme je l'ai souligné un peu plus tôt, cela vient confirmer toute l'importance d'investir tôt, tant dans l'acquisition de programmes que dans le recrutement mieux avisé des employés et l'adoption d'une approche globale en matière de sécurité afin de ne pas se retrouver en position de rattrapage.

M. Glen Motz: D'accord, merci.

Monsieur Flynn, les circonstances actuelles et d'autres avant cela nous ont appris que les données constituent la marchandise la plus courue sur le Web profond. Nous le savons. Le nom, l'adresse, la date de naissance, le numéro d'assurance sociale, l'adresse IP et le courriel des gens, toutes ces données sont de la marchandise échangée à volonté en ligne. Quelques questions me viennent d'ailleurs à l'esprit. Pouvez-vous aider la population canadienne à comprendre de quelle façon le milieu interlope utilise ces renseignements, mais aussi de quelle façon nous pouvons faire preuve de vigilance? Vous avez déjà partiellement répondu à M. Drouin, mais, en votre qualité de représentant de l'organisme national d'application de la loi, à quels signaux d'alarme les Canadiens devraient-ils prêter attention, selon vous, si leurs données ont été compromises, et même avant qu'elles le soient?

Le président: Monsieur Motz pose là une question importante. Malheureusement, il n'a plus de temps pour la réponse. Je vous invite donc à inclure votre réponse dans celle que vous ferez à une autre question. La séance dure trois heures et, si je ne respecte pas le temps alloué à chacun, nous ne nous en sortirons pas.

Madame Dabrusin, je vous en prie. Vous avez cinq minutes.

● (1410)

[*Français*]

Mme Julie Dabrusin (Toronto—Danforth, Lib.): Merci.

Quand nous avons fait notre étude au sujet des associations bancaires et de la cybersécurité, on a dit qu'il y avait beaucoup de sécurité du côté bancaire, ce qu'on remet peut-être en question maintenant, et on a parlé des individus comme s'ils étaient des boîtes de carton.

Qu'est-ce que les individus peuvent faire pour mieux se protéger? Pouvez-vous nous donner des informations et des données? Y a-t-il un endroit où les gens peuvent trouver de l'information, que ce soit sur des sites Web ou par téléphone, afin de mieux se protéger? Pouvez-vous nous aider, monsieur Boucher?

M. André Boucher: Je vous remercie de votre question.

Nous avons un très grand programme. Sur notre site Web, cyber.gc.ca, les gens peuvent trouver des mesures appropriées pour les individus. Effectivement, l'individu doit être alerte lorsqu'il navigue sur Internet. Cela est au cœur de la cybersécurité. Il faut savoir non seulement comment utiliser Internet, mais aussi ce qu'on met en commun avec les gens. Nous menons constamment des campagnes d'information sur l'utilisation des appareils et nous conscientisons les gens à l'importance de choisir ceux à qui ils communiquent de l'information privilégiée.

C'est une chose de se munir du meilleur appareil et de le tenir à jour, mais encore faut-il faire de bons choix. Il faut aller sur des sites Web d'entreprises qu'on considère comme fiables et qui ont une bonne réputation. Une fois qu'on a fait tout cela, il faut aussi choisir les renseignements qu'on transmet à l'entreprise en question. Il y a donc trois étapes, et toute cette information est disponible dans les avis que nous donnons aux gens.

Mme Julie Dabrusin: D'accord.

Il y avait aussi beaucoup d'information au sujet des mots de passe. Par exemple, on parlait des gens qui utilisent le même mot de passe pour toutes leurs activités sur Internet.

Est-ce que vous pouvez nous donner des informations sur les façons dont les gens peuvent mieux se protéger avec leurs mots de passe? C'est important.

M. André Boucher: Oui. Sur notre site Web — j'en fais toujours la promotion —, nous donnons des conseils précis sur la longueur et la complexité des mots de passe. Il y a aussi quelques trucs. Je veux laisser la chance aux gens d'aller en prendre connaissance par eux-mêmes. Il y a souvent des rumeurs disant qu'il faut changer souvent son mot de passe. Le problème, c'est que cela signifie que l'on doit mémoriser plusieurs mots de passe qui sont constamment en changement. Au fil du temps, l'avis a évolué. Maintenant, on dit qu'il faut au moins choisir un mot de passe solide, ce qui est défini par certains paramètres, que l'on peut trouver en ligne, qu'il s'agisse de la longueur ou de la complexité, selon ce que le fournisseur offre. S'il offre d'utiliser 15 caractères, on doit essayer de tous les utiliser. Si on ne nous en offre que huit, c'est déplorable, mais on doit alors choisir un mot de passe plus complexe.

Changer souvent son mot de passe n'a pas beaucoup de valeur si cela nous force à les noter quelque part ou à utiliser le même sur plusieurs sites. Ce que nous demandons aux gens, c'est d'être diligents et de choisir un mot de passe unique et aussi fort que le permettent les paramètres du fournisseur. Ils peuvent garder le même mot de passe, mais s'il y a un incident, ils doivent réagir rapidement, le changer et mettre en place des mesures de sécurité additionnelles. Il y a donc une combinaison de choses à faire.

Mme Julie Dabrusin: L'autre problème, c'est qu'une fois qu'ils ont trouvé un mot de passe qui fonctionne bien, les gens l'utilisent sur tous les sites Web. Certains sites Web nous disent qu'on a besoin de plus de caractères ou d'autres choses, mais on ne nous rappelle jamais que nous devrions avoir d'autres mots de passe et non utiliser le même partout. Est-ce que vous pouvez dire quelque chose à ce sujet aussi?

M. André Boucher: Là, vous me demandez d'être très pragmatique.

Mme Julie Dabrusin: Oui, mais c'est pragmatique.

M. André Boucher: Si je vais au-delà du conseil spécifique d'être très pragmatique, ce que je proposerais aux gens, c'est de regrouper leurs mots de passe selon le niveau d'incertitude qu'ils ont à l'égard des différents services qu'ils utilisent. Par exemple, pour leurs services bancaires, ils voudront utiliser plusieurs mots de passe distincts et les plus complexes possible. Par contre, pour leur compte sur le site de leur club local de curling ou d'autres comptes similaires, ils pourraient peut-être se donner la latitude d'utiliser le même mot de passe quelques fois, même si je ne le leur recommande pas.

Mme Julie Dabrusin: Qu'est-ce que les banques peuvent faire pour donner de meilleures informations aux gens qui utilisent leurs services?

M. André Boucher: Je crois que la plupart, sinon toutes les banques demandent un minimum de sophistication quant au mot de passe. Elles ont déjà établi une certaine norme pour se protéger elles-mêmes d'un client qui ne serait peut-être pas diligent dans la sélection de son mot de passe.

[*Traduction*]

Le président: Merci, madame Dabrusin.

Bienvenue au Comité, monsieur Clarke. La parole est à vous. Vous avez cinq minutes.

[*Français*]

M. Alupa Clarke (Beauport—Limoilou, PCC): Merci, monsieur le président. Je suis très content d'être ici.

Je vous remercie, messieurs, d'être ici aujourd'hui et de donner de votre temps pour rassurer les Canadiens et répondre à nos questions.

Une des pierres angulaires du contrat social que nous avons sur notre territoire, c'est la protection des citoyens, non seulement celle qu'ils s'offrent réciproquement entre eux, mais aussi celle qu'ils reçoivent de l'État. Depuis trois semaines, les citoyens de toutes nos circonscriptions sont extrêmement préoccupés. Deux jours après que la fuite de données a été rendue publique, des gens venaient à mon bureau. Lorsque je faisais du porte-à-porte, c'est tout ce dont ils me parlaient. Il y a donc une vraie préoccupation et les gens sentent qu'il n'y a aucune réponse de la part du gouvernement.

Ce que mes concitoyens voudraient savoir de votre part, monsieur Boucher, est très simple: est-ce que le Centre canadien pour la cybersécurité peut effectivement assurer la sécurité en bonne et due forme des 2,9 millions de Canadiens qui ont été touchés par ce vol de données personnelles, oui ou non?

Est-ce que votre institution a les outils nécessaires pour faire face à cette situation et assurer la protection des citoyens victimes de vol d'identité?

● (1415)

M. André Boucher: Il est juste de dire que le Centre canadien pour la cybersécurité a les moyens de prendre des mesures concernant tous les aspects de la cybersécurité. Nous traitons aujourd'hui d'un cas de menace interne et de vol d'informations. Ce n'est pas, au sens strict, une question de cybersécurité...

M. Alupa Clarke: Je ne parle pas de l'événement qui est arrivé, je parle de ce qui va arriver prochainement. C'est cela qui inquiète les citoyens. Je veux savoir si le Centre canadien pour la cybersécurité a la capacité de faire face aux fraudeurs internationaux ou nationaux qui tentent d'envoyer des messages textes ou quoi que ce soit.

Votre organisme a-t-il la capacité de faire face à cela?

M. André Boucher: Je ne tente pas d'échapper à votre question, mais elle concerne plutôt un problème de loi ou de fraude, et non un problème de cybersécurité. Cela ne veut pas dire que, si nous voyons des manifestations, nous les ignorerions.

Nous commençons chaque journée en discutant avec nos partenaires, incluant ceux de la GRC, afin de leur faire part de ce que nous savons et de ce qu'il y a de nouveau. Nous nous assurons que l'intervenant responsable du dossier fera quelque chose de cette information. L'équipe nationale est la meilleure qui soit et ces gens ne vont rien laisser tomber. Ils vont tenter de régler les problèmes et de faire le maximum pour prendre soin de la sécurité des Canadiens.

M. Alupa Clarke: Je vais profiter de votre expertise en cybersécurité.

Notre système actuel de numéros d'assurance sociale est-il adéquat dans ce monde contemporain où Internet prend toute la place? C'est rendu à un point où les gens font leurs achats avec leur téléphone ou paient en quelques secondes à une caisse. Notre système de numéros d'assurance sociale est-il adéquat dans le monde dans lequel nous vivons aujourd'hui?

M. André Boucher: Je vous remercie encore de votre question. Vous ne posez pas des questions faciles, monsieur Clarke.

Je ne suis pas un expert en numéros d'assurance sociale et leur utilisation, mais je peux parler d'identifiants. Quels que soient les identifiants dont on se munit, que ce soit des identifiants cryptologiques complexes ou simples, il y a toujours un problème de gestion de l'information et de vol possible de l'information. C'est un problème très complexe et je vais laisser aux experts en numéros d'assurance sociale le soin de répondre à l'aspect spécifique de votre question.

Selon moi, le problème plus large est la gestion des identifiants. C'est un morceau d'information clé qu'il faut apprendre à gérer dans les systèmes de sécurité larges dont je parlais.

M. Alupa Clarke: Monsieur le surintendant, j'ai une question qui va dans le même sens que celle de mon collègue M. Motz.

Tous les gens qui m'ont abordé dans la rue, au bureau ou lors d'un porte-à-porte m'ont posé la même question. Ils m'ont demandé quels actes criminels ces fraudeurs commettront ultérieurement et à quoi il faut s'attendre. Quels actes criminels seront posés en ce qui concerne les 2,9 millions de Canadiens touchés par cette immense fuite de données?

Ensuite, dans combien de temps ces actes seront-ils posés? En ce moment, les médias disent toutes sortes de choses. On dit notamment que cela prendra cinq ou dix ans avant que les fraudeurs n'agissent et qu'ils attendront que la poussière retombe.

[*Traduction*]

Le président: Ici encore, la question est importante. Vous avez une quinzaine de secondes pour y répondre.

Surint. pr. Mark Flynn: Le fait est que, dès que des renseignements personnels, des mots de passe, etc. se retrouvent sur Internet, ils y demeurent à perpétuité. Les gens doivent être vigilants par rapport à cela, et utiliser les services à leur disposition, comme la surveillance du crédit, pour s'assurer que des déclencheurs sont activés quand quelqu'un essaie d'utiliser ces renseignements, ce qui les prévient et contribue à lutter contre la fraude.

C'est ce que je peux vous dire avec le temps qui m'est imparti.

● (1420)

Le président: Merci, monsieur Clarke.

Monsieur Graham, vous avez cinq minutes.

[*Français*]

M. David de Burgh Graham: Il y a une quinzaine d'années, j'étais sur un canal d'IRC — je ne sais pas si vous connaissez cela —, et quelqu'un y offrait des numéros de cartes de crédit avec les trois chiffres derrière ainsi que l'adresse; tout était prêt. Il demandait aux gens s'ils souhaitaient les acheter. Je trouvais que cela n'avait pas d'allure et j'ai voulu appeler la police ou différents services, mais personne ne répondait ou ne savait quoi faire.

Si quelqu'un voyait quelque chose de semblable sur Internet aujourd'hui, y a-t-il un endroit où il pourrait le rapporter?

[*Traduction*]

Surint. pr. Mark Flynn: La GRC, en collaboration avec la Police provinciale de l'Ontario et le Bureau de la concurrence, exploite le Centre antifraude du Canada. C'est l'un des meilleurs endroits où signaler des activités frauduleuses, que ce soit un numéro de téléphone utilisé par les fraudeurs, un vol d'identité ou un cas de fraude. Le Centre compile ce type de renseignements. Il les transmet. Des enquêtes policières sont lancées d'après ces renseignements. C'est le premier endroit où vous devriez appeler, de même qu'à votre poste de police.

Les forces de l'ordre locales, que ce soit la GRC ou un autre corps policier dans le cas de l'Ontario et du Québec, doivent être mises au courant des crimes perpétrés. Il y a un lien entre le crime organisé impliqué dans les cas de fraude et les autres activités criminelles.

[*Français*]

M. David de Burgh Graham: Quels sont les pouvoirs du Centre canadien pour la cybersécurité? Que peut-il faire?

M. André Boucher: Parlez-vous en général ou du cas qui nous occupe?

M. David de Burgh Graham: Je parle en général. Les gens de ce centre prennent-ils les commentaires de l'extérieur ou travaillent-ils seulement avec les entreprises? Expliquez-moi ce qu'ils font.

M. André Boucher: Comme je l'expliquais tout à l'heure, le Centre canadien pour la cybersécurité est responsable de donner des avis. Il prépare et protège l'information d'intérêt national. Il s'occupe de la gestion des incidents et des stratégies d'atténuation qui s'ensuivent. Toutes les étapes se déroulent en coordination avec les partenaires du Centre, conformément à son mandat. Quand il y a des problèmes de fraude, on fait appel à l'équipe nationale, qui est formée des centres qui ont déjà été nommés. On s'assure que l'information disponible est mise en commun et on va de l'avant. Le dossier se poursuit, et si plus d'information est disponible, on la transmet à la personne responsable.

Voici ce que ce modèle d'affaires a d'intéressant. S'il survient un changement pendant que le dossier est en cours, par exemple s'il ne s'agit plus d'une enquête, le Centre canadien pour la cybersécurité va le prendre en charge jusqu'à ce que la victime ait eu... jusqu'à la fermeture du dossier, si vous voulez.

M. David de Burgh Graham: Tout à l'heure, on a parlé de mots de passe. Maintenant, on voit beaucoup plus l'authentification de deux facteurs en ce qui concerne les comptes de banque. Pourrait-on faire la même chose pour le numéro d'assurance sociale?

M. André Boucher: Je vais répondre la même chose que tout à l'heure. Je ne suis pas un expert en numéros d'assurance sociale, mais nous recommandons fortement aux gens, quand c'est possible, de se servir des deux facteurs. Ce n'est pas parfait, mais cela améliore la sécurité de leurs renseignements.

M. Michel Picard: J'aimerais revenir sur la question de l'identifiant unique.

Il y a d'autres modèles. Dans d'autres comités, on a parlé du fameux modèle de l'Estonie, je crois. Ce système va dans le sens des discussions que nous avons eues sur le système bancaire ouvert, où toute l'information est centralisée et où les gens peuvent y avoir accès en fournissant un numéro d'identification unique.

Au bout du compte, peu importe le nom qu'on lui donne, le numéro d'assurance sociale est un numéro d'identification unique. Il faut comprendre les limites de notre système. On a beau avoir un système ultra moderne et par excellence, si on revient à une seule et unique façon d'identifier quelqu'un, la donnée sera toujours vulnérable si quelqu'un met la main dessus.

M. André Boucher: Tout à fait. On ne peut pas les nommer aujourd'hui, mais plusieurs pays ont tenté d'avoir un numéro d'identification unique national. Quelques-uns ont connu du succès et d'autres, un peu moins, parce que, comme vous l'avez dit, ce numéro devient une donnée essentielle et que, s'il y a la moindre faiblesse, il risque d'être exploité.

M. Michel Picard: Votre organisation gère-t-elle elle-même les données personnelles de ses employés?

M. André Boucher: Oui, absolument, avec toutes les mesures dont je parlais tout à l'heure.

M. Michel Picard: Comment fait-on pour se protéger d'un employé qui est de mauvaise humeur un matin et qui décide de traverser la clôture?

M. André Boucher: Nous avons un programme exhaustif de sécurité qui s'applique dès la sélection du personnel. Évidemment, il y a une culture de sécurité dans l'ensemble de notre organisation, ce qui comprend la sécurité du personnel, la sécurité physique et la sécurité des systèmes informatiques.

Les processus sont en place. C'est un système *evergreen*, c'est-à-dire qu'il doit toujours être mis à jour. On ne se repose pas sur le système en place, on revoit celui-ci périodiquement. C'est vaste et complexe, mais c'est un investissement qui en vaut la peine.

● (1425)

M. Michel Picard: Votre approche est-elle utilisée ailleurs sur le marché? Y a-t-il un organisme qui a mis en place une culture de sécurité semblable à celle que vous développez?

M. André Boucher: Notre approche est moderne et nous n'avons pas le monopole en la matière. Vous pouvez trouver des documents. Sécurité publique Canada a publié un document décrivant la façon de se munir d'un système de sécurité. C'est une très bonne source de référence et cela touche les mêmes modèles que ceux que nous avons.

M. Michel Picard: Merci, monsieur Boucher.

[*Traduction*]

Le président: Merci, monsieur Picard.

Monsieur Dubé, vous avez trois minutes.

Monsieur Fortin, il nous restera ensuite quelques minutes. Souhaitez-vous avoir un peu de temps pour poser des questions?

M. Rhéal Fortin: Oui, s'il vous plaît.

Le président: Allez-y, monsieur Dubé.

[*Français*]

M. Matthew Dubé: Merci, monsieur le président.

Monsieur Boucher, je n'ai pas eu la chance de vous poser des questions tout à l'heure.

Ma première question concerne ce qu'a dit votre collègue M. Scott Jones, qui a comparu devant notre comité dans le cadre de l'étude à laquelle on fait référence régulièrement aujourd'hui. Il a mentionné qu'il était important que les institutions et les entreprises signalent les vols ou les fuites de données qui les touchent.

La recommandation du Comité était plutôt vague. Devrait-on insister sur le fait qu'il faut signaler ce genre de fuites à la police, afin de minimiser les dégâts pour la population et arrêter ceux qui ont commis le crime?

Cela m'amène à deux autres questions, lesquelles s'adressent à vous, monsieur Flynn.

Étant donné que l'information va demeurer sur Internet à perpétuité, la police doit-elle traiter ces menaces de la même façon que les menaces physiques? Si un meurtrier ou quiconque pose une menace physique, j'imagine qu'il y a un certain sentiment d'urgence dans les enquêtes policières. Devrait-on faire la même chose dans le cas des cybermenaces? Desjardins a quand même communiqué avec la SQ au mois de décembre, si je ne m'abuse.

Ma dernière question concerne les vérifications d'antécédents et les vérifications continues de sécurité. Maintenant que des individus possèdent une expertise très élevée en la matière, ces vérifications doivent-elles devenir la norme?

Je vous laisse répondre dans le temps qui reste.

M. André Boucher: Concernant le signalement d'incidents, je vous rappelle que nous recommandons d'investir avant l'incident. Il faut qu'il y ait un programme de sécurité et de détection, et ainsi de suite. Nous recommandons toujours aux gens de signaler un incident et d'en faire part à leur communauté, parce qu'il y a probablement des points communs. Ainsi, tous pourront apprendre de cet incident.

En tant que centre national de cybersécurité, nous essayons de recueillir de telles informations dans toutes les communautés, de trouver les points communs et d'émettre des avis qui pourraient augmenter la sécurité à l'échelle nationale. Effectivement, il faut signaler les incidents.

[*Traduction*]

Surint. pr. Mark Flynn: En ce qui a trait aux menaces physiques par rapport aux cybermenaces, je suis d'accord avec vous. C'est très difficile à comprendre. Les forces de l'ordre peinent à établir l'allocation de leurs ressources, car elles cherchent toujours à cibler ce qui aura le plus d'effet sur la réduction des méfaits.

Prenons la fraude. C'est une menace très grave, tant au Canada qu'à l'échelle mondiale. Il est difficile de comparer une fraude de 400 000 $ ou de 2 millions de dollars à une menace physique ou à un homicide, voire à une agression. Cela nous donne bien du mal, mais je peux vous confirmer que nous en sommes conscients et que nous évaluons actuellement notre façon de jauger ce risque et d'établir nos priorités.

[*Français*]

M. Matthew Dubé: Ne serait-il pas pertinent de dire que cela a une incidence permanente sur la vie d'une personne et de voir les choses de cette façon?

[*Traduction*]

Surint. pr. Mark Flynn: Oui, c'est indéniablement un facteur.

Le président: Merci, monsieur Dubé.

[*Français*]

Monsieur Fortin, vous avez deux minutes.

M. Rhéal Fortin: J'aimerais poser rapidement une question à M. Flynn. Je dis « rapidement » parce que je n'ai que deux minutes et que j'avais aussi une question à poser à M. Boucher.

Il y a deux ans, 19 millions de Canadiens ont été l'objet d'une fraude chez Equifax. Il s'agissait d'un vol de données semblables. L'an dernier, on parlait d'environ 90 000 clients de la CIBC et de la BMO. Cette année, il s'agit de clients de Desjardins.

Pouvez-vous nous dire s'il y a eu une augmentation des crimes liés à l'utilisation de ces données à la suite de ces événements?

[*Traduction*]

Surint. pr. Mark Flynn: Des données tirées de ces comptes compromis en tant que telles?

[*Français*]

M. Rhéal Fortin: Oui, mais je parle de ce type de crime.

● (1430)

[*Traduction*]

Surint. pr. Mark Flynn: Nous constatons que les fraudeurs utilisent des renseignements compromis pour effectuer leurs transactions. L'enquête de la GRC sur Leakedsource.com s'est avérée concluante: ce site revendait des renseignements tirés d'une imposante banque de données compromises rendues publiques. L'accusé a plaidé coupable.

La revente de tels renseignements n'est pas inhabituelle, comme en témoignent divers incidents.

[*Français*]

M. Rhéal Fortin: D'accord, mais est-ce que le taux de criminalité lié à l'utilisation de ces données volées a augmenté?

[*Traduction*]

Surint. pr. Mark Flynn: Je n'ai pas pris en note le taux de criminalité en particulier, mais il va sans dire que c'est le genre d'activités criminelles dont nous sommes témoins.

[*Français*]

M. Rhéal Fortin: D'accord.

Ma seconde question s'adresse à M. Boucher.

Monsieur Boucher, dans votre témoignage écrit, vous donnez trois recommandations. La deuxième consiste à investir dans la formation et la sensibilisation pour que les personnes aient les moyens d'agir. Est-ce que le gouvernement fédéral a prévu des investissements pour collaborer avec le gouvernement du Québec en vue d'améliorer la sécurité des Québécois?

M. André Boucher: Je peux parler de mon organisation. Nous avons une responsabilité nationale, et travailler avec nos partenaires du Québec en fait partie. Nous investissons dans l'éducation et la formation et nous offrons aussi nos services aux entreprises québécoises...

M. Rhéal Fortin: Excusez-moi de vous interrompre, je ne veux pas vous bousculer, mais comme vous le savez, deux minutes, c'est court.

Y a-t-il des projets d'investissement, et si c'est le cas, pouvez-vous les chiffrer? Par exemple, le fédéral a-t-il dégagé une enveloppe d'un certain nombre de millions de dollars pour s'entendre avec Québec sur un programme de formation ou autre en lien avec la cybercriminalité?

M. André Boucher: Je n'ai pas cette information avec moi aujourd'hui.

M. Rhéal Fortin: D'accord.

Je vous remercie.

[*Traduction*]

Le président: Vous n'aurez malheureusement pas le temps de répondre à cette question.

Avant de suspendre la séance, je voudrais simplement revenir au point trois de votre présentation, monsieur Boucher, où vous dites: « II faut également déterminer et protéger les actifs essentiels. II importe de savoir où se trouvent les données clés. Assurez-vous donc de leur protection et surveillez les mesures de protection prises. Soyez prêts à intervenir. » Autrement dit, des réseaux à confiance zéro, ce dont nous entendons parler depuis six mois.

Est-ce la norme qui devrait s'appliquer à toute institution financière, pas seulement à Desjardins?

M. André Boucher: Je crois que toute grande entreprise doit évaluer ses actifs essentiels et leur valeur, puis décider de l'ampleur de ses investissements dans leur protection en fonction du risque. En partant du principe de la confiance zéro, le fait est que nous vivons aujourd'hui dans un environnement complexe. Il ne faut donc pas présumer que le système va fonctionner en vase clos. Il faut investir dans un programme de sécurité de façon globale, soit dans les bonnes personnes, les bons processus et la bonne technologie. L'ensemble de ces éléments vont...

Le président: C'est une norme qui fait l'unanimité dans le milieu du cyber, si je puis dire, cette idée de confiance zéro, à votre point trois.

M. André Boucher: On s'entend pour dire qu'il faut investir dans tous ces éléments.

Le président: Merci, monsieur Boucher.

Sur ce, nous allons suspendre la séance.

Nous devons entendre des représentants du gouvernement et faisons somme toute des progrès intéressants. Je présume, mais sans savoir si j'ai raison, que si je suspends la séance pendant deux ou trois minutes, nous pouvons reprendre les travaux avec les témoins du gouvernement et poursuivre sur notre lancée. Est-ce que cela vous convient, chers collègues?

D'accord. Sur ce, la séance est suspendue et reprendra avec les témoins du gouvernement. Merci.

● (1430)

(Pause)

● (1435)

Le président: Reprenons nos travaux. Je tiens à remercier les représentants du gouvernement pour leur souplesse et les prie de faire preuve d'un peu plus de patience, car le Comité attend toujours l'arrivée des représentants de Desjardins.

J'invite les divers représentants de Revenu Canada, du ministère des Finances, du ministère de l'Emploi et du Développement social et du Bureau du surintendant des institutions financières à être brefs. Si les représentants de Desjardins ont un temps limité à nous consacrer, je vais, s'ils se présentent, suspendre la séance un instant après vos déclarations et vous prier de vous asseoir au fond de la salle afin que nous puissions discuter avec eux pendant un certain temps. Ensuite, je vous demanderai de revenir devant le Comité, et les membres pourront vous poser des questions, si cela vous convient. Même si cela ne vous semble pas une façon convenable de mener la séance, c'est ainsi que nous allons procéder, donc je vais simplement demander au représentant de Revenu Canada ou du ministère des Finances de prendre la parole, selon celui qui souhaite s'exprimer en premier.

Mme Annette Ryan (sous-ministre adjointe déléguée, Direction de la politique du secteur financier, ministère des Finances): Merci, monsieur le président. Je vais commencer, si cela vous convient.

[*Français*]

Je m'appelle Annette Ryan. Je suis sous-ministre adjointe déléguée de la Direction de la politique du secteur financier au ministère des Finances. Je suis accompagnée de Robert Sample, directeur général de la Division de la stabilité financière et des marchés des capitaux, ainsi que de Judy Cameron, directrice principale du Bureau du surintendant des institutions financières du Canada, ainsi que de son collègue. Nous sommes heureux d'être ici avec vous aujourd'hui.

● (1440)

[*Traduction*]

Mes remarques porteront sur deux sujets que je crois pertinents dans le contexte des questions dont vous êtes saisis. Plus particulièrement, je vais préciser les rôles des ministères et agences du gouvernement ainsi que des acteurs du secteur privé dans le cadre fédéral régissant le secteur financier, et fournir une mise à jour au Comité quant aux efforts entrepris par le ministère des Finances, les organismes fédéraux de réglementation et les banques pour appuyer la cybersécurité et la protection des données.

La protection de la vie privée et des données personnelles et financières des Canadiens est un objectif partagé du gouvernement et du secteur privé; il s'agit d'un objectif qui est essentiel au maintien continu de la confiance dans le système bancaire canadien.

Je vais aborder la question des rôles au sein du gouvernement fédéral, puis de celui des gouvernements provinciaux et des acteurs du secteur privé.

Le ministère des Finances et les organismes fédéraux de surveillance du secteur financier sont chargés des lois et des règlements qui régissent le système bancaire canadien sous juridiction fédérale. Collectivement, nous établissons les attentes et en surveillons la mise en œuvre afin de garantir que les risques opérationnels liés à la cybersécurité et à la protection de la vie privée sont convenablement gérés par les institutions financières que nous réglementons.

Le ministre des Finances a une responsabilité générale envers la stabilité et l'intégrité du système financier canadien. La cybersécurité est un aspect essentiel de la stabilité du secteur financier, car elle permet au secteur de demeurer résilient face aux cybermenaces et aux cyberattaques.

Le ministère de la Sécurité publique a, à son tour, reconnu le secteur des services financiers comme un secteur d'importance critique dans le cadre de sa Stratégie nationale sur les infrastructures essentielles.

Le ministère des Finances travaille étroitement avec un ensemble d'intervenants responsables de la réglementation du secteur financier et de la cybersécurité, tant au niveau national qu'avec nos partenaires internationaux, afin de s'assurer que le secteur adopte des pratiques appropriées pour favoriser la cyber-résilience et la protection des données et aussi afin de faire en sorte que les besoins du secteur financier soient pris en compte dans les politiques portant sur l'ensemble de l'économie et la législation ayant trait à la cybersécurité et à la protection des données.

Je vais maintenant aborder les responsabilités des différents régulateurs du secteur financier. Le Bureau du surintendant des institutions financières, l'organisme de réglementation prudentielle des institutions financières fédérales — par exemple, les banques — élabore des normes et des règles pour gérer les risques en matière de cybersécurité. Ceci est conforme à son mandat plus vaste de surveillance des risques opérationnels que les institutions financières doivent gérer.

La Banque du Canada surveille les infrastructures du marché financier, comme les systèmes de paiements, afin d'accroître leur résilience aux cybermenaces et coordonne les réponses de l'ensemble du secteur en cas d'incident opérationnel systémique.

D'autres organismes fédéraux sont responsables de la législation entourant le respect de la vie privée. Le Commissariat à la protection de la vie privée veille à ce que les banques respectent la Loi sur la protection des renseignements personnels et les documents électroniques, qui régit la protection des renseignements personnels dans le secteur privé canadien. Cette loi établit les exigences auxquelles les entreprises doivent satisfaire relativement à la collecte, à l'utilisation ou à la divulgation de données personnelles dans le cadre d'activités commerciales. Ces exigences comprennent la mise en place de mesures de protection appropriées pour protéger les données personnelles contre la perte, le vol ou la divulgation non autorisée.

Le ministère de l'Innovation, des Sciences et du Développement économique a une responsabilité stratégique globale à l'égard de la Loi sur la protection des renseignements personnels et les documents électroniques. En novembre 2018, le gouvernement du Canada a modifié les dispositions de la loi relatives au signalement d'atteinte à la protection des données et aux sanctions pécuniaires connexes pour ne pas avoir signalé une fraude.

Comme vous l'avez entendu plus tôt, d'autres agences et ministères fédéraux, y compris Sécurité publique, le Centre canadien pour la cybersécurité et la Gendarmerie royale du Canada, partagent des responsabilités à l'égard de plus vastes initiatives de cybersécurité du gouvernement du Canada.

[*Français*]

Il est important de noter que la responsabilité de la surveillance du secteur financier canadien est partagée entre les gouvernements fédéral et provinciaux. Les provinces sont chargées de la surveillance des courtiers en valeurs mobilières, des conseillers en épargne collective et en fonds de placement, des coopératives provinciales, ainsi que des caisses d'épargne, des sociétés de fiducie, des compagnies d'assurances et des sociétés de prêt constituées par une loi provinciale.

Par conséquent, les autorités fédérales et provinciales du secteur financier ont des protocoles en place à l'égard de l'échange de renseignements, particulièrement pour les questions relatives à la stabilité financière. Les institutions financières ont bien sûr la responsabilité première quant au maintien de la cybersécurité et de la protection des données sur une base quotidienne, puisqu'elles gèrent directement les risques opérationnels grâce à un ensemble exhaustif de mesures de protection et de prévention sur le plan individuel et à la coopération avec les autres acteurs de l'industrie.

Ces mesures sont appuyées par des politiques et des normes qui sont constamment mises à jour pour répondre aux menaces changeantes et demeurent conformes aux pratiques exemplaires de l'industrie.

● (1445)

[*Traduction*]

Les cyberattaques sont une menace sérieuse et permanente. J'aimerais aborder quelques-unes des mesures mises en place par le gouvernement du Canada, les organismes de réglementation du secteur financier et les banques afin de renforcer la cybersécurité dans le secteur financier.

Dans le budget de 2018, le gouvernement fédéral a investi plus d'un demi-milliard de dollars dans la cybersécurité et, en octobre 2018, le gouvernement a établi le Centre canadien pour la cybersécurité, qui sert de guichet unique d'expertise et de conseils techniques pour les Canadiens, les gouvernements et les entreprises. Le Centre lutte contre les auteurs de cybermenaces qui ciblent des entreprises canadiennes, y compris les institutions financières fédérales et provinciales, en vue d'obtenir des données de leurs clients, des renseignements financiers et des systèmes de paiement. Les efforts de lutte contre la cybercriminalité ont été stimulés par le Centre national de coordination de la lutte contre la cybercriminalité nouvellement créé au sein de la GRC, qui fournit un mécanisme national de signalement des cybercrimes, y compris les atteintes à la protection des données ou les fraudes financières.

Plus récemment, dans le budget de 2019, le gouvernement a proposé une loi et un financement afin de protéger les cybersystèmes essentiels dans les secteurs canadiens des finances, des télécommunications, de l'énergie et des transports.

[*Français*]

Nos collègues du Secrétariat du Conseil du Trésor continuent de travailler conjointement avec les gouvernements provinciaux, les institutions financières et les partenaires fédéraux à l'élaboration d'un cadre de confiance pancanadien sur l'identité numérique qui vise à renforcer la protection de l'identité numérique dans le contexte des cybermenaces.

[*Traduction*]

En ce qui concerne la réglementation, plus tôt cette année, le Bureau du surintendant des institutions financières a publié un nouveau guide sur les exigences de signalement des incidents liés à la technologie et à la cybersécurité par l'entremise du préavis sur le signalement des incidents liés à la technologie et à la cybersécurité. Ces directives visent à aider le bureau à déterminer où les banques peuvent prendre des mesures pour prévenir de façon proactive les incidents liés à la cybersécurité ou, lorsqu'un incident survient, à améliorer leur résilience cybernétique.

Bien que notre principal rôle soit de prévenir les atteintes à la protection des données, la réalité est que ces incidents surviennent et ils ne se limitent pas qu'au secteur financier. Cela étant dit, lorsqu'un incident lié à la cybersécurité survient dans une institution fédérale sous réglementation fédérale, des mécanismes de contrôle et de surveillance sont en place pour le gérer.

En résumé, la cybersécurité est un domaine d'une importance critique pour le ministère des Finances. Nous collaborons activement avec des partenaires de l'ensemble du gouvernement et du secteur privé pour nous assurer que les Canadiens sont bien protégés contre des incidents liés à la cybersécurité et que, lorsqu'ils surviennent, les incidents sont gérés de façon à atténuer les répercussions sur les consommateurs et le secteur financier dans son ensemble.

Je vous remercie de votre temps. Je serai heureuse de répondre à vos questions.

[*Français*]

Le vice-président (M. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, PCC)): Merci, madame Ryan.

Nous passons maintenant à Mme Boisjoly.

Mme Elise Boisjoly (sous-ministre adjointe, Direction générale des services d'intégrité, ministère de l'Emploi et du Développement social): Merci beaucoup, monsieur le président.

Je m'appelle Elise Boisjoly et je suis la sous-ministre adjointe responsable des services d'intégrité à Emploi et Développement social Canada. Je suis accompagnée par Mme Anik Dupont, responsable du programme du numéro d'assurance sociale.

Je vous remercie de m'avoir donné l'occasion de m'adresser à vous aujourd'hui. Mon allocution portera sur le programme du numéro d'assurance sociale. Plus précisément, j'aimerais clarifier ce qu'est le numéro d'assurance sociale, fournir des renseignements sur son émission et son utilisation, informer le Comité sur la protection de la vie privée en ce qui concerne le numéro d'assurance sociale, et fournir de l'information sur notre approche en cas de fuite d'informations personnelles.

Le numéro d'assurance sociale est un identificateur de dossier ou un numéro de compte utilisé par le gouvernement du Canada pour coordonner l'administration des prestations et services fédéraux, et par le système du revenu. Le numéro d'assurance sociale est requis pour chaque personne qui occupe un emploi assurable ou donnant droit à une pension au Canada, et pour produire une déclaration de revenus.

Un numéro d'assurance sociale est émis avant le premier emploi, en arrivant au Canada pour la première fois ou même à la naissance. Au cours de la dernière année financière, plus de 1,6 million de numéros d'assurance sociale ont été émis.

Le numéro d'assurance sociale sert, entre autres, à verser plus de 120 milliards de dollars en prestations et à percevoir plus de 300 milliards de dollars en impôts. Il facilite l'échange d'information pour permettre l'allocation de prestations et de services aux Canadiens tout au long de leur vie, comme les prestations pour la garde d'enfants, les prêts étudiants, l'assurance-emploi, les pensions et même les prestations de décès. Ainsi, un numéro d'assurance sociale est attribué à une personne pour la vie.

Le numéro d'assurance sociale n'est pas un identificateur national et ne peut pas être utilisé pour obtenir une identification. En fait, il n'est même pas utilisé par tous les programmes du gouvernement fédéral, seulement par un certain nombre. Le numéro d'assurance sociale seul n'est pas suffisant pour accéder à un programme ou à un avantage gouvernemental, ou même pour obtenir du crédit ou des services dans le secteur privé. Des informations supplémentaires sont toujours requises.

● (1450)

[*Traduction*]

Bien que les fuites de données soient de plus en plus courantes, le gouvernement du Canada suit des procédures rigoureuses et établies pour protéger les renseignements personnels des particuliers. Ma collègue a fait mention de la Loi sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels et les documents électroniques, qui est administrée par Innovation, Sciences et Développement économique Canada. Ces lois établissent le cadre juridique régissant la collecte, la conservation, l'utilisation, la divulgation et l'élimination des renseignements personnels dans le contexte de l'administration des programmes des institutions gouvernementales et des activités du secteur privé.

Comme l'a dit ma collègue, le 1er novembre 2018, une nouvelle modification a été apportée à la Loi sur la protection des renseignements personnels et les documents électroniques exigeant que les organisations faisant face à une fuite de données et ayant des raisons de croire qu'il y a un risque réel de préjudice grave en informent le Commissariat à la protection de la vie privée, les personnes affectées ainsi que les organisations associées dès que possible. La violation de cette disposition peut conduire à des amendes allant jusqu'à 100 000 $ par infraction.

Au sein d'Emploi et Développement social Canada , nous avons des stratégies de surveillance interne, des politiques de confidentialité, des directives et des outils d'information sur la gestion de la protection de la vie privée, ainsi qu'un code de conduite ministériel et des formations obligatoires pour nos employés sur la protection des renseignements personnels. Nous croyons que toute atteinte à la sécurité touchant le numéro d'assurance sociale est très grave et, en fait, le gouvernement du Canada n'est pas à l'abri de telles situations. Par exemple, en 2012, des informations concernant des prêts étudiants canadiens ont été potentiellement compromises. Cette fuite a servi de catalyseur à l'amélioration des pratiques de gestion de l'information au ministère.

La prévention de la fraude en matière de numéro d'assurance sociale commence par l'éducation et la sensibilisation. C'est pourquoi notre site Web et nos documents de communication contiennent des renseignements qui aident les Canadiens à mieux comprendre les mesures qu'ils devraient prendre pour protéger leur numéro d'assurance sociale. Les Canadiens peuvent visiter le site Web du ministère, nous appeler ou visiter l'un de nos centres Service Canada pour apprendre la meilleure façon de se protéger. II est important de noter que la protection des renseignements personnels des Canadiens est une responsabilité partagée entre le gouvernement, le secteur privé et les particuliers. Nous encourageons fortement les Canadiens à ne pas donner leur numéro d'assurance sociale à moins d'être certains qu'il est légalement requis ou que c'est nécessaire. Les Canadiens devraient également surveiller activement leurs renseignements financiers, notamment en communiquant avec les agences d'évaluation du crédit du Canada.

[*Français*]

La perte d'un numéro d'assurance sociale ne signifie pas automatiquement qu'une fraude s'est produite ou se produira.

Cependant, si des Canadiens détectent une activité suspecte touchant leur numéro d'assurance sociale, ils doivent agir rapidement afin de minimiser les répercussions potentielles en signalant tout incident à la police, en contactant le commissaire à la protection de la vie privée et le Centre antifraude du Canada, et en informer Service Canada. Dans les cas où il est prouvé que le numéro d'assurance sociale a été utilisé à des fins frauduleuses, Service Canada travaillera en étroite collaboration avec les personnes touchées.

Le nombre de Canadiens dont le numéro d'assurance sociale a été remplacé par Service Canada en raison d'une fraude est demeuré stable à environ 60 par année depuis 2014, malgré les fuites de données de plus en plus importantes.

Cela dit, nous savons que de nombreux Canadiens ont signé une pétition demandant à Service Canada d'attribuer un nouveau numéro d'assurance sociale aux personnes touchées par cette atteinte aux données. La raison principale pour laquelle nous n'attribuons pas automatiquement un nouveau numéro d'assurance sociale dans ces circonstances est simple: l'obtention d'un nouveau numéro d'assurance sociale ne protégera pas les particuliers contre la fraude. L'ancien numéro d'assurance sociale continue d'exister et est toujours lié aux particuliers. Par exemple, si un fraudeur utilise l'ancien numéro d'assurance sociale d'une personne et que son identité est mal vérifiée, les prêteurs peuvent quand même demander à la personne fraudée de payer les dettes.

Également, il incombera à la personne de fournir son numéro d'assurance sociale à chacune des institutions financières, à ses créanciers, à ses fournisseurs de régime de retraite, à ses employeurs actuels et passés, ou à toute autre organisation à laquelle elle aurait donné son numéro d'assurance sociale. Le faire incorrectement pourrait mettre à risque l'octroi de bénéfices ou laisserait la porte ouverte à la fraude ou au vol d'identité.

Cela signifierait aussi de doubler la surveillance. Les particuliers devraient quand même surveiller leur compte et leurs rapports de solvabilité pour leurs deux numéros d'assurance sociale de façon régulière et continue. La multiplication des numéros d'assurance sociale augmente donc le risque de fraude potentielle.

La surveillance active des bureaux de crédit ainsi que l'examen régulier des relevés bancaires et des relevés de cartes de crédit demeurent la meilleure protection contre la fraude.

En terminant, la protection de l'intégrité du numéro d'assurance sociale est importante pour nous. Je peux vous assurer que nous continuerons à prendre toutes les mesures nécessaires pour y parvenir, incluant la lecture du rapport de ce comité ou d'autres informations provenant de ce comité ou autres sur les meilleures façons d'améliorer la situation.

Je vous remercie de votre temps. Je me ferai un plaisir de répondre à vos questions.

● (1455)

Le vice-président (M. Pierre Paul-Hus): Merci, madame Boisjoly.

Y a-t-il d'autres intervenants qui veulent prendre de parole avant que nous passions aux questions?

Monsieur Guénette, vous avez la parole.

M. Maxime Guénette (sous-commissaire et chef de la protection des renseignements personnels, Direction générale des affaires publiques, Agence du revenu du Canada): Merci, monsieur le président.

Bonjour à tous les membres du Comité.

[*Traduction*]

Je m'appelle Maxime Guénette et je suis sous-commissaire de la Direction générale des affaires publiques et chef de la protection des renseignements personnels de l'Agence du revenu du Canada. Ma collègue Gillian Pranke, sous-commissaire adjointe de la Direction générale de cotisation, de prestation et de service de l'Agence, m'accompagne aujourd'hui.

L'Agence du revenu du Canada est une organisation qui touche la vie de pratiquement tous les Canadiens. Elle est l'un des plus importants détenteurs de renseignements personnels du gouvernement du Canada. À l'Agence, nous traitons plus de 28 millions de déclarations de revenus de particuliers chaque année. II est donc essentiel qu'elle dispose d'un cadre de protection des renseignements personnels exhaustif pour gérer et protéger les renseignements de tous les Canadiens.

[*Français*]

L'intégrité en milieu de travail est la pierre angulaire de la culture mise en avant par l'Agence. L'Agence aide ses employés à bien agir en leur fournissant des lignes directrices claires et des outils visant à assurer la sécurité et la confidentialité ainsi qu'à protéger les renseignements personnels, les programmes et les données.

L'Agence est tenue de respecter la Loi sur la protection des renseignements personnels ainsi que les politiques et directives du Conseil du Trésor qui y sont liées pour assurer la gestion et la protection des renseignements personnels des Canadiens. L'article 241 de la Loi de l'impôt sur le revenu impose également des exigences en matière de confidentialité aux employés de l'Agence et aux autres personnes ayant accès aux renseignements sur les contribuables.

L'Agence observe aussi la Politique sur la sécurité du gouvernement et les orientations fournies par les principaux organismes de sécurité, comme le Centre de la sécurité des télécommunications et le Centre canadien pour la cybersécurité, qui sont intervenus tantôt.

En avril 2013, l'Agence a nommé son premier chef de la protection des renseignements personnels, qui est, entre autres, responsable des fonctions liées à l'accès à l'information et à la protection des renseignements personnels à l'Agence.

[*Traduction*]

En tant que chef de la protection des renseignements personnels, mon rôle consiste, entre autres, à faire en sorte que la protection des renseignements que l'Agence détient soit assurée et renforcée par la supervision des décisions liées à la protection des renseignements personnels, y compris l'évaluation des répercussions de nos programmes sur la protection de ces renseignements; la défense des droits relatifs à la protection des renseignements personnels, ce qui comprend la gestion des atteintes à la vie privée à l'interne; et le rapport à la haute direction de l'Agence sur l'état de la gestion de la protection des renseignements personnels.

À l'Agence, la responsabilité quant à la saine gestion de la protection des renseignements personnels ne se limite pas à nommer un chef de la protection des renseignements personnels; il s'agit d'une responsabilité que partagent tous les employés.

Pour préserver son intégrité, l'Agence doit avoir en place les systèmes appropriés pour protéger les renseignements de nature délicate des menaces externes. Les réseaux et les postes de travail de l'Agence sont dotés de logiciels de détection et de suppression de logiciels malveillants et de virus. lls sont mis à jour quotidiennement et protègent l'environnement de l'Agence contre les menaces de virus et de codes malveillants.

[*Français*]

Pour ce qui est des employés de l'Agence, leurs ordinateurs sont dotés d'un ensemble de produits de sécurité allant de logiciels antivirus à des logiciels de détection des intrusions au niveau de l'hôte.

Les services externes sont pris en charge par des plateformes sécurisées et protégées par des pare-feu et des outils de prévention des intrusions visant à détecter et à prévenir l'accès non autorisé aux systèmes de l'Agence.

Pour ce qui est des transactions en ligne, nous nous assurons que les renseignements de nature délicate sont chiffrés lors de la transmission entre l'ordinateur d'un contribuable et nos serveurs Web. Peu importe la façon dont les Canadiens choisissent d'interagir avec l'Agence, ils doivent suivre un processus d'authentification en deux étapes pour accéder à leur compte.

Ces étapes sont essentielles pour que seules les personnes autorisées aient accès aux renseignements personnels. Le processus comprend la validation d'un ensemble de points de données personnelles et confidentielles, dont, entre autres, le numéro d'assurance sociale d'une personne, mais aussi le mois et l'année de sa naissance, et des renseignements tirés de sa déclaration de revenus de l'année précédente.

[*Traduction*]

L'Agence mettra sous peu en œuvre un nouveau numéro d'identification personnel pour les contribuables qui appellent la ligne des demandes de renseignements sur l'impôt des particuliers. De plus, l'Agence étudie actuellement des procédures de sécurité supplémentaires pour protéger les renseignements des contribuables. Comme la cybercriminalité et l'hameçonnage sont maintenant fréquents et que les techniques utilisées sont de plus en plus sophistiquées, l'Agence agit de façon proactive en avertissant le public que des fraudeurs communiquent avec les gens en prétendant travailler pour elle.

Une façon simple pour les contribuables de se protéger contre la fraude est de s'inscrire à Mon dossier ou à Mon dossier d'entreprise afin de gérer leur dossier fiscal facilement et en toute sécurité au moyen des portails sécurisés de l'Agence. Ceux qui sont inscrits à Mon dossier peuvent aussi s'inscrire au courrier en ligne afin de recevoir des alertes du compte qui les informent des arnaques possibles ou d'autres activités frauduleuses qui pourraient avoir une incidence sur eux.

L'Agence est fière de sa réputation d'organisation de pointe engagée à assurer l'excellence de l'administration du régime fiscal du Canada. Toutefois, des activités inappropriées ou frauduleuses peuvent se produire en milieu de travail. L'Agence a mis en place toute une gamme de contrôles pour s'assurer que les seules personnes qui accèdent aux renseignements des contribuables sont les employés tenus de le faire dans le cadre de leur travail. Elle peut ainsi détecter les cas d'inconduite qui pourraient se produire.

● (1500)

[*Français*]

La surveillance de l'accès des employés aux renseignements des contribuables est centralisée, ce qui garantit un processus indépendant permettant à l'Agence de détecter des activités douteuses dans ses systèmes et d'intervenir quand c'est nécessaire. De cette façon, les utilisateurs autorisés ont accès uniquement aux applications et aux données auxquelles ils ont droit d'accéder en fonction de règles administratives strictes.

[*Traduction*]

En 2017, l'Agence a mis en œuvre une solution de gestion de la fraude d'entreprise, qui complète les contrôles de sécurité existants et réduit encore plus les risques d'accès non autorisé et d'atteinte à la vie privée. La solution de gestion de la fraude d'entreprise permet la surveillance proactive et la détection de l'accès non autorisé des employés. L'Agence prend très au sérieux toute allégation ou tout soupçon d'inconduite de la part d'un employé et fait minutieusement enquête. Lorsque les soupçons d'actes répréhensibles ou d'inconduite sont fondés, des mesures disciplinaires appropriées sont prises, qui peuvent aller jusqu'au congédiement. Si l'on soupçonne une activité criminelle, la question est renvoyée aux autorités compétentes.

[*Français*]

Au moment de leur embauche, les employés de l'Agence doivent attester avoir lu le Code d'intégrité et de conduite professionnelle ainsi que le Code de valeurs et d'éthique du secteur public.

Le code décrit de façon claire la norme de conduite que les employés doivent respecter, dont l'obligation de protéger les renseignements des contribuables, conformément à l'article 241 de la Loi de l'impôt sur le revenu. L'accès non autorisé à ces renseignements est considéré comme une inconduite grave, comme l'indique la Directive sur la discipline de l'Agence.

[*Traduction*]

Le code veille à ce que les employés, actuels et anciens, soient au courant que l'obligation de protéger les renseignements des contribuables se poursuit même après leur départ de l'Agence. Chaque année, on demande à tous les employés de relire et de confirmer leurs obligations en vertu du Code d'intégrité et de conduite professionnelle de l'Agence.

Toute atteinte à la vie privée qui survient est évaluée conformément aux politiques et aux procédures du Secrétariat du Conseil du Trésor afin de consigner et d'évaluer tous les risques potentiels pour la personne touchée. Un représentant de l'Agence spécialisé lui offrira un soutien afin qu'elle puisse poser des questions et obtenir les renseignements dont elle a besoin, et selon le cas, accéder à des services gratuits de protection du crédit.

Dans les rares cas où les renseignements d'un contribuable sont véritablement compromis, l'Agence prend des mesures pour résoudre toutes les questions en suspens. Ces mesures comprennent l'examen de toutes les activités frauduleuses qui pourraient avoir eu lieu dans le compte, y compris les remboursements frauduleux.

[*Français*]

L'Agence est fermement résolue à maintenir la confiance des Canadiens en notre organisation et à répondre à leurs attentes concernant la mise en place des contrôles nécessaires pour assurer la sécurité des renseignements qui lui sont confiés. Nous avons travaillé fort pour gagner la confiance du public, puisque celle-ci est à la base d'un régime fiscal fondé sur l'autocotisation.

[*Traduction*]

II faut des années pour se forger une bonne réputation, et nous maintenons la nôtre en demeurant vigilants dans nos efforts pour protéger les contribuables contre les atteintes à la sécurité et pour protéger le système d'administration de l'impôt du Canada contre toute inconduite et infraction criminelle.

Je vous remercie, monsieur le président. Je répondrai maintenant avec plaisir à vos questions.

[*Français*]

Le vice-président (M. Pierre Paul-Hus): Merci, monsieur Guénette.

S'il n'y a personne d'autre, nous allons commencer la période de questions.

Monsieur Drouin, vous avez sept minutes.

M. Francis Drouin: Merci beaucoup, monsieur le président.

Je remercie tous les témoins de comparaître devant le Comité à court préavis.

Je tiens à dire que je suis une des victimes de la fuite de données chez Desjardins, tout comme plusieurs de mes concitoyens.

Madame Boisjoly, vous avez fait allusion à la pétition en ligne visant à faire changer les numéros d'assurance sociale des gens touchés. Pouvez-vous expliquer au Comité pourquoi on ne le ferait pas et pourquoi cela ne ferait que compliquer les choses sans donner plus de sécurité aux Canadiens et aux Canadiennes?

Mme Elise Boisjoly: J'en ai fait brièvement mention dans ma présentation, et je vous remercie de me donner l'occasion d'en parler plus longuement.

Tout d'abord, une fuite d'information ne signifie pas nécessairement qu'il y a eu fraude ou vol d'identité. Ensuite, si on ne change pas automatiquement les numéros d'assurance sociale à la suite d'une fuite comme celle-ci, c'est d'abord parce que cela ne résout pas vraiment le problème et n'écarte pas nécessairement tout risque de fraude.

Laissez-moi vous expliquer un peu plus ce premier point. Si on ne change pas le numéro d'assurance sociale associé à un certain numéro de crédit et qu'un bureau de crédit utilise l'ancien numéro de crédit, l'individu concerné ne pourra pas nécessairement obtenir du crédit. De plus, si un prêteur ne fait pas une bonne vérification de l'identité de ce dernier et qu'un fraudeur emprunte de l'argent en son nom, le prêteur pourrait lui demander de payer la dette. Il peut donc y avoir d'autres fraudes si le prêteur ne vérifie pas correctement l'identité de l'individu.

La deuxième raison, c'est que cela peut créer de graves problèmes d'accès à des avantages et à des services. Comme je l'ai dit dans ma présentation, la personne qui est victime d'une fuite d'information doit prévenir toutes les personnes, les institutions financières, les agences de crédit, les employeurs passés et futurs et les gestionnaires des régimes de pensions auxquels elle a adhéré avec son ancien numéro d'assurance sociale et faire les changements nécessaires. Souvent, les gens ne se souviennent plus des personnes à qui ils ont donné leur numéro d'assurance sociale, surtout au début de leur carrière. Cela peut empêcher une personne de recevoir sa pension, par exemple, car on ne pourrait plus faire le lien entre l'individu et les avantages auxquels il a droit.

Au sein du fédéral, nous aviserions certainement l'Agence du revenu et tous les organismes concernés, mais les changements pourraient se faire de façon manuelle et il pourrait y avoir des erreurs, ce qui pourrait compliquer le calcul des pensions ou des prestations d'assurance-emploi. Si on oublie un employeur et que celui-ci fait des erreurs, il pourrait y avoir un mauvais calcul des prestations d'assurance-emploi ou de la pension de vieillesse.

● (1505)

M. Francis Drouin: En d'autres mots, changer notre numéro d'assurance sociale ne protège pas nécessairement nos renseignements personnels.

Pourquoi émet-on un autre numéro d'assurance sociale dans les cas où la fraude a été prouvée?

Mme Elise Boisjoly: Quand la fraude est prouvée, on en détermine le type et on discute avec le citoyen touché. Souvent, celui-ci va décider de ne pas changer son numéro d'assurance sociale. Il va s'inscrire ou être inscrit à un bureau de vérification de crédit. Par le fait même, il sera mieux protégé qu'il ne le serait en changeant son numéro d'assurance sociale. Souvent, après avoir été informé, le citoyen décide de ne pas changer son numéro d'assurance sociale. Dans un très petit nombre de cas, soit 60 cas par année depuis 2014, le citoyen tient absolument à faire un changement lorsque la fraude est confirmée. À ce moment-là, on va permettre l'émission d'un nouveau numéro d'assurance sociale, mais on va aussi lui faire comprendre que cela ne réglera pas nécessairement la situation.

M. Francis Drouin: Voici une question plus pragmatique.

Comme les citoyens qui sont dans la même situation que moi, je me dis qu'il y a un risque de fraude. Comment puis-je donc aviser les autorités, que ce soit Revenu Canada ou Service Canada, que mon numéro d'assurance sociale va peut-être être utilisé de façon frauduleuse? Est-ce que je peux appeler Service Canada pour l'en aviser? Est-ce qu'il existe un processus interne qui permet aux citoyens de faire cela?

Mme Elise Boisjoly: Absolument. Je dirais deux choses là-dessus.

Premièrement, depuis que la fuite a été rendue publique, nous avons reçu directement de 1 400 à 1 500 demandes de citoyens. Ils nous ont appelés pour savoir comment mieux protéger leurs renseignements personnels, et nous leur avons donné beaucoup d'information à ce sujet. Souvent, les citoyens prendront les mesures que nous leur conseillons de prendre, c'est-à-dire regarder les rapports des bureaux de crédit et vérifier leurs transactions bancaires.

Deuxièmement, s'ils constatent une activité suspecte, ils doivent suivre des procédures très claires pour nous en informer. Si des transactions suspectes sont détectées, nous leur demandons de communiquer avec Service Canada, qui pourra prendre les mesures nécessaires pour les aider.

M. Francis Drouin: D'accord.

Sur le site Web, il est question de 29 cas où il est permis aux Canadiens et aux Canadiennes de communiquer leur numéro d'assurance sociale, par exemple à des institutions bancaires ou à d'autres entités.

Que fait Service Canada pour que les Canadiens et les Canadiennes sachent quand ils devraient communiquer leur numéro d'assurance sociale et quand ils ne devraient pas le faire? Quel est le recours possible quand un organisme demande un numéro d'assurance sociale alors qu'il ne devrait pas le faire?

● (1510)

Mme Elise Boisjoly: Notre site Web, nos centres d'appel et les centres de Service Canada indiquent aux citoyens à qui ils devraient donner leur numéro d'assurance sociale. À vrai dire, lorsque nous émettons un numéro d'assurance sociale à un citoyen, nous lui mentionnons à qui ils devraient le donner et à qui ils ne devraient pas le donner. Un certain nombre d'organismes sont réglementés pour obtenir le numéro d'assurance sociale, par exemple quand une banque ou un créditeur donne des intérêts, ce qui concerne l'Agence du revenu du Canada.

Si quelqu'un ne faisant pas partie de cette liste demande le numéro d'assurance sociale d'une personne, cette dernière peut refuser et demander de produire une autre forme d'information. Par exemple, il y a longtemps de cela, les propriétaires demandaient souvent le numéro d'assurance sociale d'un locataire potentiel pour vérifier son crédit. La personne concernée peut simplement remettre un rapport de crédit plutôt que donner son numéro d'assurance sociale. La personne qui pose la question doit...

[*Traduction*]

Le président: Merci.

Il est utile que les témoins jettent un coup d'œil à la présidence de temps à autre afin que je puisse leur faire signe.

Mme Elise Boisjoly: Merci beaucoup.

Ces lunettes ne...

[*Français*]

Le président: Monsieur Paul-Hus, vous avez sept minutes, s'il vous plaît.

M. Pierre Paul-Hus: Merci, monsieur le président.

Merci à vous tous d'être présents aujourd'hui.

À vous écouter, nous nous sentons comme dans *Les Douze travaux d'Astérix*. Nous nous mettons à la place des citoyens. Ce qui les inquiète, c'est qu'ils ne savent pas trop ce qui va arriver. Nous avons demandé à vous rencontrer pour avoir de l'information à cet égard. On sait que le numéro d'assurance sociale est une mesure en place, mais y a-t-il autre chose qui devrait être fait à l'avenir pour changer le système? Pourrait-on faire ce qu'ont fait d'autres pays, c'est-à-dire avoir plus d'identification numérique, que ce soit au moyen d'empreintes digitales ou d'autre chose?

Madame Boisjoly, vous avez dit qu'il y a environ 60 cas par année, mais là, les données de 2,9 millions de personnes ont été volées. Vous attendez-vous à une grande augmentation de changements requis du numéro d'assurance sociale à la suite de ces vols d'identité?

J'ai aussi une question pour vous, monsieur Guénette.

Les gens qui suivent ce qui se passe actuellement veulent savoir ce qu'on fait. Vous avez proposé une bonne solution, et c'est ce que les gens ont besoin qu'on donne, des solutions. On a parlé d'aller sur le site du gouvernement du Canada et d'ouvrir son dossier de finances. Si j'ai bien compris, en ouvrant son dossier, on peut recevoir des alertes ou des avis.

Cela fait trois semaines maintenant. Nous sommes ici aujourd'hui à la suite d'une demande d'urgence. Pourquoi n'a-t-on pas communiqué avec le public immédiatement ou dans la semaine qui a suivi les vols pour lui faire savoir ce que le gouvernement du Canada peut faire pour l'aider? C'est ce qu'on a besoin de savoir.

Je vous écoute, madame Boisjoly.

Mme Elise Boisjoly: Merci.

Pour répondre à votre première question sur les nouvelles mesures, toute situation comme celle-ci nous donne l'occasion de revoir nos mesures de sécurité et de protection de la vie privée. Tous nos collègues et moi nous penchons certainement là-dessus lorsqu'il y a de tels incidents. Nos collègues qui nous ont précédés ont beaucoup parlé de l'évolution de la cybersécurité. Ils ont dit qu'il fallait toujours être prêt. Il est certain que nous nous penchons toujours là-dessus.

Ma collègue a mentionné le Conseil du Trésor, dont le mandat comprend la gestion de l'identité. Il se penche sur les façons dont on peut mieux résoudre les problèmes liés à l'identité numérique, notamment en menant des projets pilotes avec les provinces. Nous participons à ces forums et nous pensons à des façons de faire avancer la discussion en ce qui concerne l'identité numérique.

Deuxièmement, au sujet du nombre de vols d'identité, on nous a signalé de nombreux vols d'identité au cours des 14 ou 15 dernières années. Ce sont probablement des millions de personnes qui ont déjà été touchées et, malgré cela, le nombre de personnes qui demandent un nouveau numéro d'assurance sociale demeure plutôt faible. Alors, je ne peux pas répondre à votre question, puisque je ne connais pas l'avenir, mais je peux dire qu'il y a eu beaucoup de vols et que le nombre semblait constant, soit près de 60 par année.

M. Maxime Guénette: Je vous remercie de votre question, monsieur Paul-Hus.

Comme Mme Boisjoly le disait, toutes les occasions sont bonnes pour rappeler aux gens les choses qu'ils peuvent faire. Pendant la période des impôts, nous avons mené des campagnes publicitaires et des initiatives de communication sur le Web et sur les médias sociaux pour rappeler aux gens les services qui sont à leur disposition. Cela dit, il y a toujours plus à faire de ce côté-là. Nous cherchons toujours des occasions de communiquer davantage là-dessus. Alors...

● (1515)

M. Pierre Paul-Hus: D'accord, mais dans le cas qui nous occupe, il s'agit de gérer une crise. Nous sommes ici pour savoir si un organisme fédéral peut donner un coup de main à Desjardins, qui prend ses propres mesures pour rectifier la situation du mieux qu'elle le peut. À l'heure actuelle, je vois des mesures interagences, mais il n'y a pas vraiment de mesures proactives pour aider les citoyens, mis à part un message qu'on a déjà fait passer.

Selon vous, pourquoi le gouvernement semble-t-il aussi passif et ne dit-il rien? Est-ce parce qu'il n'y a rien à faire? N'y a-t-il pas de solution?

Nous cherchons des solutions, parce que les gens sont inquiets. Si vous nous dites que les agences en place n'ont pas les moyens ou les outils pour les aider, nous allons nous tourner vers d'autres solutions.

Est-ce que les solutions comme celle proposée par Desjardins, c'est-à-dire les services d'Equifax, sont assez efficaces, selon votre expérience et votre évaluation de la situation? Nous cherchons à rassurer les gens avec les vraies choses; nous ne voulons pas dire n'importe quoi.

M. Maxime Guénette: À l'heure actuelle, puisque l'enquête est encore en cours, il y a pas mal d'information...

M. Pierre Paul-Hus: L'enquête n'a rien à y voir, car on sait comment la fuite de données a eu lieu. On a aussi une idée de l'endroit où elles ont été envoyées, mais, pour l'instant, ce n'est pas cela qui nous intéresse. On sait qu'il y a quelqu'un, quelque part sur la planète, qui a nos coordonnées et qui peut nous faire du mal en volant notre identité. Nous voulons donc savoir si nos agences peuvent intervenir de façon proactive ou non, et ce qu'on peut faire si ce n'est pas le cas.

Vous avez une solution concernant mon dossier, alors c'est déjà un élément qui pourrait être communiqué aux citoyens. Ce serait important de le faire rapidement, parce que les gens ne sont pas de très bonne humeur pendant leurs vacances. Ensuite, il faudra voir si on peut faire autre chose.

La question du numéro d'assurance sociale a été soulevée partout. Plusieurs ont fait des suggestions. Vous êtes responsable de ce dossier et vous dites qu'il n'y a rien à faire, du moins pas de cette façon. Ce sont des réponses qu'on doit entendre, mais il reste qu'il faut sortir d'ici en disant aux gens ce que le gouvernement peut faire pour aider Desjardins, premièrement, et deuxièmement, les 2,9 millions de personnes touchées. On entend beaucoup parler de protocoles internes, mais, pour les citoyens qui nous écoutent, cela ne veut pas dire grand-chose. Voilà pourquoi j'aime entendre des réponses claires. Je sais que vous en donnez quand vous le pouvez, mais en fin de compte, lorsqu'on va sortir d'ici, il faudra savoir ce qu'on peut faire.

M. Maxime Guénette: Je peux vous assurer qu'il y a des discussions très proactives entre les différents ministères concernés.

Du côté de l'Agence du revenu, comme je le disais dans mon allocution, le numéro d'assurance sociale, l'adresse et la date de naissance sont certaines des informations dont on a besoin pour s'identifier auprès de l'Agence. Cela prend aussi de l'information sur les déclarations de revenus des années précédentes, ce qui ne fait pas partie de l'information qui a été volée chez Desjardins, selon les discussions que nous avons eues. Cela dit, encore une fois, l'enquête est toujours en cours. Alors, ces questions...

M. Pierre Paul-Hus: Comme je vous l'ai dit, cela ne change rien, en fin de compte.

Combien de temps me reste-t-il, monsieur le président?

[*Traduction*]

Le président: Vous avez une dizaine de secondes.

[*Français*]

M. Pierre Paul-Hus: S'il y a un vol d'identité, quelle est la première chose qu'un citoyen doit faire? Appeler la police?

Mme Elise Boisjoly: Oui.

M. Maxime Guénette: Effectivement.

Le président: Merci, monsieur Paul-Hus.

Monsieur Dubé, vous avez sept minutes.

M. Matthew Dubé: Merci, monsieur le président.

Merci à vous tous d'avoir pris le temps de venir ici aujourd'hui.

Madame Boisjoly, j'ai retenu un point dans votre réponse à M. Drouin. Vous avez dit qu'une fuite de données personnelles ne mène pas au vol d'identité. C'est un peu ce qui nous amène ici aujourd'hui. Les citoyens veulent justement éviter un vol d'identité; c'est la préoccupation principale. Dans ce contexte, j'ai quelques questions à poser.

Vous avez dit que les gens devraient rapporter les activités suspectes liées au numéro d'assurance sociale. Je suis un législateur fédéral et je ne sais pas ce qu'est une activité suspecte liée au numéro d'assurance sociale. Dieu merci, je n'ai jamais été victime de fraude, et c'est la même chose pour les gens de mon entourage. Je touche du bois. Cependant, je connais des gens qui en ont été victimes. Ils l'apprennent quand ils reçoivent une facture de téléphone cellulaire qu'ils n'ont pas ou une carte de crédit de Canadian Tire qu'ils n'ont jamais demandée. Ils se retrouvent avec des dettes et ont des obligations qui ne sont pas les leurs.

Pouvez-vous me dire ce qu'est exactement une activité suspecte liée au numéro d'assurance sociale?

Mme Elise Boisjoly: Je vous remercie de votre question.

Vous avez bien cerné certaines activités suspectes, comme vous le dites. Nous demandons aux gens de se protéger le mieux possible en faisant affaire avec un bureau de crédit, pour que les transactions soient suivies du plus près possible. Ils doivent regarder leurs transactions bancaires et de cartes de crédit. S'ils voient qu'on leur attribue une transaction qu'ils n'ont pas faite, nous leur demandons de contacter le bureau...

● (1520)

M. Matthew Dubé: Pardonnez-moi de vous interrompre, mais mon temps est limité et j'ai juste un tour.

Ces activités suspectes ou ces transactions problématiques que nous pourrions voir sur notre relevé de carte de crédit peuvent être liées à toutes sortes de choses. Ce peut être quelqu'un qui a volé notre courrier et qui a obtenu notre adresse. Il s'agit d'informations qui sont vraisemblablement plus faciles à obtenir. Vous avez justement mentionné qu'en ce qui concerne la situation dont nous discutons aujourd'hui, la personne a de telles informations complémentaires. En principe, avec toutes les informations qui ont été volées, la personne pourrait facilement appeler Revenu Canada et obtenir un nouveau mot de passe. On a toute l'information nécessaire, si on a le dossier complet d'un individu.

Mme Elise Boisjoly: Oui, et c'est le point le plus important. On parle du nombre d'identifiants. Il revient à chacune des organisations de vérifier l'identité du citoyen.

Mon collègue a dit qu'on doit aussi avoir une ligne de la déclaration de revenus. Dans le cas de l'assurance-emploi, il y a un code d'accès, et on vous demande de donner les deux chiffres de ce code d'accès. En tant que vérificateur d'identité, il faut nous assurer de poser des questions d'identification secrètes et qui ne sont partagées qu'avec les personnes que nous connaissons. Cela nous permet ainsi de mieux vérifier l'identité des gens et de leur fournir le service. Par exemple, vous ne pourriez pas appeler Service Canada et obtenir des prestations d'assurance-emploi avec l'information qui est divulguée présentement.

M. Matthew Dubé: Concernant l'obtention d'un nouveau numéro d'assurance sociale, j'ai un peu de difficulté à comprendre. Dans le fond, l'argument, c'est que cela devient compliqué pour le citoyen. En principe, on attribue un numéro d'assurance sociale pour des raisons d'efficacité. Un identifiant unique vise à faciliter les transactions avec les instances gouvernementales.

Vous me pardonnerez cette comparaison qui n'est peut-être pas exacte. Si, aujourd'hui, je constate un problème lié à ma carte de crédit, la banque ou la compagnie émettrice est quand même en mesure de transférer un solde ou de faire le lien entre les transactions légitimes sur ma carte de crédit fraudée et le nouveau numéro de carte qu'elle m'a envoyée.

Pourquoi une institution financière pourrait-elle faire cela alors que, de votre côté, vous n'êtes pas capable de dire que le numéro d'assurance sociale d'une personne est compromis et qu'elle a un nouveau numéro? Un ancien employeur pourrait devoir s'occuper, par exemple, de questions qui concernent la pension de cette personne. Sachant que c'est la même personne, pourquoi n'êtes-vous pas capable de faire le lien entre l'ancien et le nouveau numéro d'assurance sociale? Il faudrait peut-être faire une vérification additionnelle, étant donné que le numéro a été compromis, mais il reste que j'ai un peu de difficulté à comprendre pourquoi vous ne pouvez pas faire cela.

Mme Elise Boisjoly: Au départ, vous avez énoncé que la première raison pour laquelle on ne donne pas automatiquement le numéro d'assurance sociale est que cela pourrait rendre la vie difficile aux citoyens. Or la première raison est plutôt que cela ne préviendrait pas nécessairement la fraude. C'est un point très important. Il faudrait que le citoyen continue à faire la vérification de son ancien numéro d'assurance sociale parce qu'il existe encore...

M. Matthew Dubé: Je suis désolé de vous interrompre, mais, si je perds ma carte de crédit, cela ne veut pas nécessairement dire qu'elle a été volée. Elle est peut-être tombée quelque part dans un égout, de sorte qu'on ne la reverra plus jamais et qu'elle ne sera pas utilisée. J'appellerais tout de même ma banque, Visa ou peu importe, pour lui demander d'annuler cette carte. Je ferais quand même des vérifications et j'aurais la paix d'esprit en sachant que je suis protégé.

Pourquoi ne pas suivre la même logique pour un citoyen victime d'une fuite de données personnelles, qui, en plus, est hautement médiatisée? Le citoyen veut mettre tous les points-virgules qu'il peut pour se protéger. Il change ses cartes de crédit et tout le reste, comme on le fait quand on perd son portefeuille. Pourquoi ne pas procéder de la même façon?

Mme Elise Boisjoly: Le numéro d'assurance sociale n'est pas comme une carte de crédit, qui est le seul identifiant de cette personne pour la banque. C'est un identifiant utilisé par les employeurs d'une personne depuis qu'elle est sur le marché du travail. Ce numéro est aussi utilisé par différents programmes et services.

Présentement, il n'y a pas de système informatique qui relie tous ces systèmes pour faire une mise à jour du numéro d'assurance sociale utilisé par les employeurs et les différents groupes et programmes. Ce travail se ferait de façon manuelle. C'est pour cela que nous ne connaissons pas l'ensemble des employeurs. Au sein du gouvernement fédéral, cela se ferait de façon manuelle. Comme je l'ai dit, c'est ce que nous avons fait un petit nombre de fois. Il y a des risques d'erreur. Je ne fais que le mentionner au Comité.

● (1525)

M. Matthew Dubé: Il me reste moins d'une minute.

Au risque de nous emmêler dans les détails techniques, j'aimerais mieux comprendre. Si un employeur veut utiliser le numéro d'assurance sociale, comment cela fonctionne-t-il? Il doit bien y avoir une sorte d'alignement, quand on remonte l'échelle.

J'ai une dernière question, qui revient à ce que M. Paul-Hus a dit à juste titre.

Je vais prendre l'exemple du Québec. Quand il y a des inondations, les forces de l'ordre et le gouvernement du Québec font des consultations publiques sur place pour que les gens puissent se déplacer.

Monsieur Guénette, je respecte ce que vous avez dit, mais les programmes publicitaires ou les publications sur les médias sociaux ne sont peut-être pas suffisants.

Compte tenu de l'ampleur du vol et de la fuite, avez-vous considéré organiser des consultations en personne dans des endroits névralgiques au Québec ou dans des grands centres à Longueuil, à Montréal ou ailleurs?

[*Traduction*]

Le président: Encore une fois, monsieur Dubé, vous avez posé une question importante, mais vous n'avez pas prévu de temps pour la réponse, alors vous devrez y revenir de quelque façon à un autre moment.

Vous êtes pourtant si efficace habituellement, monsieur Dubé.

[*Français*]

Je vous souhaite la bienvenue au Comité, madame Lapointe. Vous avez sept minutes.

Mme Linda Lapointe (Rivière-des-Mille-Îles, Lib.): Merci beaucoup, monsieur le président.

Bonjour à vous tous et merci d'être avec nous.

Je ne siège pas à ce comité ordinairement, mais c'est avec plaisir que j'ai accepté de remplacer un de ses membres permanents.

J'ai discuté avec plusieurs concitoyens dans ma circonscription de Rivière-des-Mille-Îles, qui est au nord de Montréal et qui comprend Deux-Montagnes, Saint-Eustache, Boisbriand et Rosemère, et ils sont très inquiets. C'est quelque chose qui revient constamment depuis que la Chambre a ajourné, le 21 juin dernier. C'est pour cela que j'ai accepté avec empressement d'être ici aujourd'hui, même si je ne connais pas toutes les études qu'a faites ce comité.

Madame Ryan, tantôt, vous avez commencé par dire que c'est le ministère des Finances qui établit les lois et les règlements qui régissent le système bancaire canadien. Vous avez dit par la suite que la surveillance du secteur financier canadien est partagée entre les gouvernementaux fédéral et provinciaux.

Revenons au Québec spécifiquement. Les provinces sont chargées de la surveillance des courtiers en valeurs immobilières, des conseillers en épargne collective et en fonds de placement et des coopératives provinciales, entre autres. Desjardins est une coopérative provinciale. Je viens de parler de mes concitoyens, mais toute ma famille et moi faisons aussi partie des 2,9 millions de personnes touchées. Cela nous préoccupe énormément et nous nous demandons quelles seront les répercussions futures de ce vol sur notre vie.

Avez-vous reçu des demandes de Desjardins? M. Guénette a dit qu'il y a des discussions continues entre les ministères, mais les gens de Desjardins ont-ils communiqué avec vous pour obtenir des informations supplémentaires?

[*Traduction*]

Mme Annette Ryan: Puisque Desjardins est en grande partie régie par des lois provinciales, son premier interlocuteur gouvernemental serait l'Autorité des marchés financiers du Québec. Quand j'ai parlé de la réglementation qui régit le système bancaire au fédéral, il faut savoir qu'elle s'applique aux institutions qui ont opté pour une réglementation fédérale.

Puisque Desjardins est en grande partie régie par des lois provinciales, nombre des exigences d'exploitation mises en œuvre avant cet incident l'ont normalement été par l'intermédiaire de l'Autorité des marchés financiers.

Ma collègue du Bureau du surintendant des institutions financières peut vous expliquer de quelle façon cela fonctionne au fédéral. Dans l'incident en question, l'institution s'est empressée de prendre diverses mesures responsables afin de ne rien camoufler de la fuite, ce qui est conforme aux lois provinciales et fédérales en matière de confidentialité. Les commissaires à la protection de la vie privée du Canada et du Québec ont également entamé une enquête conjointe sur cet incident, quoique nombre des dispositions relatives à la réglementation financière de Desjardins, mais aussi à la protection des consommateurs, soient ici de compétence provinciale. Nous pouvons traiter du système fédéral, mais nombre des questions que vous pourriez avoir dans ce dossier devraient être posées aux responsables provinciaux.

● (1530)

[*Français*]

Mme Linda Lapointe: J'ai une autre question. Les bureaux de crédit sont-ils de compétence fédérale?

[*Traduction*]

Mme Annette Ryan: Ils sont en grande partie de compétence provinciale et, dans ce cas-ci, il est question de compétence provinciale.

[*Français*]

Mme Linda Lapointe: D'accord.

Les gens d'Equifax ont-ils communiqué avec vous?

[*Traduction*]

Mme Annette Ryan: Equifax ne communiquerait pas avec nous ni avec le ministère; elle est principalement régie par les lois provinciales sur la protection des consommateurs dans ce cas-ci.

[*Français*]

Mme Linda Lapointe: Merci.

J'ai écoulé la moitié de mon temps de parole et je vais maintenant m'adresser à vous, monsieur Guénette.

Vous avez parlé tantôt de règles externes sur la prévention des vols d'identité, mais vous n'avez pas parlé beaucoup des règles internes. J'aimerais savoir quelles sont les règles internes à l'Agence du revenu du Canada. Après tout, nous sommes ici aujourd'hui parce qu'il y a eu un vol de données à l'interne.

Comment cela fonctionne-t-il à l'Agence du revenu du Canada? Les employés doivent-ils être à certains échelons pour avoir accès aux systèmes? Vous avez parlé de centraliser ou de détecter les problèmes en intervenant, si nécessaire. Vous avez dit qu'il y a des règles strictes et j'aimerais que vous m'en parliez un peu plus. Les gens peuvent-ils travailler avec leur équipement électronique quand ils sont devant des écrans de l'Agence du revenu du Canada? J'aimerais en savoir plus.

M. Maxime Guénette: Je vous remercie de votre question.

Évidemment, nous appliquons des règles de sécurité à plusieurs niveaux. D'abord, nous faisons un filtrage du personnel que nous embauchons. Les gens qui ont des accès plus privilégiés ont une cote « Secret » plutôt qu'une cote moins élevée. Une panoplie de mesures de sécurité physique sont en place. Les gens qui travaillent dans les centres d'appel et qui ont accès à des écrans contenant de l'information sur des contribuables n'ont pas le droit d'avoir leur téléphone personnel avec eux. Il y a des mesures prises de ce côté-là.

Quant à l'accès aux données des contribuables, ces données sont sur des serveurs distincts et non branchés à l'Internet. Il y a un mécanisme selon lequel l'accès des employés aux données est révisé sur une base annuelle ou chaque fois qu'ils changent de poste. L'accès de ces employés est vérifié sur une base régulière par les gestionnaires.

En ce qui concerne la charge de travail, dans mes notes d'allocution, j'ai parlé des règles administratives. Quand nous confions une charge de travail à des employés, notre système de gestion de la fraude d'entreprise fait en temps réel une vérification par algorithme. Ce système applique plusieurs douzaines de règles. Par exemple, si un employé vérifie son propre compte d'impôt, une alerte est automatiquement émise et le système la voit tout de suite. Si un employé exécutait un travail ne lui ayant pas été confié, le système émettrait immédiatement une alerte au gestionnaire, qui serait alors en mesure de demander à l'employé ce qu'il faisait dans le système. Des captures d'écran sont faites à la minute près, ce qui nous permet de savoir quelles pages l'employé a consultées ou quels changements il y a apportés. Ce système a été mis en place en 2017 et il est très avancé. Il nous permet d'avoir des contrôles en place.

Pour ce qui est de la prévention de la fuite de données, les employés sont incapables de copier de l'information sur des CD, des DVD ou des clés USB. Le système ne le leur permet pas.

Mme Linda Lapointe: Merci.

Le président: Merci, madame Lapointe.

[*Traduction*]

Passons maintenant à M. Motz, puis à M. Clarke.

M. Glen Motz: Merci, monsieur le président.

Je tiens à remercier une fois de plus les représentants des ministères qui sont ici.

Je n'ai que deux questions brèves pour la représentante du ministère des Finances. Vous dites que votre objectif premier est de prévenir la fuite de données. Nous savons cependant que ces fuites se produisent et qu'elles ne se limitent pas au secteur financier.

Madame Ryan, vous avez dit que, lorsqu'un incident lié à la cybersécurité survient dans une institution fédérale sous réglementation fédérale — ce dont il est question aujourd'hui —, il y a des mécanismes de contrôle et de surveillance en place pour le gérer. Pouvez-vous expliquer concrètement aux Canadiens ce qui arrive quand cela se produit?

● (1535)

Mme Judy Cameron (directrice principale, Affaires réglementaires et politique stratégique, Bureau du surintendant des institutions financières): Permettez-moi de vous répondre.

Je représente le Bureau du surintendant des institutions financières, dont le mandat est de surveiller les institutions financières et de leur imposer des règles afin de protéger les droits et les intérêts des déposants et des créditeurs. En gros, le bureau assure la sûreté et la fiabilité des institutions financières, mais il veille aussi à ce qu'elles se conforment à toute la réglementation fédérale. Par exemple, il s'attend à ce qu'elles aient des systèmes conformes aux lois sur la protection de la vie privée.

Le bureau établit les attentes par rapport aux activités des institutions, comme le respect des lois sur la protection de la vie privée. Il s'attend également à ce qu'elles effectuent des autoévaluations des risques pour établir les protections nécessaires contre les menaces internes de cybersécurité. Il supervise donc les institutions pour s'assurer qu'elles respectent les attentes établies de sorte à confirmer la présence de systèmes de gestion dûment conformes.

M. Glen Motz: Essentiellement, c'est de la surveillance, sans plus. Et, dans le cas présent, c'est de la surveillance par rapport à ce qui s'est passé pour s'assurer que...

Mme Judy Cameron: C'est la surveillance de leurs systèmes pour prévenir ce genre de situations, en fait.

M. Glen Motz: D'accord. Va pour cette question. L'autre question est pour Mme Ryan ou quiconque peut...

Je vais simplement lire le résumé que vous avez fourni. Vous avez dit: « ... la cybersécurité est un domaine d'une importance critique pour le ministère des Finances. Nous collaborons activement avec des partenaires de l'ensemble du gouvernement et du secteur privé pour nous assurer que les Canadiens sont bien protégés contre des incidents liés à la cybersécurité et que, lorsqu'ils surviennent, les incidents sont gérés de façon à atténuer les répercussions sur les consommateurs et le secteur financier dans son ensemble ».

À quoi est-ce que cela ressemble pour les consommateurs touchés, pour l'ensemble des consommateurs, pour l'institution financière, pour le secteur bancaire et pour les divers ministères? Vous pouvez certes faire ce genre de déclarations, mais à quoi cela ressemble-t-il concrètement?

Mme Annette Ryan: Je pense que le nombre de partenaires fédéraux que vous avez entendus aujourd'hui en témoigne.

Les investissements dans le centre pour la cybersécurité faisaient partie de la première ligne de défense en vue du renforcement de la capacité de prévenir les atteintes à la cybersécurité et, comme l'a dit André Boucher, ils sont axés sur la mise en œuvre d'une réponse adaptée à celles-ci. Dans ce cas-ci, un type particulier d'atteinte à la cybersécurité s'est produit, une infraction commise par un employé, si bien qu'un grand nombre des moyens de défense mis en place par le centre pour la cybersécurité n'ont pas été déployés, mais les ressources de ce centre sont complétées par les nouvelles ressources de la GRC. Vous avez entendu cette dernière parler du centre national de lutte contre la cybercriminalité et de ses efforts au sein du Centre antifraude du Canada.

Nous sommes également conscients que les atteintes à la cybersécurité ou aux données relèvent de la protection de la vie privée. Par conséquent, des mesures telles que les nouvelles exigences obligeant les entreprises à aviser leurs clients de toute atteinte sont essentielles pour permettre aux citoyens de se montrer vigilants quant à leurs propres finances et de savoir que des renseignements importants à leur sujet ont été touchés. Il est important de faire appel à des services de surveillance comme Equifax parce qu'ils permettent à ces personnes de savoir quand quelque chose est fait en leur nom à leurs dépens.

M. Glen Motz: J'ai une question complémentaire à ce sujet. Si j'étais l'un des 2,9 millions de Canadiens concernés par cette situation, ou l'un des millions de Canadiens qui ont déjà été victimes d'atteintes aux données de toutes sortes, je voudrais moi aussi obtenir de l'aide pour reprendre le contrôle de ma vie. On parle actuellement beaucoup de ce en quoi pourrait consister cette aide, mais concrètement, les Canadiens veulent savoir comment reprendre le contrôle de leur vie. Ils veulent atténuer les risques et les répercussions qu'une telle atteinte peut avoir sur leur vie personnelle, sur leur avenir financier et sur celui de leur famille.

Je suis curieux; il semble que le ministère des Finances a un rôle à jouer dans la création d'un lieu où les Canadiens puissent obtenir les renseignements dont ils ont besoin, suivre un modèle, trouver des numéros à appeler ou autre pour mettre de l'ordre dans leur vie, car ces événements sont et seront catastrophiques pour ceux dont ces criminels vont profiter.

En tant que gouvernement, nous avons la responsabilité de veiller à protéger les Canadiens du mieux que nous le pouvons. Ces problèmes ne vont pas disparaître.

● (1540)

Le président: Je vais devoir en rester là. Je vous remercie de votre témoignage.

Chers collègues, j'ai besoin de votre avis. Nos prochains témoins sont à l'extérieur et, comme vous le savez, ils sont soumis à des contraintes de temps. Je propose de suspendre la séance. Ma question, chers collègues, est la suivante: voulez-vous suspendre la séance et laisser ces témoins partir, ou voulez-vous suspendre la séance et leur demander de rester pour que nous puissions poser notre dernière série de questions?

M. David de Burgh Graham: S'ils sont disposés à rester, j'aimerais poser mes questions.

M. Alupa Clarke: J'aimerais poser mes questions à ces témoins, s'il vous plaît.

Le président: Sur ce, je vais suspendre la séance. Je vais demander aux témoins de quitter la salle, mais de rester à proximité, et de revenir quand nous aurons terminé avec le prochain témoin...

[*Français*]

M. Rhéal Fortin: Monsieur le président, j'aurais des questions pour les témoins, mais je vous laisse décider à quel moment il sera opportun de les poser.

[*Traduction*]

Le président: Nous avons hâte de les entendre, monsieur Fortin

Sur ce, nous allons suspendre la séance pour quelques minutes pendant que nous accueillons notre prochain groupe de témoins. Je vous remercie.

● (1540)

(Pause)

● (1540)

Le président: Chers collègues, veuillez vous asseoir.

Je demande au prochain groupe de témoins de se joindre à nous — M. Brun, M. Cormier et M. Berthiaume.

Je vais demander aux caméras de quitter la salle. Cela concerne toutes les caméras, y compris celle de CBC. Merci.

Monsieur Cormier, j'aimerais vous remercier, vous et vos collègues, de votre présence. Vous semblez être très populaires dernièrement.

Nous avons encouragé les témoins à faire de brèves déclarations, en insistant sur le fait qu'elles doivent être courtes, parce que les députés souhaitent vivement poser des questions. Monsieur Cormier, on m'a communiqué des renseignements contradictoires quant à l'heure à laquelle vous devez partir. À quelle heure devez-vous nous quitter au juste?

M. Guy Cormier (président et chef de la direction, Mouvement Desjardins): Nous sommes censés partir vers 16 h 30, mais nous pouvons peut-être ajouter...

Le président: Je vous encourage à rester plus longtemps si possible.

M. Guy Cormier: Nous pourrions probablement rester une heure.

● (1545)

Le président: D'accord. Je pense que cela suffira. Vos collègues pourront peut-être rester après votre départ.

Le fait est qu'il s'agit d'une réunion d'urgence et que des gens sont venus de partout au Canada pour entendre ce que vous avez à dire.

Sur ce, je vous demande de formuler vos observations, après quoi nous passerons aux questions.

M. Guy Cormier: Merci beaucoup.

[*Français*]

Monsieur le président, mesdames et messieurs les membres du Comité permanent de la sécurité publique et nationale, bonjour. Je suis accompagnée cet après-midi de M. Denis Berthiaume, premier vice-président exécutif et chef de l'exploitation, et de M. Bernard Brun, vice-président des relations gouvernementales, du Mouvement Desjardins.

D'entrée de jeu, j'aimerais dire que, chez Desjardins, nous étions ambivalents à l'égard de cette séance extraordinaire du Comité.

D'une part, cette séance peut paraître prématurée, dans la mesure où nous sommes en train de gérer cette situation et que des enquêtes policières sont en cours. Il est donc beaucoup trop tôt pour faire un bilan de la situation. Dans ce contexte, nous nous engageons à vous dire tout ce que nous savons de façon, toutefois, à ne pas nuire aux enquêtes en cours.

D'autre part, cette séance spéciale représente à nos yeux une occasion d'alerter les législateurs et l'opinion publique sur l'enjeu de la sécurité des renseignements personnels et sur la nécessité de repenser la notion d'identité numérique au Canada. Dans ma réflexion, c'est ce point qui l'a emporté.

Je vais d'abord dire une évidence: ce qui s'est produit chez Desjardins s'est produit ailleurs et pourrait se reproduire ailleurs, dans n'importe quelle entreprise privée ou n'importe quel organisme public dont la mission comporte la gestion de renseignements personnels. Qu'on pense à plusieurs banques dans le monde, par exemple Chase, aux États-Unis, Sun Trust, le Korea Credit Bureau ou, encore, plusieurs entités gouvernementales du Canada et des États-Unis, pour ne nommer que ceux-là, qui ont d'ailleurs été victimes d'employés malveillants.

Desjardins est une institution financière de premier plan et l'un des plus importants groupes financiers coopératifs dans le monde, avec plus de 300 milliards de dollars d'actifs. En 2015, le Mouvement Desjardins a été classé par Bloomberg au premier rang des institutions financières les plus sûres en Amérique du Nord, devant toutes les banques canadiennes. En d'autres mots, même les meilleurs ne sont pas à l'abri, et ce message doit être entendu, selon nous.

Personnellement, je travaille au Mouvement Desjardins depuis 27 ans. J'ai choisi cette organisation dès le début de ma carrière parce que c'est une institution financière qui réussit, après près de 120 ans, à très bien conjuguer l'économie et le social dans notre société.

Les agissements d'un employé malveillant sont à l'origine de cette situation déplorable, lequel est aujourd'hui congédié. Il a contrevenu à toutes les règles de notre coopérative. Dans cette situation, nous avons agi le plus rapidement possible et de la façon la plus transparente possible, avec pour seul objectif la protection de l'intérêt de nos membres. C'était notre priorité.

Dès le 20 juin, quelques jours après avoir appris l'ampleur de la situation, nous sommes sortis publiquement et avons donné toute l'information disponible, en concertation avec les forces policières. Nous avons aussi annoncé dès ce moment les mesures mises en place concernant la fuite des renseignements personnels.

Nous avons déployé tous les moyens que requiert la situation. Nous avons rapidement apporté des mesures additionnelles de surveillance et de protection, afin de protéger les renseignements personnels et financiers de nos membres et de nos clients. Nous avons avisé toutes les autorités compétentes: le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, l'Autorité des marchés financiers, le Bureau du surintendant des institutions financières, ainsi que les ministères des Finances du Québec et du Canada.

Nous avons mis en place des mesures additionnelles pour confirmer l'identité des personnes lorsqu'elles font appel à nous et assurons une vigie constante de l'ensemble des comptes de nos membres. Les procédures pour confirmer l'identité de nos membres et de nos clients, lorsqu'ils appellent les caisses Desjardins, les centres Desjardins Entreprises et notre centre d'appel AccèsD, ont également fait l'objet de mesures additionnelles.

Nous avons communiqué avec les membres concernés par la messagerie privée AccèsD et par lettre personnalisée, afin de les informer de la situation et des actions qu'ils devaient poser.

Nous avons aussi ajouté des mesures complémentaires pour faciliter l'activation du forfait de surveillance d'Equifax. Les membres touchés peuvent maintenant s'inscrire de quatre façons: sur le site Internet d'Equifax, par le service téléphonique d'AccèsD, par l'application Web et mobile d'AccèsD et directement dans nos caisses Desjardins en parlant avec leur conseiller.

Nous poursuivons activement notre collaboration avec les différents corps policiers. Finalement, nous travaillons avec des experts externes pour continuer à protéger les renseignements personnels de nos membres.

Je peux vous confirmer que nous avons agi avec diligence. À la suite des informations transmises par le Service de police de Laval, notre enquête interne a rapidement permis de remonter à la source de la fuite: un employé unique. Cet employé a été suspendu, puis congédié.

À l'heure actuelle, notre première priorité est de rassurer, d'accompagner, de soutenir et de protéger chacun des membres qui ont été touchés par cette situation.

● (1550)

Encore ce matin, nous avons annoncé de nouvelles mesures de protection pour l'ensemble de nos membres. Dans cette ère du numérique, nous croyons, chez Desjardins, que tous nos membres doivent être protégés.

Comme je le disais, ce matin, Desjardins a annoncé qu'à compter de maintenant tous les membres de notre coopérative vont bénéficier d'une protection contre les transactions financières non autorisées et le vol d'identité. L'adhésion est automatique et sans frais, qu'ils aient été touchés ou pas par cette fuite de données. Depuis ce matin, Desjardins protège tous ses membres, tant les membres particuliers que les membres entreprises. C'est un précédent dans le monde des services financiers au Canada; nous sommes la première institution à faire cela. Dans cette situation, Desjardins agit avec rigueur, un sens du devoir et la volonté d'honorer son lien particulier avec ses membres.

Nous sommes entrés dans une ère où les données sont une ressource au même titre que l'eau, le bois et les matières premières essentielles au fonctionnement de pans entiers de notre économie. C'est la matière première, dorénavant, de toute une économie innovante qui va permettre des gains de productivité formidables et faciliter la vie des citoyens.

Le Canada est à quelques mois de l'opérationnalisation de la connectivité mobile 5G, qui va décupler les flots de données en circulation. Selon les spécialistes, cette connectivité ultrarapide sera le déclencheur d'applications futuristes liées à l'intelligence artificielle, un domaine où le Canada figure déjà parmi les leaders mondiaux avec ses trois pôles, Montréal, Toronto et Edmonton. Également, à l'heure où on se parle, le ministère des Finances du Canada est en consultation sur l'*open banking*, un système bancaire ouvert qui amènerait une ouverture du secteur transactionnel. Le virage a d'ailleurs déjà été entrepris dans plusieurs pays d'Europe.

À vous, législateurs, je me permets humblement de poser les questions suivantes.

Le Canada est-il bien outillé actuellement pour encadrer ces développements technologiques pleins de promesses, mais qui comportent aussi des risques nouveaux? Y a-t-il lieu d'adapter nos systèmes d'identification à cette ère du numérique pour garantir la protection des renseignements personnels et mieux lutter contre les cybercriminels? C'est toute la notion de l'identité numérique à laquelle j'ai fait allusion il y a quelques minutes.

Je vous soumets respectueusement que ce sont des questions réelles soulevées par la situation survenue chez Desjardins.

En terminant, je me permets de faire une proposition. J'invite ce comité à recommander au gouvernement du Canada la formation d'un groupe de travail spécial multipartite qui conseillerait le gouvernement sur la manière d'encadrer la gestion des données personnelles et l'identité numérique. Un tel groupe à l'écoute des préoccupations des citoyens devrait rassembler minimalement, selon nous, des représentants des gouvernements, du secteur des services financiers et des assurances, du secteur des télécommunications, ainsi que des juristes et des experts, ou tout autre groupe que le gouvernement trouverait pertinent de faire participer à la réflexion.

Le mandat de ce comité devrait consister en ceci: conseiller le gouvernement en matière de lois et de règlements; assurer la protection du public; favoriser un développement technologique innovant au bénéfice des citoyens et des communautés; et assurer une veille stratégique des meilleures pratiques dans le monde, afin que le Canada soit toujours à la page.

Personnellement, j'estime que le Canada ne peut viser l'excellence en technologie numérique et en intelligence artificielle sans avoir la même ambition en ce qui a trait à la gestion des données et des renseignements personnels. Nous devons tous tirer des leçons de la situation que vit le Mouvement Desjardins actuellement.

Merci.

Le président: Merci, monsieur Cormier.

Monsieur Picard, vous avez sept minutes, s'il vous plaît.

M. Michel Picard: Messieurs, bienvenue. Je vous remercie de vous prêter à l'exercice. Votre présence est très appréciée.

Monsieur Cormier, d'entrée de jeu, je vais vous rassurer en vous disant que le Comité permanent de la sécurité publique et nationale et le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique ont commencé, en janvier dernier ou même avant, à traiter de questions entourant l'identifiant unique. Nous avons regardé des modèles de l'étranger, par exemple celui de l'Estonie, qui pose un certain nombre d'autres problèmes.

Avant de vous poser des questions d'ordre plus pratique, j'aimerais vous soumettre que l'identifiant unique fait partie des problèmes liés à la cybersécurité. La journée où quelqu'un mettra la main sur l'identifiant unique, on fera face au même problème.

Je suis content d'apprendre que vous offrez une protection à tous vos membres. Cependant, les institutions financières ont tendance à faire payer leurs clients pour protéger leurs données contre le vol d'identité. L'offre est faite par les institutions financières elles-mêmes. Avez-vous la même philosophie?

Pour que mon salaire soit déposé dans mon compte bancaire, pour faire des transactions, des retraits automatisés et des paiements Interac, je suis obligé de donner mon nom, mon adresse et mon numéro d'assurance sociale à l'institution avec laquelle je fais affaire. Or, je dois recourir à une tierce personne pour protéger ces informations. Pourquoi dois-je compter sur quelqu'un d'autre que l'entité à qui je donne ces informations?

● (1555)

M. Guy Cormier: Pour répondre à la première partie de votre question, je vous dirais que nous avons pris la décision, dès ce matin, de mettre en place un programme de protection pour l'ensemble de nos membres, tant les particuliers que les entreprises. Le volet entreprises n'est parfois pas couvert par d'autres institutions, voire par Equifax. Nous avons décidé d'offrir ce service gratuitement à nos membres tant qu'ils restent chez Desjardins. Il n'est pas question de leur facturer quoi que ce soit. Je répète très rapidement que le programme couvre toutes les transactions financières non autorisées sur le compte d'une personne, ses dépôts et son argent. Si une transaction n'a pas été autorisée, nous allons rembourser la personne. C'est une première chose.

Deuxièmement, si une personne est malheureusement victime d'un vol d'identité, nous lui offrirons une assistance, et non pas une liste de ce qu'elle doit faire. Nous allons lui offrir l'assistance de nos experts, qui pourront même participer à des conférences téléphoniques pour l'aider à restaurer son identité.

Troisièmement, nous allons offrir une protection allant jusqu'à 50 000 $ pour rembourser des frais que les membres auront pu subir, que ce soit une perte de salaire, des frais de gardiennage d'enfants ou d'obtention de documents.

Ce concept de gratuité est extrêmement important pour nous. Si vous êtes membre de la coopérative, vous avez accès à ce programme.

Nous proposons humblement qu'on mette sur pied un comité pour, entre autres, répondre à la question de savoir si la protection des données personnelles doit être gérée par des tierces entreprises. Je pense que le statu quo n'est pas une option.

M. Michel Picard: Il y a deux problèmes à la solution que je considère comme temporaire de faire affaire avec une tierce partie. Vous demandez aux gens de faire affaire avec une tierce partie pour protéger leurs renseignements personnels, tierce partie qui, il y a deux ans, a aussi été victime d'actes de piratage. Nous avons fait une étude là-dessus ici.

Quelle serait la limite de votre responsabilité si l'entité à qui vous faites confiance, notamment Equifax, se faisait pirater les renseignements personnels de vos clients?

M. Guy Cormier: C'est une question pertinente. Au Canada, la firme qui détient une part de marché de plus de 70 % dans le domaine de la protection et de la gestion de renseignements et de données est Equifax.

Quand cet événement est survenu, nous avons décidé de nous tourner vers l'entreprise canadienne qui offrait ce service aux Canadiens. Nous avons donc travaillé avec elle, mais, au cours des jours suivants, nous avons constaté qu'il y avait des problèmes. Nous avons rapidement pris nos propres mesures pour remédier aux problèmes liés à l'inscription des membres sur le site Internet d'Equifax. Nous l'avons vécu. Nous avons vu qu'il fallait améliorer les procédures et les façons de faire, et nous avons pris cela en charge.

Maintenant, faudrait-il que ce soit une seule, deux ou trois entreprises privées au Canada qui pilotent tout cela? La réflexion s'impose tout à fait.

M. Michel Picard: Le vol d'identité a ceci de particulier que la donnée est active et à jamais sur le marché, à moins que la personne qui l'utilise ne meure. La donnée est virtuellement présente partout dans le monde. Elle peut être utilisée sur le marché noir après 24 heures, comme dans les cas de fraude de cartes de débit ou de crédit.

Le problème du vol d'identité ne concerne pas la sécurité des données du client à sa propre institution financière. Je suis convaincu que vos systèmes sont à jour quant à la protection contre le piratage de l'extérieur et que votre responsabilité envers vos clients est à la hauteur des attentes des Québécois et des Canadiens. S'il y a un problème dans le compte, vous allez rembourser l'argent qui a été détourné de façon criminelle.

Le problème du vol d'identité est le suivant. Disons qu'une personne se présente à une banque demain matin, dise s'appeler Guy Cormier et avoir besoin d'un prêt hypothécaire pour acheter une maison. L'hypothèque serait dans cette autre banque et non chez Desjardins.

Le vol d'identité fait des dommages dans d'autres milieux. Il y a eu les fameux *flips* immobiliers à Saint-Lambert, dans la Rive-Sud, où des personnes ont contracté de fausses hypothèques sous de fausses identités. Il y en a eu treize à la douzaine, et ce n'était qu'au Québec. Après cela, ce sera le Canada et l'Europe. Le vol d'identité a des répercussions et prend effet à l'extérieur du système financier du Mouvement Desjardins.

La protection que vous offrez, qui est appréciée et nécessaire, est quand même limitée à la vie financière du client, si je puis dire, au sein de son institution.

● (1600)

M. Guy Cormier: Essentiellement, la réflexion derrière la nouvelle mesure que nous avons annoncée ce matin, c'est qu'on est à l'ère numérique. Il y aura de moins en moins de transactions sur papier au cours des prochaines années. Cette donnée devient une matière première pour notre économie. Compte tenu de l'importance de ces données, chez Desjardins, nous avons pris la responsabilité d'offrir une protection à l'ensemble de nos membres.

Je disais qu'il y avait trois piliers. Le premier est la dimension financière à laquelle vous faites allusion. Si un membre de Desjardins voit une transaction non autorisée par lui-même apparaître dans ses comptes d'opération, Desjardins va totalement l'indemniser. Cela répond à la première partie de votre question sur la dimension des transactions financières.

S'il survient d'autres types de vol d'identité liés à des transactions de carte de crédit effectuées ailleurs, par exemple, des achats de téléphones cellulaires ou des locations de véhicules, la personne peut communiquer avec Desjardins et on va s'occuper d'elle. Deuxièmement, si elle a besoin de soutien pour restaurer son identité, pas sur le plan financier, mais relativement à d'autres éléments de la vie privée, Desjardins va l'accompagner. S'il faut appeler des agences gouvernementales ou des firmes privées, ou encore l'aider à préparer des documents notariés ou une présentation, nous allons le faire. On n'est donc plus dans la dimension financière, on accompagne la personne dans les autres démarches qu'elle pourrait avoir à entreprendre.

[*Traduction*]

Le président: Merci, monsieur Picard.

[*Français*]

Monsieur Paul-Hus, vous avez sept minutes.

M. Pierre Paul-Hus: Merci, monsieur le président.

Merci, monsieur Cormier, messieurs, d'être avec nous.

Nous comprenons très bien que c'est une situation très émotive et très compliquée pour Desjardins. Monsieur Cormier, vous avez mentionné qu'il était prématuré de tenir une réunion de comité. Ce que je veux expliquer de nouveau à tout le monde, c'est que les conservateurs ont demandé cette réunion, avec l'appui du NPD, dans le but de voir ce que le gouvernement fédéral pouvait faire pour aider l'entreprise Desjardins et les quelque 3 millions de membres touchés.

L'objectif n'est pas d'enquêter sur la situation ou de connaître la façon dont les données ont été subtilisées. Ce sont les policiers qui s'en occupent. De mon côté, j'espère bien que l'individu va être puni avec toute la rigueur de la loi. J'espère que la loi est assez forte pour l'envoyer en prison longtemps, mais c'est une autre question.

Nous avons rencontré des fonctionnaires de différents ministères, notamment du ministère des Finances et de l'Agence du revenu du Canada. Ce sont de grands ministères, mais il est difficile de savoir si le gouvernement du Canada peut être utile dans cette situation.

Je veux savoir si vous avez reçu un soutien efficace du gouvernement. Sinon, que pourrait-il faire pour vous aider?

M. Guy Cormier: Il y a deux ou trois éléments de réponse. Lorsque cet événement s'est produit, nous sommes entrés en contact avec plusieurs agences des gouvernements fédéral et provincial. Nous avons parlé aux différents ministères des Finances et, je tiens à vous le dire, nous avons senti une bonne collaboration et un bon soutien. M. Bernard Brun pourra confirmer qu'il y a eu des discussions très claires et très franches.

Ce que je constate, c'est que les autorités gouvernementales, tant fédérales que provinciales, veulent rassurer la population. Vous ne savez pas à quel point cela est important pour nous. Parfois, on voit ce qui s'écrit et ce qui se dit, et je comprends que les gens aient des inquiétudes et des questions. Comme députés, vous devez en recevoir beaucoup de vos concitoyens dans vos circonscriptions.

Je constate que les gens des gouvernements fédéral et provincial veulent rassurer les gens et les informer adéquatement. Cela aide beaucoup Desjardins. Il faut dire aux gens de communiquer avec nous afin que nous puissions leur présenter les programmes que nous avons annoncés ce matin. Chaque fois que nous rencontrons les gens, que ce soit dans nos caisses ou dans nos centres de contact avec la clientèle, nous sommes en contact direct et nous les rassurons.

Sans vouloir banaliser la situation, plusieurs études et plusieurs experts qui nous accompagnent actuellement nous disent très clairement qu'il y a une différence entre une fuite de données et ce qui se matérialise en un réel vol de données. Ce n'est pas un cas de « un pour un ». Ce sont des proportions très infimes.

En ajoutant la protection que nous avons annoncée ce matin, à nos yeux, nous venons dire à tous nos membres, y compris les entreprises, de ne pas s'inquiéter. S'il y a un problème, ils doivent appeler Desjardins. Nous nous occupons de les accompagner.

● (1605)

M. Pierre Paul-Hus: Depuis l'incident, vous offrez aux membres touchés un abonnement gratuit de cinq ans aux services d'Equifax. Est-ce que la nouvelle protection annoncée ce matin est un abonnement à vie aux mêmes services, ou s'agit-il d'une nouvelle protection interne?

M. Guy Cormier: C'est exact, il y a une nouvelle protection interne. Comme je le disais, il s'agit du premier pilier. Si les gens voient une transaction non autorisée passée à leur compte, ils doivent aviser Desjardins. Nous allons ensuite regarder cela avec eux et les rembourser en totalité. Il est important de mentionner qu'il n'y a pas de plafond, que ce soit 10 000 $ ou 100 000 $.

Deuxièmement, s'ils sont victimes d'un vol d'identité, ils doivent communiquer avec nous. Nous allons les accompagner et faire des conférences téléphoniques. Nous offrons même des heures de soutien psychologique, par l'entremise de nos compagnies d'assurance-vie, aux gens qui vivent cette situation avec beaucoup d'émotion.

Troisièmement, il s'agit de la nouvelle protection de 50 000 $ pour les gens qui doivent engager des dépenses personnelles pour restaurer leur identité. Desjardins va assumer ces dépenses. C'est extrêmement important.

Pour ce qui est des services d'Equifax, je répète qu'il est important que les gens victimes de la fuite de données continuent de s'y inscrire activement, car cela leur donne le service d'alerte. Celui-ci pourrait les alerter d'une transaction non autorisée dans les semaines ou les mois suivants, ce qui n'est pas inclus dans le forfait de Desjardins. Le Mouvement Desjardins recommande très fortement aux membres victimes de cette fuite de s'inscrire aux services d'Equifax.

M. Pierre Paul-Hus: Je suis membre de Desjardins, mais également client de la Banque Royale...

M. Guy Cormier: Merci.

M. Pierre Paul-Hus: La Banque Royale a un système que je ne connaissais pas. Je l'ai appris d'un employé la fin de semaine dernière. Sur son site, il y a un lien vers le site de TransUnion et, en cliquant dessus, mon dossier de crédit et ma cote de crédit apparaissent, et c'est tout à fait gratuit.

Est-ce que Desjardins va offrir un service semblable?

M. Guy Cormier: Je vais laisser M. Berthiaume répondre à cela. Il va sûrement être très content.

M. Denis Berthiaume (premier vice-président exécutif et chef de l'exploitation, Mouvement Desjardins): Nous offrons le même type de service avec TransUnion. Sur le Web et sur les appareils mobiles, on peut avoir accès à sa cote de crédit en temps réel. En ce qui a trait au système d'alerte, je pense que nous l'avons bien expliqué. Nous faisons affaire avec Equifax, mais nous considérons également la possibilité d'offrir un système d'alerte avec TransUnion.

M. Pierre Paul-Hus: Vous avez fait un travail extraordinaire pour mettre tout cela en place. Je vous félicite.

Maintenant, je voudrais parler des citoyens qui ont peur que leurs données qui ont été envoyées quelque part dans le monde soient utilisées pour faire des transactions ou quoi que ce soit. Vous ne pouvez pas être responsables de tout le monde. Vous avez une responsabilité envers vos membres, et 90 % des Québécois sont membres de Desjardins, mais vous ne pouvez pas savoir si une donnée envoyée à l'étranger provient de cette fuite précise.

En d'autres mots, si mes données volées sont envoyées à l'étranger, allez-vous me couvrir quand même, alors qu'elles auraient pu être envoyées par une autre source?

M. Guy Cormier: Ce n'est pas seulement la situation que nous vivons chez Desjardins qui nous a amenés à faire la proposition de ce matin, mais nous avons certainement accéléré les choses. À chaque début d'année, nous faisons une planification et, en fonction de la sécurité, de nos nouveaux produits et de nos nouvelles offres, nous nous demandons ce qu'il est pertinent d'offrir à nos membres en fonction des besoins.

M. Pierre Paul-Hus: Je vais vous interrompre, parce que j'ai compliqué les choses inutilement. Ce que je voulais dire, c'est que même s'il y a eu une fuite de données de votre côté, il se pourrait qu'une autre organisation envoie mes informations ailleurs. Dans un tel cas, le gouvernement n'aurait-il pas une certaine responsabilité? On dirait que vous vous occupez des problèmes de tout le monde. À un moment donné, ne devrait-on pas suggérer que le gouvernement du Canada donne un coup de main à tous les citoyens?

M. Denis Berthiaume: Écoutez, en ce moment, ce qui est important, c'est de rassurer les membres et d'offrir une protection à tout le monde. On ne va pas se mettre à déterminer si une donnée envoyée à l'étranger provient de la fuite de données chez Desjardins ou d'une autre fuite de renseignements dans une autre organisation. Nous voulons couvrir et rassurer nos membres.

Pour répondre à votre question, si une fraude survient dans un compte Desjardins, nous allons couvrir le membre concerné. Comme c'est le cas chez d'autres institutions financières, en cas de tentative de fraude, qu'il s'agisse d'un compte d'opérations courantes, d'un compte de carte de crédit ou d'un autre type de compte, nous n'en tenons pas les membres responsables.

Le président: Merci, monsieur Paul-Hus.

Monsieur Dubé, vous avez sept minutes.

M. Matthew Dubé: Merci, monsieur le président.

Messieurs Cormier, Brun et Berthiaume, je vous remercie d'être ici. Vous êtes les bienvenus. Je crois que vous avez très bien saisi notre intention, c'est-à-dire échanger pour rétablir la confiance des personnes qui sont extrêmement inquiètes. Vous l'avez bien dit. Comme vous, nous entendons parler ces gens-là. C'est encore plus intéressant pour nous, puisque nous venons de terminer une étude. En fait, nous avons plutôt ouvert la porte aux députés de la prochaine législature en ce qui concerne la cybersécurité dans le secteur financier. Dans ce contexte-là, cela nous intéresse particulièrement.

Puisqu'on ne l'a pas mentionné encore, je dirais que, comme députés québécois, nous ne sommes pas ici pour faire une chasse aux sorcières. Avec le nombre d'activités auxquelles nous assistons, nous constatons clairement que Desjardins est un partenaire local de la communauté. Nous voulons travailler ensemble, et je pense que votre recommandation d'aujourd'hui va dans ce sens-là. Alors, je vous remercie.

J'aimerais aborder quelques éléments, en espérant que vous puissiez répondre à quelques questions. Je comprends les contraintes sous lesquelles vous vous présentez. La première chose est toute simple et semble niaiseuse, mais il s'agit des services français d'Equifax. Quelques personnes ont signalé qu'elles avaient de la difficulté à obtenir des services en français. Avez-vous collaboré avec eux pour vous assurer que vos membres, dont la très grande majorité est francophone, reçoivent un service en français?

● (1610)

M. Denis Berthiaume: Oui. Tout d'abord, nous voulions agir rapidement avec Equifax, et je pense que cela a été le sens de la démarche. Les gens d'Equifax ont été très collaboratifs. Ils ont même ajusté leur offre de service pour nous accommoder à plusieurs égards. Nous avons donc eu une excellente collaboration.

Maintenant, au fil du temps, nous avons réalisé effectivement que la capacité francophone atteignait certaines limites chez Equifax. C'est la raison pour laquelle nous avons apporté un certain nombre de mesures additionnelles. Le président vous a mentionné les quatre initiatives qui ont été mises en place.

Premièrement, les gens peuvent aller, que ce soit sur le Web ou sur leur téléphone cellulaire, s'inscrire directement aux services d'Equifax. Nous nous occupons de les diriger vers ces services, de faire le lien avec Equifax et de faire l'authentification.

Deuxièmement, les gens peuvent obtenir un service francophone en joignant nos centres d'appels AccèsD. Les temps d'attente sont très raisonnables. Nous faisons l'interface, en quelque sorte, entre nos membres et Equifax afin d'améliorer l'expérience. C'est ce que nous avons mis en place au cours des derniers jours et des dernières semaines. Nous croyons que cela a porté ses fruits.

M. Matthew Dubé: Ce n'est pas nécessairement propre à ce qu'on veut examiner, et cela ne relève pas du mandat du Comité, mais vous comprendrez que je voulais tout de même avoir l'heure juste là-dessus. Merci.

J'aimerais revenir sur la réglementation. On en a un peu entendu parler de la part des représentants du gouvernement qui vous ont précédés. Cela devient-il encombrant pour ce qui est d'atteindre vos objectifs et d'assurer la sécurité des données de vos membres? Vous êtes dans une situation particulière où vous êtes assujettis à la fois à la réglementation du gouvernement du Québec et à celle du gouvernement fédéral. Comparativement aux institutions financières traditionnelles et aux grandes banques, vous êtes dans une situation un peu unique. Vous me pardonnerez la terminologie qui n'est peut-être pas appropriée, mais je pense que vous comprenez ce que je veux dire. Cette situation différente peut-elle causer des ennuis?

Plus simplement, aurait-on intérêt à assurer une meilleure harmonie entre les exigences du gouvernement du Québec et celles du gouvernement fédéral, de sorte que vous n'ayez pas à tourner à gauche et à droite pour vous conformer à deux entités réglementaires différentes?

M. Bernard Brun (vice-président, Relations gouvernementales, Mouvement Desjardins): Je vous remercie de votre question.

Effectivement, c'est extrêmement pertinent, parce que nous évoluons dans un système bijuridictionnel. Cela dit, dans l'ensemble, Desjardins est parfaitement à l'aise dans le cadre actuel. Évidemment, avec les échanges technologiques, l'interrelation au sein du système financier est de plus en plus manifeste. À ce sujet, il est primordial de ne pas agir en vase clos.

Plus tôt, M. Cormier a souligné que nous avions eu une bonne collaboration. Nous avons pu discuter avec tous les intervenants des gouvernements fédéral et provincial. Nous les incitons beaucoup à travailler ensemble. Nous sentons qu'il y a une collaboration, mais nous insistons pour que les gouvernements eux-mêmes discutent.

Quant au fait qu'une entité comme le Mouvement Desjardins navigue des deux côtés, je ne vois pas cela comme étant un problème. Cependant, nous avons manifestement besoin de soutien à cet égard. Nous le sentons et nous mettons l'accent là-dessus. Cela vient rejoindre notre suggestion de mettre sur pied un comité multipartite avec des gens des différents gouvernements. C'est ce qui nous permettra d'avancer et d'avoir des politiques efficaces qui vont toucher tout le monde.

M. Matthew Dubé: Merci.

Il sera peut-être plus difficile de répondre à ma prochaine question, puisque l'enquête policière est toujours en cours.

Compte tenu de l'expertise en hausse en matière de cybersécurité, surtout chez les gens qui en font leur travail, croyez-vous qu'il serait approprié de recommander la vérification continue des comportements ou des antécédents d'employés qui ont accès à de l'information sensible et qui sont en mesure d'exploiter les informations d'autres utilisateurs, c'est-à-dire d'autres employés?

Je ne suis pas en train de dire que vous n'avez pas été à la hauteur à cet égard, mais tout le monde commence à reconnaître qu'il y a des personnes qui ont de plus en plus d'expertise. On se sert de leur expertise, mais cela peut aussi avoir des conséquences plus néfastes.

● (1615)

M. Guy Cormier: Mon collègue peut parler de nos pratiques, puis je compléterai ses remarques selon ma perspective.

M. Denis Berthiaume: La première des choses, c'est qu'il y a des enquêtes de sécurité rigoureuses qui se déroulent chez Desjardins de façon continue. Ensuite, effectivement, les enquêtes sont liées au niveau d'emploi. C'est un élément important.

En ce qui concerne la situation qui nous occupe, on pourrait se demander si on aurait pu détecter quoi que ce soit. J'aime bien rappeler que la fraude interne par un employé malveillant est le risque contre lequel il est le plus difficile de se prémunir. C'est reconnu partout dans l'industrie, et il y a beaucoup de cas patents.

Outre les enquêtes de sécurité, il y avait des mécanismes de sécurité en place. Évidemment, on parle d'un employé malveillant qui a trouvé une façon de contourner toutes les règles et qui a utilisé un stratagème pour exfiltrer les données. Cela dit, je tiens à vous rassurer: il y a des mécanismes de sécurité en place.

M. Guy Cormier: Est-ce qu'avec le temps nous pourrons aller plus loin en ce qui concerne la situation que nous vivons? Comme je le disais, à l'ère du numérique, des gens manipulent des données personnelles non seulement dans les institutions financières, mais également dans toutes sortes d'entreprises. Aujourd'hui, lorsqu'une personne veut inscrire son enfant à la garderie, elle doit donner son numéro d'assurance sociale, et ce numéro peut demeurer sur la table pendant cinq, dix ou quinze minutes, le temps de l'inscription. C'est la réalité au Canada.

Je crois que toute entreprise où des employés manipulent des renseignements personnels doit s'assurer que ces derniers ont fait l'objet de vérifications.

[*Traduction*]

Le président: Nous allons devoir en rester là.

[*Français*]

Merci, monsieur Dubé.

Madame Lapointe, vous avez la parole.

Mme Linda Lapointe: Merci beaucoup, monsieur le président. Je vais partager mon temps de parole.

Messieurs, je vous remercie beaucoup d'être ici.

Je suis membre de Desjardins depuis 1980 à peu près. Comme mon collègue le disait, Desjardins est partout. Ma circonscription est Rivière-des-Mille-Îles et elle comprend Deux-Montagnes, Saint-Eustache, Boisbriand et Rosemère. Il y a une caisse Desjardins à Deux-Montagnes et une à Thérèse-De Blainville. Ce sont deux grosses institutions dans la région. Il y a deux MRC et deux caisses Desjardins.

M. Guy Cormier: Il y a M. Bélanger.

Mme Linda Lapointe: Oui.

Vous avez dit que la fraude interne est la plus difficile à détecter et contre laquelle il est le plus difficile de se prémunir. Un peu plus tôt aujourd'hui, des représentants du ministère des Finances et de l'Agence du revenu du Canada nous ont parlé.

Comment cela fonctionne-t-il à l'interne chez Desjardins? Comment les superviseurs auraient-ils pu repérer cet employé malveillant? Il est clair qu'il a été capable de se faufiler dans le système. Y a-t-il des niveaux d'accès et des captures d'écran? Le système émet-il des alertes s'il repère des choses inhabituelles? Vos employés ont-ils le droit d'avoir leur téléphone cellulaire avec eux lorsqu'ils travaillent sur des données?

Je suis sûre que vous allez réévaluer les mesures en place. Vous avez parlé d'un seul employé malveillant, mais qu'allez-vous faire pour vous prémunir contre d'autres employés malveillants? Quelles sont vos règles? Comment cela fonctionne-t-il?

M. Guy Cormier: Monsieur Berthiaume, pouvez-vous parler des opérations?

M. Denis Berthiaume: Oui.

En ce qui concerne les opérations, je tiens d'abord à vous dire que personne, en ouvrant son ordinateur au bureau le matin, n'a accès à toutes les données. Ce n'est pas ainsi que cela fonctionne. Chez Desjardins, les emplois sont catégorisés en fonction des données qui sont nécessaires pour faire le travail. C'est la première chose.

Ensuite, notre organisation a mis en place plusieurs mécanismes internes de sécurité et de contrôle, mais nous ne voulons pas en parler publiquement, car même nos employés ne sont pas au courant de ces mécanismes. Je ne peux donc pas donner beaucoup de détails là-dessus.

Quant au cas particulier qui nous intéresse, une enquête policière est en cours, ce qui rend le sujet fort sensible. Honnêtement, nous ne voulons en aucun cas nuire à l'enquête policière en cours.

Comme je viens de le dire, nous ne voulons pas donner de détails sur nos mécanismes de sécurité, car ils sont importants pour éviter que la situation dont il est question aujourd'hui ne se reproduise. Cette situation met en cause un seul employé, mais je peux vous dire que nos mécanismes de sécurité détectent des éléments de fraude externe ou autres. Je réitère qu'il est extrêmement difficile de se protéger complètement d'un employé malveillant.

● (1620)

Mme Linda Lapointe: Allez-vous revoir vos règles internes?

M. Denis Berthiaume: Concernant les mesures de sécurité, nous sommes en évolution constante. Bon an, mal an, Desjardins investit 70 millions de dollars par année dans la sécurité et la protection des données et des renseignements personnels. Nous nous améliorons continuellement pour nous adapter aux nouvelles technologies qui créent de nouvelles possibilités de fraude. Des gens essaient de créer de nouveaux stratagèmes et nous sommes en évolution constante pour nous permettre de les repérer.

Mme Linda Lapointe: Merci beaucoup.

Je suis contente que vous ayez parlé des quatre procédures que vous avez mises en place. Mes parents sont des personnes âgées et n'ont pas Internet. Ils se sont rendus en personne à leur caisse Desjardins pour que quelqu'un les aide, et cela n'a pas très bien fonctionné.

M. Guy Cormier: Dans les premiers jours, l'inscription à Equifax a représenté un défi pour nous.

Mme Linda Lapointe: Les gens qui n'ont pas accès à Internet ne sont pas capables de s'y inscrire.

M. Guy Cormier: Nous avons donc pris la décision d'offrir un service aux gens qui n'ont pas accès à Internet. Dès aujourd'hui, les gens qui le souhaitent pourront quand même bénéficier du service d'alerte. Ce service sera pris en charge par Desjardins, qui pourra communiquer avec eux par la suite. Nous avons innové en ce qui concerne Equifax, afin de trouver une solution pour ces gens.

Mme Linda Lapointe: Merci.

M. Francis Drouin: Merci beaucoup, monsieur le président.

Monsieur Cormier, vous et moi, comme Mme Lapointe, sommes victimes de cette fuite. Je comprends très bien qu'il soit difficile de contrôler complètement un employé malveillant. C'est quasi impossible.

Cela dit, cette fuite aura diverses répercussions sur les membres de Desjardins. Pour certains, rien ne va arriver, alors que d'autres seront victimes de fraude quelque temps dans le futur. Mes concitoyens m'ont demandé pourquoi vous offrez le service Equifax gratuitement pour 5 ans, et pas pour 10, 15 ou 20 ans.

M. Guy Cormier: Monsieur Berthiaume, vous pouvez répondre à la question au sujet de la période de cinq ans, puis nous reviendrons à la réponse de ce matin. C'est une question qu'on nous a déjà posée.

M. Denis Berthiaume: Premièrement, nous avons voulu agir rapidement en offrant une protection de cinq ans. Comme nous n'étions pas satisfaits de cette période de protection, nous avons décidé de la prolonger. Le président a annoncé ce matin que Desjardins s'engage à fournir une protection à vie. Nous ne nous sommes pas contentés d'une période de protection de cinq ans. Nous avons un partenariat avec Equifax pour fournir cette protection, ce qui est important de deux façons.

Nous observons une bonne augmentation des inscriptions à Equifax, mais nous ne sommes pas satisfaits de ce nombre. À en juger par la tendance actuelle, nous craignons que, au bout du compte, seuls 20 % ou 25 % de nos membres s'inscrivent à Equifax. Cela laisse quand même des gens sans couverture et qui choisissent de ne pas bénéficier du système d'alerte, pour des raisons qui leur sont propres. Or nous ne voulons pas laisser 75 % ou 80 % de nos membres sans aucune protection. Nous voulons leur fournir un service d'assistance, s'il arrive quelque chose. C'est ce qui a mené à l'annonce de ce matin. Nous voulons aller au-delà de la protection d'Equifax et offrir à nos membres une couverture parapluie.

M. Francis Drouin: Hier, j'ai vécu une expérience en communiquant avec Equifax. Son site Web ne fonctionnait pas et j'ai appelé. Finalement, entre 45 minutes et une heure et demie plus tard, j'ai pu m'inscrire.

Dans l'Est de l'Ontario, les caisses du Mouvement Desjardins sont très populaires et très présentes dans les communautés. Les employés sont formés pour aider les personnes âgées qui ne peuvent pas aller sur Internet pour s'inscrire. J'ai la chance d'aller sur Internet et de vérifier mon rapport de crédit chaque jour, mais qu'en est-il pour ma grand-mère, par exemple? Quelqu'un de Desjardins va-t-il l'aviser qu'il y a eu un mouvement sur son rapport de crédit?

M. Denis Berthiaume: Oui, c'est la nouvelle solution que nous venons de lancer. Nous allons nous organiser pour que les gens puissent s'inscrire à Equifax. Par la suite, plutôt qu'Equifax communique avec la personne par courriel, Desjardins va faire le lien entre Equifax et la personne. Nous allons recevoir les alertes et vérifier qu'elles sont réelles, puis nous allons contacter les membres concernés, comme votre grand-mère, de la façon qui leur convient. C'est ce que nous mettons en place.

M. Francis Drouin: Merci.

M. Guy Cormier: J'aimerais souligner brièvement quel est le message important ici. Le Mouvement Desjardins a décidé rapidement d'être transparent et de donner l'information le 20 juin. Quand nous sommes entrés dans les données des 2,7 millions de gens, nous avons réalisé que des personnes n'avaient pas accès à Internet. Il y avait aussi des comptes de succession. Des situations ont émergé et nous avons vu qu'il fallait innover et trouver des solutions pour eux. Jusqu'à maintenant, pour tous ces cas, nous avons une bonne collaboration avec les gens d'Equifax. Ils nous aident à trouver une solution différente, notamment pour des personnes comme votre grand-mère.

● (1625)

[*Traduction*]

Le président: Merci, monsieur Drouin.

Monsieur Motz, vous avez cinq minutes.

M. Glen Motz: Merci, monsieur le président.

Merci d'être présents, messieurs.

Si l'on en croit les renseignements que nous avons reçus, environ 200 000 Canadiens à l'extérieur du Québec ont été touchés par cette situation particulière. Savez-vous combien de personnes sont concernées dans chaque province?

[*Français*]

M. Denis Berthiaume: Les membres touchés sont principalement au Québec. Il y en a un certain nombre en Ontario et très peu dans les autres provinces. On parle de personnes qui ont sans doute déménagé dans d'autres provinces et qui sont membres de Desjardins. C'est un volet important. Ce sont les membres des caisses Desjardins qui sont touchés.

Les clients de State Farm ou de Patrimoine Aviso, avec qui nous avons un partenariat, ne sont pas touchés. On ne parle que des membres des caisses qui ont pu déménager dans d'autres provinces ou des membres de nos caisses en Ontario.

[*Traduction*]

M. Glen Motz: D'accord.

Vous avez mentionné que vous avez acquis State Farm en 2015. Vous dites qu'aucun de ses clients n'est touché.

M. Denis Berthiaume: Ils n'ont pas du tout été touchés, non.

M. Glen Motz: En 2017, vous avez créé Aviso Wealth. Il s'agit de la fusion de Credential Financial, de Qtrade Canada et de NEI Investments. Ces entreprises ont toutes été fusionnées.

M. Denis Berthiaume: C'est exact.

M. Glen Motz: Certains de ces clients ont-ils été touchés?

M. Denis Berthiaume: Ils n'ont pas été touchés du tout en dehors de la portée de ce dont nous avons parlé...

M. Glen Motz: Qu'en est-il des anciens clients de Desjardins dont les comptes ont été fermés? Certaines de leurs données ont-elles été touchées?

M. Denis Berthiaume: Je ne suis pas certain que je...

M. Glen Motz: Ils ont fait partie de vos clients. Conservez-vous toujours leurs données bien que ce ne soit plus le cas? Ces données ont-elles été compromises ?

M. Denis Berthiaume: Je tiens à me montrer très, très précis. Seuls les membres de notre réseau de caisses sont touchés. Supposons que vous en étiez membre il y a un an et que vous avez fermé votre compte pour une raison quelconque. Si vous ne recevez pas de lettre, vous ne serez pas touché. Il n'y a pas de répercussions. Vous n'avez pas été touché...

M. Glen Motz: Pour que ce soit clair, si vous n'avez pas de compte actif chez Desjardins, vous n'avez pas été touché par cette atteinte à la protection des données. Ai-je bien compris?

M. Denis Berthiaume: Si vous n'avez pas reçu de lettre... La clé est de savoir si vous avez personnellement reçu une lettre. Si vous avez reçu une lettre, cela signifie que vous faites partie des membres qui pourraient être touchés, et nous vous encourageons à vous abonner à Equifax.

M. Glen Motz: Cela ne répond pas vraiment à ma question. Si j'ai bien compris, il faut avoir un compte actif chez Desjardins pour avoir été touché par cette atteinte à la protection des données. C'est exact?

M. Denis Berthiaume: Non, parce que vous pourriez être un ancien membre de Desjardins et avoir fermé votre compte il y a un an...

M. Glen Motz: C'est la question que j'ai posée plus tôt.

M. Denis Berthiaume: ... mais vous pourriez être touché si vous recevez une lettre.

M. Glen Motz: Je ne me soucie pas de la lettre parce que les Canadiens s'en moquent. Ils veulent savoir si les membres actuels ont été touchés ou non. La réponse est oui. Les clients actuels ou les anciens clients pourraient être touchés.

M. Denis Berthiaume: Oui

M. Glen Motz: Si je me souviens bien, en 2018, Desjardins Ontario a fusionné avec environ 11 coopératives de crédit de l'Ontario. Certains de ces clients potentiels seraient-ils touchés par cette atteinte à la protection des données?

M. Denis Berthiaume: Nous parlons des caisses de l'Ontario...

M. Guy Cormier: La réponse est oui. Il est possible que certains membres des caisses de l'Ontario, fusionnées ou non, aient été touchés par cette atteinte.

M. Glen Motz: En 2013, le Mouvement Desjardins a acheté des compagnies d'assurance dans l'Ouest, notamment Coast Capital Insurance, en Colombie-Britannique, First Insurance dans cette même province, Craig Insurance, en Alberta, et Melfort Agencies et Prestige Insurance, en Saskatchewan.

Certains de ces clients pourraient-ils être touchés par l'atteinte à la protection des données survenue chez Desjardins?

M. Denis Berthiaume: La réponse est non.

M. Glen Motz: Les téléphones des clients qui utilisent Apple Pay ou Android Pay pour effectuer leurs opérations bancaires peuvent-ils être compromis par cette atteinte à la protection des données, et courent-ils de plus grands risques de recevoir des messages frauduleux pouvant découler de cette situation?

M. Denis Berthiaume: Les données qui ont été extraites comprennent des numéros de téléphone et des courriels. Pour répondre à votre question, oui, il est possible que ces personnes fassent l'objet d'hameçonnage, mais encore une fois, uniquement s'ils sont membres d'une caisse, pas s'ils sont clients. S'ils sont clients d'Aviso Wealth, s'ils ont eu une assurance dans le passé, s'ils ont une assurance vie et santé, ou s'ils ont une assurance incendie, accidents et risques divers, ils ne sont pas touchés.

● (1630)

M. Glen Motz: Il ne s'agit que de l'aspect financier.

M. Denis Berthiaume: Il ne s'agit que de membres des caisses.

M. Glen Motz: Je vais partager mon temps avec M....

Le président: Vous allez devoir partager six secondes avec lui.

Passons à M. Graham, pour cinq minutes.

[*Français*]

M. David de Burgh Graham: Je vais suivre un peu les propos de M. Motz. Parmi ceux qui n'ont pas reçu de lettre, beaucoup s'inquiètent et se demandent s'ils sont touchés ou non.

Peut-on dire clairement à tous ceux qui n'ont pas reçu de lettre qu'ils ne sont pas touchés?

M. Denis Berthiaume: Selon l'information que nous avons, seulement ceux qui reçoivent une lettre sont touchés.

M. David de Burgh Graham: Alors si on ne reçoit pas de lettre, on n'est pas touché; c'est bien cela?

M. Denis Berthiaume: S'ils n'ont pas reçu de lettre, ils ne sont pas touchés.

M. Guy Cormier: Le 14 juin, nous avons reçu de l'information du corps policier de Laval. C'est grâce à cette information que nos équipes d'investigation informatique ont été capables de nous fournir les chiffres de 2,7 millions de particuliers et de 173 000 entreprises. Ce sont à ces gens-là que nous avons transmis des lettres écrites.

Malgré tout, nous entendons les préoccupations des gens. C'est pourquoi, ce matin, nous avons décidé d'accélérer le lancement de ce programme de protection pour tous les membres, qu'ils soient touchés ou non.

M. David de Burgh Graham: Cette protection est une bonne chose, mais dans certaines villes de ma circonscription, Laurentides—Labelle, plusieurs gens n'ont pas d'accès à Internet ni de téléphone cellulaire. Ils sont moins nombreux que lorsque je suis arrivé, mais il y en a encore. Plusieurs ont même perdu leur succursale Desjardins. Qu'est-ce que ces gens peuvent faire?

J'ai un compte chez Equifax depuis plusieurs années. Quand il y a un changement, on m'envoie un courriel, mais je dois aller sur le site Web et essayer de comprendre de quoi il s'agit, car ce n'est pas clair du tout. Alors, pour ceux qui ont une connexion Internet, les renseignements d'Equifax ne sont pas clairs, et ceux qui n'ont pas de connexion n'ont rien du tout.

Vous en avez parlé un peu, mais pourriez-vous en parler un peu plus?

M. Guy Cormier: Il y a deux choses. Premièrement, il est urgent de brancher les citoyens de partout au pays à Internet, si on veut arriver au XXI^{e} siècle. De notre côté, puisque certains de nos membres ne sont pas branchés à Internet — parfois, c'est par choix, parfois, c'est parce qu'ils n'y ont pas accès —, nous avons proposé une solution supplémentaire en partenariat avec Equifax. M. Berthiaume peut l'expliquer.

M. Denis Berthiaume: Les personnes qui ne vont pas sur le Web et qui n'ont pas nécessairement d'adresse courriel doivent tout de même être jointes. Nous avons donc mis en place un centre d'appels afin qu'elles puissent communiquer avec nous par téléphone. Nous allons nous charger de les inscrire aux services d'Equifax.

Nous avons mis en place une solution innovante avec Equifax, qui va les enregistrer, s'occuper de la surveillance et des alertes, puis nous envoyer les résultats. À ce moment-là, nous nous chargerons de communiquer avec ces personnes qui n'ont pas d'accès à Internet ou au courriel. C'est ce que nous avons mis en place aujourd'hui même.

M. David de Burgh Graham: Equifax s'occupera donc de l'aspect technique, et non Desjardins.

M. Denis Berthiaume: Oui. Actuellement, c'est Equifax qui a la capacité de s'occuper des alertes. Comme nous le disions plus tôt, Equifax détient 70 % du marché canadien pour ce qui est des bureaux de crédit et des systèmes de détection et d'alerte. Ce sont donc ses services que nous utilisons pour ce volet.

Encore une fois, nous faisons le lien pour les personnes qui ont plus de difficulté à accéder à Internet ou qui n'ont pas d'adresse courriel. Nous rassurons les gens et, en cas d'alerte, nous prenons contact avec eux.

M. David de Burgh Graham: D'accord.

Dans votre allocution, vous avez parlé de changer notre système d'identité numérique. Quels exemples voudriez-vous que l'on suive?

M. Guy Cormier: Loin de moi l'idée de vous donner l'exemple parfait qui devrait être suivi, parce qu'il y aura toujours des lacunes dans les solutions parfaites qu'on pense avoir trouvées. Il y aura toujours des gens malhonnêtes qui essaieront de défaire ces solutions. Toutefois, des pays comme l'Estonie, l'Inde et même certains pays d'Europe ont mis en place des mesures concernant les identifiants uniques ou, à tout le moins, des mesures visant à ce que les cartes émises par le gouvernement, que ce soit les permis de conduire ou les cartes d'assurance-maladie, ne deviennent pas des façons d'identifier les gens. Ces pays avaient pour objectif de rétablir le rôle premier de ces cartes, qui sont devenues des pièces d'identification au fil du temps. Le Canada devrait s'inspirer de ces pays.

● (1635)

M. David de Burgh Graham: D'accord.

J'ai une dernière question. Qu'est-ce que les 2,9 millions de clients de Desjardins touchés avaient en commun? Est-ce qu'on sait pourquoi ils ont été touchés et pas les autres?

M. Denis Berthiaume: À ce sujet, nous n'avons rien de concluant. Nous nous sommes basés sur les données que les services de police nous ont fournies. Nous n'avons pas de données concluantes sur ce qui fait que quelqu'un est sur la liste ou non. Nous n'avons pas cette information.

M. David de Burgh Graham: Merci.

[*Traduction*]

Le président: Nous allons passer à M. Clarke.

[*Français*]

M. Alupa Clarke: Monsieur Cormier, je voudrais simplement réitérer ce que mon collègue a dit. L'objectif fondamental de la réunion d'aujourd'hui, pour nous les conservateurs, était de déterminer ce que le gouvernement, ses agences et ses institutions pouvaient faire pour vous aider et, par ricochet, pour aider les membres de Desjardins, ce qui est le plus important. Ce sont des citoyens canadiens et québécois.

Par ailleurs, vous n'êtes pas sans savoir que j'ai joint les trois directeurs des caisses Desjardins de ma circonscription pour leur exprimer mon soutien.

Le ministère de l'Emploi et du Développement social du Canada a-t-il pris contact avec vous pour obtenir la liste des 2,9 millions de citoyens? C'est une question très importante.

M. Guy Cormier: Le ministère est en contact avec nous et collabore avec nous. Cela fait plus de deux semaines que nous discutons directement avec ses représentants, que ce soit au sujet des numéros d'assurance sociale ou de la situation que vit Desjardins.

Je ne crois pas que la demande de transmission de l'information ait été faite, du moins sur le plan opérationnel. Je n'ai pas cette information. Je ne sais pas si M. Brun ou M. Berthiaume en savent plus, mais je ne pense pas.

M. Alupa Clarke: Quand vous aurez la réponse, pourriez-vous la donner aux analystes ou au greffier? Ce serait important pour nous de le savoir. S'il se trouve que la demande a été faite, pourriez-vous fournir la liste de ces Canadiens? Nous, nous cherchons à savoir ce que le gouvernement peut faire, mais il faudrait d'abord qu'il sache de qui il est question. Alors, seriez-vous en mesure d'envoyer cette liste au gouvernement canadien? Malheureusement, il s'agirait encore d'envoyer des données, mais le destinataire serait le gouvernement.

M. Denis Berthiaume: Il faudrait voir si cela est possible. D'un point de vue juridique, je n'en suis pas certain.

M. Alupa Clarke: Ensuite, j'aimerais savoir si un membre du Cabinet actuel vous a contactés depuis le 20 juin.

M. Guy Cormier: Lorsque vous parlez du Cabinet actuel, vous parlez du Cabinet...

M. Alupa Clarke: Je parle du Cabinet fédéral. Ce serait donc un ministre.

M. Guy Cormier: Oui, tout à fait. J'ai eu une discussion avec le ministre Morneau sur la situation. Il m'a offert son soutien pour voir comment le gouvernement fédéral pouvait accompagner Desjardins dans cette situation.

M. Alupa Clarke: D'accord.

Dans votre introduction, vous avez mentionné très humblement et respectueusement que vous aviez quelques questions. Personnellement, j'aurais aimé connaître vos réponses en tant qu'expert dans votre domaine. Je ne me souviens pas très bien de votre première question, mais c'était quand même intéressant. Vous vous demandiez si le Canada avait un système adéquat en ce qui a trait aux numéros d'assurance sociale, par exemple. J'aimerais connaître votre perspective là-dessus.

M. Guy Cormier: La première question était de savoir si le Canada est bien outillé pour encadrer le développement technologique, qui est plein de promesses, mais qui comporte aussi des risques nouveaux.

Y a-t-il lieu d'adapter nos systèmes d'identification?

M. Alupa Clarke: J'aimerais avoir vos réponses sur les deux points.

M. Guy Cormier: Mes deux réponses sont simples: je pense que le statu quo n'est pas une option. Le statu quo, actuellement, au Canada, n'est pas suffisant à l'ère du numérique, à l'ère du 5G qui s'en vient et à l'ère de réflexions sur le monde des services financiers, notamment les services financiers ouverts. Sur ces deux questions, je pense qu'on ne doit pas se satisfaire du statu quo.

C'est pour cela que nous proposons, humblement, la création d'un comité composé de plusieurs parties prenantes, y compris des citoyens, des gouvernements, des entreprises — pas seulement les institutions financières, mais les entreprises qui traitent des données —, pour réfléchir à ces questions et voir si, au moyen d'exemples d'autres pays du monde, on peut continuer d'être des leaders.

Comme je l'ai mentionné au début, je pense qu'en intelligence artificielle, le Canada est en train de prendre une position de leadership importante dans le monde. Parallèlement, il faut avoir la même ambition en ce qui a trait aux renseignements personnels et à la protection des données. Ma réponse tourne autour de ces points-là.

M. Alupa Clarke: J'ai une question supplémentaire, qui sera probablement la dernière. Je m'adresse ici à M. Cormier, le citoyen.

Vous avez fait une annonce fort importante ce matin. Vous dites que la protection s'applique à l'ensemble des membres, qu'ils soient touchés ou non par ce malheureux événement. Vous avez dit qu'ils n'ont qu' à vous appeler pour que vous vous occupiez d'eux. Vous allez établir les contacts, prendre les mesures et entreprendre les démarches qui s'imposent.

Pensez-vous que ce soit exactement ce genre d'attitude que le gouvernement, l'État fédéral, devrait avoir en ce moment envers les 2,9 millions citoyens canadiens?

On demande aux citoyens de prendre contact avec nous, or je pense que c'est le gouvernement fédéral qui devrait prendre contact avec les citoyens. Disons que les citoyens entrent en communication avec le gouvernement fédéral, ce dernier ne devrait-il pas avoir la même approche que vous et dire qu'il s'occupe de tout?

La représentante d'Emploi et Développement social Canada disait que, si l'on changeait les numéros d'assurance sociale des citoyens, ceux-ci devraient appeler tous leurs anciens employeurs. Ce n'est pas ce que vous faites. Vous, incroyablement, vous dites que vous allez vous occuper de tout le monde à la dernière minute.

En tant que citoyen, aimeriez-vous que le gouvernement fédéral agisse de la même façon envers les membres touchés?

● (1640)

M. Guy Cormier: Je dirais, en tant que citoyen, que les élus sont élus, justement, pour assurer un encadrement et adopter des lois. Dans la situation qu'on vit actuellement à l'ère du numérique, il faut mettre en place des paramètres réglementaires qui protègent les citoyens à cet égard. C'est mon message, comme citoyen.

C'est aussi pourquoi, malgré le fait que nous trouvions cette réunion prématurée, nous avons quand même pris la décision d'être présents. Nous sentons que cette situation tire une sonnette d'alarme et qu'il y a une prise de conscience et une réelle volonté de la part des élus de se pencher sur cette question. Nous voulions apporter notre point de vue sur ce sujet.

[*Traduction*]

Le président: Merci, monsieur Clarke.

Nous allons passer à M. Dubé pour trois minutes, puis à M. Fortin pour trois minutes.

[*Français*]

M. Matthew Dubé: Merci, monsieur le président.

J'avais une question qui rejoint un peu ce que M. Graham disait par rapport à l'accès à Internet et au téléphone. Les personnes âgées ont des besoins particuliers.

Veille-t-on à cela également?

M. Denis Berthiaume: C'est ce que je disais. Souvent, les personnes âgées n'ont pas nécessairement une connexion Internet ou une adresse courriel. Nous nous occupons d'elles. Ces personnes peuvent nous téléphoner. Nous allons prendre la situation en charge à partir de ce moment et ferons office d'intermédiaires avec Equifax concernant le système d'alerte et ce que ces personnes vont recevoir comme message.

M. Matthew Dubé: Il y a un article intéressant dans *La Presse* d'aujourd'hui, si je ne me trompe pas. On y parle de la façon dont sont réglementées les agences de surveillance de crédit, soit les compagnies comme Equifax, et que cette réglementation porte davantage sur des questions liées aux consommateurs.

C'est peut-être trop de spéculation pour ce dont vous êtes à l'aise de parler aujourd'hui, mais, étant donné la relation un peu symbiotique qu'elles entretiennent avec les institutions financières et la brèche dont Equifax a été victime, croyez-vous qu'il serait pertinent, à l'ère numérique, de revoir la façon dont ces agences sont réglementées?

C'est devenu un plus important que la protection des consommateurs; elles ont maintenant une responsabilité au regard du maintien des données. On voit qu'il y a des conséquences importantes.

Devrait-on revoir cela dans le contexte de tous ces changements auxquels vous avez fait allusion?

M. Guy Cormier: Je vous l'ai dit il y a quelques minutes: je pense que le statu quo n'est pas une option. C'est la raison pour laquelle nous comparaissons devant vous aujourd'hui. Desjardins sera très honoré de participer aux réflexions, le cas échéant.

Je crois qu'il faut rassembler les parties prenantes qui travaillent dans le domaine des données au Canada pour réfléchir à la façon dont on veut faire évoluer la situation. Parfois, il pourrait s'agir de réglementation, parfois, de processus d'affaires, ou, parfois, de façons de travailler ensemble. Je pense que le statu quo n'est pas une option.

M. Matthew Dubé: Il me reste une minute. J'aimerais vous dire, en terminant, que nous sommes heureux de votre présence ici. Nous comprenons que c'est une situation difficile. J'apprécie le fait que vous comprenez la raison pour laquelle nous avons le devoir de faire cela.

Des citoyens nous interpellent. Cela les touche, ils sont inquiets. Notre objectif n'est pas uniquement de les rassurer dans le cas présent, mais aussi de nous assurer qu'eux et d'autres citoyens qui sont des clients d'autres institutions financières ne vivent pas la même chose. Vous partagez votre expérience, ce qui est très utile non seulement aujourd'hui, mais aussi pour une prochaine législature. Nous voulons quand même mettre en place une feuille de route dans ce domaine qui évolue rapidement.

M. Guy Cormier: C'est pour cela que nous avons accepté l'invitation.

M. Matthew Dubé: C'est très apprécié, merci.

Le président: Monsieur Fortin, vous avez trois minutes, s'il vous plaît.

M. Rhéal Fortin: Merci, monsieur le président.

Messieurs Cormier, Brun et Berthiaume, je vais commencer par vous féliciter moi aussi. J'avoue qu'en arrivant ici ce matin, j'avais des questions et des inquiétudes, auxquelles vous avez répondu. Je pense que votre déclaration de ce matin est tout à l'avantage de Desjardins. Moi aussi, je suis affecté par ce qui s'est passé chez Desjardins, et j'apprécie les mesures que vous avez prises.

Il y a environ deux ou trois semaines, la Banque du Canada a mis en place le Groupe sur la résilience du secteur financier, afin de contrer les menaces informatiques. À ce que je sache, le Mouvement Desjardins n'a pas été invité à se joindre à ce groupe. On a invité des banques à charte, entre autres, et celles qui sont d'importance systémique.

D'abord, pouvez-vous me confirmer que le Mouvement Desjardins n'a pas été invité? Ensuite, considérez-vous qu'il serait opportun qu'il participe à un tel groupe de travail?

M. Guy Cormier: Monsieur Brun, je sais que vous avez discuté avec ce groupe. Pouvez-vous donner l'heure juste à ce sujet?

M. Bernard Brun: Je vous remercie de cette question bien pertinente.

La Banque du Canada a, évidemment, un rôle extrêmement important à jouer pour assurer la stabilité financière. Récemment, elle a annoncé la constitution d'un comité pour faire évoluer la supervision et revoir un peu l'encadrement en échangeant avec toutes sortes de partenaires. Naturellement, elle s'est tournée vers les grandes banques et le régulateur. Nous avons eu des discussions avec des gens de la Banque et nous sentons qu'ils ont une ouverture pour explorer cela.

Comme on l'a déjà évoqué, le système financier est extrêmement interrelié. Tous les acteurs de ce secteur ont des enjeux, une réglementation et des régulateurs, mais il faut qu'ils soient capables de travailler ensemble, d'aller au-delà de cela et de discuter. Nous avons certainement un grand intérêt à participer à tout cela. Nous avons senti qu'il y avait une ouverture en ce sens et nous attendons de voir comment ce sera articulé.

C'est sûr que le Mouvement Desjardins est une institution financière canadienne et québécoise d'importance systémique. S'il y a des discussions, il faudrait que nous y participions.

● (1645)

M. Rhéal Fortin: Vous avez l'appui du Bloc québécois là-dessus. J'espère que mes collègues d'en face y donneront suite et proposeront à la Banque du Canada de vous inviter.

Présentement, il y a des discussions sur l'établissement d'un système national de validation de l'identité. Avant, le numéro d'assurance sociale était utilisé dans les relations entre l'employeur et les employés et le gouvernement. Or maintenant, on voit qu'il est utilisé à presque toutes les sauces. On ne sait plus trop comment se comporter relativement à cela, mais il est clair que le simple numéro d'assurance sociale ne suffit plus à assurer une certaine sécurité des citoyens.

À votre avis, un système de validation de l'identité, qui inclurait un NIP, une empreinte ou je ne sais quoi, serait-il utile dans une situation comme celle que vous avez vécue?

M. Guy Cormier: C'est pour cela que nous nous permettons humblement de faire une recommandation au Comité aujourd'hui.

Au Canada, il y a 30, 40 ou 50 ans, on a mis en place certains mécanismes, qui, aujourd'hui, ne servent plus à ce pour quoi ils ont été créés. Il est temps que les acteurs de l'industrie s'assoient ensemble pour relancer une réflexion, qui, comme je le vois très bien, a déjà débuté, et essaient de s'inspirer des meilleures pratiques partout dans le monde.

[*Traduction*]

Le président: Merci, monsieur Fortin.

Je tiens à remercier les témoins de leur présence ici. Je suis heureux de constater que l'annonce de votre ensemble de mesures a coïncidé avec votre comparution ici. C'est assez heureux. Quatre ou cinq membres de ce comité sont particulièrement vulnérables en tant que membres de votre association. Je me demande si leurs vulnérabilités uniques en tant que personnalités publiques sont couvertes par l'annonce que vous faites aujourd'hui.

M. Guy Cormier: Tous les renseignements, selon l'annonce que nous avons faite ce matin, de l'ensemble des personnes qui figuraient sur la liste des membres qui ont été touchés par cette atteinte à la sécurité des données seront pris en charge par ce programme. Qu'il s'agisse d'activités financières sur leurs comptes, de l'obtention d'une aide pour récupérer leur identité ou de problèmes relativement à certains frais liés à la récupération de leur identité, ils pourront se prévaloir de ce programme de protection.

Le président: J'en ai pris note, car vous l'avez mentionné plus tôt. Cependant, je me réfère à la vulnérabilité unique des titulaires de charges publiques. Si cette vulnérabilité se manifeste, sera-t-elle traitée par cet ensemble de mesures particulier?

M. Guy Cormier: C'est quelque chose que nous examinons actuellement dans nos dossiers. Nous cherchons actuellement à savoir si parmi ces 2,7 millions de personnes, certaines sont plus vulnérables que d'autres. Vous avez probablement lu des articles sur des policiers, des juges, des gens comme des titulaires de charges publiques. C'est quelque chose que nous sommes en train d'examiner. Notre priorité était d'envoyer les lettres pour prendre contact avec les gens. Nous étudions maintenant ce qui pourrait constituer une autre vulnérabilité à laquelle nous devrions faire plus attention...

Le président: Donc, pas nécessairement dès le début.

M. Guy Cormier: Oui. Nous allons l'examiner.

Le président: Ma question concerne le fait que nous faisons cela depuis un certain temps déjà et que l'une des normes de protection de référence est ce qu'on appelle la « confiance zéro », qui a été mentionnée par un témoin précédent, qui a dit « repérez et protégez les biens essentiels. Sachez où se trouvent vos données clés, protégez-les, surveillez leur protection et soyez prêts à réagir. »

Pensez-vous que Desjardins a appliqué le principe de la confiance zéro qui semble être la norme de référence en matière de protection des données?

M. Denis Berthiaume: Lorsque nous utilisons le terme « confiance zéro », nous devons définir ce dont nous parlons. Confiance zéro, certaines personnes ont accès aux données. Ils en ont besoin pour faire leur travail. Avec la confiance zéro, nous voulons clairement nous assurer d'avoir mis en place des mécanismes de sécurité qui visent à appliquer le principe de la confiance zéro. Cependant, il existe parfois une différence entre la théorie et ce que vous pouvez vraiment faire dans la pratique. L'objectif est de s'assurer que les données qui nous sont fournies par nos clients sont entièrement sécurisées. C'est notre objectif.

● (1650)

Le président: C'est l'objectif.

Sur ce, je tiens à vous remercier encore une fois pour votre présence ici. Nous allons suspendre la séance pendant quelques minutes, puis nous reprendrons avec les fonctionnaires et nous terminerons notre série de questions avec eux. Je vous remercie.

● (1650)

(Pause)

● (1650)

Le président: Reprenons nos travaux. Merci à tous les fonctionnaires de leur patience. Nous étions au milieu de la période des questions, et je crois que la parole est à M. Graham pour cinq minutes, s'il vous plaît.

[*Français*]

M. David de Burgh Graham: Merci.

Madame Boisjoly, vous avez entendu les gens de Desjardins tout à l'heure parler du besoin de repenser le système du numéro d'assurance sociale. Est-ce qu'on fait des recherches pour savoir quel est le futur du numéro d'assurance sociale?

Mme Elise Boisjoly: Je vous remercie de votre question.

Comme vous le savez, le numéro d'assurance sociale est un identifiant parmi tant d'autres. Comme nous l'avons déjà dit, sur notre site Web, nous indiquons aux citoyens qu'ils ne devraient donner leur numéro d'assurance sociale que dans des circonstances très limitées. Cela leur est expliqué. Nous leur disons de ne pas donner leur numéro d'assurance sociale à des organismes qui ne peuvent pas légalement le demander. Par contre, selon ce que nous entendons, les citoyens le donnent souvent volontairement à des organismes qui ne sont pas habilités à le prendre.

C'est certain que nous entendons les discussions. Nous regardons toujours ce que nous pouvons faire pour améliorer la protection de nos systèmes et de nos pratiques liées au numéro d'assurance sociale.

Nous souhaitons entendre les recommandations ou voir le rapport que va publier ce comité ainsi que d'autres rapports.

Je peux vous assurer que nous travaillons régulièrement à augmenter la sécurité de nos systèmes. Je sais que le Conseil du Trésor travaille aussi très activement à des projets sur l'identité numérique. Nous participons à ces discussions pour voir comment on peut améliorer l'identité numérique des citoyens sur le territoire du Canada.

● (1655)

M. David de Burgh Graham: Parmi les données qui sont sorties, on sait qu'il y avait beaucoup d'informations, et pas seulement des numéros d'assurance sociale. Il y avait aussi des adresses, des numéros de téléphone, notamment. Vous avez parlé à plusieurs reprises d'informations supplémentaires pour authentifier le numéro d'assurance sociale. Toutes ces informations figurent-elles parmi les données qui sont sorties?

Mme Elise Boisjoly: Le numéro d'assurance sociale est un identifiant qui permet d'avoir accès à des programmes et à des services fédéraux, ainsi qu'aux systèmes de revenus et d'impôts. Dans le cas qui occupe le gouvernement fédéral, en ce qui a trait aux prestations, par exemple, mon collègue a expliqué qu'à l'Agence du revenu du Canada il faut poser une question supplémentaire, secrète, pour identifier les personnes, tel que le montant inscrit à une certaine ligne de la déclaration de revenus. Dans le cas de l'assurance-emploi, un code d'accès au programme est donné aux participants, et ceux-ci doivent donner deux chiffres de ce code afin d'avoir accès aux informations privées liées au programme de l'assurance-emploi.

Le numéro d'assurance sociale est un identifiant, mais il est accompagné d'autres questions afin de valider l'identité de la personne avec qui nous faisons affaire.

M. David de Burgh Graham: Il y a des agents de Service Canada dans toutes les villes. Si des gens se présentent à leur bureau afin de savoir ce qu'ils doivent faire relativement à la situation actuelle, quelles instructions recevront-ils?

Mme Elise Boisjoly: Je vous remercie de votre question.

Tous nos centres d'appels, les bureaux de Service Canada et nos agents ont reçu des instructions très claires. Nos centres d'appels et les bureaux de Service Canada ont répondu aux questions d'environ 1 500 citoyens. Ils ont informé ces derniers des mesures à prendre, notamment de prendre contact avec un bureau de crédit, de vérifier leurs transactions financières et bancaires et de redoubler de vigilance relativement aux transactions qu'ils font. S'ils repèrent des activités qui ne sont pas liées avec leurs transactions, ils doivent communiquer avec la police, les bureaux de Service Canada et les différentes institutions pour que nous puissions régler la situation. À ce jour, aucune fraude n'a été signalée.

M. David de Burgh Graham: La fuite est toutefois récente.

Mme Elise Boisjoly: Comme je le disais, malgré la quantité de fuites détectées depuis quelques années, il y a environ 60 cas par année exigeant un changement du numéro d'assurance sociale.

M. David de Burgh Graham: Existe-t-il une manière d'indiquer quelque part que le numéro d'assurance sociale n'est plus valide et alors retirer la responsabilité qui y est liée?

Si je fais changer le numéro d'assurance sociale et que je suis toujours responsable de l'ancien, à mon avis, cela n'a pas entièrement d'allure. Pouvez-vous nous en dire plus à ce sujet?

Mme Elise Boisjoly: Une des raisons est que nous ne savons pas à qui un citoyen a donné son numéro d'assurance sociale. Le numéro d'assurance sociale doit être utilisé seulement comme un identifiant pour relier certaines informations afin de donner des prestations. Les individus sont les seuls à savoir à qui ils ont donné leur numéro d'assurance sociale et à quelle fin. On peut donner son numéro d'assurance sociale pour des pensions privées, des assurances ainsi que des locations ou des achats de voitures, par exemple.

Le numéro d'assurance sociale ne devrait pas être utilisé pour identifier la personne. Il s'agit d'un numéro qui permet de relier certains dossiers. Nous avons besoin de ce numéro pour relier les informations. Nous relions maintenant les deux numéros d'assurance sociale dans nos systèmes, mais le premier ne devrait plus jamais être utilisé par l'individu.

● (1700)

[*Traduction*]

Le président: Merci, monsieur Graham.

Monsieur Clarke, vous avez cinq minutes.

[*Français*]

M. Alupa Clarke: Merci, monsieur le président.

Bonjour à tous.

Je vous remercie d'avoir patienté et d'être demeurés sur place.

Madame Boisjoly, vous êtes la sous-ministre adjointe au ministère de l'Emploi et du Développement social du Canada. Est-ce que votre ministre vous a donné la directive d'obtenir la liste? J'ai posé la même question à M. Cormier. Avez-vous reçu la directive ministérielle d'obtenir la liste des 2,9 millions de Canadiens touchés par la fuite de données massive chez Desjardins?

Mme Elise Boisjoly: Vous soulevez une question intéressante.

Selon la Loi sur la protection des renseignements personnels et les documents électroniques, la première chose à faire est d'informer les tierces parties. Comme vous l'avez entendu, Desjardins a communiqué avec nous pour s'assurer que nous fournirons l'information et que nous aiderons les caisses Desjardins à obtenir le plus de renseignements pertinents possible pour aider leurs membres. Dans ce cas-ci, nous avons donné beaucoup d'informations sur la façon de protéger leurs membres.

M. Alupa Clarke: Donc, il n'y a pas eu de directives. Autrement dit, vous êtes réactifs. Je ne parle pas de vous, bien entendu. Vous suivez les ordres politiques, et nous comprenons cela. En ce moment, tout est réactif et absolument rien n'est proactif.

Vous avez dit avoir reçu 1 500 demandes ou appels au sujet du numéro d'assurance sociale. Notre objectif est de savoir comment le gouvernement peut aider les gens de façon proactive. Comme vous ne savez pas quels Canadiens sont touchés, vous devez nécessairement attendre qu'ils communiquent avec vous. C'est ce qui se passe en ce moment. Vous attendez que les gens touchés prennent contact avec vous, et non l'inverse. C'est impossible, parce que vous n'avez pas les données. M. Cormier, de Desjardins, semblait dire qu'eux seraient prêts à envoyer ces données. Je sais que je vous demande d'émettre une opinion politique, mais que vous ne le pourrez pas.

Je dois exprimer quelque chose qui écœure royalement les gens de ma circonscription. J'ai fait beaucoup de porte-à-porte la semaine dernière et l'autre avant. Les gens m'ont dit systématiquement qu'ils doutaient que le gouvernement puisse faire quelque chose. Cela m'a beaucoup attristé. Comment est-ce possible? Moi, je voudrais briser le cynisme et écouter les gens. Les gens versent 50 % de leurs revenus à l'État canadien. Nous, les conservateurs, voulons que le gouvernement travaille pour les citoyens, et non l'inverse.

M. Cormier a dit que, quand une personne appelle chez Desjardins, ils sont proactifs et ils s'occupent de choses pour elle.

Nous avons appris quelque chose de très important aujourd'hui. En fait, nous le savions déjà parce que cela avait été ébruité ici et là. J'ai appris d'un officiel comme vous qu'on peut changer de numéro d'assurance sociale. Je sais que c'est complexe et que, même si on le changeait, il faudrait tout de même joindre une myriade d'institutions, ses anciens employeurs, et ainsi de suite. Or c'est le gouvernement qui oblige le citoyen à avoir un numéro d'assurance sociale. C'est un système qui devrait peut-être même être remis en cause et nous en discutons aujourd'hui, en quelque sorte.

Ne serait-il pas de votre devoir de prendre contact avec les 2,9 millions de personnes? Le gouvernement libéral devrait faire cela pour être proactif. Il connaît ces personnes. Par exemple, à la Pizzeria D'Youville où je travaillais en 2004 quand j'avais 17 ans, c'est le patron qui s'occupait d'envoyer la TPS au gouvernement fédéral. Toutes ces choses sont très connues. Vos ministères pourraient facilement relier ces informations et changer le numéro d'assurance sociale, peut-être pas de manière exhaustive, mais il devrait épauler le citoyen dans ce très lourd travail qui consiste à joindre tous ses anciens employeurs ou les agences gouvernementales.

C'est ce qui me déplaît énormément. Je sais que ce n'est pas votre faute. Vous avez des directives politiques qui viennent du gouvernement libéral, mais on n'est pas proactif en ce moment. Cela me déplaît énormément. Que pouvez-vous dire à ce sujet?

Mme Elise Boisjoly: Dans l'optique des multiples fuites qui peuvent survenir, le but est de s'assurer de toujours protéger les citoyens et les prestations qui leur sont dues, que ce soit des remboursements d'impôt ou d'autres prestations. C'est pour cela que nous avons travaillé très étroitement avec Desjardins pour définir quelles mesures nous permettraient de l'épauler dans ses relations avec les citoyens touchés.

Desjardins a mis des mesures en place. Quand il y a eu des fuites au niveau fédéral, on a pris des mesures très similaires relativement aux bureaux de crédit, parce que c'est vraiment le meilleur moyen de protéger les citoyens contre la fraude. Nous continuons à travailler avec Desjardins. Si un échange d'information s'avérait une bonne solution, nous l'envisagerions. Par contre, à ce stade-ci, les mesures mises en place sont les meilleures qu'on aurait pu prendre.

● (1705)

M. Alupa Clarke: Merci, madame Boisjoly.

[*Traduction*]

Le président: Y a-t-il des questions ici? Non.

Monsieur Dubé, vous avez trois minutes.

[*Français*]

M. Matthew Dubé: Merci, monsieur le président.

J'aimerais revenir à la question que j'ai posée, à savoir si on souhaite tenir des séances d'information dans les grands centres au Québec, entre autres. Je sais qu'il y a des gens à l'extérieur du Québec qui sont aussi touchés, mais c'est au Québec que la fuite a eu le plus gros impact. Il faut renseigner la population.

J'ai oublié ce que c'était, mais j'ai déjà reçu une lettre par la poste concernant un changement de politique fédérale. J'ose croire qu'il est possible d'envoyer des lettres par la poste à la population du Québec pour l'informer de l'horaire des consultations publiques ou des séances d'information qui auront lieu dans les deux prochains mois. Vous nous donnez de l'information aujourd'hui et je pense que les gens nous écoutent, bien entendu. Il faudrait néanmoins s'assurer de joindre le plus de gens possible. Malgré l'omniprésence des médias sociaux, je ne suis pas convaincu que cette réponse est adéquate.

Est-ce une chose à laquelle vous êtes ouverts? Je crois que le ministère des Finances et l'Agence du revenu du Canada ont aussi un rôle à jouer.

Mme Elise Boisjoly: Absolument.

De façon proactive, nous avons mis de l'information supplémentaire sur notre site Web. Nous avons diffusé des communiqués. Nous avons utilisé les médias sociaux, comme vous le disiez. Nous tenons des ateliers sur le numéro d'assurance sociale, et ce, dans plusieurs communautés. Ce sont des ateliers qui sont donnés de façon régulière et je ne verrai pas pourquoi nous ne pourrions pas utiliser ce moyen aussi.

Alors, merci de la recommandation. Nous allons la prendre en considération.

M. Matthew Dubé: Parfait. Nous vous en remercions parce qu'effectivement, il s'agit de circonstances particulières, et quand il y a des catastrophes naturelles, par exemple, le gouvernement de proximité — que ce soit les municipalités ou le gouvernement du Québec — répond toujours.

Comme mes collègues le disaient, et ce n'est pas pour insulter qui que ce soit, le fédéral est le plus loin. Dans le cas qui nous concerne, il y a des répercussions réelles sur la vie des gens.

Quoi qu'il en soit, si nous-mêmes — je parle juste de moi pour l'instant — ne savons pas nécessairement comment naviguer dans le système de numéro d'assurance sociale alors que nous sommes législateurs au fédéral, je ne pense pas que cela soit dû à notre propre ignorance. C'est simplement un système très complexe. C'est pour cela que vous êtes là aujourd'hui, et ce serait des connaissances qu'il vaudrait la peine de transmettre.

Je vous remercie de votre ouverture. Cela complète mes questions.

Le président: D'accord.

Vous avez deux minutes, monsieur Fortin.

M. Rhéal Fortin: Merci, monsieur le président.

Je vais commencer avec Mme Boisjoly.

Si l'on considère que le numéro d'assurance sociale a été créé en 1964 pour régir les relations employeurs-employés et avec l'État, on voit qu'il est utilisé à toutes les sauces maintenant, mais en tout cas, beaucoup plus largement qu'auparavant.

N'y aurait-il pas lieu de revoir les règles de sécurité concernant son utilisation? Par exemple, avoir un NIP assorti à la carte d'assurance-maladie, à des empreintes ou autres données, par exemple.

À votre avis, y a-t-il quelque chose à faire avec cela?

Mme Elise Boisjoly: C'est une excellente question.

Comme je le dis toujours, il est important, quand on a des situations comme cela, de revoir et de repenser certaines choses.

En ce qui concerne le numéro d'assurance sociale, comme je l'ai dit, c'est un identifiant parmi plusieurs. Nous, au fédéral — et bien sûr à plusieurs endroits —, les gens sont invités à ajouter des questions secrètes auxquelles eux seuls peuvent répondre. Ce n'est pas un NIP, mais ce sont des façons supplémentaires d'assurer la sécurité et d'identifier la bonne personne.

M. Rhéal Fortin: Corrigez-moi si je me trompe, mais le numéro d'assurance sociale est valide, peu importe qu'on ait ou non des questions assorties.

On me demande mon numéro d'assurance sociale pour une transaction, quelle qu'elle soit, avec une banque, ou peu importe. Je n'ai pas de NIP. J'ai juste le numéro.

Mme Elise Boisjoly: Vous avez absolument raison. Vous n'avez pas de NIP.

Est-ce quelque chose que l'on pourrait considérer? Peut-être. Ce qu'il est important de dire, c'est que, pour avoir accès à un service, vous devez donner d'autres identifiants comme la ligne...

M. Rhéal Fortin: Cela dépend des entreprises à qui l'on demande des services, mais, j'en conviens, vous avez raison.

N'y aurait-il pas lieu d'imposer une pénalité? On voit que des commerçants ou des banques demandent fréquemment les numéros d'assurance sociale, et cela n'est pas toujours nécessaire. N'y aurait-il pas lieu d'instaurer un système de pénalités pour ceux qui font une demande de numéro d'assurance sociale alors qu'ils n'en ont pas besoin?

● (1710)

Mme Elise Boisjoly: C'est une question intéressante. Je ne sais pas si des prédécesseurs se sont penchés sur cette question.

Actuellement, nous avons une liste très claire énumérant qui peut le faire. Nous avons des instructions très claires pour les citoyens. Lorsque quelqu'un leur demande un numéro d'assurance sociale et que cela ne fait pas partie de la liste des gens qui devraient le leur demander, ils ont des recours auprès du commissaire à la protection de la vie privée du Canada.

M. Rhéal Fortin: Ne pourrait-on pas inclure à la Loi des dispositions pénales pour cela, que ce soit une amende ou autre?

Mme Elise Boisjoly: Oui, ce serait quelque chose qu'il faudrait vérifier, pour lequel je n'ai pas d'information aujourd'hui.

M. Rhéal Fortin: D'accord. Parfait.

J'ai une dernière question si vous...

Le président: C'est fini, malheureusement, monsieur Fortin.

[*Traduction*]

Cela conclut notre période des questions.

Au nom du Comité, je tiens à remercier les fonctionnaires non seulement d'avoir témoigné au début, mais de l'avoir fait aussi plus tard et d'avoir attendu les autres témoins.

Nous allons suspendre la séance et poursuivre à huis clos. Nous prendrons quelques minutes pour vider la salle.

[*La séance se poursuit à huis clos.*]