CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 156 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le lundi 8 avril 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le lundi 8 avril 2019

● (1640)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Mesdames et messieurs, je constate que nous avons le quorum.

Mesdames et messieurs les témoins, je vous présente nos excuses pour les difficultés découlant des votes; cependant, nous n'y pouvons rien et nous sommes dans cette période de l'année.

Avant de commencer, il y a eu quelques discussions à propos de la motion proposée par M. Dubé. Je vais accorder la période généreuse d'une minute afin de voir si les membres souhaitent se pencher sur cette motion.

Ma première question... Je ne devrais même pas demander cela. Je devrais plutôt déclarer que nous discuterons de cette motion dans le cadre d'une séance publique, plutôt qu'à huis clos. Sinon, nous gaspillerons davantage de temps.

Monsieur Dubé, souhaitez-vous proposer votre motion? Nous verrons si nous pouvons régler cela en une minute.

M. Matthew Dubé (Beloeil—Chambly, NPD): J'espère qu'il me faudra moins de temps que cela. Je l'ai déjà présentée et j'en ai expliqué les motifs. C'est déjà consigné dans le compte rendu, donc je suis heureux de demander de passer aux voix.

Le président: Madame Sahota.

Mme Ruby Sahota (Brampton-Nord, Lib.): Je souhaite souligner que j'appuie la motion; toutefois, selon moi, le délai n'est pas très serré. La date limite est le 21 juin. À mon sens, il y a une certaine urgence en la matière, parce qu'un grand nombre de personnes se sentent mal à l'aise en ce qui concerne la façon dont le rapport a été diffusé initialement en décembre. Je recommanderais vivement que le ministre comparaisse dans les plus brefs délais.

Il s'agit d'un amendement favorable, pour ne pas permettre un délai aussi long, et qu'il comparaisse plutôt dès que possible.

Le président: Monsieur Dubé.

M. Matthew Dubé: Merci. Je comprends. Vu que notre comité a un calendrier chargé, j'apporterais un amendement pour que la motion se lise « à comparaître dans les plus brefs délais, mais au plus tard », et que l'on conserve la date qui figure déjà dans la motion, pour que l'expression « dans les plus brefs délais » ne signifie pas le moment où certains d'entre nous reviendront à la Chambre.

Mme Ruby Sahota: Oui, je crois que c'est un bon amendement.

Le président: D'accord, avons-nous un consensus quant à l'amendement?

Pour respecter la procédure, je dois demander à Mme Sahota de proposer l'amendement, et ensuite nous pourrons le mettre aux voix. Souhaitez-vous proposer votre amendement?

Mme Ruby Sahota: Oui, voici mon amendement: que la motion soit modifiée par adjonction, après les mots « à comparaître », de ce qui suit : « dans les plus brefs délais, mais ».

Le reste de la motion demeure inchangé.

Le président: Très bien. L'amendement est mis aux voix.

(L'amendement est adopté. [*Voir le Procès-verbal*])

(La motion modifiée est adoptée. [*Voir le Procès-verbal*])

Le président: C'est parfait. Merci beaucoup.

Nous allons maintenant porter notre attention aux témoins. Remarquez l'extraordinaire collaboration entre les membres du Comité de la sécurité publique, qu'on ne peut malheureusement pas retrouver ailleurs.

Nous accueillons d'abord Mme Terri O'Brien, d'Interac Corporation, qui sera suivie de M. Ferrabee et de M. Kyle, de Paiements Canada. Je vous remercie de votre patience.

Je vais vous demander de présenter vos exposés.

Je souligne à mes collègues qu'il est prévu que nous votions de nouveau à 17 h 30. Je présume que c'est à ce moment-là que la sonnerie d'appel retentira.

Le greffier du comité (M. Naaman Sugrue): Il se peut que la sonnerie retentisse à 17 heures.

Le président: D'accord, donc commençons au moins par les exposés. Nous avons entamé la réunion. Dieu merci.

Les membres consentent-ils de façon unanime à poursuivre les travaux jusqu'à ce que nous devions nous arrêter?

Des députés: D'accord.

Le président: Très bien. La séance sera peut-être prolongée d'environ 20 minutes.

Allez-y. Encore une fois, je vous prie de nous excuser des procédures, mais nous devons les respecter.

Madame O'Brien, allez-y.

Mme Terri O'Brien (agente principale de gestion des risques, Interac Corp.): Bonjour à tous. Je vous remercie beaucoup de l'occasion de présenter un exposé au Comité.

Je m'appelle Terri O'Brien. Je suis agente principale de gestion des risques à Interac Corp.

Dans ma déclaration préliminaire d'aujourd'hui, j'ai comme objectif de fournir des informations et des recommandations concernant la cybersécurité émanant de notre situation particulière dans le domaine des services financiers. Nombre d'entre vous connaissent déjà le service Interac. Comme des millions de Canadiens le font chaque jour, vous utilisez nos produits et nos services pour retirer de l'argent, effectuer des paiements et virer des fonds en toute sécurité et de façon pratique.

Ce que vous ne savez peut-être pas, c'est que la propriété et l'exploitation d'Interac sont entièrement canadiennes. Ce qui nous distingue, c'est non seulement nos racines canadiennes, mais aussi la confiance que nous accordent les Canadiens, confiance que nous avons gagnée au cours de nos 35 années d'existence. L'an passé, les Canadiens ont effectué 6,6 milliards de transactions et ont déplacé plus de 415 milliards de dollars à l'aide de notre gamme de produits, y compris le service de paiement par débit Interac et le service de virement électronique Interac.

Notre entreprise offre depuis des décennies des produits pour faciliter les paiements en temps réel entre les Canadiens, y compris notre service de virement électronique Interac, qui est offert depuis 2002. Bien entendu, la prestation de ces services comprend la détection des fraudes en temps réel, 24 heures sur 24, 7 jours sur 7. Les paiements en temps réel s'accompagnent de la nécessité d'offrir des capacités en matière de sécurité, de prévention et de détection en temps réel, que nous avons bâties au fil du temps. Nos capacités en temps réel relatives à la cybersécurité et aux fraudes aident les Canadiens à effectuer des transactions numériques en toute confiance à l'aide d'une variété de dispositifs et de plateformes, y compris des appareils mobiles. Cependant, nous respectons nos valeurs fondamentales, qui sont au coeur de notre histoire, notamment la responsabilité, la sécurité et la solidité de l'entreprise.

La sécurité constitue un élément clé de toutes nos activités, qu'il s'agisse de lutter contre la fraude dans notre réseau ou de protéger les renseignements financiers personnels des Canadiens. En conséquence, la cybersécurité est quelque chose à laquelle nous réfléchissons beaucoup.

Alors que notre économie et notre société sont devenues de plus en plus numériques, ce n'est un secret pour personne que le rythme de la cybercriminalité s'est accéléré. Comme vous l'avez assurément entendu dans certains témoignages, et comme nous l'avons lu et vu dans des rapports, il n'a jamais été aussi facile pour les gens dans le monde entier d'avoir accès à des biens et des services issus de la cybercriminalité. Les sites Web où l'on offre des produits liés à des activités frauduleuses et au cybercrime vendent actuellement de tout, de numéros de cartes de crédit à des authentifiants de comptes de médias sociaux de même que des attaques par déni de service. Tout cela est accessible grâce à un simple clic et moyennant plusieurs centaines de dollars.

À cet égard, les responsables d'Interac sont très satisfaits de constater que le gouvernement a créé le Centre canadien pour la cybersécurité l'an passé et a affecté de nouveaux fonds au domaine de la cybersécurité dans le dernier budget. Nous appuyons aussi la création de l'unité centralisée de lutte contre la cybercriminalité de la GRC.

Interac occupe une position unique au centre du secteur des services financiers au Canada. Nous agissons à titre de centre d'échange de paiements et de renseignements numériques visant à faciliter l'interopérabilité des paiements et des renseignements apparentés entre les banques canadiennes, les coopératives de crédit, les caisses populaires, les entités qui traitent les paiements, les entreprises et les consommateurs canadiens. En conséquence, notre situation unique nous permet de détecter des activités de cybercriminalité, y compris la fraude et le blanchiment d'argent, quand les fonds circulent dans notre système et entre les institutions.

Ainsi, Interac joue un rôle unique au centre de l'écosystème. Alors que chaque institution financière peut détecter des activités de fraude et de blanchiment d'argent dans les comptes de ses clients seulement, Interac peut déceler des activités criminelles dans toutes les institutions.

Afin de cerner des schémas d'activité criminelle, nous avons recours à des outils sophistiqués qui utilisent l'apprentissage machine et la modélisation comportementale prédictive. Quand nos systèmes relèvent un risque élevé d'activités frauduleuses, ou des activités qui soulèvent des soupçons à cet égard, nous prenons immédiatement des mesures, y compris l'arrêt ou l'interdiction de transactions.

Nous communiquons aussi directement avec les institutions de l'ensemble du système financier. Nous collaborons et échangeons des renseignements pour renforcer notre résilience et notre sécurité collectives dans l'économie canadienne. Pour vous donner un exemple pratique, cela s'applique quand nous constatons que des criminels financiers utilisent de nombreux comptes différents pour cibler une banque, une coopérative de crédit ou une caisse populaire en particulier. Dans cette situation, nous alertons l'institution visée, tout en travaillant simultanément à bloquer l'activité et à éliminer les vulnérabilités dans les différentes institutions d'envoi.

Parce que la cybercriminalité peut frapper à toute heure, nous ne baissons jamais la garde. Nos systèmes de détection et de prévention fonctionnent 24 heures sur 24, 7 jours sur 7, et nous avons toujours du personnel en poste, ce qui nous permet de lutter contre la cybercriminalité en temps quasi réel.

Nous améliorons constamment notre approche pour assurer la sécurité des transactions effectuées par les Canadiens au moyen de nos réseaux. En 2018, nos pratiques en matière d'atténuation des risques liés à la fraude ont permis de prévenir plus de 100 millions de dollars en perte causée par des fraudes, et nous avons fait fermer plus de 4 300 sites Web malveillants.

Nous collaborons aussi maintenant avec la GRC et les forces policières locales pour les soutenir et leur fournir de l'aide dans le cadre d'enquêtes liées à la fraude et aux activités criminelles connexes. La protection des renseignements financiers des Canadiens dans l'environnement changeant des modes de paiement constitue la principale priorité d'Interac.

● (1645)

Depuis la création des portefeuilles électroniques, les consommateurs effectuent maintenant des paiements à l'aide de téléphones intelligents et d'autres appareils, vu que les paiements mobiles sont de plus en plus populaires auprès des consommateurs canadiens et répandus dans les commerces.

Afin de sécuriser les transactions effectuées à l'aide du réseau de paiement par carte de débit sur appareils mobiles, Interac a été, à l'échelle internationale, parmi les premières entreprises offrant un réseau national de paiement par débit à devenir fournisseur de service de jeton, ou FSJ. La plateforme FSJ d'Interac fait en sorte que les renseignements personnels liés à l'identité, y compris les numéros de compte, sont remplacés par des informations randomisées, ou des jetons, qui ne peuvent être utilisées par des pirates informatiques ou par d'autres criminels.

Accroître l'utilisation des jetons constitue une façon pour nous d'améliorer la cybersécurité au bénéfice des Canadiens. La collaboration et la coordination entre les entités privées et publiques jouent aussi un rôle central pour combattre le grand nombre de cybermenaces qui existent de nos jours.

À nos yeux, il y a trois domaines d'intérêt particulier qui peuvent grandement profiter aux Canadiens. Le premier concerne l'échange de renseignements avec les responsables de la nouvelle unité de lutte contre la cybercriminalité de la GRC. Le deuxième porte sur une approche plus ciblée de la détection des cybercriminels. Le troisième tient à l'éducation et à la sensibilisation continues du public.

Les responsables d'Interac sont d'avis qu'il y a une occasion de réduire les obstacles qui existent actuellement afin d'accroître l'échange de renseignements concernant des cybermenaces entre Interac et le gouvernement par l'entremise de canaux sécurisés et fiables. Pour cela, il faudra apporter des modifications législatives, de même qu'ajouter des dispositions refuges, afin de créer des canaux de communication et de dissiper les préoccupations touchant les mesures d'application.

Par ailleurs, en ce qui concerne la détection de cybermenaces, nous sommes d'avis qu'il est avantageux d'utiliser une approche plus ciblée comme point clé. La façon dont les cybermenaces sont détectées aujourd'hui s'apparente à la pêche à la drague, en ce sens que toutes les transactions font l'objet d'un examen et d'une analyse de même envergure. Un modèle plus efficace consisterait à mettre l'accent sur les listes de cybercriminels et de cybermenaces connus, ainsi que sur les vecteurs et comportements, en utilisant des renseignements provenant du gouvernement et des services de police, des institutions financières et d'Interac.

Interac pourrait jouer un rôle central à cet égard, compte tenu de sa capacité à détecter les activités criminelles dans l'ensemble de son réseau et de ses liens avec plus de 300 institutions financières. Interac, qui est au coeur de l'écosystème actuel, pourrait constituer un partenaire fiable en matière d'échange de renseignements avec la GRC à l'avenir, pour permettre aux deux organisations d'appliquer une approche ciblée à la détection et à la prévention des crimes, au lieu de soumettre toutes les transactions à un examen. Nous sommes d'avis que le gouvernement peut, et devrait, adopter un rôle de leadership en établissant et en maintenant des processus et des chaînes de responsabilité clairs.

Pour terminer, les responsables d'Interac reconnaissent qu'il est nécessaire d'informer et de sensibiliser de façon continue les Canadiens aux cybermenaces et aux pratiques exemplaires en matière de sécurité pour qu'ils connaissent davantage les risques actuels et les moyens de protéger leur sécurité. Nous menons de façon régulière des campagnes proactives conçues pour éduquer et informer. Nous participons aussi à des forums, comme le groupe de travail sur l'éducation du public du Bureau de la concurrence, pour échanger nos idées et communiquer nos résultats. Nous collaborons aussi activement avec la GRC et les organismes locaux d'application de la loi.

Nous serons heureux de collaborer davantage avec le gouvernement à l'avenir en matière d'échange de renseignements, de détection ciblée et d'éducation du public.

Enfin, j'aimerais souligner l'engagement d'Interac à l'égard de la cybersécurité et notre volonté de collaborer avec le gouvernement, comme nous le faisons aujourd'hui. Nous appuyons les initiatives et les investissements récents du gouvernement fédéral, et nous croyons que des activités continues d'éducation et des discussions comme celle-ci peuvent faire progresser des solutions à l'échelle de l'industrie pour aider à protéger les Canadiens contre la cybercriminalité.

Merci beaucoup.

● (1650)

Le président: Merci beaucoup, madame O'Brien.

Monsieur Ferrabee, allez-y.

[*Français*]

M. Justin Ferrabee (chef des opérations, Paiements Canada): Bonjour.

Je suis Justin Ferrabee. Je suis le chef des opérations de Paiements Canada.

[*Traduction*]

Merci d'avoir invité Paiements Canada à contribuer à l'étude.

Laissez-moi commencer par rassurer le Comité quant au fait qu'à Paiements Canada, la sécurité est notre plus grande priorité dans tout ce que nous faisons. Elle retient l'intérêt et exige des ressources et des investissements plus que tout autre besoin. Cela signifie que nous concevons, examinons, modifions, mettons à jour et exploitons nos systèmes pendant que nous surveillons les risques. Nous considérons la sécurité comme une condition préalable à l'innovation dans le milieu du paiement. Nous demeurons dans un état de vigilance constant et intervenons de façon décisive, au besoin, afin de nous assurer que nous gérons les risques adéquatement et que nous restons en sécurité.

Au cours des prochaines minutes, je vous expliquerai qui nous sommes et ce que nous faisons, je décrirai notre approche axée sur la collaboration en matière de cybersécurité, et je vous adresserai nos recommandations pour la réduction du risque dans le secteur financier.

Paiements Canada exploite les systèmes de compensation et de règlement nationaux du Canada. Même si l'organisme est peu connu de la plupart des Canadiens, il joue un rôle essentiel dans l'économie et dans les activités quotidiennes d'institutions financières et d'entreprises de partout au pays. Les systèmes de Paiements Canada permettent de s'assurer que les paiements entre institutions financières — l'ensemble des paiements effectués dans l'économie — sont effectués de façon sûre et sécurisée, chaque jour. La valeur des transferts est supérieure à 50 billions de dollars par année.

Nous sommes guidés par notre mandat et par les objectifs en matière de sécurité publique que sont la sûreté, la sécurité et l'efficience du système de compensation et de règlement canadien. En consultation avec les membres et les intervenants, nous maintenons également un cadre de règles et de normes qui atténuent les risques et facilitent l'échange de paiements et le déploiement de nouveaux produits et services de paiement.

Étant donné que les cybermenaces évoluent rapidement, Paiements Canada accroît continuellement ses défenses. Nous avons établi un plan d'action en matière de cybersécurité fondé sur des principes de conception sécurisés et sur les normes de l'industrie. Le plan garantit que nous surveillons constamment nos activités et que nous corrigeons les lacunes afin de maintenir leur résilience.

Paiements Canada fonctionne au sein d'un réseau d'institutions financières, d'organismes de réglementation et d'autres infrastructures des marchés financiers. Nous sommes tenus de respecter les normes de sécurité mondiales les plus élevées, y compris les consignes de la Banque des règlements internationaux intitulées *Guidance on Cyber Resilience for Financial Market Infrastructures*, le programme pour la sécurité de la clientèle de SWIFT et le Cadre de cybersécurité du NIST.

Nous travaillons également en étroite collaboration avec la Banque du Canada pour nous assurer que nous répondons aux exigences relatives à l'atténuation des cybermenaces au moyen d'évaluations internes et externes. En dehors de ces exigences, nous établissons des règles et des normes que nos membres doivent respecter relativement à la sécurité des effets de paiement et à la connectivité des systèmes.

D'un vaste point de vue industriel axé sur la collaboration, nous travaillons très étroitement avec des partenaires du secteur financier par l'entremise de groupes industriels du domaine de la cybersécurité, comme le Conseil canadien de gouvernance en matière de cybersécurité des services financiers, le groupe de spécialistes de la cybersécurité de l'Association des banquiers canadiens et du Financial Services Sharing and Analysis Center.

Par ailleurs, nous participons à des exercices pour la continuité des activités et la cyberrésilience au sein de l'industrie et dirigeons de tels exercices, et nous échangeons des renseignements avec des organismes et organisations partenaires dans le milieu de la cybersécurité. Il s'agit notamment du Centre canadien pour la cybersécurité, de la Direction générale de la protection des infrastructures essentielles de Sécurité publique Canada, de l'Équipe nationale des infrastructures essentielles de la GRC et de l'Échange canadien de menaces cybernétiques. En plus de ces collaborations, nous intervenons activement au sein du milieu international du cyberrisque avec nos partenaires de la Banque du Canada.

Dans le cadre de toutes ces activités, nous nous classons continuellement dans le premier percentile de l'industrie mondiale pour la sûreté et la sécurité et nous nous comparons constamment à nos homologues étrangers.

En étroite collaboration avec nos institutions financières membres, la Banque du Canada et le ministère des Finances, nous entreprenons actuellement un programme majeur visant à moderniser les systèmes de paiement du Canada afin de répondre à la demande croissante en produits de paiement nouveaux, sécuritaires et novateurs. La modernisation se soldera par l'établissement d'une nouvelle infrastructure de paiement conçue pour renforcer le système actuel.

Grâce à notre diligence et à notre progression vers des systèmes de paiement modernes, nous avons cerné des lacunes qui existent en dehors de notre domaine, sur lesquels l'étude pourrait avoir une incidence. La coordination entre les secteurs public et privé est manifestement nécessaire dans le cadre de la réaction aux attaques perpétrées contre l'infrastructure essentielle, de même qu'un point de contact unique et clair dans le secteur public. Ces améliorations nous aideront à mieux échanger de l'information, de façon protégée, ainsi qu'à gérer et à prévenir les futures attaques. La publication en 2018 de la Stratégie nationale de cybersécurité et les récentes avancées réalisées par le Centre canadien pour la cybersécurité seront utiles à ce chapitre.

En même temps, il faut rendre prioritaire la reprise des systèmes cybernétiques essentiels en cas de panne généralisée. Une politique qui étend les exigences en matière de cybersécurité jusqu'à la chaîne d'approvisionnement des systèmes essentiels contribuerait à l'amélioration de la résilience des composantes qui dépendent de l'infrastructure nationale et du système financier dans leur ensemble.

● (1655)

Des investissements dans les politiques et dans la cybersécurité peuvent également favoriser l'atténuation du risque pour la chaîne d'approvisionnement numérique. La chaîne d'approvisionnement moderne comprend souvent des centaines, voire des milliers, de composants logiciels qui sont intégrés dans des systèmes essentiels provenant d'entreprises et de communautés de partout dans le monde. Il est important de faire le suivi et l'inventaire de tous les composants d'un système et de s'assurer qu'ils restent sécurisés.

Dans le milieu de la salubrité des aliments, des normes d'étiquetage obligent les entreprises à informer les clients au sujet des ingrédients des produits et de leur valeur nutritive, mais, dans le monde informatique, aucune norme de ce genre n'aide les clients à comprendre quels composants et risques pourraient être associés au logiciel. Une politique favorisant l'atténuation du risque pour la chaîne d'approvisionnement numérique est nécessaire, et l'étiquetage systémique des composants logiciels devrait être étudié du point de vue de ses avantages pour l'économie.

En outre, nous croyons fermement que l'on pourrait en faire plus pour remédier à la pénurie de main-d'oeuvre qualifiée en matière de cybersécurité. On manque déjà de gens aptes et, compte tenu de la gravité croissante des menaces, on a besoin de politiques et de stratégies permettant de former, d'attirer et de maintenir en poste des travailleurs qualifiés. On pourrait ainsi s'assurer que les entreprises canadiennes sont capables de croître et d'innover en toute sécurité à mesure qu'elles étendent leur utilisation des technologies numériques.

Enfin, nous considérons qu'il faut informer et sensibiliser les Canadiens au sujet de l'importance d'une bonne hygiène cybernétique afin de protéger leurs renseignements personnels et financiers en ligne. Par exemple, actuellement, des millions de Canadiens recherchent des applications technologiques et financières qui imitent les services des systèmes bancaires ouverts. En cherchant ces services, ils regroupent des informations relatives à leurs comptes sur de multiples plateformes et s'exposent ainsi à des cybermenaces.

Paiements Canada a été ravi de constater que plusieurs de ces problèmes — et des engagements à l'égard de les régler — ont été inclus dans le budget fédéral de 2019, mais nous savons que les cybermenaces ne disparaîtront pas. Elles évoluent tout aussi rapidement, voire plus vite, que la numérisation et la modernisation dans toutes les industries. Nous devons travailler ensemble afin de renforcer la résilience face à ces menaces d'une manière qui garantira que l'innovation ne sera pas ralentie.

Même si toutes les organisations ont la responsabilité de se protéger contre les attaques cybernétiques, il est beaucoup plus efficace de le faire de façon collective ou sous la forme d'un réseau. La cybersécurité est un enjeu qui touche l'économie canadienne et notre sécurité nationale dans leur ensemble. Paiements Canada est enthousiaste à l'idée de contribuer à l'établissement d'une stratégie de défense fondée sur un réseau et de la soutenir.

Merci.

● (1700)

Le président: Merci.

Chers collègues, il nous reste 12 minutes. Si nous continuons jusqu'à cinq minutes avant le vote, vous obtiendriez quatre minutes, puis il y aurait un autre tour de quatre minutes, et ce serait à peu près tout.

Je vous demanderais ce que vous pensez de la possibilité que nous puissions revenir passer une heure auprès de ces personnes, si elles sont disponibles. Pouvons-nous faire cela?

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Je ne serai pas là.

Le président: D'accord, il n'y a pas de votes, pas de motions. C'est entendu. Nous reviendrons pour une heure. J'ai simplement l'impression que nous abusons du temps de ces personnes.

Nous serons de retour ici, probablement vers 17 h 30.

Sur ce, Mme Sahota dispose de quatre minutes, puis M. Paul-Hus aura le même temps de parole.

Mme Ruby Sahota: Merci.

Madame O'Brien, vous avez parlé de sites Web malveillants. À quelle fréquence observez-vous la création de tels sites Web? Quelle part de vos capacités est utilisée pour leur traçage? Pourriez-vous nous expliquer un peu comment vous tentez de sensibiliser les consommateurs afin qu'ils ne soient pas dupés?

Mme Terri O'Brien: L'an dernier, Interac a traité 4 300 de ces sites Web d'hameçonnage. Nous avons travaillé avec un chef de file de l'industrie, un de nos partenaires, afin de les retirer. C'est un partenaire semblable qui travaille auprès de nombreuses institutions financières. Les grandes institutions financières font l'expérience d'un bien plus grand nombre d'incidents d'hameçonnage ou de sites Web frauduleux qui sont créés.

Les sites Web sont conçus pour recueillir des renseignements personnels qui permettent d'identifier une personne — les justificatifs d'identité et autres renseignements du genre —, afin de pouvoir s'emparer de leurs comptes bancaires ou d'avoir accès à d'autres systèmes de traitement des paiements dans le but de vider les fonds. Voilà l'intention des gens qui créent ces sites Web. Nous constatons qu'ils se sont complexifiés au cours des dernières années. Je pense que les gens conviendraient du fait qu'ils s'améliorent pour ce qui est de voler les logos et les marques et d'avoir l'air de sites Web légitimes.

Nous participons activement à la sensibilisation du public à cet égard. Il est très important que vous sachiez que votre institution financière ne vous enverra pas de liens et de courriels afin que vous cliquiez et vous retrouviez sur ces sites Web malveillants. Nous avons des moyens de sensibiliser le public afin qu'il vérifie pour s'assurer qu'il se trouve bel et bien sur le site Web de sa propre institution financière ou sur le site Web d'Interac, pas sur un faux site.

Mme Ruby Sahota: Vous avez également abordé un peu les portefeuilles mobiles, et cela fait maintenant un moment qu'Interac utilise un système sans contact. Cette situation a-t-elle entraîné une augmentation au chapitre des incidences de la fraude? Renonçons-nous à la sécurité par souci de commodité? Pourrez-vous nous éclairer un peu à ce sujet?

Mme Terri O'Brien: En fait, je dirais que non. La technologie mobile est plus sécuritaire. Elle s'apparente à la technologie sans contact, alors elle utilise la technologie des cartes EMV. Cette technologie comprend un assez bon nombre de niveaux. J'ai également mentionné la création de jetons. Ce qui est stocké dans les téléphones, en réalité, c'est un jeton, pas le numéro de carte. On mise sur la technologie sans contact, qui est très sécuritaire. Nous avons presque éliminé la fraude par débit Interac. C'est en grande partie grâce aux cartes à puce et aux NIP. Ce qui reste, et le taux est vraiment bas — il ne pourrait pas être plus bas —, découle de codes malveillants exploitant une faille de sécurité aux États-Unis, où il existe encore des terminaux à bande magnétique, mais, effectivement, au Canada, cette technologie est extrêmement sécuritaire.

Mme Ruby Sahota: Nous avons un peu entendu parler du fournisseur de service de jeton par les témoins de Mastercard quand ils ont comparu. Je n'en avais jamais entendu parler auparavant. On dirait que — et corrigez-moi si je me trompe — ce système n'est pas utilisé constamment. Pourquoi Interac n'adopte-t-il pas complètement le système de jetons afin que les renseignements personnels soient éliminés?

● (1705)

Mme Terri O'Brien: Interac a élaboré et déployé son propre fournisseur de service de jeton. Il est exact de dire que nous n'avons recours aux services d'aucun autre fournisseur, que ce soit Mastercard ou un autre. Nous possédons notre propre fournisseur de service de jeton. Nous déployons notre propre technologie parce qu'elle est très sécuritaire et que nous pouvons gérer et maintenir les mesures de sécurité qui s'y rattachent.

Le président: Je vous remercie, madame Sahota.

[*Français*]

Monsieur Paul-Hus, vous avez la parole pour quatre minutes, s'il vous plaît.

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

Messieurs, je vous remercie de votre présence. Nous sommes désolés du chambardement dû aux votes à la Chambre.

Dans le cas d'Interac, si je fais un virement, le destinataire aura 30 jours pour accepter les fonds. À quel endroit l'argent qui sort de mon compte de banque virtuellement est-il gardé? Quel est le fonctionnement?

[*Traduction*]

Mme Terri O'Brien: C'est une très bonne question. Je pense qu'elle concerne notre produit Virement Interac, qui compte plusieurs options différentes. Le dépôt automatique est une transaction immédiate en temps réel. Celle que vous avez décrite, c'est notre service de transaction de type « question et réponse », où le destinataire doit répondre à une question de sécurité afin que l'argent soit déposé dans son compte. Dans ce cas, comme la personne ne consulte peut-être pas ses courriels tous les jours, elle dispose de 30 jours pour accepter le virement. Toutefois, ce qui arrive, dans le cas de la personne qui envoie la transaction, c'est que l'argent est retiré de son compte. Il s'agit d'un modèle de fonds immédiatement disponibles alors les fonds sont accessibles. Ils sont détenus par l'institution financière qui les envoie dans un compte en suspens, puis, une fois que le destinataire a répondu à la question de sécurité, ils sont libérés. Ils sont sécurisés en tout temps.

[*Français*]

M. Pierre Paul-Hus: Si j'ai bien compris, si je fais affaire avec la Banque Royale, l'argent ne s'en va pas chez Interac. L'argent va rester dans un compte de la Banque Royale.

En fait, souvent, il y a une inquiétude. Quand le transfert est effectué, on n'a plus de contact. On attend que le destinataire accepte les fonds. Par contre, si cette personne ne reçoit pas l'argent, on s'inquiète de savoir où est rendu l'argent. C'est donc la banque émettrice qui l'a.

J'essaie de comprendre le système technique. D'un point de vue virtuel, est-ce qu'une autre personne pourrait intercepter l'envoi? Est-ce possible qu'un pirate informatique intercepte un transfert? Dans un tel cas, qu'est-ce qui pourrait être fait?

[*Traduction*]

Mme Terri O'Brien: La réponse est non. Il s'agit d'un réseau privé en boucle infinie hautement sécurisé. Même si Interac exploite l'infrastructure, il a également établi la réglementation et la gouvernance des activités par lesquelles les fonds sont virés à partir de chaque institution financière. Ce que nous faisons, c'est fournir nos services aux institutions financières qui veulent offrir l'option du type « question et réponse ». Toutefois, la transaction ne pourrait à aucun moment être interceptée. L'argent est détenu en toute sécurité par l'institution financière, puis, une fois libéré, il est acheminé vers l'institution destinataire, de façon sécuritaire, par l'entremise de l'infrastructure d'Interac.

[*Français*]

M. Pierre Paul-Hus: Donc, vous dites que le chemin du transfert est parfaitement sécurisé. Il n'y a aucune possibilité d'intervenir.

[*Traduction*]

Mme Terri O'Brien: Exactement.

Nous disposons d'un réseau privé entièrement sécurisé et en circuit fermé parmi les quelque 300 institutions financières, coopératives de crédit et caisses populaires de tout le Canada.

[*Français*]

M. Pierre Paul-Hus: Vous avez parlé un peu du gouvernement. Quelles lois actuellement devraient être modifiées pour être plus efficaces pour vous? Il y a sûrement des mesures législatives qui ne sont pas efficaces, qui devraient être améliorées.

[*Traduction*]

Mme Terri O'Brien: C'est une excellente question.

Aujourd'hui, nous travaillons activement avec la GRC et les forces de l'ordre sur l'échange de certaines informations, même si cela nécessite souvent l'obtention d'une ordonnance de communication. Nous proposons que certaines mesures législatives relatives à la protection de la vie privée et d'autres dispositions refuges soient adoptées, ce qui permettrait d'avoir une approche beaucoup plus ciblée relativement aux canaux de confiance que nous avons aujourd'hui, ce qui nous permettrait de nous concentrer sur la cybercriminalité et de gérer cet enjeu de manière beaucoup plus ciblée.

Nous constatons que nos communications sont aujourd'hui assez efficaces, mais elles sont imprécises et limitées à bien des égards. Nous pensons que certaines dispositions législatives nous permettraient assurément d'accroître les échanges ouverts d'information, ce qui bénéficierait à...

Le président: Merci, monsieur Paul-Hus.

Sur ce, je vais suspendre la séance, et nous poursuivrons dès que possible pendant une autre heure. Il n'y aura aucune motion ou autre.

Encore une fois, je vous remercie de votre patience.

● (1705)

(Pause)

● (1725)

Le président: Nous reprenons. Je constate que nous avons le quorum.

Monsieur Motz, vous n'avez jamais été aussi populaire de toute votre vie.

Nous allons commencer par des séries de questions de quatre minutes, puis nous aurons des tours de quatre minutes, puis de cinq minutes. M. Dubé devrait normalement être le prochain, mais je ne le vois pas; je vais donc passer à M. Picard. Quand M. Dubé arrivera, nous reviendrons à lui.

Encore une fois, je vous remercie de votre patience.

Monsieur Picard, vous avez quatre minutes.

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

Madame O'Brien, vous avez parlé de cybercriminalité et de fraude. Quelle est la nature de la fraude que vous avez détectée sur votre système et à laquelle vous avez réagi dans le passé?

Mme Terri O'Brien: La fraude change constamment, et elle se propage également en fonction des vulnérabilités des différentes institutions financières. La fraude la plus courante que nous observons, c'est ce qu'on appelle la fraude impliquant la prise de contrôle de comptes. Dans l'exemple de tout à l'heure, nous avons parlé de certaines évaluations relatives à l'hameçonnage, aux justificatifs d'une personne ou aux renseignements personnels identifiables qui permettent aux criminels de prendre le contrôle des comptes bancaires de ces personnes. Ensuite, ils commencent une pratique systémique qui consiste à vider les comptes bancaires en question, pour parfois envoyer les fonds à différentes institutions de réception, et ainsi retirer l'argent du système financier.

À Interac, nous nous trouvons dans une position unique, car nous pouvons voir que la fraude s'étend d'une institution à une autre dans tout notre réseau et que l'argent est envoyé à différentes institutions financières. Nous avons élaboré un système de détection des fraudes qui reconnaît les tendances et qui peut détecter ce comportement. Ensuite, soit le système bloque les transactions, soit il les suspend pour qu'on puisse réaliser un examen approfondi.

M. Michel Picard: Quand vous bloquez une transaction, cela signifie qu'une personne qui se trouve quelque part possède les informations du titulaire de la carte. La personne peut donc ensuite avoir accès au compte bancaire du titulaire de la carte, et commencer à chercher à avoir plus que de l'argent, à obtenir des renseignements personnels qui peuvent être utilisés pour le vol d'identité et ainsi de suite. Vous pouvez bloquer une transaction, mais une partie des dommages a déjà été causée, et nous n'avons encore aucun contrôle sur le type d'informations qui ont été volées à ce stade.

● (1730)

Mme Terri O'Brien: Pas toujours. Je ne vais pas décrire tous les modèles comportementaux, mais je dirais que — il est à noter que 99,9 % des transactions sont approuvées, et que c'est simplement un indicateur de notre volume —, quand une transaction est réellement bloquée, c'est qu'il s'agit d'une opération frauduleuse connue. Nous disposons de renseignements qui nous permettent de reconnaître certaines transactions comme étant frauduleuses, généralement grâce à l'échange d'informations auquel nous participons activement avec les institutions financières, dans le cadre duquel nous recevons et transmettons de l'information. Cela arrive parfois avec la GRC et les forces de l'ordre également. C'est cet échange de renseignements qui est réellement essentiel pour que nous puissions bloquer les transactions frauduleuses connues. Dans le cas des blocages, les clients ne sont pas touchés.

M. Michel Picard: Nous sommes encore coincés avec les NIP à quatre chiffres, ce qui donne peut-être 10 000 combinaisons possibles. Est-ce suffisant de nos jours?

Mme Terri O'Brien: Je dirais que oui. Les cartes à puce et le NIP, les technologies des cartes à puce avec les niveaux de sécurité EMV, combinées au NIP connu uniquement par l'utilisateur, ont été très efficaces. Nous avons presque éradiqué la fraude sur les transactions Interac. La fraude se situe bien en deçà du point de référence. Comme je l'ai mentionné tout à l'heure, il s'agit seulement des derniers terminaux à bande magnétique aux États-Unis.

Je pense que c'est également efficace grâce à la sensibilisation du public. Le public a été beaucoup sensibilisé sur le fait de ne pas communiquer son NIP. Même dans les médias populaires, dans les émissions télévisées, on parle du fait que parfois, même des conjoints ne communiquent pas leur NIP entre eux. Sensibiliser le public sur la protection du NIP et sur le fait de le garder secret a été très efficace.

M. Michel Picard: Vous avez dit avoir un réseau privé dans les banques, mais quand j'achète quelque chose dans un magasin, ma transaction passe-t-elle par un réseau entièrement privé et fermé? Si ce n'est pas le cas, dois-je le faire sur Internet ou ailleurs pour que ce soit entièrement sécurisé?

Mme Terri O'Brien: Vous êtes entièrement en sécurité. Les claviers d'identification proviennent tous des acquéreurs et des services de traitement des paiements, et ils font tous partie du réseau en circuit fermé. Chaque point du réseau est sécurisé.

M. Michel Picard: Qu'en est-il du fait d'aller...

Le président: Merci, monsieur Picard.

Mme Terri O'Brien: Cela ne passe pas par un réseau Internet ouvert.

Le président: Je sais que vous étiez sur une lancée.

M. Michel Picard: Non, je sais. Merci.

Mme Terri O'Brien: Ce sont de bonnes questions. Merci.

Le président: Monsieur Cannings, bienvenue au Comité. Je vois que vous n'êtes pas M. Dubé.

M. Richard Cannings (Okanagan-Sud—Kootenay-Ouest, NPD): Non, pas à ma connaissance.

Le président: Nous avions réservé quatre minutes pour M. Dubé étant donné qu'il était le prochain intervenant, mais vous pouvez peut-être reprendre votre souffle, et nous reviendrons à vous.

M. Richard Cannings: J'aimerais reprendre mon souffle et comprendre de quoi nous parlons exactement.

Le président: Eh bien, nous essayons de comprendre la même chose.

Monsieur Motz, vous avez cinq minutes.

M. Glen Motz: Merci, monsieur le président.

Tout d'abord, je remercie les deux organisations d'être ici aujourd'hui.

Je commencerai par vous, madame O'Brien. Les Canadiens se demandent — et je pense connaître la réponse, mais vous pouvez peut-être nous éclairer — si les virements électroniques Interac sont traçables.

Mme Terri O'Brien: Pourriez-vous nous en dire plus sur la question? Que voulez-vous dire par traçables?

M. Glen Motz: Nous parlons aujourd'hui de la cybersécurité, donc si nous avons un problème avec un virement électronique, cette transaction est-elle traçable, s'il s'agit d'une personne mal intentionnée?

Mme Terri O'Brien: Une partie de mon témoignage aujourd'hui a porté sur le fait d'encourager la collaboration ouverte, d'augmenter l'échange d'information et d'adopter les dispositions refuges relativement à la GRC. Les transactions sont traçables. Toutefois, dans le contexte actuel, si la GRC est à la recherche d'une personne mal intentionnée, comme vous le dites, elle gardera secrètes certaines informations sur cette personne. Elle émettra parfois une ordonnance de communication, auquel cas nous communiquerons l'information que nous avons, comme l'exige la loi, et elle continuera son enquête sur cette personne.

Chez Interac, nous échangeons certaines informations avec les institutions financières et les forces de l'ordre. Nous pouvons donc disposer d'indicateurs qui guident nos modèles comportementaux, mais la GRC nous communique la façon dont elle retrace les personnes mal intentionnées dès qu'elle est en mesure de le faire.

● (1735)

M. Glen Motz: Merci.

Dans votre déclaration préliminaire, vous avez parlé d'un système d'échange proactif; du moins, je crois que c'est le terme que vous avez utilisé.

Pourriez-vous nous décrire, dans un monde idéal, quel serait le type d'échange entre votre organisation ou l'industrie de manière générale et les forces de l'ordre pour protéger les consommateurs? À quoi cela ressemblerait-il?

Mme Terri O'Brien: Bien sûr. Je serai heureuse d'utiliser mon don de voyance et de proposer quelques bonnes idées. Nous adorerions certainement...L'unité de la cybercriminalité, en particulier au sein du gouvernement et de la GRC, ainsi que les forces de l'ordre surveilleront régulièrement certains sites de vente en ligne sur le Web indexé ou sur le Web invisible ou caché. Ces plateformes de vente en ligne ouvrent et ferment assez fréquemment, car ils tentent de cacher certains de leurs sites et certaines de leurs caractéristiques identifiables.

Dans un environnement d'échange ouvert, nous saurions cela très rapidement, et, par conséquent nous aurions la capacité — pour répondre à votre question de tout à l'heure — de tracer les personnes malveillantes qui apparaissent sur ces sites de vente en ligne en temps réel. Si cette information nous était ouvertement communiquée, nous pourrions en faire beaucoup plus pour bloquer ou surveiller les transactions potentiellement frauduleuses.

M. Glen Motz: Les représentants de Paiements Canada, pourraient-ils intervenir sur cette question? Dans un monde idéal, quel véhicule ou quel moyen les institutions financières ou le secteur financier auraient-ils pour échanger des informations avec les forces de l'ordre, de façon à mieux protéger les consommateurs, par rapport à ce que nous faisons maintenant?

M. Justin Ferrabee: Je vais laisser notre chef de la sécurité de l'information, Martin Kyle, répondre à cette question, car nous sommes actifs à cet égard.

M. Martin Kyle (chef de la sécurité de l'information, Paiements Canada): Il existe beaucoup d'organisations et de groupes d'échange qui sont déjà mis en place. Dans nos commentaires, nous avons un peu parlé d'un groupe d'échange d'informations avec l'Association des banquiers canadiens, par exemple. Nous avons parlé d'échange d'informations avec une organisation sans but lucratif, l'Échange canadien de menaces cybernétiques, dont un représentant a témoigné devant le Comité, je crois. Nous échangeons des informations avec le Centre canadien pour la cybersécurité et avec la GRC. Tous ces différents groupes d'échange nous permettent d'avoir davantage d'information sur les menaces existantes et d'apprendre à détecter ces menaces dans nos systèmes, ce qui nous permettra ensuite de réagir à ces menaces.

M. Glen Motz: Vous avez dit dans votre déclaration préliminaire que Paiements Canada transfère quotidiennement plus de 200 milliards de dollars par différents réseaux. Si c'est le cas, comment gardez-vous ces grosses sommes d'argent en sécurité pendant vos transferts? À quoi cela ressemble-t-il?

M. Martin Kyle: Comme vous le savez, notre priorité est la sécurité de ces transferts. Nous assurons la sécurité de nos systèmes en réduisant la surface d'attaque, comme nous l'appelons dans le métier. Nous avons un groupe de membres très restreint à qui nous autorisons l'accès à ce réseau, lequel est très distinct des autres réseaux. Cette petite surface d'attaque nous permet de prêter une grande attention à ce qui s'y passe et d'identifier les menaces, de surveiller les activités et de réagir aux choses qui se produisent en temps réel.

Le président: Merci, monsieur Motz.

Monsieur Cannings, avez-vous retrouvé votre souffle ou dois-je passer à Mme Dabrusin?

M. Richard Cannings: J'improviserai.

Le président: D'accord, vous avez quatre minutes.

M. Richard Cannings: Merci.

Comme vous pouvez le comprendre, je suis un peu surpris d'être ici. Je viens de descendre de l'avion et j'ai voté, puis on m'a amené ici. Malheureusement, je n'ai pas pu entendre votre témoignage. Je n'ai aucune idée des questions qui ont déjà été abordées dans cette étude non plus.

Une question me vient à l'esprit au sujet des paiements avec les cartes à puce. Vous avez peut-être abordé la question, et je m'en excuse dans ce cas. Le Canada a été un utilisateur précoce, du moins par rapport aux États-Unis. Je m'interroge sur deux choses. Est-ce un problème si le Canada utilise largement les cartes à puce et pas les États-Unis? Je ne sais pas si cela est en train de changer. Y a-t-il un problème entre les deux pays au sujet de la sécurité de ces systèmes? La situation aux États-Unis est-elle plus préoccupante qu'ici, ou vice versa?

● (1740)

Mme Terri O'Brien: C'est une très bonne question. Nous avons pratiquement éradiqué la fraude au Canada liée aux cartes de débit avec la puce et le NIP. C'est une technologie très efficace contre la fraude, doublée d'une mesure de contrôle, et seul le détenteur de la carte connaît le NIP. Jusqu'à présent, la technologie des cartes EMV a été très efficace.

Le fait que les États-Unis n'aient pas adopté la technologie EMV présente des risques pour nous. Le secteur exerce de plus en plus de pressions sur le pays pour qu'il l'adopte. Là-bas, le nombre de terminaux de point de vente permettant l'utilisation de cette technologie augmente. Dans certains terminaux de point de vente, il est possible d'utiliser la carte à puce et la signature, mais les États-Unis ne sont pas complètement passés à un environnement permettant l'utilisation des cartes à puce et à NIP.

C'est un très bon exemple d'une situation où un consortium du secteur, en collaboration avec les entreprises de traitement des paiements qui sont au coeur de l'industrie et les partenaires de règlements, peuvent lutter contre la fraude lorsqu'ils s'unissent pour trouver des solutions.

Aux États-Unis, les Canadiens courent certainement moins de risques, mais la fraude liée aux cartes à bande magnétique est toujours d'actualité.

M. Richard Cannings: Utiliser ma carte aux États-Unis pour acheter de l'essence présente un inconvénient, car on demande une carte à bande magnétique et un code postal. Bien entendu, les codes postaux canadiens ne fonctionnent pas là-bas.

M. David de Burgh Graham (Laurentides—Labelle, Lib.): Je peux vous l'expliquer.

M. Richard Cannings: Je ne sais pas. Au Texas, c'est un problème.

J'allais vous poser une question sur les copieurs de cartes et les puces. Cela ne présente-t-il pas un problème?

Mme Terri O'Brien: C'est beaucoup moins problématique pour ce qui est des cartes à puce et à NIP. Les copieurs de cartes existent toujours, bien qu'ils doivent être dotés de caméras pour saisir le NIP, mais ce n'est pas une méthode de fraude très astucieuse, car une main pourrait gêner la saisie du NIP. Donc, les risques sont minimes au Canada. Les copieurs de cartes qui copient la bande magnétique continuent de présenter un risque aux États-Unis. La bande magnétique est facile à copier.

M. Richard Cannings: Ce sera tout pour moi.

Merci.

Le président: Si vous avez besoin d'aide concernant le piratage, M. Graham peut vous aider.

Madame Dabrusin, vous disposez de cinq minutes, s'il vous plaît.

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

Ma première question s'adresse probablement davantage aux représentants de Paiements Canada. Je lisais une lettre que j'avais reçue d'une personne qui habite dans ma collectivité. Nous sommes à un point tournant où une personne peut encore signer un chèque en papier, mais le destinataire peut aussi maintenant le déposer en le prenant en photo. Toutefois, ce chèque continue de circuler avec le destinataire, qui détient les renseignements personnels et la signature de l'émetteur du chèque. Ce dernier compte sur cette personne pour qu'elle protège ses renseignements, quoiqu'il puisse s'agir d'un particulier qui ne dispose d'aucun moyen de les utiliser.

Vous a-t-on déjà informé que cela posait problème? Si c'est le cas, avez-vous des conseils à donner aux personnes à ce sujet et sur ce qu'ils peuvent faire pour protéger leurs renseignements personnels?

M. Justin Ferrabee: Je peux parler au nom de Paiements Canada. Nous sommes à l'échelon de l'infrastructure. Nous rédigeons les règles portant sur la manière dont cela fonctionne, et nous exploitons les systèmes qui produisent l'imagerie des chèques et permettent la production de l'image numérique. Mais le consommateur est protégé et reçoit tous les services par l'entremise de sa banque. Nous appuyons la banque, soutenons nos membres à cet égard, mais la banque doit avoir des politiques.

Mme Julie Dabrusin: D'accord.

Mme Terri O'Brien: Au cours des nombreuses années où j'ai travaillé dans le domaine bancaire, j'ai pu constater que la technologie a grandement évolué et que l'imagerie des chèques fonctionne très bien à l'heure actuelle. Bien entendu, on encourage les clients à détruire le chèque une fois qu'il est déposé. Cependant, la détection de doubles de chèques s'est également grandement améliorée. Si une personne tente de déposer deux fois un chèque, il ne sera pas possible de le faire.

Mme Julie Dabrusin: Merci.

Je m'adresse aux représentants de Paiements Canada. Vous avez parlé de l'étiquetage dans les chaînes d'approvisionnement numériques et de la manière de créer un étiquetage adéquat. Y a-t-il quelqu'un au monde qui fait de l'étiquetage? Existe-t-il une norme à cet égard?

M. Martin Kyle: Non. En fait, c'est pourquoi nous...

Mme Terri O'Brien: J'en connais une.

Mme Julie Dabrusin: Vraiment?

Mme Terri O'Brien: Oui.

M. Martin Kyle: Allez-y, je vous prie.

Mme Terri O'Brien: J'ai examiné le modèle. Il est plutôt bon. Les responsables de SWIFT ont adopté un modèle dans lequel ils publient les normes de sécurité de tous leurs homologues, comme ils les appellent, non pas du point de vue d'un créancier, mais seulement d'un homologue du système. C'est un bon modèle que nous aimons beaucoup.

Cela permet à chacun des participants de l'écosystème... Si une institution financière ou une caisse populaire voit le niveau de sécurité diminuer et que cela ne répond pas aux normes, elle pourra atténuer ou limiter les risques liés à un partenariat entre institutions financières. Des choses très intéressantes ont été mises en place au cours de la dernière année.

● (1745)

Mme Julie Dabrusin: Sachant qu'il y a une seule norme et qu'une personne s'en occupe, quel rôle le gouvernement joue-t-il à cet égard? Le gouvernement doit-il adopter un modèle d'étiquetage et l'imposer à nos institutions financières, ou s'agit-il d'un rôle qui revient à un autre secteur?

M. Martin Kyle: Je peux répondre à cette question.

Le programme de certification dont a fait mention Terri a été mis sur pied par l'organisation SWIFT pour permettre aux homologues de publier leurs certifications à l'intention d'autres parties. Si les responsables d'une organisation ont l'impression que l'autre organisation avec laquelle ils font affaire présente trop de risques, ils peuvent, en tant que propriétaires d'entreprise et grâce à leur certification, réduire eux-mêmes les risques ou demander à ce que certaines exigences soient respectées avant de continuer à faire affaire avec cette organisation.

M. Justin Ferrabee: J'aimerais revenir sur la question de l'étiquetage des composants. La certification est une version de cela, mais c'est une version préliminaire. Il n'existe aucun précédent permettant de définir tous les éléments de la chaîne de valeur et de les communiquer et les gérer. Cela comprend de nombreux aspects. À notre connaissance, cela ne se fait pas ailleurs.

Mme Julie Dabrusin: Selon ce que nous avons entendu, je crois, en partie, que cela se fait de plus en plus de l'autre côté de la frontière. Cela n'est pas unique au Canada, pour ce qui est de la manière de s'y prendre. Je tente de savoir quelle entité, quelle organisation est la mieux placée pour permettre au gouvernement canadien de collaborer à cet égard. Nous pouvons encourager d'autres gouvernements internationaux à participer, mais à qui la responsabilité devrait-elle revenir?

Mme Terri O'Brien: C'est une excellente question. SWIFT est une organisation mondiale qui a emprunté cette voie très tôt. Je proposerais certainement d'inclure aussi Interac. À l'heure actuelle, nous appliquons nos règlements opérationnels et nos normes minimales, qu'il s'agisse de normes de sécurité ou de normes relatives aux participants, à l'égard de toutes les institutions financières de notre écosystème.

Nous avons mis en place une politique de gouvernance très rigoureuse et des règlements opérationnels dans le marché d'aujourd'hui. Chaque jour, nous cherchons un moyen d'améliorer ces règlements au sein du marché. Les participants prennent part au marché avec enthousiasme et respectent ces règlements, car ils leur assurent la réciprocité des paiements et l'accès à l'écosystème.

Mme Julie Dabrusin: Merci.

Le président: Merci, madame Dabrusin.

Monsieur Motz, vous avez cinq minutes.

M. Glen Motz: Merci, monsieur le président.

Je suis certain que vous avez entendu ou lu que le Canada doit décider si Huawei fera désormais partie de notre importante infrastructure. À l'approche de la technologie 5G, je me demande si les plateformes de vos deux organisations sont prêtes à utiliser des serveurs qui sont mis au point, en totalité ou en partie, par des entités étrangères susceptibles d'être assujetties à des directives extrajudiciaires provenant d'un gouvernement étranger.

Mme Terri O'Brien: Je ne peux répondre qu'au nom d'Interac, mais je peux affirmer que ce n'est pas notre cas. Nous ne sommes pas disposés à permettre la sortie de données, compte tenu de la constitution canadienne et de nos racines. Notre société, qui a été constituée il y a environ un an, est solidement enracinée au Canada. Toutes nos données doivent demeurer au pays. Nous faisons également appel à des fournisseurs canadiens pour la prestation de tous nos services, mais nous concevons nos propres technologies. Pour répondre à votre question sur les fournisseurs de services étrangers, je dirais que nos racines sont profondément canadiennes.

M. Glen Motz: Avant d'entendre la réponse des représentants de Paiements Canada à la question que j'ai posée précédemment, j'aimerais faire suite à votre commentaire. Si un serveur ne provient pas d'une entité étrangère, que se passe-t-il si l'infrastructure avec laquelle on transfère des données peut être dotée de commutateurs qui peuvent être piratés par une entité étrangère? Comment cela a-t-il une incidence sur vos programmes de sécurité?

Mme Terri O'Brien: Toutes nos infrastructures et nos données demeurent au Canada et sont détenues et exploitées par Interac.

Pour répondre à votre question sur un pirate informatique étranger, je vous dirais, selon notre expérience, que la plupart des pirates informatiques sont étrangers. Nous n'avons vu que très peu de pirates informatiques canadiens.

● (1750)

M. Glen Motz: Ils accèdent à l'information par la porte dérobée; ils ne piratent pas le système. Il s'agit de certains intervenants étrangers qui, en raison de la technologie en place, pourraient intercepter des communications qui sont transmises au quotidien, sans même que nous le sachions.

Mme Terri O'Brien: Nous effectuons des analyses de vulnérabilité ainsi que des analyses rigoureuses de la sécurité. Nous utilisons uniquement des réseaux canadiens, faisons appel à des fournisseurs de services de télécommunications canadiens et disposons de centres de données canadiens dans différentes provinces. Nous effectuons nos transactions uniquement par l'entremise de nos centres de données canadiens. Donc, je ne m'attends pas à cela.

M. Glen Motz: D'accord. Merci.

Je m'adresse aux représentants de Paiements Canada. Quelle est votre réponse à la première question?

M. Justin Ferrabee: Comme vous pouvez le constater, nous ne parlons pas en détail de nos moyens ou de nos principes ni de la manière dont nous gérons notre infrastructure.

Vous soulevez un enjeu très grave dont nous sommes conscients et qui nous préoccupe. L'une des raisons pour lesquelles il faut assurer le suivi des composants de la chaîne d'approvisionnement, c'est que nous savons que, si un fournisseur de services offre une technologie dont il ne connaît peut-être pas la provenance, nous n'aurions aucun moyen de savoir.

Nous devons supposer que cela n'est ni sûr ni sécuritaire, et nous devons nous préparer à cela — et c'est ce que nous faisons. Nous sommes conscients de ces risques, mais sans ce genre d'information, même s'ils affirment que c'est vrai, ce n'est peut-être pas le cas. Nous ne pouvons nous permettre de courir ces risques. Nous effectuons donc notre planification comme si ce n'était pas le cas et tentons d'y arriver.

Le président: Vous disposez d'un peu plus d'une minute.

M. Glen Motz: Il y a quelque temps, une personne est venue témoigner devant le Comité — et j'ai posé cette question l'autre semaine — et a dit que les Canadiens sont innocents, qualification qui, selon moi, était une manière très polie de dire que nous ne connaissons rien de notre propre cybersécurité.

Selon vos points de vue respectifs, que faut-il changer au Canada pour que les clients comprennent la nécessité de faire preuve de plus de vigilance à l'égard de la cybersécurité et donc de protéger leurs renseignements confidentiels? Que pouvons-nous faire en tant que législateurs pour les inciter à prendre des mesures?

Mme Terri O'Brien: Je ne connais pas le contexte de ce commentaire du témoin, mais il semble porter davantage sur les connaissances de la population en général.

M. Glen Motz: Oui.

Mme Terri O'Brien: La capacité d'adaptation du Canada, en particulier à l'égard des institutions financières, est très solide à l'échelle mondiale.

Quant à votre question sur les clients canadiens, je suis d'accord. Je crois que l'éducation du public a une très grande importance. Il est certain qu'en cette période de l'année, compte tenu du nombre de fraudes liées à l'ARC qui se produisent, par l'intermédiaire d'appels téléphoniques et d'envois de courriels — et je suis convaincue que vous êtes tous au courant de la situation —, des Canadiens se font avoir par ces arnaques. Ils ne sont pas suffisamment informés pour savoir qu'ils doivent raccrocher le téléphone ou supprimer le courriel, et qu'ils doivent aussi renforcer le système de sécurité de leur ordinateur à domicile, car c'est une mesure importante à prendre.

Le président: Je vous remercie, monsieur Motz.

Monsieur Graham, vous avez cinq minutes.

M. David de Burgh Graham: Je vous remercie. J'espère que ce sera suffisant.

Monsieur Cannings, je vais vous dire comment fonctionnent les choses dont nous avons parlé plus tôt. Le code postal de votre bureau de circonscription est le V2A 5B7. Si vous essayez d'utiliser votre code postal, vous devrez utiliser les numéros suivants: deux, cinq et sept, et ajouter zéro, zéro.

Aux États-Unis, votre code postal pour utiliser votre carte est le 25700. Maintenant, vous savez comment cela fonctionne.

M. Richard Cannings: D'accord. La prochaine fois que je serai au Texas, je m'en souviendrai.

M. David de Burgh Graham: Faites bon voyage et n'oubliez pas que votre code postal est du domaine public. Tout le monde sait comment cela fonctionne à présent, alors voilà.

Le président: C'est peut-être de la fraude, mais c'est une autre question.

Des députés: Ha, ha!

M. David de Burgh Graham: Pour en revenir à la question qui nous occupe, il s'agit d'appareils fabriqués à l'étranger. Il y a une chose qui m'intrigue, et cela s'applique aux deux organisations. Lorsque des tiers vous fournissent un logiciel, ou encore du matériel, obtenez-vous toujours le code source, et procédez-vous vous-mêmes à la vérification et à la compilation?

M. Martin Kyle: Nous faisons des évaluations des risques pour tous les logiciels et les projets que nous déployons. Ces évaluations comprennent un inventaire des bibliothèques qui sont incluses dans les applications que nous élaborons, ainsi que les défauts associés à ces bibliothèques.

La chaîne d'approvisionnement numérique provient de partout dans le monde. Ce microphone provient probablement de nombreux différents pays, de sorte qu'il faut évaluer les risques que représentent les composants utilisés dans la fabrication de l'équipement. On doit évaluer les risques afin de déceler les vulnérabilités qui pourraient permettre à des groupes rivaux de s'infiltrer dans cet équipement ou dans un logiciel.

Lorsque nous déployons quelque chose, nous nous assurons qu'il est soumis à un processus rigoureux d'évaluation des risques dans le cadre duquel nous évaluons tout ce qu'il est possible d'évaluer.

● (1755)

M. David de Burgh Graham: La question centrale est de savoir si vous avez accès au code source de ce que vous utilisez, ou si vous vous dites ce qui suit lorsque vient le temps d'évaluer les risques: « Nous n'en avons pas besoin en l'occurrence, parce que nous faisons confiance à cette entreprise. »

M. Martin Kyle: Nous nous assurons d'effectuer des vérifications auprès des organisations qui nous fournissent le code source. Nous avons certainement accès à une partie du code source. Nous créons du code source. Lorsque nous n'y avons pas accès, nous suivons un processus rigoureux d'évaluation des risques auprès de l'entreprise qui nous le fournit.

M. David de Burgh Graham: Terri, est-ce pareil pour vous?

Mme Terri O'Brien: Pas vraiment. Tous nos systèmes à risque élevé et nos systèmes transactionnels s'appuient sur des codes propriétaires. Le code propriétaire signifie que nous avons une grande équipe de développement qui crée elle-même le code. Nous l'avons soumis à des normes de sécurité assez rigoureuses et à des analyses de vulnérabilité. Nous disposons d'un système de détection et de réponses géré, de protocoles de sécurité hiérarchisés assez robustes et d'un réseau privé en circuit fermé.

Nous avons, bien sûr, le code source, parce que nous avons une équipe qui l'écrit et nous avons des couches de sécurité très robustes. Nous revoyons constamment notre position en matière de sécurité.

M. David de Burgh Graham: Qu'est-ce qu'Interac sait au sujet d'une transaction? Si je vais au magasin et que j'achète quelque chose, que savez-vous à l'égard de la transaction?

Mme Terri O'Brien: Je peux dire au Comité que toutes les données satisfont aux normes minimales requises pour traiter la transaction et que tous les renseignements personnels permettant de vous identifier qui sont nécessaires pour faire la transaction dans votre compte bancaire et non dans celui d'une autre personne sont entièrement protégés.

M. David de Burgh Graham: Qu'en est-il de la raison de la transaction?

Mme Terri O'Brien: Parlez-vous du but et de l'utilisation prévue de l'objet de la transaction en ce qui concerne le commerçant chez qui celle-ci a été effectuée?

M. David de Burgh Graham: Si vous allez à la station-service et achetez de l'essence et une tablette de chocolat, Interac sait-il que vous avez acheté ces choses ou que vous êtes allé à la station-service?

Mme Terri O'Brien: Je ne peux pas communiquer tous les éléments de données qui sont recueillies, mais je crois que la transaction concerne le mouvement d'argent en soi. Cela ne concerne pas les biens et les services que vous achetez.

M. Richard Cannings: Faites attention à ce que vous achetez.

M. David de Burgh Graham: Cela s'applique à vous deux. Avez-vous des institutions membres qui ne respectent pas vos normes? Je sais que, dans le cas de Paiments Canada, l'adhésion est requise par la loi pour certaines organisations. C'est probablement la même chose pour Interac. Avez-vous des organisations trainardes après qui vous devez toujours courir et qui ne répondent pas à vos normes? Vous n'avez pas besoin de les nommer, mais y en a-t-il?

M. Martin Kyle: Je dirais que toutes les organisations qui participent à Paiements Canada ont des normes de sécurité élevées et qu'elles satisfont toutes à des normes très rigoureuses en matière de sûreté et de sécurité.

Mme Terri O'Brien: Je dirais tout à fait la même chose. En tant que centre de l'écosystème, Interac passe beaucoup de temps avec tous ses participants — et nous avons beaucoup plus de participants — afin de leur donner du temps pour la préparation et les essais lorsque nous rehaussons les normes de sécurité, ce que nous faisons constamment. Nous travaillons activement avec eux pour nous assurer qu'ils sont en mesure de respecter les nouvelles normes.

M. David de Burgh Graham: Je vous remercie.

Le président: Merci, monsieur Graham.

Monsieur Cannings, vous avez trois minutes si vous souhaitez les utiliser.

M. Richard Cannings: Vous me prenez par surprise.

Le président: Je peux revenir à quelqu'un d'autre.

M. Richard Cannings: D'accord. Je suis désolé, habituellement, dans mon comité, je n'ai jamais de deuxième chance.

Le président: Je vais revenir à moi-même et parler de ce qui m'intéresse.

J'ai ici ma carte Visa de la Banque CIBC et j'ai ma carte de débit. Pour des raisons de sécurité, je crois comprendre, d'après votre témoignage, madame O'Brien, que celle-ci est beaucoup plus sécuritaire que celle-là.

Mme Terri O'Brien: C'est exact. Je souscris à cette affirmation.

Le président: Pourquoi? Est-ce parce que vous avez 300 organisations pour celle-ci et que vous êtes en circuit fermé? Il y a des milliers d'organisations de plus pour celle-là.

Essentiellement...

M. David de Burgh Graham: John, faites attention de ne pas montrer les chiffres; la séance est télévisée.

Le président: Celle-ci a déjà été piratée. Celle-là ne peut pas être piratée.

M. Michel Picard: Il n'a pas d'argent de toute façon.

Le président: En effet, c'est exact.

Qu'y a-t-il dans la structure qui rend l'une plus sûre que l'autre?

Mme Terri O'Brien: Je pense qu'il y a de nombreux facteurs. Comme je l'ai mentionné plus tôt, Interac possède une structure de gouvernance et de réglementation opérationnelle très solide et hiérarchisée. Il ne s'agit pas seulement de la sécurité d'un réseau en circuit fermé. Il s'agit du niveau de sécurité des participants, des émetteurs et des acquéreurs, comme le niveau de sécurité du clavier NIP, ainsi que de divers degrés de types d'opérations et de structures de limites, ce qui est différent de certains de nos partenaires dans le secteur des cartes de crédit au Canada, qui peuvent avoir un goût du risque plus grand.

Ils ont différents types de participants dans leurs marchés et différents types de méthodes de surveillance de la fraude, de sorte que je ne peux pas parler du degré de surveillance de la fraude ni de leur goût du risque. Je sais simplement qu'il est plus grand que le nôtre à certains égards, en ce qui concerne les limites de certains types de cartes. Comme vous le savez peut-être bien en tant que consommateur, de nombreuses cartes ont des limites beaucoup plus élevées. Ce sont là des cibles beaucoup plus attrayantes pour la cybercriminalité que les cartes de débit.

● (1800)

Le président: Donc, cela ne dépend pas de la façon dont le système est mis en place ou de la sécurité qui y est intégrée; cela dépend du niveau de risque que nous voulons prendre pour être en mesure de faire un grand nombre de transactions.

Mme Terri O'Brien: Je pense que cela dépend des deux. C'est une approche multidimensionnelle. Cela repose sur la sécurité des participants, les règles de fonctionnement, la structure des limites, la surveillance des risques de fraude — c'est sans aucun doute un élément essentiel déterminant dans cet écosystème.

Le président: Je vous remercie.

J'ai une autre question au sujet du partage qui se fait entre les diverses institutions. Toutes les institutions n'auront pas le même degré d'intérêt — ce n'est pas tout à fait exact. Elles ont toutes un intérêt, mais elles auront des programmes différents. Plus particulièrement, le gouvernement aura un programme, les responsables de la sécurité auront un autre programme, les institutions financières en auront un autre, et il en va de même pour toutes les parties concernées.

Êtes-vous convaincue que, compte tenu des divers programmes en cours et des données que vous fournissez, la sécurité s'en trouve renforcée au bout du compte?

Mme Terri O'Brien: Je répondrais que oui, tout à fait. Elle est davantage améliorée grâce au nombre de partages de renseignements qu'il y a.

Bien sûr, nous participons, comme Justin et Martin l'ont dit, à de nombreux forums centraux, à la communication de renseignements dans certains comités, et l'ECMC a été un excellent ajout ces dernières années. Toutefois, la communication d'un événement en temps réel concernant un thème particulier ou un vecteur de menace qui se trouve sur le marché à un moment donné est vraiment essentielle pour détecter et prévenir la fraude. Cela profite ensuite à l'ensemble de l'écosystème. Chez Interac, nous communiquerons quotidiennement avec chaque institution financière, car ces facteurs de menace changent constamment. Cela s'est avéré très efficace.

Le président: Je suppose que Paiements Canada répondrait la même chose. N'est-ce pas? D'accord.

J'ai une dernière question pour Paiements Canada. Je n'ai jamais vraiment compris pourquoi, lorsque je paie une facture en ligne, l'argent sort manifestement de mon compte bancaire, mais il n'est pas crédité au vendeur avant un, deux ou trois jours. Je ne comprends pas pourquoi il ne s'agit pas d'une transaction instantanée. Avez-vous une réponse à cela?

M. Justin Ferrabee: Oui. En tant que couche d'infrastructure, nous n'interagissons pas avec les consommateurs au moment du paiement des factures; toutefois, une partie de notre programme de modernisation comprend la création d'une voie de paiement en temps réel, qui permettrait de faire exactement cela — éliminer le retard dans les dépôts, les retenues de chèques, les paiements de factures, etc. Donc, en croisant les doigts, vous verrez cela bientôt.

Le président: D'accord. Eh bien, j'attendrai cela jour et nuit.

Des députés: Ha, ha!

Le président: Nous passons à M. Cannings, puis à M. Eglinski.

M. Richard Cannings: Je vais simplement revenir sur ce que M. McKay demandait au sujet de la comparaison entre les cartes de crédit et le modèle Interac.

La semaine dernière, des représentants de MasterCard sont venus dans mon bureau me parler de leur système. Si je me souviens bien, MasterCard et Visa sont plutôt des intermédiaires entre les banques, les fournisseurs et les particuliers, alors qu'Interac dispose d'une sorte d'accès direct à votre compte bancaire. Je me demande simplement si cet accès direct au compte bancaire rend une transaction plus risquée, alors que les autres semblent avoir plus de couches où des mesures de sécurité pourraient être appliquées. C'est peut-être l'inverse. Je n'utilise pas beaucoup Interac, et ce n'est pas à cause de cela, mais je suis simplement curieux concernant cet accès direct aux comptes bancaires. Quel genre de questions de sécurité entrent en ligne de compte?

Mme Terri O'Brien: Je pense en réalité que le fait d'avoir un réseau privé en circuit fermé réduit le risque. Pour plus de précision, la connexion directe s'appelle une API, ou une interface de programmation d'applications que nous avons avec l'institution financière, par laquelle toutes les transactions passent. L'institution expéditrice — votre banque, par exemple — vérifierait que les fonds sont disponibles et les enverrait ensuite en temps réel à l'institution destinataire par l'intermédiaire de notre infrastructure de paiement, et nous serions en mesure de faciliter ces transferts. Je crois que le lien direct réduit les risques. Nous pouvons surveiller et gérer le système de façon appropriée.

● (1805)

M. Richard Cannings: M. McKay a également mentionné les paiements de factures, par exemple. Est-ce la même chose? Lorsque je paie une facture, je ne pense pas qu'Interac intervient, mais quand je le fais à ma banque, est-ce le même processus?

Mme Terri O'Brien: Interac effectue certaines de ces transactions, et nous examinons cela. Certainement, il est facile de comprendre les virements électroniques. Si vous payez un fournisseur de services, par exemple, un plombier pour une réparation chez vous, vous pouvez choisir d'utiliser le service Virement Interac, et ce sont des paiements en temps réel aujourd'hui.

L'interface de paiement de factures que vous pourriez utiliser, disons avec Rogers, pour payer votre facture de câblodistribution, par exemple... À l'heure actuelle, ces paiements sont retenus à l'institution financière et ensuite versés par lots. Nous travaillons activement avec les institutions financières afin que l'on puisse faire ces paiements en temps réel parce que nous sommes déjà en mesure de le faire, mais, aujourd'hui, ces paiements sont versés par lots par chaque institution financière canadienne. C'est ainsi que l'on a toujours procédé.

Le président: Merci, monsieur Cannings.

Nous avons maintenant M. Eglinski.

M. Jim Eglinski (Yellowhead, PCC): Merci.

La question porte sur Interac. Plus tôt, vous avez indiqué que vous gardiez tout sur des serveurs canadiens, mais vous offrez un service international aux titulaires de cartes étrangers, n'est-ce pas?

Mme Terri O'Brien: Notre produit débit Interac permet d'effectuer des transferts internationaux de fonds. Je pense que quelqu'un en a donné un exemple. Si on se trouve aux États-Unis et qu'on veut retirer de l'argent avec la carte Interac de sa banque, on pourrait utiliser le guichet automatique d'une autre banque. Nous offrons la possibilité de retirer des fonds lorsqu'on est dans un autre pays.

M. Jim Eglinski: Un étranger ne peut pas utiliser votre système. Entretenez-vous une relation avec des banques étrangères dans un tel cas?

Mme Terri O'Brien: Non, nous n'avons pas de relations avec des banques étrangères.

Si vous, à titre de consommateur canadien détenteur d'un compte bancaire canadien, choisissez de retirer des fonds au Texas, par exemple, vous pouvez le faire grâce à votre carte de débit Interac. Mais non, nous n'entretenons pas de relations avec des banques étrangères.

M. Jim Eglinski: Je pensais à la sécurité.

Je vais laisser la parole à mon collègue, qui a une question pour vous.

Mme Terri O'Brien: Certainement.

[*Français*]

M. Pierre Paul-Hus: Merci, monsieur Eglinski.

J'ai été absent quelques minutes. Je ne sais pas si la question a déjà été posée, mais je ne crois pas.

Combien d'attaques directes sur les systèmes subissez-vous, par jour ou par mois?

Par ailleurs, êtes-vous en mesure de nous dire d'où viennent les attaques? Sont-elles l'oeuvre d'individus, de gens au Canada ou à l'étranger? Des attaques sont-elles commises par des pays en particulier?

Les deux témoins peuvent répondre.

[*Traduction*]

M. Martin Kyle: Comme vous pouvez le comprendre, nous ne décrivons pas en détail nos capacités précises en matière de sécurité ou les incidents ou les événements liés à la sécurité. Je dirai simplement que l'industrie financière fait l'objet d'attaques en tout temps et de partout.

[*Français*]

M. Pierre Paul-Hus: Sans donner le détail de vos organisations, pouvez-vous dire de quels genres d'attaques il s'agit? Proviennent-elles plus d'individus isolés ou d'organisations? Pouvons-nous avoir ce type d'information?

[*Traduction*]

Mme Terri O'Brien: Il pourrait être important pour le Comité de faire la différence entre les tentatives d'attaque et les attaques elles-mêmes.

Je dirais que toutes les institutions financières, tous les fournisseurs d'écosystème de paiement et tous les fournisseurs de services de règlement vont subir des tentatives d'attaque. À Interac, nous gérons la détection et la réponse, alors lorsqu'on tente d'infiltrer notre système, nous pouvons le voir. Nous surveillons activement ces tentatives et nous les bloquons afin qu'elles ne se concrétisent pas.

Selon moi, relativement peu d'attaques sont lancées. Ce que je sais, par l'entremise de nos partenaires et de forums où on les signale, c'est que, au cours des dernières années, il s'est agi d'attaques sophistiquées. À mon avis, il y a très peu d'attaques isolées comme celles vous avez décrites. Ce sont plutôt des tentatives d'attaques sophistiquées.

[*Français*]

M. Pierre Paul-Hus: Avez-vous une obligation de divulgation auprès des banques? Vous êtes un intermédiaire entre les différentes banques. Lorsqu'il y a des menaces qui sont plus importantes, avez-vous un délai, un nombre d'heures où vous devez informer les banques et le gouvernement?

En ce qui concerne le gouvernement, je crois qu'il n'y a pas d'obligation de divulgation, mais, pour vos partenaires d'affaires, y a-t-il une obligation de divulgation?

● (1810)

[*Traduction*]

Mme Terri O'Brien: Nous n'avons pas d'obligation de divulgation auprès des diverses institutions financières. Ce n'est pas une exigence législative, mais nous avons des voies sécurisées par lesquelles nous pouvons communiquer une partie de cette information afin d'améliorer la sécurité et la solidité de l'écosystème. Nous allons communiquer l'information à l'institution financière concernée de façon très spécifique.

[*Français*]

M. Pierre Paul-Hus: Vous avez clairement parlé d'opérations sophistiquées, donc qui demandent des moyens énormes. Pouvez-vous nous donner une idée d'où viennent les menaces?

[*Traduction*]

Mme Terri O'Brien: Je pense que la nouvelle unité de cybersécurité de la GRC est probablement mieux placée pour dire d'où viennent les tentatives d'attaque dans le monde. Divers pays subissent certainement des tentatives d'attaque et des attaques, mais celles-ci changent d'endroit. C'est un problème mondial d'attaques sophistiquées.

[*Français*]

Le président: Merci, monsieur Paul-Hus.

[*Traduction*]

Vous avez cinq minutes, monsieur Spengemann.

M. Sven Spengemann (Mississauga—Lakeshore, Lib.): Merci beaucoup, monsieur le président.

Merci d'être avec nous.

J'aimerais donner suite aux questions de mon collègue M. Paul-Hus. Je siège également au Comité permanent de la défense nationale. Les infrastructures essentielles sont un des secteurs où il y a un certain chevauchement.

Sans entrer dans les détails, comme vous l'avez souligné, ou sans nous donner des renseignements qui ne devraient pas être divulgués, dans quelle mesure êtes-vous préoccupé, de façon générale, par une attaque de la part d'un autre pays, et à quel point considérez-vous faire partie de notre infrastructure de base? Je vais poser deux autres questions. Que se passera-t-il si votre service tombe en panne pendant une période prolongée en raison d'une attaque? Quelles seraient les répercussions pour le pays?

M. Martin Kyle: Tout d'abord, comme vous l'avez entendu, nous sommes en sécurité. La sécurité est notre principale priorité. Nous appuyons nos membres, les institutions financières au Canada, dans leurs programmes de sécurité, et ils nous appuient dans les nôtres. Les attaques et les menaces viennent de tous les côtés. Nous devons demeurer vigilants en tout temps, et nos membres doivent faire la même chose. Chaque citoyen canadien doit être responsable de sa propre sécurité. Nous croyons également que, ensemble, nous pouvons améliorer et renforcer la sécurité du pays tout entier.

M. Sven Spengemann: Travaillez-vous d'une quelconque façon avec des analystes ou du personnel du ministère de la Défense nationale pour vous protéger? Y a-t-il une collaboration sur des questions comme l'IA, la quantique et des choses qui toucheraient d'autres parties de nos infrastructures essentielles si on nous attaquait?

M. Martin Kyle: Absolument.

M. Sven Spengemann: Pouvez-vous nous en parler un peu plus en détail?

M. Martin Kyle: Non.

M. Sven Spengemann: D'accord.

Le financement est-il suffisant, selon votre évaluation, pour faire ce genre de travail? Y a-t-il d'autres aspects dans lesquels nous devrions investir davantage, que ce soit le talent, le travail structurel ou une façon différente de voir les choses, à mesure que nous passons à l'IA et à ces types d'enjeux?

M. Justin Ferrabee: Nous avons pleine confiance dans ce que nous avons à l'heure actuelle. Il y a toujours des possibilités et un besoin de continuer à réaliser des investissements et à améliorer les systèmes. Nous sommes certains d'avoir bien réagi, tout comme nos partenaires au gouvernement et ailleurs. Des besoins émergent également à mesure que nous progressons, comme vous l'avez entendu. C'est toujours de plus en plus exigeant, alors il faut poursuivre les investissements et possiblement les augmenter.

M. Sven Spengemann: Le degré de centralisation du système d'autorisation que nous avons au Canada est-il typique de celui d'autres démocraties développées — le G7 et le Groupe des cinq — ou serait-il justifié de décentraliser le système d'autorisation afin que toute attaque cause moins de dommages si elle réussit?

M. Justin Ferrabee: Notre système d'autorisation central est très similaire à celui d'autres pays du G7 et d'autres infrastructures financières de pointe. Nous cherchons toujours des possibilités de poursuivre le renforcement de la sécurité. Nous nous sentons en confiance relativement à la position dans laquelle nous nous trouvons actuellement et nous continuerons toujours d'être à l'affût. Nous avons effectué beaucoup de recherches, qui ont été publiées, sur les registres distribués et leur application. Le secteur moins vulnérable et le degré élevé de confiance entre les parties sont des facteurs qui diminuent le besoin d'avoir une sorte de registre distribué ou une nouvelle technologie à cet égard, mais nous examinons toujours la situation et investissons dans l'innovation.

● (1815)

M. Sven Spengemann: C'est très utile. Merci beaucoup.

Ma dernière question porte strictement sur un intérêt personnel.

Quel pourcentage des transactions de consommateurs au Canada, selon vous, sont effectuées de manière non électronique, c'est-à-dire avec de l'argent comptant? Quels types de tendances observez-vous? Avez-vous ces données?

M. Justin Ferrabee: Chaque année, nous publions un rapport intitulé « Les modes de paiement et les tendances des paiements au Canada », qui porte sur ce sujet. L'utilisation de l'argent comptant diminue. Nous pensons que l'argent comptant continuera à connaître un déclin, mais il ne disparaîtra jamais. C'est moins de 50 % maintenant, et il diminue à un taux d'environ 5 à 7 % par année.

M. Sven Spengemann: Merci beaucoup, monsieur le président.

Le président: Eh bien, je dois alors faire partie de la minorité en déclin.

C'est au tour de M. Picard et de M. Graham.

M. Michel Picard: Puis-je retirer de l'argent d'un guichet automatique à Londres ou à Paris?

Mme Terri O'Brien: Je crois que, en Europe, il y a certaines restrictions, mais, oui, vous pourriez certainement retirer de l'argent de certains guichets automatiques à Paris.

M. Michel Picard: Puis-je retirer de l'argent à Saint-Pétersbourg ou à Moscou?

Mme Terri O'Brien: Non, cela violerait les règles associées aux sanctions.

M. Michel Picard: Je ne peux pas du tout utiliser ma carte Interac en Russie.

Mme Terri O'Brien: Non. Nous respectons absolument toutes les règles associées aux sanctions du Canada.

M. Michel Picard: D'accord. J'ai terminé.

Le président: C'était rapide.

Monsieur Graham.

M. David de Burgh Graham: Je vais donner suite à une question qu'a posée plus tôt Mme Dabrusin sur la possible désuétude du chèque papier tel que nous le connaissons.

Est-il temps de laisser tomber les numéros de banque, les adresses et les signatures sur nos chèques et de passer à...? Je ne sais pas si nous pouvons avoir une version papier d'un jeton, mais existe-t-il une façon de faire cela?

Mme Terri O'Brien: Oui. Absolument.

Nous innovons tous les jours dans le domaine des nouvelles technologies de transmission de paiements. Je dirais que ce sont surtout les petites entreprises ainsi que les acheteurs au détail qui utilisent encore le chèque, mais dans une moindre mesure. On n'a plus vraiment besoin du chèque papier.

M. Justin Ferrabee: Nous constatons un déclin rapide chez les consommateurs. Des gens s'en servent encore, et, dans certaines circonstances, c'est la seule méthode de paiement qui va fonctionner, pour toutes sortes de raisons. Le plus grand besoin, c'est dans le secteur des petites entreprises, et on s'en sert habituellement pour gérer l'information parce que, à l'heure actuelle, elle ne circule pas de manière fluide dans l'ensemble du système pour ce qui est de toutes les notations; les petites entreprises reçoivent une copie du chèque et peuvent le voir.

Tant qu'on n'aura pas réglé ce problème, les chèques continueront d'être utilisés. Nous prenons un certain nombre de mesures en publiant des normes afin d'améliorer l'information qui voyage avec les paiements. Une des normes mondiales les plus récentes pour l'information est la norme ISO 20022, qui inclut d'énormes quantités d'information voyageant avec le paiement, ce qui permettrait à un propriétaire d'une petite entreprise de recevoir plus de renseignements, y compris une facture et toutes sortes d'informations qui l'accompagnent.

Nous pensons que, avec l'introduction d'un meilleur système d'information avec le paiement, le chèque connaîtra un déclin.

M. David de Burgh Graham: Le chèque continuera d'exister. Allez-vous retirer l'information du chèque papier?

M. Justin Ferrabee: Non. Nous allons la remplacer.

M. David de Burgh Graham: Vous allez complètement la remplacer. D'accord.

[*Français*]

Monsieur Picard, avez-vous autre chose à ajouter?

[*Traduction*]

M. Michel Picard: Je vais revenir à la Russie.

M. David de Burgh Graham: Les Russes s'en viennent.

M. Michel Picard: Une partie de la transaction, j'imagine... il peut s'avérer un peu compliqué de connaître chaque membre de votre groupe, mais si je retire de l'argent en Europe, les banques qui s'y trouvent font en quelque sorte partie de votre réseau. Je ne sais pas comment il fonctionne. Savez-vous, ou est-il possible de savoir, si les banques à l'extérieur de la Russie, en Europe et ailleurs, qui appartiennent à des intérêts russes, font partie de votre réseau?

Mme Terri O'Brien: Elles ne font certainement pas partie de notre réseau. Je dirais que l'écosystème financier au Canada est maintenant très mature et très solide pour ce qui est d'appliquer les sanctions et comprendre les agences de transfert et ces types de choses. Nous sécurisons assurément le réseau.

Nous effectuons très peu de transactions à l'extérieur du Canada, alors ce n'est pas un problème auquel nous nous heurtons ou que nous constatons.

M. Michel Picard: Maintenant j'ai terminé.

Le président: D'accord.

Monsieur Eglinski, voulez-vous poser d'autres questions?

M. Jim Eglinski: Je ne pense pas.

Le président: Monsieur Paul-Hus.

[*Français*]

M. Pierre Paul-Hus: Merci.

Nous avons rencontré des représentants de Mastercard. Chez Mastercard, il y a des *red teams*, qu'on appelle en français des « pirates éthiques ». Je sais qu'il y a des discussions sur le terme, et je ne sais pas comment vous le traduisez. Ce sont des gens qui travaillent à l'interne et qui vont vraiment essayer de briser, de déjouer le système pour voir s'il comporte des failles. Est-ce que vous avez des équipes semblables chez vous?

● (1820)

[*Traduction*]

Mme Terri O'Brien: Nous en avons. Nous avons une équipe solide chargée de la sécurité des TI, qui utilise un certain nombre d'outils pour nous permettre de balayer le système de façon proactive à la recherche de vulnérabilités et de gérer la capacité de détection et de réponse également. Nous balayons activement nos systèmes quotidiennement et nous nous tenons à jour.

[*Français*]

M. Pierre Paul-Hus: Vous avez des équipes internes en technologies de l'information. Vous faites des balayages de vérification, mais vous n'engagez pas véritablement de pirates informatiques, qui vont essayer de trouver les failles de votre système.

[*Traduction*]

Mme Terri O'Brien: Nous avons une très grosse équipe chargée de la sécurité des TI. Nous ne l'appelons pas une équipe de « pirates éthiques ». Nous l'appelons une équipe de « sécurité des TI ». C'est une grosse équipe qui effectue constamment de la vérification — nous appelons cela des tests de pénétration — et qui balaie le système. J'estime que c'est essentiellement la même chose. « Pirate éthique » et « agent de cybersécurité » sont des mots à la mode ces derniers temps.

[*Français*]

M. Pierre Paul-Hus: Je vous remercie.

[*Traduction*]

M. Justin Ferrabee: Je peux répondre pour Paiements Canada. Comme vous pouvez le constater, nous ne divulguons pas de détails par rapport aux techniques que nous utilisons, mais nous connaissons très bien ces techniques, en plus des autres, et nous utilisons celles qui sont les plus appropriées pour garantir la sécurité et la protection du système.

[*Français*]

M. Pierre Paul-Hus: Pour terminer, notre étude vise à voir le système bancaire et financier dans sa globalité sur le plan de la cybersécurité. Selon vous, en tant que partenaires du système bancaire, où serait la principale brèche de la cybersécurité?

[*Traduction*]

Mme Terri O'Brien: Nous constatons deux vulnérabilités, dont j'ai parlé plus tôt dans ma déclaration préliminaire. La première concerne l'incapacité du gouvernement, de la GRC et des forces de l'ordre d'échanger librement des renseignements. L'activité criminelle évolue rapidement. Il s'agit d'un environnement frauduleux en temps réel, la capacité à avoir accès à ces renseignements plus rapidement nous permettrait donc d'avoir des moyens de défense plus robustes que ceux que nous avons présentement.

La deuxième concerne l'éducation du public, comme vous le savez tous. L'éducation du public par rapport à ce qui devrait être fait et ce qui ne devrait pas être fait contribuerait grandement à sécuriser le système et l'écosystème.

[*Français*]

M. Pierre Paul-Hus: Oui, nous le savons.

[*Traduction*]

M. Justin Ferrabee: C'est un écosystème auquel bon nombre d'intervenants participent, et dans lequel le degré de capacité et le risque varient. Nous savons que nous sommes plus forts lorsque nous travaillons ensemble, et la réponse au repérage des vulnérabilités est de travailler ensemble pour les cerner et de faire chacun sa part pour les résoudre et les gérer. Voilà ce à quoi nous consacrons notre temps et nos efforts, et nous croyons que nos homologues font de même. Nous soutenons nos membres et tous ceux qui travaillent dans les institutions financières à cet égard, et nous sommes convaincus qu'il s'agit de la meilleure stratégie.

[*Français*]

M. Pierre Paul-Hus: Je vous remercie.

[*Traduction*]

Le président: M. Spengemann et M. Graham vont partager cinq minutes.

M. Sven Spengemann: Merci, monsieur le président.

Encore une fois, je comprends parfaitement que vous devez maintenir une certaine confidentialité, mais, aux yeux de ce comité ou de la population canadienne, nous avons parfois l'impression qu'il y a une différence qualitative entre une attaque commise ou organisée par un État et ce qui vient du secteur privé ou du monde clandestin. Y a-t-il une différence qualitative notable entre ces attaques? Est-ce qu'un État-nation a une plus grande capacité à nous causer du tort, ou est-ce injustifié, dans la mesure où, si nous luttons efficacement contre les attaques qui proviennent du « secteur privé », nous sommes bien équipés pour faire face à une attaque dirigée par un État ou à une série d'attaques coordonnées?

M. Martin Kyle: Certainement, les États-nations ont plus de ressources que la plupart des organisations criminelles, mais malheureusement, nous avons vu que quelques exploits qui ont été divulgués par des États-nations ont abouti entre les mains de criminels, ce qui crée un environnement de menace qui est en constante évolution. Bien que nous surveillons ces choses et que nous nous concentrons sur la sécurité du système national de paiement, nous reconnaissons qu'il faut continuer d'investir et de déployer des efforts pour remédier à toutes ces menaces.

M. Sven Spengemann: Les deux fronts s'équivalent, et si vous procédez de la bonne façon, vous pouvez les éviter, peu importe leur origine.

M. Martin Kyle: C'est exact.

M. Sven Spengemann: D'accord, voilà qui est utile. Merci.

Le président: Monsieur Graham.

M. David de Burgh Graham: Pour poursuivre un peu sur cette voie, l'intention d'un acteur étatique dans le système financier ne serait pas de prendre l'argent. Ce n'est pas son objectif. Il veut voir qui effectue des transactions avec qui, obtenir les métadonnées, comme nous aimons le dire, et être en position de miner le système s'il doit appuyer sur le bouton.

Est-ce que cela serait une évaluation exacte des acteurs étatiques au sein du système?

M. Martin Kyle: Il y a un certain nombre de choses qui motivent les différents acteurs étatiques. Nous avons vu par le passé que certains d'entre eux utilisent des systèmes financiers pour contourner les sanctions. D'autres ont des motivations différentes. Il y a une multitude de raisons possibles pour toute menace contre le système financier, et nous devons être au courant de toutes ces raisons et prendre des contre-mesures proactives contre ces menaces.

● (1825)

M. David de Burgh Graham: Si un pays étranger souhaitait miner notre structure financière, son intention ne serait pas de prendre des données, ce serait de paralyser le système. J'imagine que nous faisons tout notre possible pour empêcher que cela arrive également.

M. Justin Ferrabee: Nous ne pourrions pas donner de précision sur tout incident dont nous sommes au courant. Nous vous assurons que nous y réfléchissons et que nous prenons des mesures pour prévenir cela, et que nos collègues dans d'autres organisations autour de nous le font aussi. Il ne s'agit pas de quelque chose qui nous est inconnu ou dont nous ne sommes pas conscients. Nous nous concentrons clairement là-dessus.

Mme Terri O'Brien: Oui, et nos programmes respectifs en matière de résilience... Je ne peux parler qu'au nom d'Interac, mais nous avons un temps de fonctionnement de 99,9 %. Vous pouvez l'atteindre seulement si vous avez une stratégie en matière de résilience qui inclut une infrastructure très robuste pour réaliser cela, même en cas de détérioration du service ou de toute attaque qui pourrait tenter de perturber le service.

M. David de Burgh Graham: Dans un autre ordre d'idées, en ce qui a trait à la technologie EMV, que signifie EMV? Je ne me rappelle plus ce que signifie le « E », mais « M » signifie Mastercard et « V », Visa. Est-ce exact?

Mme Terri O'Brien: Vous savez, l'acronyme existe depuis une dizaine d'années environ, donc...

Le président: C'est un magasin de musique.

M. David de Burgh Graham: HMV, c'est autre chose.

Y a-t-il une différence qualitative entre les systèmes relatifs aux cartes de crédit et aux cartes de débit concernant tout ce dont nous venons de parler? Quelles sont les différences entre les deux réseaux et les deux systèmes? Non pas que votre position est biaisée, mais est-ce que l'un d'entre eux a un avantage par rapport à l'autre?

Mme Terri O'Brien: J'ai parlé de cela un peu plus tôt. Je ne peux parler que de notre réseau en circuit fermé, mais nous avons réellement une stratégie de sécurité multidimensionnelle relative à la surveillance des fraudes et une stratégie robuste en matière de sécurité et de risque. Il s'agit d'une multitude de normes de sécurité et de mesures de contrôle qui font partie de notre réseau.

Les réseaux Mastercard et Visa sont en grande partie établis à l'extérieur des États-Unis, et fonctionnent à l'échelle internationale; ils doivent donc répondre à un ensemble de normes différentes, respecter des structures de sécurité composées différemment et composer avec un goût du risque différent. Je ne peux pas vraiment parler de leurs réseaux. Je ne peux parler que de la protection et de la stabilité que le nôtre offre aux Canadiens.

Le président: Merci, monsieur Graham.

Juste avant que l'on termine, Wayne Gretzky a prononcé une phrase célèbre: on ne parle pas de l'endroit où se trouve la rondelle, on parle de l'endroit où elle se dirige. Quelques-uns des grands projets de votre industrie sont Apple, Amazon et bien d'autres. Est-ce que l'un d'entre vous laisserait entrer Apple dans ses systèmes?

Mme Terri O'Brien: Je peux vous dire, du point de vue d'Interac, que nous avons été les premiers à faire affaire avec Apple en insérant la carte de débit Interac dans l'application Apple Wallet. Il s'agissait de la technologie de fournisseur de services de jetons dont nous avons parlé plus tôt. Nous avons également la même carte de débit Interac dans Google Wallet, et également dans Samsung Wallet. Les Canadiens veulent pouvoir utiliser leur téléphone de la même façon qu'ils utilisent leur carte. Nous avons constaté que l'abstraction et la transformation en jetons sont extrêmement sécuritaires et constituent un très bon protocole de sécurité. En tirant profit de la technologie EMV, on a créé un produit très sécuritaire qui a fait l'objet de peu de fraudes.

Le président: Les consommateurs canadiens qui utilisent l'une de ces méthodes sont donc autant en sécurité que s'ils utilisaient directement un produit bancaire canadien.

Mme Terri O'Brien: C'est semblable à l'utilisation directe de votre carte de débit Interac.

Le président: D'accord.

Paiements Canada, c'est à vous.

M. Justin Ferrabee: Nous n'interagissons pas au point de vente et n'aurions aucune raison de faire affaire avec Apple en tant que fournisseur de services de paiement. Nos employés l'utiliseraient probablement, mais ce n'est pas quelque chose qui se trouve dans nos systèmes. Il ne s'agit pas d'un point d'interaction pour nous.

Le président: D'accord.

Merci de votre présence, et encore une fois, je tiens à vous remercier de votre patience. Nous l'avons mise à l'épreuve, mais les choses sont ce qu'elles sont. Merci de vos témoignages intéressants et utiles.

Mme Terri O'Brien: Je vous remercie de nous avoir reçus.

Le président: Sur ce, la séance est levée.