CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 155 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mercredi 3 avril 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le mercredi 3 avril 2019

● (1610)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Je constate qu'il y a quorum.

Je vois aussi qu'il est 16 h 10 et que nous devons voter à 17 h 45. Cela étant, nous devrions probablement avoir terminé à 17 h 30, ou un peu plus tard, mais guère plus.

Nous accueillons M. Smolynec, du Commissariat à la protection de la vie privée...

M. Gregory Smolynec (sous-commissaire, Secteur des politiques et de la promotion, Commissariat à la protection de la vie privée du Canada): C'est exact.

Le président: ... et Mme Fournier-Dupelle.

Je vais les inviter à faire leur déclaration liminaire. Le témoin de la TD qui est sur le point d'arriver craint que la déclaration de la TD ne soit un peu différente de ce que le Commissariat à la protection de la vie privée a à dire.

Je vais y aller à l'inspiration et voir si nous allons regrouper ces deux témoins ou les entendre l'un après l'autre.

Sur ce, je vous invite à faire votre déclaration préliminaire.

[*Français*]

M. Gregory Smolynec: Bonjour, monsieur le président et membres du Comité.

Je vous remercie de l'invitation à comparaître devant vous aujourd'hui. Je suis reconnaissant de l'occasion qui m'est offerte, étant donné que votre étude porte sur des questions qui concernent les Canadiens et le Commissariat.

Je tiens à réitérer les préoccupations que j'ai exprimées lorsque j'ai comparu devant le Comité sénatorial permanent des banques et du commerce dans le cadre de son étude sur le système bancaire ouvert, à savoir que le secteur financier doit être édifié sur des assises qui comprennent le respect de la vie privée et d'autres droits fondamentaux. Les banques et les autres institutions financières doivent être dotées de normes rigoureuses en matière de cybersécurité et de protection de la vie privée.

Il est important d'expliquer la distinction entre une atteinte à la vie privée et une atteinte à la sécurité, car les deux termes sont souvent utilisés de façon interchangeable.

Une atteinte à la sécurité est un incident qui donne lieu à un accès non autorisé à des données, des applications, des services, des réseaux ou des dispositifs par le contournement des mécanismes de sécurité sous-jacents. Une atteinte à la vie privée se définit comme la perte ou la communication non autorisée de renseignements personnels, ou l'accès non autorisé à ceux-ci, peu importe les moyens utilisés. Une atteinte à la vie privée est plus vaste et peut se produire sans compromettre les systèmes de sécurité.

C'est bien là le défi. La cybersécurité et la protection de la vie privée se chevauchent dans une certaine mesure, parce que la première peut aider à protéger la seconde, mais, dans certains cas, la cybersécurité peut créer des risques pour la protection de la vie privée. Par exemple, il faudra veiller de près à ce que les stratégies et activités de cybersécurité ne conduisent pas à la mise en œuvre de régimes de surveillance massive visant un monitorage ou une analyse illimités et ininterrompus des renseignements personnels des individus.

Les secteurs privé et public ont l'obligation de signaler des atteintes à la sécurité et à la vie privée. En vertu de la Loi sur la protection des renseignements personnels dans le secteur public, cette obligation est prévue dans la politique du Conseil du Trésor, qui exige que le Commissariat soit avisé des atteintes substantielles à la vie privée. Une atteinte est dite « substantielle » si elle concerne des renseignements personnels de nature délicate, si elle peut vraisemblablement causer un préjudice ou mettre en cause un grand nombre de personnes.

Du côté du secteur privé, la Loi sur la protection des renseignements personnels et les documents électroniques exige que les organisations signalent les attaques aux mesures de sécurité concernant les renseignements personnels qui présentent un risque réel de préjudice grave pour les personnes. Les organisations doivent aviser les personnes touchées de ces atteintes et tenir un registre de tous ces incidents.

● (1615)

[*Traduction*]

L'affaire de l'Agence mondiale antidopage — aussi connue sous l'acronyme AMA — est un exemple d'atteinte très médiatisée à la vie privée. À la suite d'une attaque par hameçonnage en 2016, la base de données de l'AMA contenant des renseignements personnels de nature extrêmement délicate sur les athlètes a été compromise par des agents du renseignement militaire russe qui ont, par la suite, transféré certaines de ces données dans le domaine public, menaçant d'en publier d'autres.

Dans le cadre de notre enquête sur l'AMA, nous avons conclu que les mesures de cybersécurité devraient être proportionnelles à la fois à la sensibilité des renseignements personnels protégés et à l'intérêt de ces renseignements pour les acteurs malveillants. Ce raisonnement s'applique également à la cybersécurité dans le secteur financier. La Cour suprême du Canada a statué que les renseignements financiers sont effectivement de nature délicate. D'autres atteintes importantes dont les gens se rappellent concernent Equifax, Ashley Madison et le système de paie Phénix.

Depuis que la déclaration des atteintes à la vie privée dans le secteur privé est obligatoire, le 1er novembre 2018, nous avons constaté que le nombre de signalements provenant du secteur privé a été multiplié par près de quatre. Nous pouvons maintenant compter sur un historique représentant plus de six mois de déclarations d'atteintes à la sécurité des données dans le secteur privé, et beaucoup plus longtemps dans le secteur public, ce qui nous a permis d'émettre un certain nombre d'observations. Cela englobe les institutions qui ne sont pas toujours au courant des renseignements personnels qu'elles détiennent, de l'endroit où ils sont acheminés et des personnes qui y ont accès. Souvent, dans la course à la protection contre les pirates informatiques, la menace interne est négligée; pourtant, les atteintes à la vie privée impliquent non seulement la perte de renseignements personnels au profit de forces externes, mais aussi un accès inapproprié par des acteurs internes. Les exigences de déclaration obligatoire des atteintes peuvent permettre aux institutions de répondre au caractère adéquat — ou à son absence — des plans et des préparatifs en matière de cybersécurité. De plus, les fonctionnaires travaillant pour le Commissariat utilisent ces connaissances pour fournir des orientations aux organisations.

Pour le Commissariat et les Canadiens, le défi consiste à suivre le rythme de l'évolution de la technologie. II est tout aussi difficile de comprendre comment les données personnelles seront utilisées, par qui, et à quelle fin. Même s'il est vrai que les politiques de confidentialité sont rarement lues, nous arrivons peut-être à une époque où la façon dont les données sont utilisées est tout aussi mal comprise. Le Commissariat a examiné les notions de consentement dans ce domaine et a récemment émis des lignes directrices à l'intention des organisations assujetties à la LPRPDE sur la meilleure façon d'obtenir un consentement valable pour l'utilisation des renseignements personnels.

Comme d'autres l'ont indiqué devant le Comité, nous croyons préférable d'aborder ces questions en collaboration. À cette fin, nous collaborons à des enquêtes conjointes avec d'autres bureaux de protection de la vie privée et des données. Nous participons aux ratissages du « Global Privacy Enforcement Network », et nous avons constaté que cela permet l'échange de pratiques exemplaires. Le Commissariat est aussi membre du groupe du réseau des analystes en cybersécurité, présidé par Sécurité publique Canada, et auquel participent d'autres ministères fédéraux. Notre Direction des services-conseils au gouvernement fournit également des conseils aux intervenants du gouvernement fédéral dans ce domaine. D'autres solutions comprennent l'éducation et la sensibilisation auprès des entreprises, en particulier les petites et moyennes entreprises, qui ont souvent du mal à s'assurer que leurs renseignements, y compris leurs renseignements personnels, soient adéquatement protégés.

En conclusion, les organismes de réglementation et les défenseurs de la protection de la vie privée ont un rôle à jouer pour veiller à ce que les stratégies, les principes, les plans d'action et les activités de mise en oeuvre en matière de cybersécurité favorisent la protection de la vie privée en tant que principe directeur et norme durable. Nous devons réformer notre législation sur la protection des renseignements personnels afin de l'adapter à notre objectif, qui est d'assurer la protection de la vie privée des Canadiens à mesure que les technologies et l'économie évoluent.

Je serai heureux de répondre à vos questions.

● (1620)

Le président: Merci, monsieur Smolynec.

Avant de céder la parole à M. de Burgh Graham pour ses sept minutes de questions, j'aimerais faire une mise au point pour mes collègues. La TD craint de devoir s'asseoir à la même table qu'un organisme de réglementation. Je pense que nous devrions respecter cette façon de voir et je vais donc devoir diviser le temps en deux. Cela étant dit, les membres du Comité n'auront pas autant de temps pour poser des questions au Commissariat à la protection de la vie privée, ce que je trouve regrettable.

M. David de Burgh Graham (Laurentides—Labelle, Lib.): Monsieur le président, j'ai une brève question.

Je n'ai jamais vu de précédent où des témoins ont demandé à être séparés ainsi. Nous recevons souvent des témoins d'avis contraires dans un même groupe. Je ne vois pas pourquoi il faudrait agir ainsi, compte tenu du temps dont nous disposons.

Le président: Ce n'est pas tant que les témoins s'opposeraient, et sur ce point, je serai plutôt d'accord avec vous, mais il s'agit d'une institution financière qui se trouverait au côté d'un de ses organismes de réglementation à la table des témoins. C'est une préoccupation qui a été soulevée par l'institution financière. C'est un problème de perception, pour ne pas dire un vrai problème.

Il est donc difficile de prévoir du temps pour certaines questions...

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): À quelle heure devons-nous terminer, monsieur le président?

Le président: Je ne fais que calculer. Nous devons avoir terminé à 17 h 30. Ce sera assez difficile, parce qu'il y aura un vote à 17 h 45. Nous pourrions forcer le train...

M. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, PCC): Le vote aura lieu à 18 heures. La sonnerie retentira à 17 h 30.

Le président: Eh bien, si mes collègues donnent au président la possibilité de prolonger les audiences...

Un député:*[Inaudible]*

Le président: Très bien. Merci beaucoup.

Commençons par des tours de six minutes, parce que, dans tous les cas, nous allons devoir réduire...

M. Glen Motz: Il faut avoir terminé à 16 h 55, et les témoins suivants devront être là.

Le président: Oui, c'est à peu près cela.

M. Glen Motz: Oui.

Le président: Commençons par des questions de six minutes. Nous passerons ensuite à un tour de quatre minutes chacun, et nous verrons où ça nous amène.

Monsieur de Burgh Graham.

M. David de Burgh Graham: Merci.

Pour commencer, vous avez parlé de l'augmentation massive du nombre d'incidents signalés. Je m'intéresse davantage aux incidents non signalés. Avons-nous un moyen d'évaluer combien il y en a? Et comment pouvons-nous faire en sorte qu'il n'y ait plus d'incidents non signalés, que tous le soient?

M. Gregory Smolynec: Je ne vois pas, a priori, comment mesurer les incidents non signalés. Ce seraient des estimations plus qu'approximatives. Nous avons une comparaison fondée sur ce qui a été déclaré volontairement avant le 1er novembre. Nous avons maintenant quelques indications sur ce qui a été signalé depuis cette date.

Avons-nous étudié cette question...

Mme Leslie Fournier-Dupelle (analyste stratégique des politiques et de la recherche, Commissariat à la protection de la vie privée du Canada): Dans le secteur public, nous avons constaté que des institutions détenant des renseignements personnels font parfois des sous-déclarations, d'après des impressions tirées à la lecture d'autres rapports. Le cas échéant, nous communiquons alors avec elles pour leur suggérer une formation sur les infractions. Parfois, les infractions sont publiées dans les médias comme étant des « incidents touchant à la sécurité », tandis qu'il s'agit en fait d'atteintes à la vie privée ou qu'il en va de la protection des renseignements personnels. Nous communiquons avec les institutions ou les entreprises. Nous avons donc des impressions, mais nous ne pouvons mesurer ce que nous ignorons. Quand nous aurons plus de rapports, nous serons peut-être en mesure de suivre plus attentivement les tendances.

M. David de Burgh Graham: D'accord.

Lors de notre dernière réunion, nous avons eu une discussion approfondie avec les gens de Mastercard au sujet des systèmes de la compagnie. M. Dubé et moi-même avons beaucoup parlé du fait que les données sont traitées aux États-Unis, ce qui, du point de vue technologique, est très logique, mais qui soulève des préoccupations évidentes du point de vue de la protection des renseignements personnels, surtout au regard du U.S. PATRIOT Act. Comment, selon vous, devrions-nous traiter cette question et les données qui transitent par des pays étrangers.

M. Gregory Smolynec: Nous sommes en train d'examiner de près nos directives sur la circulation transfrontalière des données. Nous avons l'intention, dans un proche avenir, de mener de vastes consultations sur ces directives. C'est un problème réel pour notre bureau. Nous y réfléchissons en profondeur et essayons de solliciter l'avis de divers intervenants.

M. David de Burgh Graham: Nous n'avons donc pas de réponses claires pour l'instant, mais plus tard peut-être.

M. Gregory Smolynec: Oui.

M. David de Burgh Graham: Que ce soit sous l'actuelle législature ou la prochaine, quand vous aurez des réponses, pourriez-vous les faire parvenir au Comité?

M. Gregory Smolynec: Bien sûr.

M. David de Burgh Graham: Je vous en serais reconnaissant. Merci.

J'ai une dernière question. Pour gagner du temps, je partagerai ensuite le temps qu'il me reste avec M. Picard.

Peut-on protéger les renseignements personnels sans sécurité?

● (1625)

M. Gregory Smolynec: Je dirais oui, a priori, car j'imagine des circonstances où la sécurité des données n'est pas primordiale pour celle ou celui qui veut préserver tel ou tel aspect de son identité ou de ses renseignements personnels. On pourrait alors qualifier les dérapages d'incident de sécurité, mais il s'agirait davantage d'un incident lié à la protection de la vie privée. Il pourrait s'agir d'une question de protection de la vie privée quand une personne a, par exemple, accès légalement à un espace sans que les habilitations de sécurité soient un facteur pas plus dans un lieu de travail, dans un foyer que dans un quartier.

M. David de Burgh Graham: Pas vraiment. Il y a des cas limites où, en théorie, la vie privée n'est pas protégée. À la base, s'il n'y a pas de sécurité pour protéger la vie privée, la notion de vie privée est plus ou moins vide de sens en technologie.

M. Gregory Smolynec: Je ne dirais pas cela. Il pourrait y avoir des cas où des gens fouillent dans les renseignements personnels d'autres personnes sans pour autant franchir de barrières physiques ou d'autres obstacles à la sécurité. Il s'agirait malgré tout de violations de la vie privée, sans qu'il y ait pour autant atteinte à la sécurité.

M. David de Burgh Graham: Merci.

[*Français*]

M. Michel Picard (Montarville, Lib.): Bonjour.

Je vous soumets un scénario.

À l'ère des nuages numériques, par exemple iCloud, des informations sur des Canadiens sont entreposées sur des serveurs appartenant à des entreprises canadiennes à l'étranger ou sur des serveurs appartenant à des entreprises étrangères. Dans les deux cas, ces informations se trouvent sur des serveurs ailleurs qu'au Canada et qui appartiennent à des propriétaires différents.

Quelle est la capacité du Canada à légiférer sur ces informations qui sont à l'étranger et sur ces tierces parties qui ne sont pas nécessairement canadiennes? Quelles sont les limites de la législation canadienne? Quelles sont vos recommandations?

M. Gregory Smolynec: Premièrement, si des renseignements personnels de Canadiens sont en cause, ces entreprises étrangères sont assujetties aux lois canadiennes. Les lois canadiennes qui s'appliquent au secteur privé énoncent qu'il faut absolument obtenir le consentement exprès des Canadiens pour transmettre leurs données à l'étranger.

Deuxièmement, il y a des limites. Il y a certainement des évolutions technologiques et des modèles d'affaires à grande échelle, et c'est compliqué, mais les lois s'appliquent.

Le président: Merci, monsieur Picard.

Monsieur Paul-Hus, vous avez six minutes, s'il vous plaît.

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

J'ai manqué la dernière question. Je vais peut-être poser une question similaire.

Des entités étrangères contribuent à nos réseaux et à nos infrastructures de télécommunications. Actuellement, la protection de la vie privée soulève des préoccupations lorsque des entités possédant leur propre infrastructure au Canada sont contrôlées par des pays qui ont des règles différentes des nôtres. Avez-vous la même inquiétude?

M. Gregory Smolynec: Cela dépend de chaque cas.

M. Pierre Paul-Hus: Je vais donner un exemple concret. On parle beaucoup de la compagnie chinoise Huawei et de son infrastructure 5G, qui suscite de l'inquiétude. La Chine pourrait décider de déployer son infrastructure Huawei au Canada. Le Commissariat a-t-il discuté de cette inquiétude avec le gouvernement?

M. Gregory Smolynec: Oui. Étant donné que des renseignements personnels circulent sur les réseaux 5G, il y a certainement des intérêts ou des questions liés à la protection de la vie privée. C'est assez évident.

Il faut donc s'assurer que ces réseaux seront sécuritaires et adéquatement protégés contre toutes sortes de menaces, et sûrement contre des menaces connues. Quant aux entreprises d'autres pays, nous n'avons pas la compétence nécessaire pour faire cette analyse.

● (1630)

M. Pierre Paul-Hus: J'ai parlé de la compagnie chinoise Huawei, mais je vais vous ramener à la question plus générale. Selon votre mandat de protection des renseignements des Canadiens, surveillez-vous l'ensemble des infrastructures au Canada?

M. Gregory Smolynec: Oui.

M. Pierre Paul-Hus: Vous avez le devoir d'informer le gouvernement des différents dangers. Le faites-vous?

M. Gregory Smolynec: Oui.

M. Pierre Paul-Hus: D'accord.

Je vais maintenant parler des appareils mobiles. Mon iPhone fait de la reconnaissance faciale. Apple dit qu'il n'y a pas de danger et que l'information reste dans le téléphone. J'ai de la misère à croire cela. Vous penchez-vous sur la question des appareils mobiles, de la reconnaissance visuelle et par la rétine et sur l'information qui pourrait être transmise à des compagnies?

M. Gregory Smolynec: Oui, certainement.

Nous faisons des analyses techniques. Nous avons la Direction de l'analyse de la technologie.

M. Pierre Paul-Hus: Êtes-vous en mesure de nous dire si nous sommes protégés ou s'il y a des risques?

M. Gregory Smolynec: Cela dépend de l'appareil en particulier.

M. Pierre Paul-Hus: D'accord.

Vous ne pouvez pas me dire s'il y a des compagnies qui présentent plus de risques que d'autres?

M. Gregory Smolynec: Je ne peux pas pour l'instant, pas ici, non.

M. Pierre Paul-Hus: D'accord.

Cependant, c'est le genre d'information qui existe et que le gouvernement possède.

M. Gregory Smolynec: Nous avons une capacité limitée aussi. Pour l'instant, six personnes travaillent à la Direction de l'analyse de la technologie. Il n'y a donc pas une capacité énorme pour analyser tous les appareils, tous les réseaux, tous les...

M. Pierre Paul-Hus: Avez-vous de l'information qui vous dit qu'actuellement, par exemple, mon visage est enregistré et que cet enregistrement est transféré dans une base de données quelque part? D'après vous, est-ce que cela se fait?

M. Gregory Smolynec: En ce qui a trait à votre téléphone personnel, non. Toutefois, il y a d'autres enquêtes relatives à la reconnaissance visuelle.

M. Pierre Paul-Hus: Par exemple, des appareils qui peuvent se trouver sur des portes ou d'autres systèmes.

M. Gregory Smolynec: Oui.

M. Pierre Paul-Hus: D'accord.

Les lois actuelles, au Canada, sont-elles assez fortes pour s'attaquer à des organisations ou à des particuliers qui se servent de renseignements personnels à mauvais escient?

M. Gregory Smolynec: Le commissaire Therrien a déjà déclaré que nos lois doivent être mises à jour et réformées en ce qui concerne la protection de la vie privée dans les domaines public et privé. Il faut sûrement entreprendre la tâche de réformer nos lois.

M. Pierre Paul-Hus: Dans votre déclaration d'ouverture, vous mentionnez que les avancées technologiques sont très rapides actuellement. Pensez-vous justement que nos lois et votre organisme sont alignés sur l'ensemble de ce qui se passe, ou sommes-nous en retard?

M. Gregory Smolynec: Nous sommes sûrement en retard sur le plan législatif. Selon nous, la priorité est de mettre nos lois à jour ainsi que d'adopter d'autres mesures pour avoir des lois fondées sur les droits concernant la protection de la vie privée.

M. Pierre Paul-Hus: Je vous remercie.

[*Traduction*]

Le président: Vous pourrez donner vos 20 secondes à M. Motz au prochain tour.

Monsieur Dubé, vous avez six minutes.

[*Français*]

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

Je remercie les témoins d'être présents aujourd'hui.

[*Traduction*]

Avec tout le respect que je dois à nos témoins, avant de poser mes questions, j'ai eu l'occasion d'envoyer un avis de motion à mes collègues. Je comprends que je ne suis pas dans le délai de 48 heures, mais je voulais profiter de mon temps de parole pour lire ma motion et en expliquer la raison en 30 secondes ou moins. La voici:

> Que, conformément à l'article 108(2) du Règlement, le Comité invite le ministre de la Sécurité publique et de la Protection civile à comparaître, au plus tard le vendredi 21 juin 2019, afin de réagir au Rapport public de 2018 sur la menace terroriste pour le Canada déposé au Parlement le mardi 11 décembre 2018 et de répondre aux questions des membres.

Voici rapidement, et pour le bénéfice de mes collègues, le raisonnement qui sous-tend cette motion. Des représentants de certains groupes nommés dans ce rapport nous ont dit qu'ils s'inquiètent des répercussions possibles. Quand on songe à certaines activités terroristes commises ici et à l'étranger contre des groupes religieux et d'autres milieux, il est assez clair qu'il faut repenser la façon dont ces groupes sont mentionnés dans ces rapports et mieux comprendre la philosophie qui les anime.

Je comprends que tout cela est fondé sur les renseignements de nos services de sécurité nationale, mais en même temps, c'est le gouvernement qui est responsable de déposer le rapport à la Chambre. Nous envisageons d'avoir un dialogue avec le ministre à ce sujet, compte tenu des préoccupations soulevées, comme par la communauté sikhe. Au moment opportun, je proposerai que la motion soit débattue et, je l'espère, approuvée.

● (1635)

[*Français*]

Cela étant dit, je vous remercie de votre indulgence. Je profitais simplement de cette occasion.

J'ai quelques questions à vous poser.

Il est souvent question d'appareils, « *the Internet of Things* », selon l'expression anglaise. Vous avez mentionné que plusieurs entreprises ne sont pas au courant de toutes les données dont elles disposent ou que, parfois, elles le savent très bien, mais qu'elles les gardent malgré tout, même si ces données ne sont pas pertinentes.

Ma question est liée à certaines posées un peu plus tôt.

Lorsque les gens téléchargent des applications sur leur téléphone, ils se rendent rarement compte qu'ils accordent des permissions qui sont assez étendues quant à ce qui se retrouve sur l'appareil. Quelles sont les répercussions de cela, notamment en ce qui concerne notre étude? Par exemple, lorsqu'on utilise des applications bancaires ou encore une empreinte digitale pour accéder à un compte, quel est l'impact de cette utilisation des appareils?

M. Gregory Smolynec: Vous soulevez une question très pertinente. Elle touche l'éducation du public. Même pour des gens qui sont informés au sujet de l'informatique, il y a toutes sortes de détails qui ne sont pas visibles et évidents. Le Commissariat et le gouvernement en général devraient donc nécessairement faire de l'éducation pour informer les gens des problèmes potentiels de perte de leurs renseignements personnels dans plusieurs situations.

M. Matthew Dubé: En ce qui concerne l'éducation du public, on fait souvent le parallèle avec les exigences gouvernementales règlementaires pour ce qui est des voitures. Par exemple, s'il y a un rappel sur un modèle de véhicule pour une raison qui pourrait nuire à la sécurité, on fait beaucoup d'efforts pour nous en informer, on communique l'information dans les médias, on appelle les clients, on envoie un courriel et même du courrier traditionnel.

Croyez-vous qu'il devrait y avoir un peu plus d'exigences quand il y a une mise à jour du logiciel d'un téléphone? À moins qu'on suive des sites Web ou des sites abonnés à Gizmodo ou autre, c'est rare que l'on connaisse la raison précise pour laquelle il y a une mise à jour de l'iOS, par exemple dans le cas d'un appareil téléphonique.

M. Gregory Smolynec: C'est lié à la question du consentement. Si quelqu'un est au courant de changements, de nouveaux logiciels, de nouvelles techniques, et si un changement substantiel est apporté, il faut absolument avoir un nouveau consentement exprès de la part des individus. Effectivement, s'il y a des changements techniques, il faut communiquer avec les consommateurs pour les informer de ce qui a changé et de l'effet qui en découle.

M. Matthew Dubé: Merci.

J'ai deux autres questions à vous poser.

En ce qui concerne les exigences actuelles, les amendes par exemple, dans le cas de divulgation, de fuites de données, les mécanismes en place sont-ils suffisants?

Ensuite, je vais revenir à ce que vous avez dit plus tôt. Serait-il nécessaire de revoir les ressources qui sont accordées au Commissariat, à la suite de l'évolution de la technologie, entre autres par l'entremise de l'étude que nous faisons en ce moment?

M. Gregory Smolynec: Oui, sûrement.

Les pouvoirs du commissaire et du Commissariat ne sont pas adéquats pour affronter les problèmes qu'on voit dans le commerce, dans la société en général. Il faudrait donc améliorer nos lois, parmi d'autres choses, donner des pouvoirs au commissaire, par exemple celui d'imposer des amendes et des sanctions.

● (1640)

[*Traduction*]

Le président: Merci, monsieur Dubé.

Monsieur Picard, vous avez six minutes.

M. Michel Picard: Je vais céder mon temps de parole à Mme Dabrusin.

Le président: Madame Dabrusin, vous avez six minutes.

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

Ma première question porte sur les prêteurs, parce que nous avons parlé des institutions financières et des banques. J'espère que vous pourrez préciser s'il y a des différences dans les règles qui s'appliquent aux institutions financières. Je sais, par exemple, que le BSIF couvre les banques, mais pas les institutions prêteuses. Y a-t-il des différences, et cela vous inquiète-t-il, du point de vue de la protection de la vie privée, alors que nous étudions la question de la cybersécurité?

M. Gregory Smolynec: Notre bureau a le mandat d'examiner les institutions sous réglementation fédérale comme les banques. Il est aussi appelé à jouer un rôle de surveillance des banques et de protection de la vie privée dans les banques.

J'ajouterais que le monde bancaire est en train de changer. Il est possible de bénéficier de services bancaires ouverts dans d'autres pays, ce qui va bientôt se faire au Canada aussi et qui changera les modèles d'affaires et la façon dont les renseignements personnels et les données circulent entre institutions financières. Cela aussi sera lourd de conséquences.

En fin de compte, les normes, les règlements et les lois doivent être adaptés à cette évolution, qui est à la fois technologique et commerciale. Ces instruments devront être en place avant que des changements majeurs ne soient apportés.

Mme Julie Dabrusin: Je comprends ce que vous dites au sujet des services bancaires ouverts, mais je parle des entreprises installées au coin de la rue. Je ne veux pas donner de noms précis, mais je parle de ces lieux fréquentés par ceux qui n'ont pas vraiment de compte bancaire et qui vont y déposer un chèque pour récupérer du liquide à un taux d'intérêt coquet. Comme ces entreprises ne sont pas des banques, elles échappent à ce règlement. Je me demande si vous avez quelque chose à dire à ce sujet en ce qui concerne la protection de la vie privée.

M. Gregory Smolynec: Le contexte général, c'est que ces entreprises sont assujetties à notre loi sur le secteur privé ou à des lois provinciales qui sont essentiellement semblables. Elles sont assujetties à la loi, mais je ne peux pas vous en parler.

Mme Julie Dabrusin: Elles ne relèvent pas de votre compétence. Est-ce que vous les examinez également?

M. Gregory Smolynec: Oui, nous le faisons dans les cas où les lois provinciales ne sont pas foncièrement semblables.

Mme Julie Dabrusin: Il y a quelque temps, nous avons parlé avec des gens de HackerOne. Ils nous ont suggéré de songer à une mesure législative qui permettrait ce qu'ils ont appelé des « chapeaux blancs » — j'aimerais trouver un meilleur terme pour décrire des « bons pirates » — qui aideraient à s'attaquer aux systèmes et à découvrir où se trouvent les problèmes.

Que pensez-vous de la protection de la vie privée? Si nous devions créer ce genre de loi, quel genre de protection devrions-nous envisager pour autoriser des personnes qui ne font pas partie du secteur public, par exemple, à chercher comment pirater nos systèmes?

M. Gregory Smolynec: Dans ma déclaration liminaire, j'ai parlé du renforcement de la cybersécurité et de la protection de la vie privée et du fait que ces deux pôles pourraient se renforcer mutuellement. Mais il y a aussi des occasions où une cybersécurité excessive ou inappropriée pourrait avoir des répercussions sur la vie privée.

Dans quelle mesure un chapeau blanc, un hacker éthique, peut-il protéger la vie privée des gens? Il ne devrait pas avoir accès aux renseignements personnels s'il pratique cette forme de piratage au nom de la cybersécurité. Du point de vue de la protection de la vie privée, il ne serait pas convenable que des gens travaillant à l'amélioration de la cybersécurité violent la vie privée.

Mme Julie Dabrusin: Je vois. J'essaie simplement de déterminer quels genres de protections nous pourrions mettre en place pour permettre une telle chose, si nous devions opter pour la proposition des gens de HackerOne. Je ne me souviens pas de ce qu'ils ont suggéré, mais on récompenserait les pirates éthiques, les chapeaux blancs, qui trouveraient des failles dans un système, cela pour attirer des hackers imaginatifs.

Le problème, je suppose, c'est qu'une fois qu'ils ont pénétré un système, ils peuvent avoir accès à des renseignements personnels. Auriez-vous des pistes de réflexion à nous suggérer pour prévoir des protections?

● (1645)

M. Gregory Smolynec: Il y a peut-être des façons de faire dans un environnement expérimental qui n'exposerait pas de vrais renseignements personnels. Dans l'armée et dans d'autres organisations, et dans certains cas... dans l'univers de la protection de la vie privée aussi, on peut simuler des attaques cybernétiques dans un espace protégé. Ce serait peut-être une chose à étudier. Dans le monde de la protection de la vie privée, il y a même des jeux de guerre.

Mme Julie Dabrusin: Je vois qu'il me reste 30 secondes. Je vais les donner...

Le président: Vous allez les donner à M. Motz qui adore cela.

Mme Julie Dabrusin: Je voulais les verser dans le bassin commun. Je pourrais en parler pendant les 20 prochaines secondes.

Le président: Il y a un plus et un moins ici, monsieur Motz.

Vous avez quatre minutes. C'est à vous.

M. Glen Motz: Merci, monsieur le président.

Merci aux témoins.

J'aimerais poursuivre dans la même veine que Mme Dabrusin.

Le Canada ferait-il mieux de conclure une entente sur la divulgation des vulnérabilités avec ce que j'appellerais des « acteurs éthiques », afin que tout le monde soit protégé en cas de failles dans les systèmes d'une entreprise, pour que celles-ci soient corrigées avant que quelqu'un ne les exploite. Si je vous comprends bien, ce serait avantageux pour tous les Canadiens.

M. Gregory Smolynec: Ni mon bureau ni moi n'avons envisagé les conséquences du piratage éthique ou du piratage des chapeaux blancs pour pouvoir vous donner une réponse détaillée. Nous pourrions nous engager à examiner cette question et à revenir devant le Comité avec une réponse plus réfléchie.

M. Glen Motz: À mon âge, je sais qu'il m'arrive d'oublier des témoignages, mais nous avons entendu des personnes — et les gens de HackerOne en faisaient partie — qui font un excellent travail sur le plan éthique pour protéger les consommateurs.

Si le gouvernement actuel ou le prochain cherche à protéger les Canadiens contre des répercussions économiques négatives en améliorant notre cybersécurité, je pense que nous devrions savoir quelles mesures de protection adopter face à ces personnes. Qu'en pensez-vous?

M. Gregory Smolynec: Notre intérêt serait de veiller à ce que la vie privée des gens soit protégée, peu importe... Il faudrait peut-être songer à réaliser un équilibre entre les divers intérêts entrant en jeu, mais dans ce contexte, je dirais que la vie privée des citoyens doit être protégée comme il se doit.

M. Glen Motz: Oui, je suis d'accord. Je suppose que c'est un peu comme la sécurité nationale dans une certaine mesure. Il y a un équilibre entre la nécessité de protéger la vie privée et la nécessité de protéger la sécurité nationale. Dans le même ordre d'idées, si nous avions un pirate éthique capable de protéger... S'il existait une structure régissant le fonctionnement des pirates éthiques, des mesures pour les protéger et protéger les données des consommateurs, nous devrions peut-être envisager cette formule.

Je vais passer à un autre type de questions.

Vous avez formulé un certain nombre de recommandations devant le Comité sénatorial des banques, notamment que votre bureau soit investi de pouvoirs d'application de la loi, dont la possibilité de vérifier la conformité de façon indépendante, sans motif préalable, pour que les organismes puissent être effectivement tenus responsables de la protection des renseignements personnels qu'ils détiennent. Depuis que vous avez fait cette recommandation au Sénat, avez-vous constaté une résistance dans le secteur privé?

M. Gregory Smolynec: Non, aucune.

M. Glen Motz: À quoi ressemblerait le pouvoir d'application de la loi dont serait doté le Commissariat à la protection de la vie privée?

M. Gregory Smolynec: Pardon?

M. Glen Motz: Selon vous, comment ces pouvoirs seraient-ils appliqués par le Commissariat à la protection de la vie privée?

M. Gregory Smolynec: C'est quelque chose qui existe au Royaume-Uni, et nous examinons de près ce qui se fait là-bas dans ce domaine d'application de la loi afin de comprendre l'expérience britannique en matière d'inspections aléatoires.

M. Glen Motz: J'ai une dernière question.

Lundi, je crois, un témoin a qualifié les Canadiens de naïfs à propos de leur propre cybersécurité. De votre point de vue, monsieur, qu'est-ce qui doit changer au Canada pour que les citoyens soient plus vigilants à l'égard de la cybersécurité, et donc de leur propre vie privée? Vous avez mentionné quelque chose à M. Dubé à ce sujet, mais pourrait-on agir de manière plus précise en ce qui vous concerne, du point de vue législatif ou autre?

● (1650)

M. Gregory Smolynec: Je dirais que l'objectif numéro un, la grande priorité, serait de réformer la loi sur la vie privée, d'entreprendre une réforme fondée sur les droits.

Le président: Expliquez-nous cela très brièvement.

M. Gregory Smolynec: À l'heure actuelle, le droit régissant le secteur privé est fondé sur des principes et, en un sens, il est très vaste. Soit dit en passant, il est question de droit à la vie privée des Canadiens, mais une loi fondée en droit reconnaîtrait, comme le fait le Canada, que la vie privée est un droit de la personne internationalement reconnu et que des droits procéduraux sont associés aux droits de la personne. La loi reconnaîtrait également que les secteurs public et privé dans leur ensemble seraient visés. Les Canadiens devraient être informés de leurs droits et de la façon de les exercer. C'est à la fois un défi législatif et un défi connexe d'éducation du public.

M. Glen Motz: Avec des droits et des responsabilités?

Le président: Merci, monsieur Motz.

Je pense que vous avez utilisé le temps supplémentaire de M. Paul-Hus et de Mme Dabrusin.

M. Glen Motz: Merci, je vous remercie de votre indulgence.

Le président: Monsieur Graham, les quatre dernières minutes vous reviennent. Allez-y.

M. David de Burgh Graham: Merci.

Ce n'est pas directement lié à vous, mais j'aimerais profiter de l'occasion pour tirer au clair certaines questions qui reviennent sans cesse.

Chapeau noir et chapeau blanc sont des termes qui ont cours depuis longtemps dans le milieu de la haute technologie. Je tenais à le souligner, étant donné qu'il y a confusion à ce sujet. Il y a aussi des chapeaux gris, et nous pourrions en discuter en long et en large.

Je veux aussi m'assurer que tout le monde soit au courant de la différence entre « pénétrer » et « pirater » un réseau. Dans le premier cas, on s'infiltre dans un réseau sans intention de le pervertir tandis que, dans le second, l'intention est malveillante. Je tenais à ce que cette distinction soit claire.

Le président: Je ne verrai plus jamais les choses de la même façon.

M. David de Burgh Graham: Je l'espère.

J'aimerais revenir à vous pour un instant. Vous avez dit que vous aviez une division de recherche technique composée de six personnes. Quel genre d'expertise ont-elles? Envisagent-elles de démonter des serveurs, des réseaux et des routeurs? De quel genre de personnes parle-t-on et que font-elles?

M. Gregory Smolynec: Nous avons un petit groupe de technologues, de scientifiques et d'ingénieurs. Ils examinent des appareils caractéristiques de grands systèmes comme l'Internet des objets. Ils participent à l'élaboration de lignes directrices, par exemple, sur la biométrie, la dépersonnalisation, l'Internet des objets et les risques et vulnérabilités en matière de vie privée associés aux nouvelles technologies. Ils nous aident dans nos enquêtes en effectuant des analyses judiciaires, et nous sommes en train de nous doter d'une capacité pour la conservation des preuves, etc. Cela fait partie de notre programme d'enquête.

Il s'agit d'une vaste gamme d'activités et de tâches qui dépassent de loin la capacité de la petite équipe — bien que très capable en partant —, mais on ne parle que de six personnes et d'un petit laboratoire.

M. David de Burgh Graham: D'accord. C'est un laboratoire complet, mais pas très grand.

M. Gregory Smolynec: Nous avons un petit laboratoire pour faire des expériences hors ligne afin de protéger nos réseaux et les réseaux gouvernementaux.

M. David de Burgh Graham: Si ces experts démontent un téléphone, par exemple, et y trouvent une importante vulnérabilité en matière de protection de la vie privée, quelle serait leur ligne de conduite?

M. Gregory Smolynec: Cela dépendrait du contexte. Si c'était dans le cadre d'une enquête — ce qui est souvent le cas, puisque nous faisons beaucoup d'appui aux enquêtes — ces renseignements, ces preuves en quelque sorte, feraient partie du rapport des conclusions de notre enquête.

M. David de Burgh Graham: Vous travaillez avec des organismes externes comme la Electronic Frontier Foundation, qui est l'un de mes exemples préférés. La fondation fait constamment ce genre de travail, elle produit des résultats et les valide.

M. Gregory Smolynec: Oui, nous avons des réseaux de partenaires externes, notamment nos partenaires internationaux et provinciaux en matière de protection des données, ainsi que les commissaires à la protection de la vie privée du Canada et du monde entier.

M. David de Burgh Graham: Par le passé, à ce comité et à d'autres, nous avons beaucoup entendu parler de l'anonymisation des données. Au comité de l'industrie, il a été très brièvement question d'une étude de Statistique Canada sur les données bancaires, par exemple. Il est très possible d'anonymiser ce genre de données. Est-il possible de faire marche arrière, de les « dé-anonymiser »?

M. Gregory Smolynec: Oui. Nous étudions notamment la question des normes. En fait, en ce moment même, le directeur par intérim de notre Direction de l'analyse de la technologie est en Israël pour une réunion de l'International Standards Organization on de-identification. Le problème, cependant, tient à ce qu'il est possible de retrouver une identité à partir de la combinaison des ensembles de données. C'est donc un domaine très complexe.

● (1655)

M. David de Burgh Graham: Merci.

Le président: Sur ce, nous allons devoir clore cette partie de la séance. Au nom du Comité, je tiens à vous remercier tous les deux de votre témoignage. La séance est suspendue.

● (1655)

(Pause)

● (1655)

Le président: Chers collègues, nous reprenons nos travaux. M. Foster a été très généreux et nous a attendus patiemment. Pouvez-vous me dire combien de temps nous pouvons consacrer à ce groupe de témoins? Si nous terminons à 17 h 30, ce sera 35 minutes.

M. David de Burgh Graham: Nous avons un quorum réduit...

Le président: Le vote aura-t-il lieu à 17 h 45 ou à 18 heures?

M. Matthew Dubé: À 18 heures, avec sonnerie d'une demi-heure...

Le président: La sonnerie retentira donc à 17 h 30. Est-ce que tout le monde est d'accord pour aller au-delà de 17 h 30, pour au moins 10 minutes de plus?

M. Pierre Paul-Hus: Ce sera donc 17 h 40.

Le président: Ça vous va? Est-ce que tout le monde est d'accord pour 17 h 40?

Des députés: D'accord.

Le président: Je suppose que vous pouvez rester plus tard que 17 h 30.

M. Glenn Foster (chef de la sécurité de l'information, Banque Toronto Dominion): Je peux rester. Pas de problème.

Le président: Merci, monsieur Foster.

Comme vous le savez, nous permettons généralement une déclaration liminaire de 10 minutes, mais nous n'aurions rien contre le fait que vous preniez moins de 10 minutes. Donc, sur ce...

M. Glenn Foster: Je vais faire de mon mieux.

Le président: C'est une occasion à saisir. Je vous en prie, allez-y.

M. Glenn Foster: Merci.

Je m'appelle Glenn Foster. Je suis premier vice-président et chef de la sécurité de l'information à Groupe Banque TD. Je suis responsable du programme de cybersécurité de TD dans toutes ses activités à l'échelle mondiale.

TD est la sixième banque en importance en Amérique du Nord quant au nombre de succursales, et elle dessert plus de 25 millions de clients. Nous nous classons parmi les plus grandes entreprises de services financiers en ligne au monde.

Je suis ici pour vous parler de la cybersécurité et de ses répercussions sur les services financiers, les consommateurs canadiens et la sécurité nationale. Les services bancaires traditionnels sont devenus de plus en plus numériques. Selon un récent sondage de l'ABC, 76 % des Canadiens passent par des canaux numériques, en ligne et mobiles, pour effectuer la plupart de leurs transactions bancaires.

Plus de la moitié des répondants disent que c'est leur méthode bancaire la plus courante. C'est également vrai pour les clients de la TD. Nous avons plus de 12,5 millions de clients numériques actifs et 7,5 millions de clients mobiles actifs en tout. Nous effectuons 1,1 milliard de transactions numériques par année en Amérique du Nord, et nous avons le taux de pénétration numérique le plus élevé de toutes les banques au Canada, aux États-Unis, au Royaume-Uni et dans d'autres régions d'Europe.

Entretemps, les cybermenaces sont de plus en plus sophistiquées en raison: de la marchandisation de la criminalité dans l'économie souterraine; du détournement des technologies du renseignement d'État très secret, qui tombent dans les mains de mauvais acteurs; des technologies novatrices qui stimulent les progrès de l'automatisation; des tensions géopolitiques et de l'activité accrue contre les participants aux services financiers mondiaux et les systèmes de paiement.

Les récentes sanctions économiques ont accentué les tensions et motivé des mesures de rétorsion, des campagnes de cyberespionnage et des attaques contre les services financiers et les infrastructures essentielles à l'échelle mondiale par des acteurs étatiques.

La prolifération des atteintes à la protection des données a considérablement exposé les données des consommateurs et exercé des pressions sur la capacité des banques d'authentifier leurs clients.

L'exposition des données sur les consommateurs a également mené à de nouvelles attaques automatisées lors desquelles des criminels exploitent les identifiants de comptes volés et les testent en ligne sur des sites bancaires, à des rythmes infernaux, dans ce qu'on appelle du « credential stuffing » ou un bombardement sur des comptes multiples.

À la TD, nous avons investi massivement dans la cybersécurité, qui est l'une de nos priorités absolues, pour nous assurer que nous pouvons protéger nos clients et correspondre au niveau élevé de confiance qu'ils nous prêtent. Nous avons une solide tradition d'échange d'informations et de collaboration avec d'autres banques canadiennes par l'entremise de l'Association des banquiers canadiens et de divers secteurs de l'économie canadienne par l'entremise du nouvel Échange canadien de menaces cybernétiques. Nous comprenons à quel point il est essentiel d'échanger des renseignements sur les auteurs de menaces, et nous considérons que le fait de combiner nos moyens de défense est une pratique exemplaire, car notre capacité de prévenir, de détecter et de contenir les cyberattaques augmente considérablement lorsque nous travaillons de concert plutôt qu'individuellement.

L'efficacité des échanges de renseignements est limitée en raison des lois actuelles sur la protection des renseignements personnels et des obstacles juridiques. Des réformes législatives prévoyant des dispositions d'exonération pour la protection proactive pourraient nous appuyer dans les efforts que nous déployons. Nous appuyons la création par le gouvernement du Centre canadien pour la cybersécurité, qui relève du Centre de la sécurité des télécommunications. Nous préconisons depuis longtemps la centralisation des pouvoirs de collaboration avec le secteur privé.

En collaboration avec Échange canadien sur les cybermenaces, nous avons établi une structure solide pour les partenariats public-privé et le partage. L'élément essentiel de la mission du centre devrait être non seulement l'échange d'information et de renseignements, mais aussi l'élaboration et la mise en oeuvre de stratégies nationales de résilience, de préparation et d'intervention en matière de cybersécurité.

Le centre devrait disposer de ressources suffisantes pour pouvoir collaborer avec le secteur privé à l'établissement et à la mesure de bases de référence minimales en matière de sécurité pour les secteurs des infrastructures essentielles. Les secteurs public et privé bénéficieraient également des tests de résilience coordonnés et des capacités d'intervention disponibles en cas d'événements cybernétiques systémiques pour les infrastructures essentielles, ce qui préparera le centre à être le point central de coordination avec le secteur privé en réponse à une menace à la sécurité nationale.

Il est important de souligner que la cybersécurité et la sécurité sont des responsabilités qui incombent non seulement aux institutions financières et au gouvernement, mais aussi aux consommateurs canadiens.

Les pratiques de sécurité échouent lorsque les personnes ne comprennent pas leurs responsabilités personnelles et ne font pas preuve de diligence raisonnable dans leur vie numérique. Par conséquent, la nouvelle stratégie nationale est axée sur l'éducation des citoyens canadiens aux pratiques de cybersécurité sécuritaires, ce qui est d'une importance vitale pour accroître leur littératie en matière de risques et d'attentes réalistes.

La cybersécurité exige une main-d'oeuvre importante et hautement qualifiée. Des indicateurs externes donnent à penser qu'il faudrait combler plus d'un million de postes de cybernéticiens en Amérique du Nord seulement.

À la TD, qui est un employeur de premier plan au Canada, l'un des principaux piliers stratégiques de notre programme cybernétique est l'accent que nous mettons sur le recrutement de ressources. Nous faisons face à une concurrence de plus en plus féroce pour attirer les cybertalents au Canada, et nous collaborons avec des établissements d'enseignement pour créer des partenariats stratégiques comme celui que nous avons annoncé l'an dernier dans le cadre de notre collaboration avec l'Institut de la cybersécurité de l'Université du Nouveau-Brunswick.

Nous avons également étendu notre empreinte géographique aux États-Unis et à Israël pour répondre à la demande de ressources humaines. Nous sommes déterminés à augmenter le nombre de cybertalents appartenant à la prochaine génération, ici au Canada, et nous encourageons le gouvernement fédéral à accélérer l'élaboration de bons programmes d'éducation dans les universités canadiennes afin de fournir la main-d'oeuvre de demain dans le domaine de la cybersécurité.

● (1700)

Je suis heureux d'être ici pour discuter de l'approche du Canada en matière de cybersécurité, et j'ai hâte de participer à la discussion.

Le président: Merci, monsieur Foster.

Monsieur Picard, nous allons recommencer les tours de six minutes.

M. Michel Picard: Bienvenue, monsieur Foster.

Dans combien de pays peut-on trouver des bureaux ou des succursales bancaires de la Banque TD?

M. Glenn Foster: Je ne sais pas combien au juste. Il faudra que je demande au greffier.

Nous sommes principalement une banque nord-américaine et nous avons d'autres sociétés de placement de valeurs mobilières à l'étranger.

M. Michel Picard: Le réseau que vous utilisez pour vos transactions au Canada est-il un réseau privé, ou est-ce Internet — le Web en général? Comment la sécurité est-elle gérée dans le cas d'un client accédant à votre banque de l'extérieur du Canada, par l'entremise de vos succursales ou de vos bureaux?

M. Glenn Foster: Nous avons diverses méthodes de connexion fondées sur les produits ou les succursales, mais la majorité de notre trafic transactionnel se fait par l'entremise de nos applications en ligne et de nos applications mobiles, qui entreront sur Internet.

Ces connexions sont basées à la fois sur les navigateurs et sur nos applications mobiles exclusives que les clients installent très souvent sur leurs téléphones intelligents; ils utilisent le chiffrement standard basé sur l'ICP pour protéger les transmissions de point à point.

M. Michel Picard: Les renseignements concernant les Canadiens sont-ils uniquement destinés à des fins d'identification personnelle, autrement dit, les renseignements se trouvent-ils tous dans votre serveur au Canada, ou est-ce que certains de ces renseignements peuvent se trouver ailleurs dans vos succursales à l'étranger?

● (1705)

M. Glenn Foster: Tous les centres de données de la TD sont au Canada.

M. Michel Picard: Donc, les points à l'extérieur du pays, comme les succursales de la TD à l'étranger, ou les autres tiers qui parlent à votre serveur, pénètrent dans votre serveur au Canada pour avoir éventuellement accès aux données que vous détenez.

M. Glenn Foster: Oui.

Pour nos systèmes bancaires de base, il existe une connectivité directe avec nous dans nos centres de données au Canada. La Banque TD a des fournisseurs externes de services bancaires et de services à la clientèle. Ces services peuvent être offerts dans d'autres pays, comme aux États-Unis.

M. Michel Picard: Évidemment, nous ne pouvons pas comparer votre système à celui d'autres entreprises, parce qu'il est privé, mais il est de plus en plus question de services bancaires ouverts. Qu'en dites-vous?

M. Glenn Foster: En tant que professionnel de la sécurité depuis un certain nombre d'années, je suis d'avis que l'intégrité de tout régime de sécurité dépend de l'existence d'une boucle fermée entre le consommateur de services et le fournisseur de services bancaires. Tout intermédiaire entre les deux affaiblit le régime de sécurité.

M. Michel Picard: Pour ce qui est du concept de banque ouverte, vous ai-je bien compris quand vous dites que, s'il y a une tierce partie, le système est vulnérabilisé?

M. Glenn Foster: Oui.

M. Michel Picard: Ne devriez-vous pas alors disposer d'un système unique?

M. Glenn Foster: Pour ce qui est de l'authentification des identifiants, il faudrait que la tierce partie ait accès à ces identifiants pour les opérations bancaires en ligne. Bien sûr, il y a différents modèles. Il y a le modèle américain, très axé sur le marché, qui permet aux banques de passer des contrats avec des tierces parties et de leur fournir certaines garanties en matière de sécurité. Le modèle britannique est très ouvert; par conséquent, n'importe qui pourrait consommer ces services.

M. Michel Picard: Si vous êtes victime d'un piratage ou d'une attaque, le déclarez-vous à une autorité, et si oui combien de temps après?

M. Glenn Foster: Je suis désolé. Pourriez-vous répéter la question?

M. Michel Picard: Lorsque vous êtes victime d'une agression de piratage, le déclarez-vous à une autorité quelconque — au gouvernement — et combien de temps après les faits le déclarez-vous?

M. Glenn Foster: Notre principal organisme de réglementation, le BSIF, impose des normes strictes en matière de déclaration, soit 72 heures après les faits, selon une échelle de gravité spécifiée.

M. Michel Picard: Merci.

J'avais six minutes.

Le président: Il vous reste quelques minutes.

M. Michel Picard: J'ai amplement le temps. Voulez-vous un café ou quelque chose du genre?

Des députés: Oh, oh!

M. Michael Picard: A-t-on besoin d'un règlement qui non seulement fixe le délai de notification d'une attaque, le plus bref possible, mais qui prévoit aussi comment utiliser cette information et la diffuser partout sur le marché pour informer tout le monde, tout en protégeant les renseignements sur la personne ou l'entreprise, mais de manière que cette information puisse être utile d'une façon ou d'une autre?

M. Glenn Foster: En ce qui concerne les renseignements personnels et la protection des renseignements personnels des consommateurs, le dispositif législatif et les délais de déclaration me paraissent adéquats. Une banque ou grande institution comme la nôtre procède quotidiennement à divers examens de sécurité, à la détection d'activités malveillantes. Il s'agit en fait de déterminer la voie d'entrée de ces activités, lorsqu'un problème est détecté. À mon avis, le système de surveillance au niveau de notre organisme de réglementation principal est satisfaisant.

À la Banque TD, les attaques contre nos systèmes bancaires en ligne consistent généralement en des tentatives de fraude au détriment de nos clients. J'ai fait allusion aux tentatives d'infiltration simultanées dans ma déclaration préliminaire. Prises globalement, les atteintes à la sécurité des données affectant actuellement Marriott, Yahoo, etc., concernent des millions, dans certains cas des milliards d'identifiants. Yahoo fait état de 3,5 milliards d'ensembles d'identifiants. Les criminels rédigent des scénarios d'attaques contre diverses banques, à la recherche de consommateurs qui réutilisent leur nom d'utilisateur et leur mot de passe dans l'établissement. Le volume de ce trafic est considérable et force les banques et les entreprises à investir dans des technologies de pointe pour s'en défendre. Pour nous, ça finit par rentrer dans l'ordre des choses au même titre que les pertes dues à la fraude sur une période donnée.

Le président: Merci, monsieur Picard.

[*Français*]

Monsieur Paul-Hus, vous avez six minutes.

M. Pierre Paul-Hus: Mon collègue vous a posé une question concernant la conservation des données. Comme vous l'avez mentionné, la Banque TD garde en général les données au Canada, mais certaines peuvent être gardées aux États-Unis.

Lundi dernier, nous avons reçu M. Green, qui est responsable de la cybersécurité chez Mastercard. Il expliquait que c'étaient les banques qui gardaient les informations.

Dans votre cas, vous faites affaire avec Visa. Les données des cartes de crédit Visa de TD sont-elles conservées ici, au Canada, ou aux États-Unis?

● (1710)

[*Traduction*]

M. Glenn Foster: Le traitement de base est sous-traité et les données se trouvent en fait aux États-Unis.

[*Français*]

M. Pierre Paul-Hus: D'accord.

Revenons sur les fameux pirates éthiques.

Comment les appelez-vous, déjà?

M. David de Burgh Graham: Ce sont des chapeaux blancs.

M. Pierre Paul-Hus: D'accord.

En 2017, la TD a créé ce qu'on appelle la « *red team* », soit l'équipe de pirates éthiques ou de chapeaux blancs qui travaille 24 heures sur 24 pour la Banque afin d'y trouver des failles.

Quel genre de contrat de service avez-vous avec ces gens?

[*Traduction*]

M. Glenn Foster: Bonne question. Même avant la mise en place de la « red team », nous avions notre propre équipe interne de pirates éthiques. Son but était de soutenir nos activités de développement de systèmes et de s'assurer qu'un système de crédit était sécurisé avant qu'on y verse nos données de confiance ou qu'on l'ouvre aux clients. Pour répondre précisément à votre question, l'équipe est composée de pirates éthiques qui testent nos systèmes de production au jour le jour. Ce sont des employés internes. On fait appel en renfort à des experts du domaine. On le fait non seulement pour renforcer les effectifs, mais aussi pour favoriser le partage de l'expertise, parce que la façon de renforcer cette industrie consiste à faire constamment appel à de nouvelles compétences, à de nouveaux talents et à tester continuellement nos systèmes.

[*Français*]

M. Pierre Paul-Hus: J'aimerais parler de la confiance entre la banque et ces gens. À la base, ce sont des gens qui aiment pirater. Ils sont un peu criminels dans leurs actions, mais on les engage pour être amis avec le système ou avec la banque, entre autres.

Comment faites-vous pour garder un degré de confiance envers eux?

[*Traduction*]

M. Glenn Foster: Naturellement, ces employés passent par notre processus de présélection. Nous vérifions leurs antécédents, etc. Ils font partie de notre programme de gestion des risques internes et ils savent qu'en raison du poste délicat qu'ils occupent, dans la mise à l'épreuve de systèmes d'exploitation pouvant abriter les données des clients, ils feront l'objet d'une surveillance constante plus stricte que les autres employés et d'un contrôle périodique pour leur maintien dans leur poste.

[*Français*]

M. Pierre Paul-Hus: Vous avez mentionné que la TD avait un bureau de cybersécurité en Israël. Deux témoins nous ont dit préférer aller en Israël.

Pourquoi Israël est-il important pour vous sur le plan de la cybersécurité?

[*Traduction*]

M. Glenn Foster: Israël a un écosystème unique pour son service militaire obligatoire. Le pays a été parmi les premiers à adopter la cybersécurité dont il a très tôt reconnu l'importance. La disponibilité de talents et de compétences élevées est très souhaitable. Cela dit, nous sommes très sélectifs quant au personnel que nous y mettons en poste. Nous examinons les innovations en matière de sécurité, le renseignement de sécurité et nous surveillons les risques potentiels pour la Banque TD ou pour ses clients. Dans certains cas, nous faisons des démonstrations de faisabilité pour le développement rapide d'outils et de produits cybernétiques.

[*Français*]

M. Pierre Paul-Hus: Vous avez mentionné l'écosystème israélien et le côté du service militaire. Dans le fond, c'est dans la culture israélienne que vous retrouvez une façon de voir le monde. Pour ces gens, c'est un enjeu majeur. Cela fait plusieurs fois qu'on nous parle d'Israël. Comment le Canada pourrait-il prendre exemple sur ce que fait Israël pour s'assurer que les jeunes Canadiens peuvent mieux se préparer ou s'intéresser à la question?

Vous avez parlé de forces armées. J'ai servi dans les Forces. Au Canada, il y a peut-être un aspect à regarder aussi avec le service militaire. Les opérations militaires font déjà beaucoup de cybersécurité, mais c'est en vase clos. Y aurait-il une façon d'avoir une interaction?

[*Traduction*]

M. Glenn Foster: Le service militaire obligatoire donne un avantage à Israël, en ce qui a trait non seulement à l'état d'esprit, mais aussi aux réseaux qu'il crée. Ce qui est unique dans ce petit écosystème, c'est que les spécialistes tirent parti de ces réseaux militaires tout au long de leur carrière. L'un peut travailler pour Intel l'autre pour IBM, mais ils travaillent sur un problème unique. Cela suscite des collaborations très intéressantes et encourage grandement cette mentalité de nation de jeunes entrepreneurs qu'on lui prête.

● (1715)

[*Français*]

M. Pierre Paul-Hus: Je vous remercie.

[*Traduction*]

Le président: Monsieur Dubé, vous avez six minutes.

[*Français*]

M. Matthew Dubé: Merci, monsieur le président.

[*Traduction*]

Monsieur Foster, merci de votre présence.

Je veux parler de l'intelligence artificielle. La question a été soulevée à diverses reprises. Des acteurs malicieux s'en servent pour découvrir comment s'attaquer aux faiblesses des systèmes. D'après ce que je comprends, on s'en sert de plus en plus comme mesure de protection, pour apprendre à se protéger.

Je crois que, l'an dernier, la TD a acquis une entreprise d'IA en démarrage. Je commencerai par l'aspect sécurité avant de passer aux autres.

Du point de vue de la sécurité, tant pour la défense que pour votre perception de ceux qui attaquent, que pensez-vous de la situation actuelle?

M. Glenn Foster: Je commencerai par les attaquants.

Bien que l'on redoute que des adversaires puissent tirer parti de l'intelligence artificielle pour nous attaquer, la pratique n'en fournit guère d'exemples. Le domaine étant en constante évolution, notre équipe du renseignement sur les menaces le surveille de très près.

Du côté de la défense, c'est un atout et un outil important pour nous. Les produits de sécurité traditionnels étaient très bons à une époque où les attaques étaient vraiment reproductibles. On pouvait définir les signatures; on pouvait les bloquer.

Les attaques actuelles sont très sophistiquées. Elles changent d'un jour à l'autre. Entre le moment où le public est ciblé, le moment où le fournisseur commercial peut apporter des correctifs et le moment où les grandes institutions peuvent corriger les vulnérabilités constatées, le battement, même s'il est toujours plus bref, est toujours trop long vu la vitesse à laquelle les adversaires peuvent élaborer des scripts et commencer à balayer tous les comptes sur Internet. Le recours à l'automatisation et, dans certains cas, à l'intelligence artificielle pour détecter plus rapidement les vulnérabilités commence à nous poser de sérieux problèmes.

C'est en recourant à l'intelligence artificielle, à l'apprentissage automatique et aux mégadonnées que l'on détecte les acteurs les plus sophistiqués, ceux qui savent comment contourner notre équipement de sécurité traditionnel.

M. Matthew Dubé: Je vous en remercie. Ça c'est pour l'aspect sécurité.

Du point de vue des affaires ou du marketing, on peut aussi se servir de l'intelligence artificielle pour répondre aux besoins d'une entreprise, pour cerner les besoins des clients, etc. On lit ainsi dans l'énoncé de mission de Layer 6, que vous avez acquise, qu'elle utilise les technologies d'apprentissage automatique pour aider les entreprises à mieux prévoir les besoins de leurs clients, ce qui est un objectif louable. Ceux d'entre nous qui utilisent des applications bancaires constatent qu'on s'en sert pour tenter de prédire les tendances des dépenses ou des choses du genre.

Quel usage en fait-on? Vaste question, je sais, mais je veux comprendre. Du moment que votre organisation, votre entreprise ou votre banque, recueille forcément des données, comment s'y prend-elle pour les éliminer et s'assurer qu'elle ne glane pas de renseignements qui ne devraient pas être collectés ou qui le sont sans consentement, du moins sans consentement explicite?

M. Glenn Foster: En ce qui concerne la protection des données, pas seulement pour Layer 6, mais pour tout système technologique au sein de la Banque TD, nous appliquons un processus d'accréditation très rigoureux: notre programme « sécurisé SDLC ». Il permet de prévoir les mesures de protection à mettre en place sur la base d'une définition précise des besoins, d'une évaluation des risques et des facteurs relatifs à la vie privée. Nos normes de classification des données sont très au point. Tout un dispositif de protection des données vient en outre se greffer là-dessus.

La règle d'or, bien sûr, est qu'on ne doit recueillir que les données explicitement nécessaires. Ensuite, il y a diverses techniques pour protéger ces données, allant de l'obscurcissement de la tokenisation au chiffrement.

M. Matthew Dubé: Merci.

L'autre aspect que je voulais aborder concerne les applications. Un peu plus tôt, j'ai interrogé le Commissariat à la protection de la vie privée à propos de l'installation d'une application sur votre téléphone qui implique que vous donnez en quelque sorte une autorisation générale. Parfois, c'est explicite, d'autres fois, ça l'est moins dans le cas de telle ou telle application qui veut avoir accès à votre microphone, à votre caméra et ainsi de suite.

Quand votre organisation met son application au point, je me demande comment vous conciliez ce qui se passe dans l'application pour l'activité bancaire du client et le fait qu'elle peut présenter diverses failles, que ce soit le micrologiciel ou d'autres défauts qui sont exploités dans l'appareil mobile lui-même. Comment cela fonctionne-t-il? Que recommanderiez-vous à cet égard?

● (1720)

M. Glenn Foster: Tout ce que je peux vous dire, c'est comment on aborde la sécurité à la Banque TD pour nos applications.

Vous avez raison. Notre application doit vivre dans un écosystème. Ce n'est pas différent de votre ordinateur, il dépend du système d'exploitation sous-jacent et du micrologiciel. L'élaboration de ces applications obéit à quelques principes, dont la notion du moindre privilège. Pour ce qui est des données transitant dans l'application, nous essayons de ne pas les conserver. Ainsi, même s'il y a des faiblesses inhérentes, il n'y a pas de données auxquelles accéder.

Nous veillons à blinder l'application. J'ai déjà dit que nous avions notre propre équipe de piratage éthique, en plus de la « red team ». Son rôle au sein de la banque consiste, avant le lancement d'un de ces produits, à effectuer des tests de sécurité très rigoureux, pour assurer l'étanchéité de l'application aux autres processus en cours dans l'appareil lui-même.

M. Matthew Dubé: Merci.

Le président: Monsieur Graham, vous avez six minutes.

M. David de Burgh Graham: Merci. Je vais poursuivre un peu dans la même veine que M. Dubé.

Dans quelle mesure une application est-elle sûre sur un téléphone débridé?

M. Glenn Foster: Quelle est la sécurité d'une application sur un téléphone débridé?

M. David de Burgh Graham: Oui.

M. Glenn Foster: Elle n'est pas très sûre du tout et c'est pourquoi nous avons la détection de débridage dans nos applications. En fait, on suspend les services pour cette application si elle est débridée.

Le problème, évidemment, c'est qu'un code malveillant pourrait très facilement se retrouver sur ce téléphone. On a aussi parlé du chiffrement de point à point. Les données pourraient être exfiltrées si un code malveillant tournait sur l'appareil.

M. David de Burgh Graham: D'accord, parce que vous avez déjà dit...

Le président: Monsieur Graham, je suis sûr qu'il y a quelqu'un d'autre au sein de ce comité qui ne sait pas ce qu'on entend par « débrider ». Pourriez-vous l'expliquer?

M. David de Burgh Graham: Je peux vous l'expliquer si vous ne comptez pas cela dans mon temps de parole.

Le président: Je ne compte pas votre temps. Je suis sûr que ce sera édifiant pour tous.

Des voix: Oh, oh!

M. David de Burgh Graham: Comment expliquer cela en 10 secondes?

Voulez-vous expliquer ce qu'est un débridage?

M. Glenn Foster: La façon la plus simple de l'expliquer est la suivante. Lorsqu'on reçoit son téléphone du fournisseur, on ne peut charger que les applications offertes sur la plateforme du fournisseur. Le débridage consiste à utiliser un outil de piratage, que l'on peut trouver sur Internet, pour accéder à des applications autres que celles approuvées par son fournisseur de services.

M. David de Burgh Graham: Il permet d'utiliser son téléphone comme un ordinateur. Il offre alors beaucoup plus de possibilités mais comme il devient moins sûr, c'est un compromis à faire.

Le président: D'accord. Je vois. Je vous remercie.

M. David de Burgh Graham: La raison pour laquelle je voulais parler un peu de débridage, c'est que, tout à l'heure, vous avez abordé la question de l'ICP: le chiffrement public, les systèmes à clé publique. Un téléphone débridé, permet d'accéder très facilement à sa clé privée et, par conséquent, à tout ce que l'on fait. Je me trompe?

M. Glenn Foster: Ce n'est pas aussi facile que cela, à cause du risque qui en découle. Le risque pour l'appareil augmente et nous voulons bien sûr savoir si le téléphone est débridé afin de pouvoir prendre des décisions fondées sur le risque à l'égard de l'utilisateur concerné ou de toute transaction qu'il essaie d'effectuer.

M. David de Burgh Graham: D'accord.

J'ai une question qui porte sur les institutions financières, heureusement pour vous. L'automne dernier, ma femme a perdu sa carte de crédit qui, bien sûr, a été abondamment utilisée par la suite. On ne pouvait rien y faire parce que c'est la fonction sans contact qui a été utilisée, et il n'y a absolument...

M. Jim Eglinski (Yellowhead, PCC): Je suis vieux...

Des voix: Oh, oh!

M. David de Burgh Graham: Il lui a fallu deux jours pour se rendre compte qu'elle l'avait perdue, mais quoi qu'il en soit... Nous n'avons pas à consigner cela au Hansard.

Ce que je veux dire, c'est qu'il n'y a pas de sécurité sur les cartes sans contact. Quelle est la méthode de sécurisation de PayPass et de payWave, la technologie d'IRF que l'on utilise actuellement? Y a-t-il quelque chose que l'on puisse faire pour assurer la sécurité?

M. Glenn Foster: Les paiements EMV utilisent une cryptographie assez avancée. Je ne dirais pas qu'ils ne sont pas sûrs.

M. David de Burgh Graham: Ils sont sûrs tant que vous avez la carte en main, mais si vous la perdez, rien ne permet de garantir que la personne qui va l'utiliser en est le détenteur de plein droit, ce qui est le cas avec les NIP et, dans une certaine mesure, avec les numéros au verso de la carte. Il n'y a absolument rien pour le paiement sans contact.

M. Glenn Foster: Tout ce que je peux dire, c'est que les banques appliquent diverses stratégies de lutte contre la fraude et limitent le montant des paiements EMV. Je suis désolé pour la mésaventure survenue à votre femme.

M. David de Burgh Graham: Il n'y a pas eu de remboursement parce qu'on n'avait pas signalé la perte de la carte. On a compris qu'elle avait disparu à la réception d'un relevé montrant des débits suspects d'environ 200 $. Tout ce que je veux dire, c'est que cela peut arriver et qu'il n'y a pas de système pratique pour l'empêcher.

Le remboursement est laissé à la bonne volonté de la banque, mais ce n'est pas sa faute en fin de compte. Je me demande s'il y a moyen de remédier à ça, mais il me semble que non.

M. Glenn Foster: Pour ma part, je suis responsable de la sécurité technique des données et des systèmes. Il faudrait que je fasse un suivi auprès de nos spécialistes des produits.

M. David de Burgh Graham: Très bien.

Quand je voyage un peu partout à l'étranger, par exemple, et que j'utilise ma carte de crédit ou ma carte de débit à différents endroits, la TD sait où et comment j'utilise ma carte; est-ce qu'elle utilise ces renseignements à des fins autres que [*Inaudible*] la transaction?

M. Glenn Foster: Non, seulement aux fins de la lutte contre la fraude.

M. David de Burgh Graham: À la seule fin de lutter contre la fraude. Il n'y a aucun objectif de commercialisation à quelque stade que ce soit?

● (1725)

M. Glenn Foster: Les systèmes de la TD enregistrent les données sur votre transaction et le point de vente. Est-ce là votre question?

M. David de Burgh Graham: Supposons que je me rende à la banque de l'autre côté de la rue, puis à Saskatoon et à Taipei. Vous savez maintenant que je voyage et vous savez à peu près ce que j'achète. Ces données servent-elles à autre chose qu'au suivi de la sécurité?

M. Glenn Foster: Encore une fois, je dois m'en remettre aux spécialistes des produits qui font ce genre de marketing ciblé.

M. David de Burgh Graham: Les mots de passe sont-ils désuets?

M. Glenn Foster: À mon avis, ils ont encore une certaine valeur — c'est le renseignement que seul le client connaît —, mais la valeur des identifiants diminue considérablement d'année en année.

M. David de Burgh Graham: Quelle est la solution de rechange?

M. Glenn Foster: Les différents outils biométriques. Cependant, il demeure nécessaire de miser aussi sur un autre paramètre, que ce soit une information connue du client ou quelque chose qu'il possède, en combinaison avec la biométrie. C'est une donnée qui vous définit et l'on parle alors « d'authentification multifactorielle ».

La fiabilité des actuels lecteurs d'empreintes digitales et de certaines des technologies de reconnaissance faciale sur le marché est de plus en plus grande. Dans la plupart des cas, il s'agit d'un authentifiant plus puissant que le nom d'utilisateur et le mot de passe d'un client.

M. David de Burgh Graham: C'est juste. Que faire si vos données biométriques sont détournées?

M. Glenn Foster: Les données biométriques sont reliées à l'utilisateur, de sorte qu'il est ensuite possible de les suspendre et de réinscrire l'utilisateur. On ne conserve pas tout votre... Dans le cas de l'empreinte du pouce, par exemple, aucun de ces appareils ne conserve l'empreinte tout entière. Tous ont leur propre algorithme de points qu'ils relèvent, et ils ne conservent que ces données. Chaque appareil a son système.

M. David de Burgh Graham: J'ai une...

M. Glenn Foster: Votre pouce est en sécurité.

M. David de Burgh Graham: Et puis, le pouce doit présenter une température normale, il doit être irrigué par le sang. Ça, c'est autre chose.

M. Jim Eglinski: Il suffit de le tenir un peu dans la main.

M. Matthew Dubé: On voit que vous y avez pensé.

M. Jim Eglinski: Mettez-le au micro-ondes.

Des députés: Oh, oh!

M. David de Burgh Graham: Sur une note un peu plus légère, au cours de la réunion de lundi, le sujet du bogue de l'an 2000 a été abordé brièvement — je ne me souviens pas pourquoi — et je n'ai pas eu l'occasion d'y revenir. La TD est-elle prête pour l'an 2038?

M. Glenn Foster: Si la TD est prête pour l'an 2038?

M. David de Burgh Graham: Si nous avons le bogue de l'an 2038.

M. Glenn Foster: Nous n'avons pas encore effectué d'évaluation rigoureuse à ce sujet.

M. David de Burgh Graham: Vous avez encore du matériel en 32 bits?

M. Glenn Foster: Non.

M. David de Burgh Graham: D'accord, alors ça va.

Merci.

Le président: Monsieur Motz, vous qui avez été policier, saviez-vous qu'on pouvait débrider autre chose que les moteurs d'auto, sans parler des chevaux évidemment?

M. Glen Motz: Oui, en fait, j'étais au courant...

Le président: Vous étiez au courant? Je suis très impressionné.

M. Glen Motz: Nous avions l'habitude de pirater des téléphones.

Le président: Je vois.

M. Glen Motz: Quoi qu'il en soit...

Le président: Quatre minutes, monsieur Motz.

M. Glen Motz: Légalement.

M. Michel Picard: Bien sûr.

M. Glen Motz: Avec autorisation judiciaire, monsieur le président.

J'aimerais revenir à une conversation que nous avons amorcée lundi avec d'autres groupes. Il était question de problèmes de longue date avec des systèmes anciens, particulièrement dans le secteur bancaire, par exemple des logiciels qui n'étaient plus pris en charge. Je crois que quelques-uns de nos guichets automatiques fonctionnent encore sous la plateforme Windows XP, qui n'est plus prise en charge.

En tant qu'institution financière, avez-vous ce genre de problèmes actuellement? Comment faites-vous pour vous assurer que vos systèmes sont sécurisés et que les anciennes données sont transférées ou mieux protégées?

M. Glenn Foster: Comme toutes les grandes entreprises, nous devons nous tenir à jour. Nous consacrons une partie importante de notre budget à mettre nos systèmes à niveau, y compris nos guichets automatiques. De même, nous avons un système de contrôles à plusieurs niveaux pour nous assurer que les réseaux sont en boucle fermée, que le cryptage est adéquat entre un appareil et nos systèmes eux-mêmes, puis nous avons des paliers de détection pour repérer tout risque d'utilisation malveillante en cours de route.

M. Glen Motz: D'accord.

Dans notre comité et à la Chambre — dans tout le pays, en fait — on s'est demandé s'il fallait accepter ou non Huawei, par exemple, dans notre infrastructure essentielle à l'avenir. Avec le réseau 5G qui s'en vient, votre banque est-elle prête à utiliser des serveurs construits en tout ou en partie par des entités étrangères qui sont parfois sous l'emprise de gouvernements étrangers? Comment composez-vous avec cela?

● (1730)

M. Glenn Foster: Nous sommes en train d'analyser cela, alors nous ne sommes pas encore fixés, et nous n'avons pas non plus publié de politique à ce sujet.

M. Glen Motz: Dans ce cas, comment faites-vous pour approuver vos logiciels et votre matériel?

M. Glenn Foster: Pour le matériel, nous avons un processus d'acquisition qui est également un processus d'accréditation de sécurité, prescrit pour tout logiciel construit ou déployé à l'interne. En ce qui concerne l'acquisition de logiciels, où il s'agit souvent de reproduire des logiciels vendus dans le commerce, nous procédons aussi à une évaluation avant de les mettre en service à notre satisfaction.

M. Glen Motz: Vous vous assurez qu'il n'y a pas de bogues cachés.

M. Glenn Foster: Exactement.

M. Glen Motz: Toutes les institutions font l'objet de cyberattaques. Le secteur bancaire n'est certainement pas à l'abri. D'après votre expérience chez TD, d'où proviennent la plupart de vos attaques et quel genre d'information est visée?

M. Glenn Foster: La majorité des attaques que nous voyons sont généralement déguisées pour donner l'impression qu'elles viennent du Canada ou de l'Amérique du Nord en général. La source première, quand nous arrivons à la localiser, se trouve souvent en Europe de l'Est, en Russie ou à l'occasion en Chine ou en Corée du Nord.

M. Glen Motz: Quelles sont les cibles visées, et prenez-vous des mesures proactives pour protéger votre propre infrastructure?

M. Glenn Foster: Oui, nous avons une équipe spécialisée dans le renseignement qui surveille le Web invisible. Nous recueillons des renseignements sur les menaces et des indices de compromission auprès de sources multiples. Nous pouvons échanger énormément d'information par l'entremise de l'Association des banquiers canadiens, et plus globalement avec le centre d'analyse FS-ISAC et les États-Unis, où on nous communique ce que la communauté du renseignement arrive à détecter. Nous nous servons ensuite des données pour examiner le trafic réel qui entre dans notre réseau et qui en sort.

Nous bloquons à l'avance des visées malveillantes connues, de sorte que si un indésirable pénètre dans notre entreprise, il est aussitôt mis en quarantaine. Nous avons des paliers de contrôle et des détecteurs à la grandeur de notre réseau et de notre infrastructure, où nous pouvons à la fois repérer toute activité potentiellement dangereuse et bloquer des appareils en temps réel.

Le président: Merci, monsieur Motz.

Madame Dabrusin.

Mme Julie Dabrusin: Dans votre exposé préliminaire, vous avez parlé de la responsabilité personnelle comme étant un problème. On a dit plus tôt que nos systèmes étaient comme des blindés qui passent entre deux boîtes de carton. Il y a donc vraiment un problème.

Est-ce que la banque présente des fenêtres contextuelles à l'écran lorsque les gens entrent leur mot de passe ou qu'ils ouvrent une session, pour leur dire par exemple: « Si vous avez utilisé ce mot de passe ailleurs, vous avez compromis votre sécurité? » Avez-vous quelque chose pour informer les gens de la nécessité de créer de nouveaux mots de passe?

M. Glenn Foster: Dans le secteur bancaire, nous ne présentons pas de fenêtres contextuelles à l'ouverture d'une session. Dans nos sites de services en ligne, nous donnons tous des conseils sur ce qui fait la force d'un mot de passe. Nous prenons l'initiative de désactiver un compte si nous soupçonnons une activité malveillante, ou si nous avons repéré ses justificatifs d'identité sur le Web invisible ou ailleurs. Le client doit alors faire la démarche de réinitialisation de son mot de passe et réattester par d'autres moyens qu'il est bien celui qu'il dit être. Ensuite, nous rétablissons son compte.

Mme Julie Dabrusin: Je réfléchis simplement à ce que je veux dire, et à ce que d'autres ont dit, et je pense pouvoir dire sans me tromper que des gens utilisent un certain nombre de mots de passe qui reviennent finalement à du pareil au même. C'est un des meilleurs moyens de compromettre leur cybersécurité personnelle.

M. Glenn Foster: [*Inaudible*] obtient habituellement des mots de passe ou la réutilisation d'un mot de passe. Cela se fait aisément par différentes intrusions dans des systèmes moins perfectionnés.

Mme Julie Dabrusin: Bien souvent, lorsqu'on ouvre une session sur un site, on se fait dire: « Vous avez besoin d'un mot de passe plus fort. » On met une majuscule, on ajoute un symbole quelconque, un chiffre ou autre chose, et un certain nombre de caractères, mais il n'y a rien à mon sens qui dise: « Hé, avez-vous déjà utilisé ce mot de passe? » N'est-ce pas là une façon simple de rafraîchir la mémoire des gens? Bien sûr, on fait cela parce que c'est pratique, mais on compromet sa sécurité. N'y a-t-il pas quelque chose que vous pourriez mettre là-dedans, dans ces huit symboles ou lettres, ou quoi que ce soit que vous pourriez inciter les gens à faire?

M. Glenn Foster: Nous pouvons évidemment examiner d'autres moyens d'éduquer les clients et les consommateurs en cours de route.

Mme Julie Dabrusin: Merci.

Vous avez parlé de la nécessité d'avoir plus de programmes de formation. Ce qui n'est pas clair pour moi, c'est la nature de cette formation. Il semble que les exigences varient et que certains endroits embauchent des personnes qui n'ont pas de diplôme en cybersécurité, alors que d'autres non. De quoi avez-vous besoin comme formation pour votre effectif? Qu'est-ce que vous recherchez comme formation?

● (1735)

M. Glenn Foster: Il faudrait qu'un plus grand nombre d'établissements offrent des programmes liés à la cybersécurité, et on revient à ce que vous dites quant aux différences de niveau. Il y a des programmes qui portent sur les opérations de sécurité de base, comme ceux offerts par les collèges locaux, ou sur les rudiments de la cybersécurité et du réseautage. On peut parler des « bons » pirates avec un sens de l'éthique, ou des chapeaux blancs dont il était question tantôt. Puis, il y a le niveau de sécurité beaucoup plus technique que nous appelons communément la « sécurité des applications ». Ce serait bénéfique.

Si vous regardez le nombre d'écoles qui offrent ce genre de formation, vous verrez que même si nous avons des programmes de pointe au Canada, ils ne sont pas aussi étendus qu'ils devraient l'être, et le nombre d'étudiants qui s'y inscrivent n'est pas non plus à la hauteur des besoins.

Au cours de la prochaine décennie, je vois la pénurie de ressources humaines comme étant probablement la principale crise au sein des grandes institutions pour ce qui est de contrer la montée des cybermenaces.

Le président: Il nous reste environ quatre minutes, et je suis sûr que M. Spengemann aimerait que M. Eglinski veuille bien les partager avec lui.

M. Sven Spengemann (Mississauga—Lakeshore, Lib.): Bien sûr.

Le président: Vous pouvez poser une question chacun.

M. Jim Eglinski: J'ai trois questions, mais je suppose que je vais devoir y aller très rapidement.

Vous avez parlé d'Israël et de l'excellente collaboration qu'on trouve là-bas, parce que beaucoup de gens ont été formés indirectement par le service militaire, entre autres.

Avez-vous une collaboration avec les autres grandes institutions prêteuses au Canada? Travaillez-vous ensemble et échangez-vous de l'information, par exemple, sur ce qui est mauvais, sur ce qui est bon, etc.?

M. Glenn Foster: Oui.

M. Jim Eglinski: Et dans votre système, avez-vous la capacité de découvrir si quelqu'un pirate le système du client à la maison? Pouvez-vous en informer le client par vos moyens de vérification?

M. Glenn Foster: Pour la première question, à savoir si nous échangeons de l'information entre nous, oui, il y a un groupe de travail chargé du renseignement sur les menaces, qui relève du groupe spécial de la cybersécurité à l'Association des banquiers canadiens; toutes les banques et le CST assistent à ses réunions et ils lui fournissent également des mises à jour, ce que nous trouvons très utile.

Nous échangeons des indices de compromission, c'est-à-dire des indicateurs techniques qui permettent d'identifier des types de menaces et des mauvais joueurs. C'est un outil très puissant. Nous savons que des adversaires, des criminels, font amplement usage du Web invisible et d'autres canaux pour échanger sur les points faibles qu'ils décèlent dans les institutions et les banques. Je pense que nous avons intérêt à faire de même.

Pour ce qui est de votre deuxième question, est-ce que nous détectons les atteintes au système du client chez lui? Non, nous ne les voyons pas. Généralement, tout ce que nous voyons, c'est la transaction qui arrive à nos serveurs.

M. Jim Eglinski: Est-ce que cela vous a paru deux minutes?

Le président: Presque, mais M. Spengemann va aimer votre générosité. Il pourrait même vous envoyer une carte de fête.

M. Jim Eglinski: Merci. C'est très gentil de votre part, monsieur le président.

M. Glen Motz: Je vais envoyer des bougies.

M. Sven Spengemann: Merci, monsieur le président, et merci, monsieur Eglinski.

Merci beaucoup, monsieur Foster. En tant qu'ancien employé de TD, je suis heureux de vous accueillir.

Je vais résumer mes questions en une seule. Nous avons le privilège de vous recevoir, vous qui êtes chef de la sécurité de l'information d'une grande banque. Pouvez-vous nous dire en gros comment votre rôle est structuré, quelles sont vos responsabilités et comment elles se recoupent avec les autres grandes composantes de la banque?

En même temps, pouvez-vous nous donner une idée de la marge de manoeuvre dont dispose une grande banque pour concevoir ses propres plateformes de sécurité? Dans quelle mesure les contraintes de l'utilisation de la technologie numérique limitent-elles, tout d'abord, le pourcentage des dépenses affectées à la sécurité, mais aussi les options qui s'offrent à vous pour protéger les activités quotidiennes?

M. Glenn Foster: Là où je figure dans l'organigramme, je relève du chef de l'excellence opérationnelle, qui relève de notre chef de groupe, qui relève directement de notre chef de la direction. Mon groupe a un chef des technologies d'innovation et des services partagés à la Banque TD.

Pour des raisons de gouvernance, nous avons pensé qu'il valait mieux séparer du secteur technologique le rôle du chef de la sécurité de l'information, tant par souci d'objectivité que parce que la cybersécurité relève en réalité du risque d'exploitation, non du risque technologique.

Nous trouvons que l'engagement de l'entreprise, en ce qui concerne les procédés et les produits et la façon de faire participer nos clients, est essentiel au succès de notre programme de cybersécurité.

Quant à votre autre question, je ne sais pas trop si vous parliez d'un pourcentage des dépenses ou de plafonds des dépenses.

● (1740)

M. Sven Spengemann: Il s'agissait du coût de la sécurité. Autrement dit, vos options sont-elles effectivement prescrites ou limitées par le marché actuel, ou y a-t-il des options créatives et même des différences entre les grandes banques en ce qui concerne le pourcentage qu'elles consacrent à la sécurité par rapport aux coûts d'exploitation totaux?

M. Glenn Foster: Je pense que cela varie d'une banque à l'autre, en partie parce que nous ne sommes pas nécessairement tous organisés exactement de la même façon. Si vous prenez n'importe quelle organisation de sécurité de l'information, c'est la règle du 80-20: 80 % d'entre nous avons les mêmes choses dans notre organisation, et 20 % peuvent être fédérés ou décentralisés dans d'autres secteurs. Il est très difficile de comparer des pommes et des oranges.

À la Banque TD, la cybersécurité est le risque jugé primordial. Je n'ai aucun problème à obtenir des budgets. Nous avons le soutien de la haute direction et du conseil d'administration. Toute contrainte à laquelle j'aurais à faire face prendrait probablement la forme de deux choses.

Premièrement, il y a la quantité de changements que l'organisation peut subir au cours d'une année donnée. C'est un domaine qui évolue rapidement. Mes dépenses augmentent à un taux annuel composé d'environ 35 à 40 % d'une année à l'autre. C'est beaucoup de changements à faire absorber par l'organisation.

Deuxièmement, il y a l'offre de produits commerciaux. L'explosion, comme je l'appellerais, des produits de sécurité dans l'industrie rend très difficile de discerner le battage publicitaire de la protection légitime. Je dirais que pour les organisations les plus avancées — nous avons parlé des données massives et de l'intelligence artificielle —, la plus grande poussée dans les années à venir se ferait dans l'investissement dans nos propres compétences et dans nos spécialistes des données, et dans les moyens de résoudre les problèmes de nos applications sur mesure par opposition à celles des fournisseurs généralistes.

Le président: Merci, monsieur Spengemann.

Malheureusement, nous devons mettre un terme au témoignage de M. Foster.

Je tiens à vous remercier de votre patience.

Sur ce, la séance est levée.