CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

ETHI • NUMÉRO 019 • 2e SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le mardi 29 avril 2014

Président

M. Pat Martin

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le mardi 29 avril 2014

● (1100)

[*Traduction*]

Le président (M. Pat Martin (Winnipeg-Centre, NPD)): Bonjour, mesdames et messieurs.

Bienvenue à la 19e séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Nous poursuivons notre étude sur le problème grandissant du vol d'identité et ses répercussions économiques.

Nous sommes heureux d'accueillir aujourd'hui José Manuel Fernandez, professeur adjoint au département de génie informatique et de génie logiciel à l'École polytechnique de Montréal. Bienvenue, monsieur Fernandez.

Nous recevons également Susan Sproule, professeure associée en finances, opérations et systèmes d'information à l'Université Brock. Bienvenue, madame Sproule.

Par vidéoconférence, nous entendrons M. Benoît Dupont, directeur du Centre international de criminologie comparée, qui est à Montréal. Bienvenue.

Par vidéoconférence aussi, de Whitehorse, au Yukon — c'est faire preuve de détermination, car il doit être très tôt là-bas —, nous accueillons quelqu'un dont ce n'est pas la première comparution au comité: Philippa Lawson, avocate-procureure et associée de la Clinique d'intérêt public et de politique d'internet du Canada, à l'Université d'Ottawa. Merci beaucoup de vous joindre à nous, madame Lawson.

Nous allons entendre les déclarations préliminaires en commençant, je crois, par les témoins présents dans la salle.

Monsieur Fernandez, à vous la parole, pour 5 ou 10 minutes.

[*Français*]

M. José Manuel Fernandez (professeur adjoint, Département de génie informatique et de génie logiciel, École polytechnique de Montréal, à titre personnel): Merci, monsieur le président.

Mesdames et messieurs, bonjour.

Pour commencer, laissez-moi vous féliciter d'avoir pris la décision de traiter de l'important sujet qu'est le vol d'identité au Canada. Je vous remercie également de m'avoir invité. Cela me permet de présenter ce problème dans une perspective différente et de démontrer de quelle façon il est relié à d'autres problèmes qui touchent les Canadiens.

[*Traduction*]

Permettez-moi aussi de vous féliciter pour l'heureuse coïncidence et votre impeccable sens de l'opportunité, surtout compte tenu des événements des dernières semaines concernant la vulnérabilité Heartbleed. Quand j'ai reçu l'invitation à comparaître devant le comité, quelques jours à peine après ces événements, je me suis dit que ces parlementaires étaient très, très rapides à réagir ou peut-être qu'ils connaissant déjà quelque chose sur ce bogue que je ne connaissais pas.

Comme vous le savez, le bogue Heartbleed a touché les serveurs Web de l'Agence du revenu du Canada, ou ARC, et, malgré les efforts inlassables des professionnels des TI du gouvernement — efforts qui méritent d'être félicités —, ce bogue a mené à la divulgation non autorisée d'au moins 900 numéros d'assurance sociale de contribuables canadiens.

Cela souligne le risque réel posé par notre infrastructure de TI pour les Canadiens en matière de vol d'identité. Oui, des événements comme ceux-ci et l'intérêt médiatique qu'ils suscitent offrent d'excellentes occasions, à des experts comme moi, de transmettre le message. Cependant, il arrive que l'attention médiatique et la façon dont l'histoire se développe aient un effet contraire et distraire le public des enjeux vraiment importants.

L'intérêt de l'histoire de Heartbleed n'est pas dans le petit jeune calé en informatique qui a été arrêté par la GRC à London il y a deux semaines, et qui est soupçonné d'avoir piraté les serveurs de l'ARC. C'est l'histoire d'un bogue qui a touché deux serveurs Web sur trois sur toute la planète. Et le temps que ce jeune ait pu s'amuser avec les serveurs de l'ARC, la vulnérabilité a probablement déjà été exploitée par des dizaines de milliers, voire des centaines de milliers de pirates informatiques partout au monde. L'histoire de Heartbleed, c'est celle de l'état pitoyable de notre infrastructure de l'information et de la façon dont nous l'avons laissé se détériorer jusqu'à ce point.

Mais quel est le lien avec le vol d'identité, vous vous demandez. Oui, effectivement, les numéros d'assurance sociale dévoilés pourraient être utilisés par des criminels pour reconstruire assez de données personnelles afin d'effectuer des activités frauduleuses en se faisant passer pour les victimes — des activités telles que des transactions bancaires frauduleuses, la destruction des antécédents en matière de crédit et l'accès non autorisé à des comptes de courriel et de réseaux sociaux.

D'autres personnes invitées à témoigner devant le comité vont certainement parler des divers effets pervers du vol d'identité sur les Canadiens et les entreprises canadiennes. Mais ce que je suis venu vous dire ici aujourd'hui, peut-être à votre surprise, c'est que le vol d'identité n'est pas le problème. C'en est un parmi tant d'autres, et je dirais même que c'est probablement un des moins importants. Ce n'est que la pointe visible de l'iceberg. C'est peut-être le problème pour lequel vos électeurs appellent à vos bureaux de circonscription, mais ce n'est pas le plus gros des problèmes de TI qui les menace: c'est seulement celui qu'ils connaissent, car il les touche plus directement.

Quel est le problème alors? Ou plutôt, quels sont les plus gros problèmes qui devraient nous préoccuper aussi? C'est facile: la menace imminente que présentent le cybercrime, le cyberespionnage et le cybersabotage.

Mes collègues Benoît Dupont et Susan Sproule vont certainement pouvoir vous donner des chiffres plus complets sur le cybercrime, et le vol d'identité en particulier. Mais permettez-moi de vous donner quelques exemples, en ma qualité d'ingénieur: certains experts crédibles évaluent les coûts totaux reliés au cybercrime à plusieurs centaines de milliards de dollars par année. Au Canada, Symantec évalue les pertes à 3 milliards de dollars, en 2013 seulement. Cela représente 60 % du budget de la ville de Montréal, où j'habite et qui en trouverait l'utilité, c'est sûr.

Les cybercriminels utilisent des ordinateurs infectés dans les entreprises, les bureaux gouvernementaux et les domiciles d'usagers non avertis afin de générer un profit par divers moyens: fraude bancaire par Internet, le plus commun, mais aussi fraude publicitaire par Internet, extorsion et des formes traditionnelles de fraude et d'escroquerie.

Le cybercrime se porte très bien. C'est une industrie de croissance avec des ramifications internationales, qui met en jeu un réseau complexe de groupes criminels organisés qui travaillent ensemble. Pour vous donner une idée de l'ampleur du problème d'un point de vue technique, selon quelques sondages publiés par l'Union européenne, entre 30 et 35 % des utilisateurs sondés rapportent que leur ordinateur aurait été infecté dans une période d'un an. Nous nous sommes dit que c'est là un petit peu d'exagération européenne. Nous étions tentés d'y voir une manifestation du sens européen de l'hyperbole.

● (1105)

À notre surprise, lors d'un essai clinique réalisé en 2012 à la Polytechnique auprès de 50 sujets utilisant leur propre ordinateur durant une période de quatre mois, nous avons découvert que 5 % ont été infectés par des logiciels malveillants dangereux et 20 % par des logiciels nuisibles, malgré l'installation d'un antivirus à jour.

De plus, notre analyse a démontré que 38 % des usagers auraient été infectés par une forme de logiciel nuisible si aucun antivirus n'avait été installé. La contamination toucherait donc l'ordinateur de deux Canadiens sur cinq.

Finalement, ces Européens n'avaient pas tort. Au-delà de son seul impact économique, le cybercrime pose un autre problème, du fait qu'il génère des profits faramineux. Les cybercriminels investissent cet argent dans la recherche et le développement. Ils mettent au point des outils et des techniques de piratage qui bafouent les experts en sécurité informatique de l'industrie. Les cybercriminels ont plus d'argent que nous. Leur budget de recherche est probablement plus élevé que le mien à la Polytechnique. En fait, leurs investissements totaux en recherche et développement sont probablement plus importants que ceux de toute l'industrie de la sécurité informatique. Nous sommes donc en train de perdre la bataille. Il y a une course à l'armement. C'est un fait communément accepté, mais rarement admis en public: nous sommes effectivement en train de perdre la guerre contre les cybercriminels d'un point de vue technique.

Mais pourquoi devrions-nous nous préoccuper autant du cybercrime? Relativement peu de Canadiens sont touchés. Les pertes financières représentent un faible pourcentage et, de toute façon, on est généralement remboursé par la banque. Eh bien, les banques commencent à ne pas payer, ce qui est très bien pour moi, car ça me donne l'occasion d'aller à la cour et d'expliquer aux juges pourquoi, dans certains cas, les banques devraient payer. Mais c'est inquiétant pour les Canadiens, parce qu'on constate que la tendance commence à s'inverser. Plus cela va, plus je constate que ces cas sont fréquents.

De plus, le cybercrime ne peut se comparer aux autres fléaux de notre temps, comme le cancer, le chômage, le réchauffement de la planète, les accidents d'automobile, etc. Alors, pourquoi s'en faire? Personne n'en meurt.

Le problème est que l'avantage technologique obtenu par les cybercriminels sert maintenant à d'autres fins. Le premier phénomène dans le temps, et le plus marquant d'un point de vue politique, a été la pornographie juvénile. Les pédopornographes ont évidemment commencé à utiliser Internet et les technologies de piratage à leur avantage dans les années 1990. Cela a mené à la mise sur pied d'équipes spécialisées au sein de la police. À la Polytechnique, nous avons aidé à créer un programme de formation destiné aux policiers.

Mais ce n'est même pas le plus gros problème. Ces dernières années, il est devenu apparent que la menace la plus importante est celle du cyberespionnage et le cybersabotage. Nous commençons à peine à découvrir à quel point des services de renseignement étrangers et des intérêts économiques étrangers se promènent sur les ordinateurs et serveurs du gouvernement canadien, des entreprises canadiennes et des citoyens canadiens depuis plus d'une décennie.

Peut-être que nous n'avons pas été oblitérés de la planète Internet par des attaques de déni de service, comme ce fut le cas pour l'Estonie et la Georgie en 2007 et 2008. Notre production d'uranium de qualité militaire n'a pas été interrompue par le cybersabotage, comme ce fut le cas pour l'Iran en 2010 — heureusement, parce que le Canada ne produit pas d'uranium de qualité militaire. Et, non, nos compagnies pétrolières n'ont pas eu à remplacer 30 000 ordinateurs, à l'instar de la compagnie saoudienne Aramco en 2012, après avoir été victime d'une attaque par des pirates « patriotiques » iraniens assoiffés de vengeance.

Nous n'avons pas été victimes de ces énormes attaques de métadonnées. Cependant, il n'y a pas eu pénurie d'incidents significatifs, et on commence à parler publiquement de certains d'entre eux. Ainsi, il est possible que l'ordinateur portatif du PDG de Nortel ait été compromis par des pirates chinois dès 2001. Qui, je vous le demande, a pris la place de Nortel comme deuxième plus grand fournisseur d'équipement de réseautique au monde?

Un autre incident récent a mis en cause le code source, c'est-à-dire la « sauce secrète » qui fait fonctionner certains des composants d'une infrastructure essentielle, dont l'infrastructure énergétique... La société Telvent, de Calgary, qui assure l'approvisionnement d'une bonne part de notre infrastructure essentielle, s'est fait dérober son code source à la suite d'un piratage informatique.

● (1110)

Ce n'est pas le vol d'identité qui m'empêche de dormir la nuit; c'est ceci. Imaginez un désastre comme la crise du verglas en 1998 dans le sud du Québec et de l'Ontario; j'y étais. Trois millions de Canadiens sans électricité pendant une semaine et plusieurs centaines de milliers d'entre eux sans électricité pendant près d'un mois en plein hiver. Imaginez que ceci n'était pas causé par un rare accident de la nature, mais plutôt par quelqu'un qui l'a déclenché à partir d'un ordinateur portatif, en un seul clic, et qui pourrait le faire à nouveau. C'est bien réel. Cela pourrait se produire. C'est pire que le vol d'identité. C'est du vol d'économie. C'est du vol de sécurité nationale. Clic, plus d'économie. Clic, plus de sécurité nationale. Clic, plus de possibilité de gouverner. Songez à quel point les Canadiens perdraient confiance en leur gouvernement.

Vous direz que ceci ne fait pas partie du mandat de votre comité, mais je rétorque que c'est assurément le mandat du gouvernement. Je suis sûr que vous avez des collègues députés qui siègent à d'autres comités tels que ceux chargés de la sécurité publique et nationale, de l'industrie, des sciences et de la technologie; alors, je vous encourage à leur parler et à travailler avec eux. La raison en est fort simple. Au bout du compte, il s'agit du même problème. Les causes profondes du vol d'identité, du cyberespionnage, du cybersabotage, peu importe, sont toutes les mêmes. Il s'agit en fait de la façon dont nous gérons l'infrastructure des TI. Nous avons fermé les yeux, car nous nous plongeons dans nos gadgets électroniques.

Quelles sont les causes que nous pouvons commencer à aborder?

Premièrement, nous devons nous rendre compte qu'il y a toujours eu des escrocs et qu'il y en aura toujours. Là où il y a de l'argent, il y a toujours des escrocs. Internet ne fait pas exception. Ils se sont simplement tournés vers Internet.

Deuxièmement, nous avons adopté des technologies informatiques et Internet et nous les avons utilisées à des fins pour lesquelles elles n'avaient jamais été conçues. Un cas d'espèce est le World Wide Web qui a été inventé par des chercheurs en Suisse afin d'avoir un moyen interactif d'échanger des données de recherche, mais 30 ans plus tard, il sert à l'économie mondiale. Là n'était pas le but. Les mécanismes de sécurité et de reddition de comptes appropriés n'ont pas été intégrés dans la conception.

Les solutions technologiques existent. Elles ont été développées. Elles existent. Nous les connaissons. Nous les enseignons dans les écoles de génie, mais les incitatifs pour les mettre en oeuvre semblent absents. C'est toujours pareil. L'apathie, l'ignorance et les intérêts privés ne sont pas dans l'intérêt supérieur du public et constituent un obstacle à l'amélioration de nos vies.

Troisièmement, sur le plan historique, l'industrie des technologies de l'information est toujours relativement immature et jeune. Il y a 30 ans, les ordinateurs étaient relativement isolés les uns des autres. Quelques excentriques comme moi avaient un ordinateur personnel. C'était une industrie improvisée et déréglementée, mais ça allait. Cette situation ressemble à celle de l'industrie automobile au début du XX^{e} siècle. Il y avait peu de voitures sur les routes. Elles étaient très bruyantes, mais pas très rapides.

Il y a eu ensuite l'après-guerre, les folles années 1920; les automobiles sont devenues plus grosses et plus rapides, et c'est là que nous avons commencé à voir des accidents de voiture. Puis vint la Seconde Guerre mondiale, suivie du grand boom, des baby-boomers — en voilà l'origine —, parallèlement au boom automobile. Les autos étaient plus rapides, et on a construit de très grandes autoroutes au Canada et aux États-Unis. C'est ainsi que le problème explosa: des dizaines de milliers de décès par année. Il fallait agir, et c'est ce qui s'est passé.

Des normes d'ingénierie ont été appliquées à la fabrication et l'inspection des voitures et des pièces. Les ingénieurs devinrent les seuls à être autorisés à concevoir et à certifier des composantes essentielles. Les gouvernements partout dans le monde écrivirent et imposèrent des normes de sécurité obligatoires à l'industrie. Des codes de la route furent promulgués, et les permis de conduire et la formation pour le conducteur devinrent obligatoires. Les avocats se mirent à poursuivre en justice les conducteurs et les fabricants négligents. Même les compagnies d'assurance s'en mêlèrent et imposèrent leurs propres normes. C'est ainsi que les ceintures devinrent obligatoires et sécuritaires. Vinrent ensuite les amendements au Code criminel. La conduite avec facultés affaiblies devint un crime. On pouvait se faire incarcérer. Ce n'était pas le cas auparavant. Finalement, même la technologie et l'application de la loi s'arrimèrent pour mettre en oeuvre des technologies d'application telles que l'alcootest et les détecteurs de vitesse.

● (1115)

En comparaison, voici où nous en sommes actuellement dans l'industrie informatique. Nous nous retrouvons au début des années 1950. On a construit l'« autoroute de l'information », comme l'a nommée Al Gore, c'est-à-dire Internet, une voie qu'empruntent des millions et des millions d'utilisateurs tous les jours. Les voitures sont maintenant de grande taille — les ordinateurs —, et les gens s'en servent pour toutes sortes de choses. Elles sont toutes rutilantes, et nous voulons tous les modèles les plus récents et les plus à la mode. Notre économie et notre mode de vie en dépendent. En fait, nous sommes accros à la liberté que ces ordinateurs nous donnent de la même façon que nous sommes accros aux voitures. La différence, c'est que les « accidents d'ordinateur » ne font pas de victimes... du moins, pas encore. Mais cela viendra un jour; il suffit d'attendre.

[*Français*]

En conclusion, même si, pour s'attaquer aux causes profondes de ces problèmes, il faudra compter sur différents secteurs de la société, en l'occurrence les associations professionnelles, les éducateurs, l'industrie, la fonction publique et les agences de maintien de l'ordre, la responsabilité de nous sortir de ce marasme incombe surtout à vous, députés et membres du gouvernement, qui agissez à titre de législateurs.

Toutefois, vous n'êtes pas seuls. Nous, qui avons créé cette boîte de Pandore et vu d'autres l'ouvrir malgré nos avertissements, aimerions plus que tout vous aider à la refermer.

Je vous remercie de votre attention.

● (1120)

[*Traduction*]

Le président: Merci beaucoup, monsieur Fernandez pour cette déclaration préliminaire qui porte à réfléchir.

Nous allons maintenant passer à Mme Susan Sproule de l'Université Brock.

Madame Sproule, vous avez la parole.

Dre Susan Sproule (professeure adjointe, Finances, opération et systèmes d'information, Brock University, à titre personnel): Bonjour.

J'ai commencé à travailler dans le domaine du vol d'identité en 2005 dans le cadre d'un projet de recherche regroupant quatre universités et des experts en la matière du monde financier. Mon groupe avait la responsabilité de définir et de mesurer le vol d'identité. Pour ce qui est de la mesure, nous avons fait une étude exhaustive auprès de consommateurs canadiens en 2008, mais ces données sont trop vieilles pour avoir quelque valeur que ce soit aujourd'hui. Je vais donc plutôt mettre l'accent sur le problème de la définition et discuter par la suite de certaines des difficultés entourant la mesure des vols d'identité. J'espère que cela sera utile pour votre étude.

Avant d'en arriver à des définitions, nous avons commencé par essayer d'organiser certaines des activités qui revenaient souvent lorsqu'on discutait de vol d'identité. J'ai préparé un diagramme. Je ne sais pas si on vous l'a distribué, mais, essentiellement, au début nous avions recensé un certain nombre d'activités, qui décrivent différentes façons de recueillir de l'information sur l'identité. Au milieu, figuraient un certain nombre d'activités liées à l'établissement d'une fausse identité, des choses comme la contrefaçon de documents et la reproduction de documents. Ensuite, vers le bas, figuraient les crimes pouvant être perpétrés grâce à une fausse identité.

Nous cherchions tout simplement des définitions de travail sur lesquelles pouvaient s'entendre les divers groupes de recherche. Dans une série d'ateliers, nous avons décidé que le vol d'identité devrait englober toutes les façons illégales de recueillir de l'information ainsi que toutes les activités liées à l'élaboration d'une fausse identité. Il existe des activités préliminaires à une fraude.

Nous avons donc établi que la fraude liée au vol d'identité devait comprendre tous les crimes où l'utilisation d'une fausse identité faisait partie intégrante du crime. En d'autres mots, quelqu'un peut avoir recours à une fausse identité pour la contrebande de drogues, parce que cela serait utile si jamais cette personne était pincée, mais on peut tout de même s'adonner à cette activité sans avoir recours à une fausse identité; c'est pourquoi nous avons conclu qu'il ne s'agissait pas de fraude d'identité.

Je ne vous présenterai pas toutes les définitions officielles, mais nous avons été agréablement surpris de constater que nos définitions étaient finalement très semblables à celles établies par le ministère de la Justice du gouvernement fédéral en vue de la mesure législative portant sur le vol d'identité qui a été présentée en 2009.

Un des éléments clés découle du fait que le vol d'identité et la fraude d'identité sont deux problèmes distincts. Le vol d'identité est un problème de responsabilité personnelle ou organisationnelle, c'est-à-dire qu'il faut veiller à la sécurité des renseignements personnels que l'on détient. Par contre, la fraude d'identité est un problème d'authentification, c'est-à-dire qu'il faut être en mesure de déterminer que la personne qui présente une pièce d'identité est vraiment celle qu'elle prétend être.

Pourquoi cette distinction est-elle si importante? Et bien, parce que l'un peut avoir lieu sans l'autre, et vice versa. Le voleur d'identité et le fraudeur de pièce d'identité sont habituellement deux personnes différentes. En général, le voleur d'identité usurpe des renseignements d'identité et les vend au fraudeur. Nous avons remarqué que les cas de vol d'identité — entre autres, les cas d'atteinte à la sécurité des données — sont rarement liés aux cas de fraude d'identité, parce que l'information doit passer par une zone intermédiaire.

Essentiellement, cela nous aide à mettre l'accent sur les intérêts et les responsabilités des intervenants. Ainsi, en tant que propriétaire de l'identité, je peux contribuer à lutter contre certaines formes de vol d'identité. Je peux garder en lieu sûr les documents personnels qui contiennent des renseignements d'identité et ne pas divulguer inutilement de l'information personnelle. En fait, il m'est impossible d'empêcher la fraude de l'identité. Une fois que mon information est compromise, la seule chose que je peux faire, c'est d'en prendre connaissance et de le signaler dès que possible.

Mais, en tant que participante active à la vie d'aujourd'hui, je n'ai pas vraiment le choix de donner mon information personnelle à toutes sortes d'organisations. Ces organisations ont un rôle à jouer pour prévenir tant le vol d'identité que la fraude d'identité. Elles peuvent prévenir le vol d'identité en assurant la sécurité de tout renseignement personnel qu'elles possèdent. Elles peuvent empêcher la fraude d'identité en s'assurant qu'elles possèdent des processus d'authentification adéquats lorsqu'elles délivrent des pièces d'identité ou lorsqu'elles en font la vérification.

Il incombe aussi aux organisations de détecter le vol d'identité, lorsque l'information a été compromise, ainsi que la fraude d'identité lorsque les processus ont connu des ratés et qu'une fraude a eu lieu.

● (1125)

Au sein même des organisations, si on essaie de faire une entrevue auprès d'une organisation relativement au vol et à la fraude d'identité, les responsabilités pour ces deux problèmes sont réparties dans deux secteurs de l'organisation. Qui est chargé du problème lié à la sauvegarde des renseignements? Il s'agit habituellement des services de sécurité lorsqu'il s'agit de la sécurité physique et des services de TI lorsqu'il s'agit de la sécurité des systèmes. Qui est chargé du problème d'authentification? Quiconque contribue à la conception, la gestion, voire la conduite de tous les processus opérationnels entourant les différentes transactions.

Il y a de nombreux défis liés à la mesure du vol et de la fraude d'identité. Et tout cela revient au problème de la définition. Un sondage réalisé par Ipsos Reid en 2006 révèle que 29 % des Canadiens sont d'accord relativement à la déclaration suivante: « J'entends beaucoup parler de vol d'identité, mais je ne sais pas ce que cela signifie. » Donc, si on veut réaliser un sondage pour déterminer dans quelle mesure la fraude d'identité a eu lieu, on ne peut pas tout simplement demander aux répondants s'ils en ont déjà été victimes. C'est ce qui est fait dans bon nombre de sondages, mais on ne peut pas véritablement interpréter quoi que ce soit à partir de ces résultats. Dans notre sondage, nous avons donné des exemples bien précis des divers types de fraude d'identité qui nous intéressaient.

En plus d'effectuer des sondages, on peut examiner les rapports qui y ont été produits par des organisations comme le Centre antifraude du Canada, mais le deuxième problème qu'il faut alors affronter, c'est le manque général de rapports. Les fraudes par carte de débit et de crédit font l'objet d'enquêtes internes de la part des compagnies émettrices de cartes et des banques. Seule une petite partie de ces dossiers sont renvoyés à la police. Un sondage de Statistique Canada sur la fraude dans les entreprises de détail démontre qu'entre 40 et 50 % des dossiers n'ont jamais été signalés à la police. Moins de 40 % des victimes individuelles font rapport à la police.

Pourquoi en est-il ainsi? En général, les entreprises craignent la publicité négative. Les gens sont embarrassés de dire qu'ils ont été victimes d'escroquerie ou qu'ils n'ont pas protégé leur information. Je pense que, dans les deux cas, ils estiment que la police ne peut rien faire et, la plupart du temps, ils ont raison.

Pour ce qui est des coûts — et je suppose que cette question fait également partie de votre mandat —, le vol d'identité coûte très cher, et ce sont les particuliers, les organisations et les sociétés qui en assument les frais. Les victimes individuelles ne sont pas tenues responsables des pertes financières lorsqu'il est établi qu'une fraude a eu lieu, mais, pour en arriver là, les particuliers ont bien souvent dépensé beaucoup d'argent et de temps, ce qui engendre de la frustration et de l'anxiété.

Ce sont les organisations qui assument la plupart des pertes financières liées au vol et à la fraude d'identité. Cela se traduit par deux problèmes. D'abord, les organisations sont très réticentes à divulguer ces coûts. Deuxièmement, les coûts en tant que tels ne constituent pas des incitatifs assez puissants pour empêcher le vol et la fraude d'identité.

Lorsqu'une organisation subit des pertes liées à la fraude d'identité, ces pertes sont tout simplement transmises aux consommateurs sous forme de prix, d'honoraires ou de tarifs plus élevés. De surcroît, au Canada, le manque d'exigences quant à l'obligation de faire rapport lorsqu'il y a atteinte à la sécurité des renseignements signifie que les organisations canadiennes ne sont pas forcément touchées par une atteinte à leur réputation. À ma connaissance, le projet de loi sur la protection des renseignements personnels numériques prendra des mesures dans cette direction, et je pense que c'est une bonne chose.

Il y a aussi les coûts généraux pour la société, qui ont des effets paralysants. En effet, différentes études, y compris la nôtre, démontrent qu'entre 20 et 40 % des consommateurs disent avoir rajusté leurs comportements en ligne par crainte de vol d'identité. Cela signifie que les entreprises canadiennes ne profitent pas de tous les avantages qu'elles devraient percevoir grâce au commerce électronique.

J'aimerais que votre étude porte sur deux éléments.

D'abord, j'aimerais que les agences d'évaluation du crédit soient plus ouvertes aux interventions des consommateurs. Comme je l'ai dit, la seule chose que peuvent faire les particuliers, c'est de contribuer à déceler les fraudes, mais si nous voulons que les consommateurs agissent ainsi, ils doivent avoir un plus grand accès et un meilleur contrôle sur leurs dossiers de crédit. Les agences d'évaluation du crédit doivent vous transmettre gratuitement, chaque année, une copie de votre dossier de crédit, mais elles rendent cette tâche très difficile. Pour obtenir un exemplaire gratuit, vous devez remplir un formulaire, copier une multitude de documents, envoyer le tout par la poste et attendre quelques semaines pour qu'on vous poste votre rapport. Les agences offrent aussi un service en ligne. Les services en ligne sont plus sécuritaires, et ils sont censés être moins coûteux pour les agences, mais elles facturent 24 $.

● (1130)

De plus, les deux agences d'évaluation du crédit offrent des produits de protection contre le vol d'identité qui coûtent de 15 à 17 $ par mois. En offrant ces produits, ils profitent du problème, ce qui ne les motive que très peu à vouloir en réduire ou en éliminer les menaces.

Enfin, il est très difficile de gérer quelque chose si on ne cherche pas à le mesurer. Nous avons besoin de collectes de données régulières et périodiques pour cerner les tendances et pour mettre au point des initiatives de sensibilisation efficaces et des politiques efficaces. Étant donné qu'il n'y a aucune mesure pour le vol d'identité et la fraude, nous estimons avoir véritablement besoin d'un indice du vol d'identité de la fraude qui fonctionnerait comme un indice des prix à la consommation ou un indice sur les activités d'achat. Cet indice serait calculé à partir de renseignements recueillis au moyen de sondages réguliers auprès des consommateurs, de sondages d'entreprises ainsi que de rapports des forces de l'ordre, des agences d'évaluation du crédit, des commissaires à la protection de la vie privée, des services aux victimes et de n'importe quel autre groupe.

Merci de m'avoir écoutée; j'espère vous avoir été utile.

Le président: Merci beaucoup, madame Sproule.

Je suis certain que les membres du comité auront des questions à vous poser, en temps et lieu. Merci.

Ensuite, nous allons passer à Benoît Dupont, directeur du Centre international de criminologie comparée, qui comparaît par vidéoconférence.

Monsieur Dupont, allez-y.

M. Benoît Dupont (directeur, Centre international de criminologie comparée): Bonjour et merci, monsieur le président, mesdames et messieurs les membres du comité, de m'avoir invité à participer à vos délibérations.

Comme vous l'avez indiqué, je suis directeur du Centre international de criminologie comparée et je suis également titulaire de la Chaire de recherche du Canada sur la sécurité, l'identité et la technologie de l'Université de Montréal, où j'étudie la question du vol d'identité depuis environ sept ans.

Pendant les 10 minutes qui me sont accordées, j'aimerais aborder brièvement certains des enjeux rattachés à cette forme très complexe d'infractions et vous parler des préjudices que cela cause aux Canadiens. Mais avant d'aller plus loin, j'aimerais peut-être préciser que l'expression « vol d'identité » est peut-être quelque peu trompeuse, car elle sous-entend que la victime perd accès à son identité comme si elle perdait accès à une auto ou à son cellulaire, en cas de vol, alors que dans les faits, la victime est surtout privée de certains des avantages qu'on associe au plein contrôle de ses renseignements personnels, notamment une cote de crédit élevée ou la possibilité d'obtenir un prêt bancaire. Je crois qu'il serait plus utile d'utiliser l'expression « manipulation d'identité » ou « crime lié à l'identité », mais j'imagine qu'il est beaucoup trop tard maintenant pour changer cette terminologie. Toutefois, cela me semble être une question importante également.

J'estime que vous jouez un rôle très important ici et, en lisant la transcription des séances passées, je me suis rendu compte qu'on pouvait en apprendre énormément sur le processus et le rapport que vous produirez. Ainsi, dans mes commentaires d'aujourd'hui, je vais adopter un angle quelque peu différent puisque j'aimerais aborder brièvement quatre éléments que nous ignorons lorsque nous parlons de vol d'identité et je crois qu'en comblant ces lacunes, nous pourrons élaborer des stratégies de prévention efficaces ainsi que des outils de réglementation plus efficaces. Si vous voulez, il s'agit de ces incertitudes incontestables, pour reprendre l'expression d'un politicien américain très connu.

La première incertitude dont a parlé ma collègue Susan Sproule concerne l'ampleur actuelle du problème, à savoir le nombre réel de victimes et l'évolution de cette tendance. J'ai lu la transcription du témoignage de la GRC, et le représentant de la GRC a indiqué qu'en 2013, 24 000 victimes avaient communiqué avec l'organisation pour signaler des cas de vol d'identité. Il s'agit probablement d'une infime fraction d'un bassin général de victimes, car la plupart d'entre elles, comme l'a indiqué ma collègue, Mme Sproule, ne portent pas plainte formellement auprès des services de police. Certaines d'entre elles n'estiment pas le crime suffisamment important ou suffisamment intéressant, tandis que d'autres sont découragés par leur service de police local, lequel n'est pas équipé pour faire face à ce type de crime, notamment si les montants concernés sont inférieurs à un certain seuil.

Pour vous donner une idée d'une évaluation plus réaliste, en 2009, Statistique Canada a réalisé une enquête sur la victimisation auprès d'un très large éventail de la population canadienne et a évalué que plus de 870 000 Canadiens avaient été victimes de fraudes bancaires sur Internet au cours des 12 derniers mois, ce qui n'inclut pas d'autres formes de fraude associée au vol d'identité. Ces chiffres sont énormes, mais en matière de technologie, cinq ans constituent une très longue période et nous ne disposons pas de statistiques annuelles fiables pour évaluer la gravité du problème de vol d'identité et l'efficacité des stratégies actuelles pour le résoudre.

La deuxième chose que nous ne connaissons pas très bien, c'est que nous n'avons aucune ventilation claire des types de vol d'identité, en fonction des sources de justificatifs d'identité dérobés ou de stratagèmes de fraude dont se servent les auteurs de ces infractions pour les exploiter. J'ai réalisé une étude très semblable à celle qu'a menée Susan Sproule en 2007, au Québec, et cette étude a montré que les arnaques en ligne comme les courriels d'hameçonnage ne représentent que 6 % des renseignements personnels dérobés, tandis que le clonage de cartes ou le vol de renseignements personnels par des initiés organisationnels représentent 55 % des cas. Depuis lors, je n'ai pas vu de mises à jour concernant la situation au Canada, même si, là encore, la technologie a beaucoup changé au cours des sept dernières années et même si probablement une plus grande part des Canadiens effectuent leurs affaires et leurs transactions en ligne.

Troisièmement, nous ne connaissons pas grand-chose sur les voleurs d'identité et nous ne savons pas s'il s'agit d'une catégorie de contrevenants traditionnels qui ont migré vers ce nouveau marché lucratif ou s'il s'agit d'une toute nouvelle espèce de contrevenants dotés de compétences criminelles très différentes et de modes d'organisation sociale très différents.

● (1135)

Nous savons qu'un petit nombre d'entre eux connaissent un véritable succès et peuvent obtenir, par l'entremise de cyberattaques complexes, des millions de dossiers volés qu'ils revendent sur des marchés clandestins, comme cela a été le cas avec Winners ou, plus récemment, avec le piratage chez Target où des dizaines de millions, et dans certains cas des centaines de millions, de numéros de carte crédit ont été volés auprès de grands détaillants. Nous ne savons toujours pas grand-chose sur ces marchés, sur leur fonctionnement ou sur la part des renseignements volés qui appartiennent à des consommateurs canadiens.

Nous ne savons pas vraiment quelles organisations sont les plus efficaces, lesquelles sont les plus exposées et lesquelles font un bon travail pour prévenir le vol d'identité. Nous savons que les banques investissent une bonne part de leur argent dans les technologies antifraude. Elles sont très avancées et elles sont capables de détecter et de bloquer les tentatives de vol d'identité. Toutefois, nous ne savons pas laquelle de ces cinq ou six grandes banques est la meilleure ou laquelle est la pire ni quels sont les types d'entreprises de détail ou de service qui sont à l'origine de la plus grande fuite de renseignements personnels vers les contrevenants. Toutes les organisations ne sont pas sur un pied d'égalité face au problème du vol d'identité.

Vous allez peut-être me demander pourquoi il serait utile de le savoir. Eh bien, premièrement, cela nous aiderait à concevoir et à mettre en oeuvre des stratégies de prévention plus efficaces qui permettraient de cibler et de renforcer les maillons les plus faibles de l'écosystème des paiements.

Deuxièmement, nous en saurions également davantage sur la nécessité de créer de nouveaux outils réglementaires dans le domaine pour forcer les sociétés à protéger les renseignements personnels de leurs clients et de les aviser, le cas échéant, non seulement du point de vue des renseignements personnels, mais également du point de vue de la sécurité. Cela nous aiderait également à faire en sorte que ces outils réglementaires soient raisonnables et n'imposent pas un fardeau trop lourd aux entreprises.

Enfin, je crois que cela aiderait notre organisation et, tout spécialement, les organismes d'application de la loi à consacrer leurs ressources limitées aux réseaux les plus dangereux et les plus prolifiques de contrevenants.

Toutefois, je ne veux pas terminer sur une note pessimiste. Nous avons des raisons d'être optimistes. Nous ne devrions pas nous désespérer devant le problème du vol d'identité. Par exemple, l'intégration de la technologie de la puce et du NIP, au Canada, sur nos cartes de crédit et de débit au cours des dernières années, ainsi que les progrès des technologies antifraude déployées par le secteur bancaire ont permis de réduire grandement le nombre de vols et de fraudes d'identité s'y rattachant, ce qui montre que parfois les changements organisationnels peuvent produire des résultats systémiques à l'échelle nationale.

Par exemple, si vous regardez les statistiques d'Interac... J'ai obtenu ces statistiques sur Internet et je les ai compilées d'une manière un petit peu différente de celle d'Interac. Entre 2004 et 2012, les montants totaux de pertes attribuées à la fraude par Interac — si nous partons du principe que ces données sont justes — ont diminué de 36 %. Pendant la même période, le nombre de transactions réalisées par carte de débit a augmenté de 53 %. Ainsi, la fraude est en baisse et le nombre de transactions est à la hausse.

Pour ce qui est des cartes de crédit, nous observons une tendance semblable: les pertes totales entre 1999 et 2012 ont augmenté de 94 %, ce qui est énorme. Mais cela ne représente qu'environ la moitié des 212 % d'augmentation du montant total de transactions par carte de crédit au cours de la même période.

Ainsi, la perte monétaire moyenne par transaction Interac s'élève à environ 2 ¢, et la perte monétaire ou financière moyenne des transactions par carte de crédit s'élève à environ un sixième de 1 ¢. Ce rapport n'a pas vraiment changé au cours des 10 dernières années, ce qui est assez rassurant, car le problème du vol d'identité n'est pas aussi grave que certaines sociétés privées le laissent entendre.

Le problème que nous avons avec la puce et le NIP tient au fait, bien entendu, que nos voisins du Sud ont été plus lents à adopter cette technologie. Cela donne plein d'occasions aux contrevenants d'exploiter les données recueillies sur le dos des cartes de crédit et de débit et sur les bandes magnétiques.

● (1140)

Merci de m'avoir écouté. Cela met fin à mes remarques. Bien entendu, je me ferai un plaisir de répondre à vos questions. Merci.

Le président: Merci beaucoup, monsieur Dupont. Cela nous est très utile.

Enfin, maintenant — et merci pour votre patience — nous recevons Philippa Lawson, de la Clinique d'intérêt public et de politique d'internet du Canada, à l'Université d'Ottawa. Merci beaucoup d'être des nôtres aujourd'hui, madame Lawson. C'est à votre tour.

Mme Philippa Lawson (avocate-procureure, associée, Clinique d'intérêt public et de politique d'internet du Canada, Université d'Ottawa, à titre personnel): Merci et bonjour à tous.

Merci de m'avoir invitée à vous parler du vol d'identité aujourd'hui. Depuis près de 10 ans, j'étudie cette question et je travaille dans ce domaine dans l'intérêt des consommateurs et des victimes. Je l'ai fait d'abord pour le Centre pour la défense de l'intérêt public, puis pour la Clinique d'intérêt public et de politique d'Internet du Canada, ou CIPPIC pour le Centre international pour la réforme du droit criminel et la politique en matière de justice pénale et plus récemment, pour le Centre de soutien aux victimes de vol d'identité du Canada.

Je vous ai remis mes notes d'exposé, assorties d'une liste de publications, et j'espère qu'on vous les distribuera. Dans la liste des documents, on trouve des analyses de la gamme et des types d'actes criminels associés à l'identité, un inventaire international des pratiques exemplaires pour aider les victimes dans le secteur public et le secteur privé, une analyse des différences entre les droits et les recours des victimes de crimes liés à l'identité au Canada et aux États-Unis et des guides destinés à aider les victimes canadiennes de vol d'identité à se débrouiller elles-mêmes. Tout cela est accessible en ligne.

Comme directrice du CIPPIC, j'ai présenté des témoignages à votre comité lorsqu'il s'est penché sur le vol d'identité en mai 2007. Mes exposés de l'époque sont encore pertinents aujourd'hui. Au cours des dernières années, des changements se sont produits, notamment une modification du Code criminel qui permet aux forces de l'ordre d'arrêter et de faire condamner des voleurs d'identité. C'est une étape importante, mais seulement l'un des nombreux outils nécessaires pour lutter contre ce problème. Il y a eu aussi la création du Centre de soutien aux victimes de vol d'identité du Canada qu'on peut trouver sur Internet à www.idtheftsupportcentre.org/fr/ ou qu'on peut joindre en composant sans frais le 1-866.802.3609. Mais on peut en faire bien davantage encore, et on devrait le faire, pour prévenir, dépister les vols d'identité, mener des poursuites et atténuer les effets des actes criminels contre l'identité.

Je crois savoir que vous vous intéressez aux répercussions économiques du vol d'identité au Canada et que vous vous concentrez sur les crimes liés à l'identité ou aux renseignements personnels et non pas aux fraudes commerciales ou à la cybercriminalité en général. Je ne peux pas vous fournir de chiffres. Pour les raisons données par mes collègues, je doute qu'il soit possible d'avoir une évaluation assez juste, compte tenu du manque de données sur les actes criminels liés à l'identité au Canada. Je vais plutôt utiliser le temps qui m'est imparti pour formuler cinq suggestions de réforme aux politiques et aux lois dans ce domaine.

Premièrement, il faut adopter une loi sur les avis à donner en cas d'atteinte à la sécurité des données. On peut prendre toutes les précautions recommandées pour se prémunir contre le vol d'identité, mais on n'a aucun contrôle sur ce que des organisations font des données personnelles dont elles ont la garde. En cette époque des bases de données, il faut des mesures solides de sécurité organisationnelle pour lutter contre le vol d'identité. Pourtant, pour faire des économies, nombre d'organisations ne prennent pas les mesures qu'elles devraient prendre pour protéger les données de leur clientèle.

Une loi pourrait exiger des organisations qu'elles fassent part à la commissaire à la vie privée de toute violation de la cybersécurité, et en aviser aussi les personnes touchées. Cette loi ferait beaucoup pour prévenir le genre d'atteinte à la sécurité qui assure la prospérité des voleurs d'identité. En outre, les victimes potentielles seraient conscientes de leur vulnérabilité, ce qui leur permettrait de prendre des mesures préventives avant que des torts graves soient subis. Je félicite à ce sujet les efforts de Mme Borg, membre du comité, et j'encourage le gouvernement à faire bon accueil à son projet de loi d'initiative parlementaire sur cette question.

Le projet de loi S-4, qui porte sur la nouvelle loi sur la protection des renseignements personnels numériques, est un projet de loi d'initiative gouvernementale qui exigerait aussi des avis en cas d'atteinte à la sécurité, mais le mode de déclaration proposé fixe des critères trop restrictifs pour les déclarations à la commissaire à la vie privée et aux particuliers, ce qui permettrait aux entreprises d'éviter de s'acquitter de leur responsabilité lorsque leurs mesures de sécurité sont insuffisantes. Je sais que c'est un projet de loi que vous étudierez et j'espère que vous le ferez très soigneusement.

● (1145)

Deuxièmement, il faut que les lois sur la protection des données soient applicables. À notre époque, les bases de données personnelles sont énormes et en croissance. Ce sont des mines d'or pour les voleurs d'identité, comme pour les experts en marketing, les chercheurs et même les partis politiques. La Loi sur la protection des renseignements personnels et des documents électroniques, ou LPRPDE, est censée protéger les consommateurs contre des pratiques ouvrant la porte au vol d'identité et à la fraude, mais les pratiques qui enfreignent la LPRPDE sont encore répandues commercialement. Le problème, c'est que cette loi manque de mordant. Les entreprises ne la prennent pas au sérieux.

Le projet de loi S-4 sur la protection des renseignements personnels numériques permettrait à la commissaire à la vie privée de dénoncer les entreprises délinquantes. Le commissariat pourrait aussi prendre des mesures contre celles qui ne respectent pas les accords de conformité. Il s'agit d'améliorations considérables qui rendraient le projet de loi plus efficace, de manière qu'on puisse tenir responsables de leurs actes les organisations non conformes qui se prêtent à des pratiques facilitant le vol d'identité. Toutefois, il faut en faire plus pour que nos lois sur la protection des données numériques soient efficaces. J'espère que vous envisagerez toutes les suggestions lorsque le projet de loi S-4 vous sera confié.

Troisièmement, il faut pouvoir offrir un gel du crédit aux consommateurs canadiens. Le vol d'identité le plus dommageable donne lieu à l'ouverture de nouveaux comptes bancaires. En effet, des criminels se servent de données volées pour créer de nouveaux comptes ou demander du crédit, comme des prêts hypothécaires, au nom de la victime. Des mois peuvent passer avant que la victime se rende compte du problème. Pendant ce temps, de nombreux comptes ont été ouverts et les factures se sont accumulées en son nom. Même après que la victime a réussi à fermer les comptes et à rembourser les dettes, ce qui est déjà cauchemardesque, elle risque d'avoir à payer des taux d'intérêt supérieurs pendant des années, à cause d'un dossier de crédit entaché.

Cela ne se produit pas souvent, mais lorsque c'est le cas, c'est extrêmement coûteux pour la victime. La meilleure protection contre l'ouverture frauduleuse de compte, c'est le gel du crédit. Le gel du crédit empêche les agences d'évaluation du crédit de divulguer votre dossier de crédit, soit le résumé des emprunts et des paiements qui forment la base de votre dossier. Sans ce dossier, peu d'entreprises de crédit vont accorder un prêt. Par conséquent, si le rapport sur le crédit n'est pas divulgué, les voleurs d'identité ne peuvent pas se servir des données pour ouvrir de nouveaux comptes. Le gel du crédit est particulièrement utile pour les personnes âgées ou ceux qui n'ont pas besoin d'emprunter.

Pour des raisons évidentes, il n'est pas dans l'intérêt du secteur des agences d'évaluation du crédit d'offrir de bloquer des dossiers. C'est le principal service qu'elles offrent. Malgré une forte résistance de la part du secteur aux États-Unis, presque tous les États américains exigent maintenant que ce gel soit offert aux consommateurs, sans frais, ou à très faible coût. Et c'est pour prévenir le vol d'identité. On ne voit pas pourquoi les Canadiens ne pourraient bénéficier d'une protection semblable. C'est un domaine de responsabilité provinciale, mais à mon avis, le gouvernement fédéral devrait collaborer avec les provinces, par exemple, dans le cadre du Comité des mesures en matière de consommation pour veiller à ce que les consommateurs canadiens disposent des outils nécessaires pour prévenir, déceler et atténuer les effets des vols d'identité, notamment par la capacité de demander le blocage de leurs dossiers de crédit.

Quatrièmement, il faut coordonner les initiatives d'aide aux victimes. Le Centre de soutien aux victimes de vol d'identité du Canada, que j'appellerai maintenant le centre de soutien aux victimes, a été créé au début de 2012, grâce à des fonds fédéraux, pour renseigner et soutenir les victimes de vol d'identité. Son mandat est bien précis et limité. Le centre de soutien aux victimes reçoit actuellement environ 10 appels par jour provenant de victimes ou d'autres personnes se renseignant sur le vol d'identité. Il reçoit plus d'appels là où on fait connaître l'existence du centre. Il accompagne les victimes pas à pas, tout le long du processus complexe de recouvrement de leur identité.

● (1150)

Je crois comprendre que le centre de soutien aux victimes fournit des données au Centre antifraude canadien, mais étrangement, le Centre antifraude ne reconnaît même pas l'existence du centre de soutien aux victimes. Il est clair qu'il faut une meilleure coordination et collaboration entre ces organismes financés par les fonds publics, afin que chacun se concentre sur son mandat, plutôt que d'agir comme un rival de l'autre, pour obtenir l'attention du public et des fonds.

Cinquièmement, je propose que le Canada adopte une stratégie nationale de lutte contre la criminalité associée à l'identité. Les quatre mesures précédentes ne sont qu'un début, ce problème ayant de nombreux aspects. Le Canada doit avoir une stratégie nationale pour mieux comprendre la criminalité associée à l'identité, pour mieux lutter contre elle. Cette stratégie doit être confiée à de hauts fonctionnaires et nécessiter la participation de tous les intervenants clés. La stratégie nationale de la GRC, lancée en 2012, est un bon point de départ, mais il faut bien davantage de travail pour aller au-delà des généralités et tenir compte de la protection des consommateurs.

Le premier pilier d'une stratégie nationale devrait être la création de mécanismes de collecte de données fiables et assez complètes sur l'incidence, le type et le coût des actes criminels liés à l'identité au Canada. Là-dessus, j'abonde dans le sens de mes collègues, Mme Sproule et M. Dupont: c'est une première étape essentielle pour lutter contre ce problème. Il faut savoir quelle est la nature du problème si l'on veut le résoudre de manière efficace. Or, au Canada, nous n'avons tout simplement pas ces données encore.

Enfin, nous pouvons parfois tirer des leçons de ce qui se passe chez nos voisins du Sud, et je crois que c'est le cas ici. En 2006, le président américain a mis sur pied un groupe de travail spécial sur une stratégie nationale globale de lutte contre le vol d'identité. Le groupe de travail était coprésidé par le procureur général et le président de la commission fédérale du commerce. Y siégeaient les hauts responsables de tous les organismes gouvernementaux pertinents. En un an, le groupe de travail a examiné le problème sous tous ses angles et a publié un plan stratégique global de lutte contre le vol d'identité aux États-Unis. Ce plan a été, en grande partie, mis en oeuvre. Il comprenait une coordination nationale des réformes en matière de politiques et de lois. La commission fédérale du commerce en est responsable. Les consommateurs et les victimes aux États-Unis disposent maintenant de plus d'outils que les Canadiens pour prévenir le vol d'identité et pour réagir lorsqu'il se produit.

Monsieur le président, mesdames et messieurs les membres du comité, à mon avis, il est grand temps que le Canada s'occupe de cette question et mette au point une stratégie semblable grâce à la participation de tous les intervenants, y compris les organismes de protection des consommateurs et les commissaires à la protection des renseignements personnels des divers ordres de gouvernement.

Nous pouvons faire mieux.

Merci.

● (1155)

Le président: Merci beaucoup, madame Lawson.

Merci à tous nos témoins pour ces quatre excellents exposés. Il serait bon que nous disposions de plus de temps avec vous, j'en suis persuadé. Nous avons la chance de recevoir aujourd'hui de grands experts dans ce domaine.

Toute une heure a déjà été consacrée aux exposés, ce qui nous laisse toute une heure pour les questions. Sans plus tarder, nous donnons la parole à l'opposition officielle, en commençant par Charmaine Borg.

Madame Borg, vous avez sept minutes.

[*Français*]

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

J'aimerais remercier tous les témoins de participer à notre séance d'aujourd'hui. J'aimerais également les remercier de leurs excellents témoignages qui ont apporté de bons points à notre discussion.

Je vais poser une première question. Comme j'en ai plusieurs, il m'est difficile de choisir laquelle je devrais poser d'abord.

Vous avez tous mentionné qu'au Canada il y avait un manque de données concernant les problèmes que constituent le vol d'identité, les pertes de données et les atteintes aux données. Par exemple, l'absence au Canada d'un système d'avertissement obligatoire en cas de pertes de données ou d'atteinte aux données a contribué à ce problème, puisque la commissaire à la protection de la vie privée n'était pas mise au courant de ces situations.

Pourriez-vous commenter là-dessus?

J'aurais aussi une question plus particulière pour vous, monsieur Fernandez. Étant donné que vous travaillez davantage dans le domaine du développement des technologies, c'est peut-être plus concret pour vous. Cela a-t-il nui à votre capacité de concevoir des systèmes de sécurité qui pourraient s'attaquer à certains problèmes reliés au vol d'identité?

M. José Manuel Fernandez: En effet, le manque de données est un problème non seulement en ce qui a trait à la compréhension du problème par le gouvernement, mais aussi sur le plan de la recherche-développement de solutions de sécurité.

Comme M. Dupont l'a dit, les organisations ne sont pas toutes pareilles. Certaines ont déployé des procédures technologiques ou de gestion, et certaines sont plus efficaces que d'autres. Pour savoir lesquelles sont les meilleures et devraient devenir les bonnes pratiques, nous avons besoin de données qui confirment que les moyens déployés sont appropriés.

Les données constituent un besoin pour la recherche-développement, mais c'est aussi une nécessité pour un autre outil de gestion du risque: les assurances.

[*Traduction*]

L'industrie de l'assurance essaie de voir comment elle pourrait assurer les risques liés à la technologie informatique et au vol d'identité pour les Canadiens. Mais nous sommes quelque peu aux prises avec le problème de la poule et de l'oeuf: étant donné que le secteur n'a pas assez de données pour pouvoir évaluer le risque, il ne peut pas établir le montant de la cotisation à cette assurance et, par conséquent, il n'offre pas ce service.

Il y a deux façons de corriger le problème. La première consisterait à adopter des lois qui obligeraient les organismes dont l'information a été coulée à le déclarer de sorte que les sociétés d'assurance et d'autres associations de l'industrie puissent recueillir cette information et commencer à offrir des services d'assurance. Deuxièmement, comme dans d'autres secteurs, lorsque le secteur privé ne sait pas comment rentabiliser une opération, le gouvernement peut commencer à offrir ces services jusqu'à ce qu'il existe suffisamment de données et que les services puissent être confiés au secteur de l'assurance.

Au Québec, par exemple, l'assurance automobile appartient à l'État. Dans d'autres parties du pays, cette assurance a été privatisée. La raison pour laquelle ce service a été entrepris par la province dans les années 1960, je crois, c'est qu'aucune entreprise du secteur privé n'était prête à assumer ce risque. C'est un cas où le gouvernement peut jouer un rôle de chef de file, non seulement pour ce qui est de légiférer, mais aussi pour ce qui est de lancer la balle en offrant une protection contre ce risque.

[*Français*]

Mme Charmaine Borg: Merci.

Madame Sproule, monsieur Dupont ou madame Lawson, voudriez-vous émettre des commentaires?

● (1200)

[*Traduction*]

M. Benoît Dupont: J'ajouterai quelques mots seulement. En ce qui concerne le manque de données, il y a deux problèmes. Il existe déjà des données, mais elles sont fragmentaires, et nous devons trouver des moyens, parfois négatifs, d'inciter les organisations à rendre ces données publiques, à les compiler et à les consolider. Ensuite, il y a des données que nous devons recueillir parce que personne d'autre ne les a. L'enquête sur les victimes en est un parfait exemple. Statistique Canada recueille ces données tous les quatre ou cinq ans, et compte tenu de l'évolution de la technologie et de la rapidité de ce phénomène, je crois qu'il est nécessaire de recueillir des données à ce sujet beaucoup plus régulièrement.

Ce n'est pas une entreprise très onéreuse. Il serait peu coûteux de mener une enquête pancanadienne, mais elle devrait être dirigée par un organisme responsable. J'aime bien l'idée qu'un organisme soit chargé de cette question et soit financé pour recueillir des données et consolider les données qui existent déjà.

Merci.

Mme Philippa Lawson: Puis-je ajouter un commentaire?

Le président: Bien sûr, madame Lawson.

Mme Philippa Lawson: Sur la question de la collecte de données, il existe déjà de l'information sur la fraude financière relative à l'identité. Cette information se trouve dans les institutions financières et les bureaux de crédit. Alors le gouvernement devrait chercher des moyens d'obtenir ces données auprès de l'industrie.

Le président: Merci, madame Lawson.

Madame Sproule.

Dre Susan Sproule: Il est clair que nous devons recueillir de l'information sur les atteintes à la sécurité des données, et les exigences de notification dans le cas de telles atteintes sont un élément important de ce que nous devons examiner pour comprendre le problème, mais ce n'en est qu'une partie.

Comme je l'ai dit, il est très difficile d'établir des liens entre les vols d'identité, les atteintes à la sécurité des données et les fraudes elles-mêmes. Le Government Accountability Office des États-Unis a fait une étude au début des années 2000 dans laquelle on disait qu'on ne peut pas établir de lien entre toutes les atteintes à la sécurité des données et les fraudes. Nous devons chercher de l'information auprès de nombreuses sources différentes pour pouvoir dresser le tableau d'ensemble. Il faut mener des enquêtes sur les victimes. Il faut aussi des enquêtes sur les entreprises ou d'autres moyens d'obtenir de l'information auprès des entreprises sur la situation et sur les coûts connexes. Il faut obtenir de l'information des diverses agences d'évaluation du crédit, des banques, des organisations déclarantes, de même que des groupes qui offrent des services aux victimes. Il faut recueillir toute cette information et essayer d'établir la corrélation avec le problème principal.

[*Français*]

Mme Charmaine Borg: Merci beaucoup.

Madame Lawson, vous avez brièvement mentionné que le seuil établi dans le projet de loi S-4 pour déterminer qu'il y a atteinte aux données était trop élevé. Ce projet de loi propose que ce soient les organisations elles-mêmes qui prennent la décision d'avertir la commissaire ou les utilisateurs d'une perte de données ou d'une atteinte à des données. Au lieu de faire une évaluation objective, on se fierait plutôt à un mécanisme subjectif.

Pouvez-vous émettre des commentaires là-dessus? Cela pourrait-il poser un problème?

[*Traduction*]

Mme Philippa Lawson: Oui, je pense que c'est effectivement un problème. Les organisations sont très motivées à ne pas signaler les atteintes à la sécurité. Pour qu'une loi soit efficace, elle doit contrer cette motivation, offrir un contre-incitatif, et je pense que ce contre-incitatif doit prendre la forme d'un seuil objectif qui est assez faible afin que toutes les atteintes soient signalées. C'était pourtant la norme dans les versions précédentes de ce projet de loi, et je ne vois pas pourquoi il a été modifié sous le projet de loi S-4.

C'est problématique. En fait, il y a deux seuils en jeu. Il y a le premier seuil, où une organisation doit signaler une atteinte au commissaire à l'information, mais pas nécessairement au public, et il y a lieu de s'interroger si ce signalement devrait être rendu public. Le deuxième seuil, c'est lorsque les organisations doivent signaler une atteinte aux particuliers touchés.

Je pense qu'il est tout à fait sensé d'avoir un seuil plus faible pour rapporter les atteintes au commissaire, et un seuil plus élevé pour les signalements aux particuliers. Je ne vois pas pourquoi le gouvernement a choisi d'appliquer le seuil le plus élevé dans les deux cas. En effet, les mesures de sécurité constituent une pièce essentielle du casse-tête, et les organisations en sont les principaux responsables. En établissant un seuil objectif en vertu duquel les organisations sont obligées de signaler les atteintes au commissaire, nous pourrons enfin nous doter d'un registre digne de ce nom ou, si vous préférez, d'un répertoire des atteintes à la sécurité, et, partant, d'une liste des organisations qui n'arrivent pas à protéger l'information personnelle de leurs clients.

● (1205)

Le président: Merci, madame Lawson.

Nous avons largement dépassé le temps de Mme Borg.

Nous passons maintenant aux conservateurs, avec M. Laurie Hawn.

L'hon. Laurie Hawn (Edmonton-Centre, PCC): Merci, monsieur le président.

Merci à tous d'être venus.

Monsieur Fernandez, je suis, entre autres, coprésident de la Commission permanente mixte de la défense Canada-États-Unis. Notre mandat est de formuler des conseils sur toute question de défense et de sécurité pour l'Amérique du Nord.

On se concentre tout particulièrement sur tout ce qui est cyber: cybersécurité, cybercrime, cyberespionnage, cyberterrorisme. Puisque nous utilisons des logiciels dans tout ce que nous faisons, le risque de paralyser notre société, comme vous l'avez si bien remarqué, est énorme. C'est d'ailleurs arrivé en Estonie et en Georgie, entre autres.

Vous avez dit tout à l'heure que nous sommes en train de perdre la bataille. Je ne pensais pas que vous parliez de ce point-ci précisément, mais je pense que vous y faisiez allusion. Sans divulguer quoi que ce soit de secret, pourriez-vous nous dire si nous sommes en train de perdre la bataille et, le cas échéant, comment renverser la vapeur?

M. José Manuel Fernandez: Nous sommes en train de perdre la bataille technologique, et par cela, je veux dire que nous ne sommes pas en train de perdre au niveau du développement de nouvelles technologies, mais plutôt au niveau de leur déploiement afin de combattre, entre autres, le vol d'identité. Là encore, cela revient au fait que les entités qui ont l'autorité de déployer ces technologies n'ont aucune motivation à le faire. Il s'agit d'un triangle d'incitatifs brisé. Ce ne sont pas les ordinateurs du grand public qui sont visés, c'est-à-dire les personnes qui pourraient être victimes de vol d'identité. Non, on pirate plutôt les ordinateurs d'autres entités ou les ordinateurs de l'organisation dont on vient de discuter.

C'est là où le gouvernement doit faire preuve de leadership et réparer le triangle d'incitatifs. Autrement, ceux qui ont le pouvoir de régler le problème en subiront les conséquences fâcheuses s'ils ne le font pas, ou s'en féliciteront s'ils le font. Les incitatifs pourraient prendre la forme de primes d'assurance ou de marchés plus avantageux avec le gouvernement. Et c'est possible, car les technologies existent.

Je vais vous donner un exemple concret de vol d'identité — et il en va de même pour traverser la frontière aux États-Unis. Il s'agit de technologies biométriques, qui sont disponibles et abordables. Bien entendu, elles ne s'appliqueront pas dans tous les cas, notamment pour les services bancaires, mais il y a néanmoins un service d'authentification à deux paliers. Là encore, nos amis américains ont mandaté l'authentification à deux étapes pour toutes les applications liées au gouvernement ou pour l'accès aux serveurs du gouvernement.

Par contre, certains secteurs vont dans le sens inverse. Le secteur bancaire, dont la principale motivation est le profit, a décidé de faire marche arrière en ce qui concerne la technologie d'authentification et mise maintenant sur les cartes de crédit dotées de puces d'identification par radiofréquence qui, du point de vue de l'authentification et du vol d'identité, représentent un problème encore plus gros.

La technologie existe. Les normes existent. Les critères communs, par exemple — et vous parliez de logiciels du gouvernement —, représentent des normes techniques très exhaustives et bien rédigées, et elles sont appliquées à tous les systèmes du gouvernement hautement sécurisés. Pourquoi ne devraient-ils pas être appliqués à certains secteurs de l'industrie également?

L'hon. Laurie Hawn: On me dit que les Chinois ont plus de deux millions de personnes qui ne font que ça, car ils peuvent se permettre d'affecter autant de gens à la cybersécurité. Bien entendu, le Canada ne peut pas en faire autant. Vous avez dit que les législateurs doivent faire preuve de leadership afin de renverser la vapeur. C'est notamment à cause des universitaires et du secteur privé que nous en sommes là. Je ne pense pas que nous pouvons adopter des lois pour changer notre orientation. Je pense qu'il faudrait plutôt adopter une approche fondée sur la collaboration.

Mais comment lutter contre ce fléau? Je pense surtout à la sécurité nationale, mais on y trouve des applications dans tous les domaines. Formons-nous assez de personnes? Sommes-nous en train de former assez de personnes spécialisées dans le domaine de la cybersécurité? Je pense à la sécurité nationale, mais le problème s'applique aussi au quotidien, dans tous les secteurs où l'on craint le vol d'identité.

Doit-on mettre l'accent sur l'éducation de façon à former un maximum de gens?

● (1210)

M. José Manuel Fernandez: Oui, c'est un aspect important. Là encore, les États-Unis nous ont battus à plate couture en investissant beaucoup plus d'argent que nous, par habitant, dans l'élaboration de programmes d'éducation en matière de sécurité informatique. N'oublions pas également que — comme vous le dites si bien — la solution au problème n'est pas seulement la technologie. Les Américains ont mis au point toutes sortes de programmes de formation d'experts en sécurité de la technologie informatique, mais ce dont nous avons besoin, c'est davantage de gens comme vous qui comprennent le problème du point de vue social, économique, voire politique. Comme je le disais tout à l'heure, nous pouvons faire notre part pour fermer la boîte de Pandore, mais en tant qu'ingénieur, il y a très peu de choses que je puisse faire. C'est vous, les politiciens. Nous devons collaborer ensemble, sous votre leadership.

L'hon. Laurie Hawn: Vous avez parlé de Nortel et de l'entreprise qui en a fait l'acquisition. Nous savons tous qui a acheté Nortel. Et ce n'était qu'une reprise commerciale. Imaginez s'il se passait la même chose au niveau de la sécurité nationale: ce serait effrayant. Il me semble que l'on s'approche de l'ancien concept nucléaire de la destruction mutuelle assurée, c'est-à-dire qu'ils peuvent nous détruire quand ils le veulent, mais nous pouvons en faire autant. Il faut donc essayer d'être toujours un pas en avant, ce qui nous ramène aux données.

Monsieur Dupont, vous avez justement parlé du problème des données. Comment pouvons-nous recueillir et conserver de meilleures données?

M. Benoît Dupont: Comme on l'a déjà dit, je crois, il faut communiquer des données que détiennent les institutions financières... Mais il en va de même également pour les organismes de vente au détail. Nous avons surtout parlé du secteur financier car c'est une cible privilégiée des voleurs d'identité, mais les organismes de vente au détail sont aussi responsables d'un grand nombre de fuites de données. Ils devraient donc être tenus responsables. Et ils devraient être très transparents quant à l'incidence des vols d'identité.

Je pense que le gouvernement devrait exercer son autorité et exiger que ces données soient rendues publiques, pas nécessairement... à très grande échelle, peut-être. On a parlé de l'idée de mettre au pilori certaines entreprises. Eh bien, c'est exactement ce qui s'est passé dans les années 1970, lorsque les compagnies d'assurance et les gouvernements en ont eu assez du taux très élevé de vols d'automobiles. Un jour, on a décidé de publier le nom des 10 modèles d'automobiles les plus volés sur le marché. Douze mois plus tard, toutes ces voitures étaient équipées de dispositifs antivol, et ce, sans frais pour le contribuable.

Les fabricants d'automobiles avaient plaidé qu'ils ne pouvaient rien y faire et, du jour au lendemain, ils ont trouvé les ressources et les technologies nécessaires pour rendre leurs automobiles plus difficiles à voler. Ils l'ont fait simplement parce qu'on a mis des données à la disposition des consommateurs afin d'éclairer leurs choix.

Il revient au gouvernement d'essayer d'obtenir cette information, et non pas de façon punitive, mais plutôt de façon constructive, afin de rendre les marchés plus transparents et d'informer les consommateurs et les citoyens. Comme l'a dit ma collègue, Mme Lawson, il y a très peu de choses que le consommateur ou les particuliers peuvent faire tout seuls, mais il y a beaucoup de choses que les organisations peuvent faire pour protéger les consommateurs.

L'hon. Laurie Hawn: Je suppose que c'est la raison pour laquelle je n'achète pas de Honda Civic.

Le président: Merci, monsieur Hawn. C'est sur cette note que se termine votre temps d'intervention.

Je rappelle aux membres du comité et aux témoins que les sept minutes, c'est pour les questions et les réponses. Si vous pouviez être plus brefs, d'autres personnes auraient l'occasion de poser des questions.

Maintenant, c'est au tour du Parti libéral et de notre collègue, M. Scott Andrews.

Scott, vous avez sept minutes.

M. Scott Andrews (Avalon, Lib.): Merci, monsieur le président.

Je remercie les témoins de leur présence.

Susan, j'aimerais revenir sur ce que vous disiez vers la fin de votre exposé au sujet des agences d'évaluation du crédit. Elles peuvent probablement constituer un système d'avertissement précoce si l'identité d'une personne est compromise. Je pense qu'elles jouent un rôle essentiel pour aider les consommateurs à protéger leur identité. La plupart d'entre nous ne vérifions nos cotes ou notre dossier de crédit qu'après coup, lorsque quelque chose est arrivé.

Comment pouvons-nous les mobiliser? Nous devons entendre leurs témoignages aussi. Quel genre de questions... Comment pouvons-nous les mobiliser? À votre avis, quel rôle devraient-elles jouer? Peut-être pourriez-vous nous en dire un peu plus sur ces agences d'évaluation du crédit et en quoi elles peuvent contribuer à une détection précoce des problèmes potentiels d'usurpation d'identité.

● (1215)

Dre Susan Sproule: Comme le disait Mme Lawson, le problème le plus grave que pose le vol d'identité, c'est quand il sert à l'ouverture de nouveaux comptes. La seule façon de savoir si quelqu'un ouvre de nouveaux comptes en votre nom, c'est en vous adressant à l'agence d'évaluation du crédit.

Comme je le disais, j'arrive relativement bien à protéger mes renseignements personnels. Mes moyens sont limités, mais je ne donne pas facilement mes renseignements personnels; je fournis seulement ce qui est nécessaire. Je suis tous les conseils que l'on donne aux consommateurs en ce qui concerne la protection des renseignements.

On conseille souvent aux consommateurs de vérifier régulièrement leur dossier de crédit. Je l'ai fait une fois il y a cinq ans. Cela a été une corvée de vérifier et de rassembler tous ces renseignements. J'ai dû tout envoyer par la poste, ce qui n'est pas très sûr. Il suffit que quelqu'un intercepte l'enveloppe pour avoir en main tout ce qu'il lui faut pour voler mon identité. J'ai envoyé ce formulaire aux deux agences d'évaluation du crédit, et j'ai reçu un relevé de l'une d'elles. Je n'en ai jamais reçu de la deuxième, ce que j'ai trouvé un peu inquiétant. J'ai fini par téléphoner et on m'a dit, « Oh oui, nous l'avons reçu; il a dû se passer quelque chose ».

Pour vraiment me protéger, j'aimerais pouvoir aller en ligne une fois par trimestre et obtenir instantanément mon dossier de crédit. C'est ce que je ferais pour me protéger. Pour l'instant, ça me coûte 24 $ chaque fois que je le fais.

M. Scott Andrews: C'est 16 $ par mois.

Dre Susan Sproule: Ou je peux payer 16 $ et on m'enverra un dossier de crédit et quelques documents d'information sur la façon de me protéger. Cela me dérange vraiment que ces agences tirent parti du problème. Qu'est-ce qui les poussera, alors, à contribuer à éliminer les menaces? Cela me dérange quand la banque offre de me vendre une assurance contre le vol d'identité. Son travail n'est-il pas de protéger mes renseignements?

M. Scott Andrews: Madame Lawson, voulez-vous nous parler des agences d'évaluation du crédit pouvant constituer un système d'avertissement précoce quant le crédit d'une personne est en péril?

Mme Philippa Lawson: Oui, je suis tout à fait d'accord avec vous sur ce plan, et je suis heureuse d'entendre qu'elles viendront témoigner devant vous. Je pense que vous devriez leur poser beaucoup de questions, y compris pourquoi elles n'offrent pas aux consommateurs canadiens un gel de leur crédit quand ils sont aux États-Unis.

Elles devraient faire diverses autres choses, notamment en ce qui concerne la surveillance du crédit et la production de rapports, comme vous venez de l'entendre. Cela représente beaucoup d'argent et d'efforts pour les Canadiens. Nous avons droit à un rapport gratuit par année, que nous recevons par la poste, mais les agences de crédit facturent et rendent difficile l'accès en ligne.

Aux États-Unis, leur règle, c'est le guichet unique. Il y a trois agences d'évaluation du crédit aux États-Unis et deux, au Canada. Il serait utile pour les consommateurs — surtout les victimes de vol d'identité — de pouvoir consulter une source centrale et obtenir des rapports des deux agences. Ce serait utile.

Je trouve qu'il faudrait pouvoir accéder au rapport en ligne et obtenir des services de surveillance du crédit, gratuitement ou à très peu de frais, surtout quand on peut démontrer qu'on a été victime de fraude. Aux États-Unis, il existe des lois, sous le régime de la Fair Credit Reporting Act, que nous n'avons pas au Canada, en dehors des principes très généraux stipulés dans notre Loi sur la protection des renseignements personnels. Par exemple, les agences d'évaluation du crédit aux États-Unis doivent bloquer la transmission de renseignements lorsque le consommateur fournit des preuves de fraude. Dès que la victime les a avisées qu'il y a apparence de fraude, elles doivent en informer ceux qui ont fourni les renseignements.

Ce genre d'obligations bien précises des agences d'évaluation du crédit peuvent vraiment contribuer à prévenir, à déceler et à régler le problème de vol d'identité.

M. Scott Andrews: Je m'adresse encore à vous, Susan. Vous avez dit tout à l'heure que ce ne sont pas les voleurs d'identité qui commettent des fraudes liées à l'identité. Peut-être pourriez-vous nous expliquer cela? Y a-t-il moyen pour les organismes d'application de la loi et les particuliers d'empêcher que le vol d'identité aboutisse à la fraude d'identité?

● (1220)

Mme Susan Sproule: En fait, il y a divers types de vol d'identité. Certains sont très opportunistes et ciblés, comme lorsque quelqu'un a accès aux renseignements d'une personne et se fait passer pour elle pour commettre une fraude.

Il y a aussi l'atteinte à la sécurité des données, comme lorsque des pirates entrent dans des bases de données pour en extraire des renseignements en vue de les vendre sur le marché noir. Certaines études universitaires se sont penchées sur le marché noir et sur la valeur d'un compte de carte de crédit — c'est-à-dire la valeur des renseignements personnels comme le numéro d'assurance sociale et le nom de jeune fille de votre mère. Il est possible d'obtenir ces renseignements sur le marché noir, et c'est la différence entre le vol et la fraude. Les fraudeurs...

M. Scott Andrews: Monsieur Fernandez, vous avez quelque chose à ajouter?

M. José Manuel Fernandez: Oui. Le problème, malheureusement, c'est qu'un grand nombre de ces voleurs d'identité ne sont même pas au Canada. Ils ne sont pas sur notre territoire. C'est le crime organisé en Europe de l'Est, en Indonésie, au Brésil, et c'est tout simplement hors de notre portée. Peu de ces pays collaborent avec les organismes d'application de la loi du Canada. C'est pourquoi la Convention sur la cybercriminalité que nous devons encore ratifier est tellement importante.

M. Scott Andrews: Et qu'en est-il du marché noir? Y a-t-il moyen pour les organismes d'application de la loi de se concentrer là-dessus, ou est-ce qu'ils ne peuvent pas...

M. José Manuel Fernandez: Je vais laisser mon collègue, Benoît Dupont, répondre à cette question. Il a des idées assez intéressantes sur ce qu'on pourrait faire pour démanteler le marché noir.

Le président: Une très courte réponse, s'il vous plaît, monsieur Dupont. Il nous reste peu de temps.

M. Benoît Dupont: Une très courte réponse... À ma connaissance, le seul pays qui ait investi dans des enquêtes visant à démanteler le marché noir, c'est les États-Unis, au moyen des services secrets. Rien ne justifie que la GRC, qui peut emprunter de grosses sommes pour mener des enquêtes approfondies sur la mafia... Vous savez, l'enquête sur le Colisée de Québec a coûté environ 30 millions de dollars. La GRC pourrait très bien investir autant, ou moins, pour essayer de démanteler les marchés noirs. Elle dispose d'un réseau d'agents de liaison partout dans le monde qui collaborent les uns avec les autres. Jusqu'à maintenant toutefois, seuls les États-Unis ont investi de tels montants pour enquêter sur des crimes commis à l'extérieur de leurs frontières.

Le président: Merci, monsieur Dupont.

Merci, monsieur Andrews.

Notre prochain intervenant est M. Zimmer, du Parti conservateur.

M. Bob Zimmer (Prince George—Peace River, PCC): J'aimerais remercier tous les témoins d'être venus aujourd'hui. Nous sommes nombreux à passer beaucoup de temps sur Internet, et nous nous demandons si nos renseignements personnels sont protégés.

J'aurais quelques questions élémentaires. Comment sommes-nous arrivés au montant de 3 milliards de dollars? Je crois que quelqu'un avait dit que les Canadiens subissaient des pertes de l'ordre de 3 milliards de dollars, mais comment arrive-t-on à ce montant?

M. José Manuel Fernandez: Ce montant provient de Symantec, qui est un éditeur d'antivirus. On le retrouve dans le rapport de 2013 sur le Canada.

Je ne suis pas un expert pour quantifier ce genre de choses. Certains pourraient croire que ce montant a été avancé par une entité qui veut éventuellement amplifier le problème, mais certains de mes collègues, qui sont spécialisés dans ce domaine, sauront mieux vous répondre.

M. Bob Zimmer: Quelqu'un d'autre souhaite répondre brièvement? J'ai d'autres questions, mais si quelqu'un pouvait répondre à celle-là...

Le président: Madame Sproule, vous souhaitez intervenir en premier?

Dre Susan Sproule: À titre d'exemple, et il s'agit là de vieilles données, selon le sondage que nous avons effectué en 2008 auprès des consommateurs, 1,7 million de personnes ou 6,5 % des adultes canadiens avaient été victimes d'une certaine forme de vol d'identité au cours de la dernière année. Ils ont passé plus de 20 millions d'heures et dépensé plus de 150 millions de dollars pour résoudre les problèmes causés par ces vols. Et ce ne sont que les dépenses qui ont été assumées par les consommateurs, ce qui n'est en fait qu'une petite part d'un problème de taille.

M. Bob Zimmer: C'est non négligeable. Merci de ces renseignements.

J'aurais deux autres questions simples à vous poser.

Nos ordinateurs ont tous été contaminés par des virus ordinaires. Le son arrête de fonctionner ou autre chose. Je voudrais savoir qui est à l'origine de ces attaques. S'agit-il d'un adolescent qui veut éteindre le son sur mon ordinateur? Peut-il accéder à des données importantes, l'arrêt du son n'étant qu'un effet résiduel?

On pense toujours aux pirates professionnels, aux Chinois, ou à ceux qui mènent des attaques de front sur nos systèmes. Pourriez-vous nous expliquer comment ces attaques sont menées?

● (1225)

M. José Manuel Fernandez: Oui, je serai succinct.

La cybercriminalité s'est complexifiée au cours des dernières années. On compte au moins quatre types de pirates. Certains nous attirent vers un site Web qui contamine notre appareil. D'autres exploitent ces sites et contaminent notre appareil, mais n'en ont pas le contrôle. Ils vendent notre appareil à quelqu'un qui va l'exploiter pendant des semaines ou des mois. Ce type de pirate loue l'appareil à ceux qui fraudent et empochent de l'argent. Ces fraudeurs se servent de l'appareil compromis pour envoyer des pourriels et usurper nos données financières. C'est l'un des moyens de voler l'identité de quelqu'un. Ils pourraient également l'utiliser pour mener une attaque par déni de service contre un pays.

Il y a bien des façons de tirer profit des ordinateurs compromis. C'est un seul et même problème. On peut se servir d'un même arsenal d'ordinateurs pour le cyberespionnage, le cybersabotage, le vol d'identité et la cybercriminalité de masse. Tous ces groupes travaillent ensemble. Avant, ils le faisaient pour le plaisir, puis pour l'argent. On s'aperçoit maintenant qu'ils ont également des visées politiques et propagandistes.

M. Bob Zimmer: Je voudrais enchaîner avec une autre question.

Vous avez parlé d'une entreprise qui devait remplacer 30 000 ordinateurs. Est-ce bien cela?

M. José Manuel Fernandez: C'était Aramco. Effectivement, environ 30 000 ordinateurs de bureau avaient été...

M. Bob Zimmer: Je ne pensais pas qu'un virus pouvait à ce point endommager un ordinateur, mais il semble que ce virus en particulier a eu un effet beaucoup plus grave sur le matériel. Pouvez-vous l'expliquer?

M. José Manuel Fernandez: Oui. En général, les virus n'endommagent pas le matériel. En l'occurrence, Aramco, une riche entreprise, a décidé que le mieux, c'était de jeter tous ces ordinateurs, d'en acheter des neufs et de les réinstaller.

C'était probablement une très sage décision. Il aurait probablement coûté plus cher de les garder et de les réinstaller à partir de zéro. Faites le calcul: il aurait fallu 1 000 $ par ordinateur. C'est non négligeable.

M. Bob Zimmer: Pour revenir à l'une de mes questions précédentes, nous avons parlé des divers aspects de la cybercriminalité, et vous avez fait mention de l'espionnage.

Si le son a arrêté de fonctionner sur un ordinateur, est-ce un jeune pirate au laboratoire informatique d'une école secondaire qui essaie d'agacer les autres, ou faut-il craindre quelque chose de plus grave?

M. José Manuel Fernandez: J'ai parlé tout à l'heure des jeunes pirates, du virus Heartbleed et des étudiants de l'Université Western Ontario. Avant, ils étaient la source d'un gros problème, mais maintenant, ils ne font que nous embêter. Le problème, ce n'est pas eux.

D'un point de vue sociopolitique toutefois, dans les pays où l'économie des technologies de l'information ne s'est pas beaucoup développée, de jeunes prodiges préfèrent la cybercriminalité aux emplois qu'ils pourraient décrocher à Kanata ou à la Silicon Valley. Ils sont devenus des professionnels et se retrouvent sous le joug de personnes imposantes et bien armées.

M. Bob Zimmer: Merci. Je n'ai pas d'autres questions.

Merci.

Le président: Merci, monsieur Zimmer.

Nous allons enchaîner avec les interventions de cinq minutes.

Mathieu Ravignat, à vous la parole. Vous avez cinq minutes.

M. Mathieu Ravignat (Pontiac, NPD): Monsieur Fernandez, pour revenir sur ce qu'a dit mon collègue au sujet du virus Heartbleed, vous avez mentionné au début de votre exposé que l'infrastructure informatique du gouvernement était dans un état « pitoyable ». Je crois que c'est le terme que vous avez employé, ou en était-ce un autre plus coloré? En tout cas, cela me préoccupe.

Quelles décisions avons-nous prises dans les dernières années qui nous ont conduits à la situation dans laquelle nous sommes actuellement?

Que faut-il faire?

M. José Manuel Fernandez: Personne n'est épargné: ni le gouvernement canadien, ni le secteur privé au Canada, ni les gouvernements étrangers partout dans le monde. C'est un problème d'ordre mondial. Je ne crois pas que le gouvernement canadien soit moins diligent que les gouvernements étrangers ou les grandes sociétés. Le problème ne date pas d'hier. Cela remonte à il y a 30 ans. Dans les années 1960, 1970 et 1980, le secteur informatique était bien structuré et s'articulait autour d'IBM et de quelques autres acteurs. Tout le monde comprenait son fonctionnement, et on savait qui gronder en cas de problème.

Avec l'avènement du Web toutefois, c'est devenu une mêlée générale. N'importe qui ayant des notions de programmation pouvait développer une application web. N'importe qui pouvant contribuer à la conception de logiciels ouverts le faisait. Les normes auxquelles on était habitué ont été abandonnées. Tout était nouveau, on voulait les trucs tendances et gagner du fric le plus rapidement possible. Les banques en sont un bon exemple, n'est-ce pas? Elles ont enregistré des bénéfices faramineux en l'an 2000 grâce à cela.

Le gouvernement a emboîté le pas aux autres. Il a adopté de nouvelles technologies, comme les autres, mais a abandonné les normes qui prévalaient autrefois. Dans le monde des ordinateurs centraux, des normes régissaient le développement et d'autres aspects relatifs au système, mais avec l'avènement du nouveau paradigme client, serveur et Web, tout a été relégué aux oubliettes. On a tout abandonné. Il faut ramener ces normes.

● (1230)

Mme Susan Sproule: En matière de technologie, il est souvent question de sécurité, et la sécurité des données est le maillon faible. Nous disposons d'une technologie efficace. Nous avons des technologies de chiffrement, mais le problème, c'est que les gens ne s'en servent pas. Pensez aux nouvelles formes d'information, comme les dossiers de santé électroniques, et au transfert de ces dossiers dans les divers réseaux et systèmes. Les dossiers de santé personnels sont parfois piratés. Ne pas chiffrer ces données, c'est criminel. Cela ne devrait pas se produire. Le problème, ce n'est pas la technologie, mais les décideurs. La technologie, elle, est disponible.

M. Mathieu Ravignat: La technologie est disponible, mais les politiques publiques ne sont pas au rendez-vous.

Mme Susan Sproule: Il existe peut-être des politiques sur le chiffrement. Encore faut-il que nous les mettions en oeuvre.

M. Mathieu Ravignat: D'accord.

Le président: Monsieur Ravignat, nous pourrions demander aux témoins qui nous suivent à distance s'ils ont des observations à faire.

M. Mathieu Ravignat: Certainement.

Le président: Souhaitez-vous commenter la dernière intervention de M. Ravignat?

Non. D'accord. Je voulais que vous fassiez partie du débat. Merci.

M. Mathieu Ravignat: Ma prochaine question concerne la récente mise au point de la technologie payWave. Il s'agit de cartes de paiement automatique, et il semble que ces cartes posent un certain nombre de problèmes de sécurité, notamment pour les cartes de crédit, les cartes bancaires, etc.

Monsieur Fernandez, vous avez participé à un projet de recherche sur cette technologie. En auriez-vous les résultats? Pourriez-vous nous aider à la comprendre?

M. José Manuel Fernandez: Si cela ne vous gêne pas, je vais prendre votre carte de crédit. Je vais éteindre mon téléphone et je pourrai lire le numéro de votre carte de crédit par radio, ainsi que votre nom et la date d'expiration de votre carte. Le tout, grâce à une application.

M. Mathieu Ravignat: Étant donné qu'il s'agit d'une séance publique, je préférerais ne pas me livrer à cet exercice.

Des voix: Oh, oh.

M. José Manuel Fernandez: Oui, les banques ont malheureusement été motivées avant tout par le profit lorsqu'elles ont élaboré cette technologie. Elles voulaient leur satané profit de 3,5 % sur le marché de la petite monnaie.

Et cela s'est fait aux dépens de la vie privée des Canadiens, car cette technologie ne protège pas leurs renseignements personnels. Si je vole votre carte de crédit de votre porte-monnaie, vous vous en rendrez sans doute compte, car je dois mettre ma main dans votre poche pour y arriver. En revanche, avec cette nouvelle technologie, je n'ai même pas à agir de la sorte. Je n'ai qu'à me rapprocher de vous dans le métro, à 10 centimètres, et le problème est réglé: je peux voler vos renseignements de carte de crédit et faire des transactions. La technologie que les banques ont élaborée aurait pu empêcher cela, mais elles l'ont créée dans un mode moins sécuritaire — du moins pour l'instant —, car elles ne veulent pas investir les fonds nécessaires pour changer l'infrastructure des terminaux de paiement.

M. Mathieu Ravignat: Je présume que la réglementation n'est pas à jour.

M. José Manuel Fernandez: Quelle réglementation...?

M. Mathieu Ravignat: Très bien. Alors il s'agit d'un problème en soi.

Le président: Monsieur Ravignat, votre temps est écoulé. Y a-t-il un autre témoin qui aimerait intervenir à ce sujet? Nous vous accorderons une minute de plus.

Madame Lawson.

Mme Philippa Lawson: Monsieur le président, j'aimerais soulever un dernier point. Je pense qu'il serait utile de distinguer les deux catégories de vol d'identité. D'abord, il y a les cartes de crédit à large distribution pour lesquelles l'industrie a décidé de s'exposer à un risque de fraude accru pour obtenir plus de transactions. Ce coût est assumé par les consommateurs par l'entremise de frais et de taux d'intérêt plus élevés. Susan Sproule l'a mentionné tout à l'heure. Quand le consommateur est remboursé par l'institution financière et n'est pas tenu responsable de la fraude, cela n'aura pas la même incidence que le vol d'identité personnel, où c'est à la victime d'assumer toutes les répercussions financières.

● (1235)

Le président: Merci.

Une dernière observation...

M. José Manuel Fernandez: C'est en fait pire que cela, car, si les banques payaient, on pourrait dire qu'il s'agit d'un jeu à somme nulle. Ce que je perds, je le regagne plus tard. Le problème avec cette technologie, c'est qu'elle présente une menace sans précédent à notre vie privée. Nous ne pouvons pas éteindre ces cartes. Elles ne transmettent pas seulement ce que vous payez, elles sont toujours en service. Un magasin pourrait mettre sur pied un détecteur de cartes qui lui permettrait de savoir que vous êtes la même personne qui est venue deux semaines plus tôt pour acheter un chapeau ou encore que vous êtes la femme qui est venue la veille pour acheter, par exemple, un manteau de fourrure. Cela pourrait être fait à des fins de marketing, mais également à des fins de suivi, de harcèlement et même d'atteinte à la sécurité.

Ils ont créé un problème bien plus important que celui de la fraude bancaire par Internet.

Le président: Merci, madame Sproule.

J'ai décidé de nous accorder un peu plus de temps, car c'était la première fois que nous abordions ce sujet fort intéressant. Chad, notre greffier, vient de me dire qu'il conserve sa carte dans une pochette faite en kryptonite pour que personne ne puisse y avoir accès.

Cédons maintenant la parole au parti ministériel. C'est le tour de Mme Tilly O'Neill Gordon.

Vous avez cinq minutes, Tilly.

Mme Tilly O'Neill Gordon (Miramichi, PCC): Merci, monsieur le président.

Tout d'abord, j'aimerais tous vous remercier d'avoir pris le temps de venir nous voir et de nous avoir fourni des renseignements aussi utiles. Nous sommes tous bien au courant du virus Heartbleed, qui a posé bien des problèmes. Vous avez mentionné qu'il a mené à la divulgation non autorisée d'au moins 900 numéros d'assurance sociale.

Je me demandais si les victimes étaient au courant que leurs numéros avaient été divulgués. Est-ce que vous pensez que la plupart des victimes de vol d'identité sont au courant d'avoir été ciblées?

M. José Manuel Fernandez: En ce qui a trait à l'incident Heartbleed, un communiqué de presse émis par l'ARC a indiqué que les personnes dont le numéro avait été identifié recevraient une lettre pour les aviser. Je présume que c'est ce que l'agence fera.

En règle générale, je répondrai non à votre question. Nous avons compilé des données au fil des années en pénétrant les marchés noirs et en compilant des statistiques portant notamment sur les taux d'infection. Nous estimons que, pour chaque victime de fraude d'identité et pour chaque compte vidé, il y en a environ 10 fois plus qui auraient pu être compromis. Les mesures de prévention de la fraude des banques empêchent les cybercriminels de vider plus de comptes, mais ces criminels ont une réserve d'au moins 10 fois plus de comptes que ce dont ils ont besoin, et ils ont la capacité de les vider immédiatement. Il y a beaucoup plus de victimes de vol d'identité que de victimes de fraude d'identité. Ces victimes n'ont tout simplement pas encore été fraudées.

Mme Tilly O'Neill Gordon: Avez-vous quelque chose à ajouter?

Mme Susan Sproule: Non. Je suis d'accord.

Mme Tilly O'Neill Gordon: Qu'en est-il du suivi auprès des victimes? Est-ce qu'elles reçoivent du soutien? Qu'en est-il du suivi qu'on effectue auprès d'elles?

Mme Susan Sproule: Pippa répondra à cette question.

Mme Philippa Lawson: Je n'ai aucune idée de ce que les organisations qui ont souffert de l'incident Heartbleed font afin de communiquer de manière proactive avec leurs victimes. C'est précisément pour cette raison que des lois portant sur les signalements des atteintes à la sécurité sont essentielles. Ces lois exigeraient précisément ce que vous suggérez. Elles exigeraient que l'on avise les victimes, afin qu'elles puissent prendre les mesures nécessaires pour fermer leurs comptes et se protéger contre la fraude.

Un point fort important a été souligné tout à l'heure. La fraude pourrait survenir des années plus tard. En fait, il existe une catégorie croissante de fraude d'identité aux États-Unis qui touche les enfants. Les fraudeurs obtiennent notamment des numéros d'assurance sociale de jeunes enfants.

À la naissance, vous pouvez choisir d'obtenir un numéro d'assurance sociale pour votre enfant. Certains parents le font notamment pour inscrire leurs enfants à des régimes d'épargne-études. Une fois que vous obtenez ce numéro, il peut faire l'objet d'un vol d'identité. Une personne pourrait ne pas se rendre compte, jusqu'à ce qu'elle ait 18 ans, que son identité avait été volée. Ensuite, lorsque cette personne obtient son premier emploi ou fait sa première déclaration de revenus, elle se rend compte qu'elle a été victime de fraude d'identité pendant des années.

Le délai entre le vol de l'identité et la fraude peut être considérable.

● (1240)

M. Benoît Dupont: J'aimerais ajouter quelque chose. Nous avons mené un sondage en 2007 au Québec. Nous avons posé quelques questions au sujet du niveau de satisfaction à l'égard des institutions qui s'occupaient des victimes. Parmi les victimes de vol d'identité, le niveau de satisfaction était bien plus élevé envers les banques qu'envers la police.

Je sais qu'il existe un lobby des banques, mais j'aimerais vous dire qu'il faudrait également revoir la manière dont les organisations policières s'occupent des victimes de vol d'identité. Pour bon nombre de policiers, il ne s'agit pas d'un véritable crime. C'est tout à fait faux, car nous savons que le vol d'identité a des incidences à la fois financières mais également psychologiques pour les victimes.

Bien qu'elles soient plus responsables, les banques font un meilleur travail que les policiers lorsqu'elles s'occupent des victimes. Il faudrait peut-être comprendre comment on pourrait faire en sorte que les victimes se sentent mieux accueillies et mieux traitées qu'à l'heure actuelle.

Mme Tilly O'Neill Gordon: Je sais que nous avons couvert bon nombre de thèmes, mais... Vous avez parlé des changements que nous avons apportés en ce qui concerne la sécurité mondiale et des cartes au fil des années. Bien entendu, nous espérons que la même chose surviendra. Si on pouvait apporter un seul changement et le mettre en oeuvre immédiatement, quel serait-il?

M. José Manuel Fernandez: On éduquerait les utilisateurs. On a parlé d'un permis pour naviguer sur Internet. Je ne pense pas qu'il faille forcément restreindre l'accès à Internet, mais le gouvernement devrait prendre l'initiative d'offrir des programmes d'éducation pour les enfants ou les adultes. Je sais que cela relève en partie des provinces, mais le gouvernement fédéral pourrait sûrement faire preuve de leadership en fournissant le contenu.

Et c'est sans doute là où vous vous heurterez à moins de résistance. Personne ne va s'opposer à l'éducation. Il s'agit d'une bonne occasion de faire preuve de leadership.

Si vous décidez de mettre en oeuvre une loi qui nécessitera des mesures d'application, le secteur privé va s'y opposer. Alors optons pour la solution gagnante et misons sur l'éducation.

La vice-présidente (Mme Patricia Davidson (Sarnia—Lambton, PCC)): Nous allons maintenant céder la parole à Mme Borg. Vous avez cinq minutes.

[*Français*]

Mme Charmaine Borg: Je vous remercie.

Ma question s'adresse plutôt à Mme Lawson, puisqu'elle a fait quelques brefs commentaires sur le projet de loi S-4. Cependant, si les autres témoins veulent émettre des commentaires, ce sera un grand plaisir pour moi de les entendre.

En présentant le projet de loi S-4, a-t-on vraiment tout fait pour s'assurer que nos lois en matière de protection des renseignements personnels étaient à jour, afin de bien protéger les Canadiens contre les risques en cette ère moderne? Y a-t-il des éléments qui devraient être ajoutés au projet de loi? Y a-t-il des choses qui ne vont pas assez loin ou d'autres qui ne devraient pas figurer dans le projet de loi?

[*Traduction*]

Mme Philippa Lawson: J'ai déjà mentionné les dispositions relatives au signalement des atteintes et le fait que, à mon avis, elles peuvent être améliorées. Je n'ai pas encore fait un examen complet du dossier mais, en ce qui a trait à l'application, comme je l'ai dit dans mes observations, je pense qu'on pourrait en faire davantage. Par exemple, on pourrait donner plus de pouvoirs en matière d'application à la commissaire à la vie privée ou encore permettre aux gens d'exiger que les organisations rendent des comptes lorsqu'elles ne se conforment pas à leur obligation de protection des renseignements en vertu de la loi.

[*Français*]

Mme Charmaine Borg: Merci beaucoup.

Est-ce que d'autres personnes veulent émettre des commentaires à ce sujet?

M. José Manuel Fernandez: Oui.

Dans le cas des données qui sont dévoilées, il est important qu'il ne s'agisse pas uniquement d'une notification aux usagers. Il faut effectivement qu'il y ait de l'analyse. Or de l'analyse, ça implique peut-être que des corps policiers ou des organismes gouvernementaux enquêtent sur l'incident et en déterminent les causes, qu'il s'agisse de causes technologiques ou d'un manque de diligence quant aux procédures.

Le but n'est pas nécessairement de punir les responsables, mais d'apprendre. Il faut s'assurer, en tant que gouvernement et que société, de converger vers les bonnes façons de faire, celles qui seront les plus efficaces.

Mme Charmaine Borg: Merci beaucoup.

Madame Sproule, vous avez dit que les organismes qui détenaient des renseignements sur l'identité d'une personne avaient une certaine responsabilité quant aux mesures à prendre pour protéger ces renseignements. Évidemment, le gouvernement en fait partie, vu qu'il détient énormément d'information sur les Canadiens. Or on a vu récemment que la faille informatique Heartbleed avait compromis des données personnelles. À ce sujet, j'aimerais proposer la motion suivante:

> Que, dans le cadre de l'étude du problème grandissant du vol d'identité et ses répercussions économiques, et conformément à l'article 108(3)h)(iv) du Règlement, le Comité invite le commissaire par intérim à la protection de la vie privée à discuter de la faille informatique Heartbleed et de ses répercussions sur tous les ministères et agences fédéraux affectés.

Je pense que ce serait important dans le cadre de cette étude, vu qu'il s'agit d'un événement très récent. Nous avons plusieurs questions à poser là-dessus. Quelques membres du comité en ont même posé. Une autre possibilité, que je suggère au comité, serait d'inviter de nouveau des représentants de l'Agence du revenu du Canada.

Je crois être arrivée à la limite de mon temps de parole. Est-ce exact?

● (1245)

[*Traduction*]

La vice-présidente (Mme Patricia Davidson): Il vous reste encore une minute et demie.

[*Français*]

Mme Charmaine Borg: Je vais donc l'utiliser.

Je suis désolée d'avoir eu à déposer cette motion pendant les témoignages. C'est malheureusement la manière dont il faut procéder au sein de ce comité.

J'aimerais poser une dernière question, qui est reliée d'une certaine façon à la motion que je viens de proposer. Pensez-vous que le gouvernement fédéral, avec tous ses ministères, protège bien nos renseignements personnels?

[*Traduction*]

La vice-présidente (Mme Patricia Davidson): Excusez-moi un moment. Pardonnez-moi de vous interrompre. Êtes-vous en train de donner un avis de motion, ou êtes-vous en train de présenter une motion pour qu'on la débatte immédiatement?

Mme Charmaine Borg: Je ne pense pas qu'il serait approprié de la débattre alors que nous sommes encore en train de questionner nos témoins.

La vice-présidente (Mme Patricia Davidson): Très bien. J'avais tout simplement besoin de clarifier ce point.

Mme Charmaine Borg: Très bien, merci.

M. Paul Calandra (Oak Ridges—Markham, PCC): Madame la présidente, je suis prêt à en débattre si elle est prête aussi. Je demanderais que l'on passe à huis clos pour débattre de la motion.

La vice-présidente (Mme Patricia Davidson): Nous sommes saisis d'une motion pour passer à huis clos. Cette motion ne peut être débattue.

M. Paul Calandra: Puisqu'il s'agit d'une motion pour passer à huis clos, j'aimerais remercier les témoins d'être venus.

La vice-présidente (Mme Patricia Davidson): On vient de demander la tenue d'un vote par appel nominal.

(La motion est adoptée par 4 voix contre 3.)

La vice-présidente (Mme Patricia Davidson): Nous allons lever la séance pour quelques minutes afin de pouvoir passer à huis clos. Avant, j'aimerais remercier tous nos témoins d'être venus. Les exposés ont été fort intéressants, et nous vous remercions tous les quatre d'être venus. Vos témoignages nous ont donné un point de vue un peu différent que ceux que nous avions déjà entendus. Merci beaucoup d'être venus.

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