CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 154 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le lundi 1er avril 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le lundi 1er avril 2019

● (1600)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Mesdames et messieurs, nous avons le quorum, et nous avons perdu une demi-heure.

Je vais tout simplement demander à tous les témoins de venir directement à la table.

Ce que je propose à mes collègues, c'est de combiner nos groupes de témoins. J'ai parlé à tous les témoins et je leur ai demandé d'être prêts à présenter leurs exposés en moins de 10 minutes. Mon idée est de donner sept minutes à chaque témoin pour faire son exposé.

La première série de questions va durer six minutes, et la suivante, quatre minutes. Nous allons continuer aussi longtemps que nous le pouvons.

Je crois qu'il va y avoir un autre vote. Nous n'en sommes pas sûrs.

M. David de Burgh Graham (Laurentides—Labelle, Lib.): Est-ce que cela ne va pas durer toute la nuit?

Le président: Avez-vous apporté votre lit pliant?

Un député: Ha, ha!

Le président: D'accord. Sur ce, je vais vous demander le silence.

Je vais simplement demander aux témoins de présenter leurs exposés dans le même ordre que ce qui se trouve à l'ordre du jour: pour commencer, nous aurons M. Green, de Mastercard, puis M. Davies, de EY, M. Finlay, de Cybersecure Catalyst, et M. Gordon, d'Échange canadien de menaces cybernétiques.

Monsieur Green, vous avez sept minutes.

M. Ron Green (vice-président exécutif et chef de la sécurité, Mastercard Canada): Bonjour, et merci de m'avoir invité aujourd'hui.

Je tiens tout d'abord à féliciter le Comité d'avoir lancé cette étude. La cybersécurité représente l'un des plus grands défis que doivent relever les gouvernements et les entreprises, et les incidences sur la sécurité nationale, la stabilité financière et la protection des consommateurs peuvent être graves.

J'applaudis aussi le gouvernement du Canada qui a déployé la Stratégie nationale de cybersécurité et mis en place le Centre canadien pour la cybersécurité. J'ai eu la chance aujourd'hui de rencontrer les dirigeants du Centre, et je peux vous assurer que Mastercard sera heureuse de les épauler de toutes les manières possibles.

Pour Mastercard, la cybersécurité est une priorité mondiale. La sécurité et la protection sont des principes fondamentaux qui régissent toutes les facettes de nos activités, ainsi que les plateformes technologiques et les services de technologie novateurs que nous mettons en service. Nous savons que nos clients, les titulaires de cartes, les commerçants et d'autres partenaires comptent sur nous pour leur fournir des produits et des services sécurisés. Permettez-moi de mettre ceci en contexte.

Comme vous le savez probablement, Mastercard n'émet aucune carte de crédit ni n'a de contact direct avec les consommateurs. Les banques qui émettent nos cartes ont cette responsabilité.

Mastercard est une société technologique. Nous mettons à la disposition des consommateurs un réseau qui leur permet d'utiliser leur carte Mastercard presque partout dans le monde, dans plus de 210 pays et territoires, et de voir une transaction se réaliser en quelques secondes, ce qui permet des liens entre 2,5 milliards de titulaires de carte et des dizaines de millions de commerçants.

Pour que nous puissions apporter de la valeur aux banques, aux commerçants et aux consommateurs qui utilisent notre réseau, nous devons leur assurer sécurité et protection. Notre réseau ne doit donc souffrir d'aucune interruption.

Nous investissons aussi dans l'innovation: nous augmentons nos forces internes, nous acquérons des entreprises technologiques de pointe et nous continuons de collaborer avec les jeunes entreprises choisies dans le cadre de notre programme Start Path, dont cinq sont au Canada, et de les mettre en contact avec nos partenaires émetteurs pour que leurs affaires se développent. Le mois dernier, Mastercard a conclu une entente visant l'acquisition d'Ethoca, une société torontoise qui facilite la collaboration entre banques et commerçants pour combattre l'escroquerie en ligne.

C'est ce que nous faisons à un très haut niveau. Permettez-moi maintenant de vous faire part de nos conseils à l'intention du gouvernement. Ils sont regroupés en six volets.

Premièrement, dans un monde numérique de réseaux et d'interconnexions, nos solutions en matière de cybersécurité doivent convenir aux petites et moyennes entreprises. Les cybercriminels cherchent les points faibles d'un système avant de lancer une attaque. Nous devons donc fournir aux petites entreprises une structure qui protégera leurs opérations. Mastercard joue un rôle-clé dans la défense des PME, notamment par la mise en place du Cyber Readiness Institute, ou CRI, qui met l'accent sur l'application pratique d'outils à l'intention des PME. Le CRI facilite également la formation des employés à l'utilisation de ces outils de gestion des cyberrisques.

Pareillement, en février dernier, Mastercard et la Global Cyber Alliance ont lancé une solution de cyberdéfense conçue spécifiquement pour les PME. Ce produit gratuit propose en ligne, à l'échelle mondiale, du contenu informatif et des procédés servant à contrer les cyberattaques de plus en plus nombreuses. Cette trousse pratique comporte des outils opérationnels, des guides pratiques et des pratiques exemplaires reconnues, et elle sera régulièrement mise à jour.

Deuxièmement, les sociétés internationales sont souvent aux prises avec un nombre croissant de règlements en matière de cybersécurité qui se chevauchent dans différents pays. Ces règles doivent être harmonisées au moyen de paramètres communs. Nous savons que des progrès ont été réalisés dans le cadre des négociations pour le renouvellement de l'ALENA en ce qui concerne la conception d'une structure commune favorisant la gestion des cyberrisques, ce qui est encourageant.

Troisièmement, les processus de gestion et de vérification de l'identité doivent être améliorés, car de plus en plus d'objets sont connectés. Nous avons besoin d'un écosystème d'identité solide pour faciliter et sécuriser davantage les interactions et les transactions numériques et préserver la confidentialité des titulaires de carte.

Quatrièmement, avec l'Internet des objets, 30 milliards d'objets seront bientôt connectés. Ceci représente de gigantesques possibilités pour l'économie numérique, mais aussi de plus grands cyberrisques. Les gouvernements et le secteur privé devraient par conséquent établir des normes afin d'améliorer l'interopérabilité, la détection et la prévention des cybermenaces tout en éliminant toute friction de l'expérience utilisateur.

Cinquièmement, face à des cybermenaces croissantes, les gouvernements et le secteur privé manqueront d'employés détenant des compétences en cybersécurité. Il faut dès maintenant, partout dans le monde, entreprendre de former la prochaine génération de cyberexperts, et le gouvernement devrait contribuer à cet effort. Si vous avez des enfants ou des petits-enfants et que vous les rendez accros à la cybersécurité, ils pourront toujours très bien gagner leur vie parce que le nombre actuel de spécialistes de la cybersécurité ne suffit pas à répondre aux besoins qui sont bien réels.

Enfin, il faut que toutes les parties prenantes collaborent, se communiquent l'information et s'unissent pour lutter contre le cybercrime. Le président Obama avait commandé la mise en place d'un groupe de travail sur la cybersécurité auquel notre président et chef de la direction a siégé. Ce groupe a formulé des recommandations, et la création du CRI, que j'ai mentionné plus tôt, résulte directement de l'accent qu'il a mis sur la sécurité et les PME.

J'estime que cette question est si cruciale pour l'avenir de notre économie et de notre société qu'elle mérite l'attention d'intervenants aux plus hauts échelons. Mastercard est prête à mettre son expertise au service du gouvernement du Canada dans la même mesure.

Je pourrais parler pendant des heures de ce sujet, mais je vais m'arrêter ici. Je serai ravi de répondre à vos questions sur les aspects qui suscitent le plus votre intérêt. J'ai essayé de vous donner une bonne idée de ce que nous faisons et de ce que les gouvernements devraient accomplir d'après nous.

Je remercie encore une fois le Comité de m'avoir invité et je suis impatient de répondre à vos questions.

● (1605)

Le président: Je vous remercie, monsieur Green, et merci également d'avoir respecté le temps que vous aviez.

Nous écoutons maintenant M. Davies, pour sept minutes.

M. Thomas Davies (chef de fil mondial des services financiers et des affaires numériques, EY): Merci de nous avoir invités à venir vous donner de l'information et à répondre à vos questions sur la cybersécurité dans le secteur financier.

Je suis Thomas Davies, et je suis le dirigeant national de la cybersécurité des services financiers pour EY au Canada. Je suis également un conseiller spécial en matière de crimes financiers pour l'entreprise à l'échelle mondiale, et à ce titre, mon attention se porte particulièrement sur les menaces internes et externes. Avant de me joindre à EY, j'ai travaillé pendant huit ans comme directeur à la Banque Scotia, et mon rôle était d'assurer les trois lignes de défense.

Les cyberattaques sont en hausse, et le secteur des services financiers est considéré comme une cible de grande valeur à l'échelle mondiale. Le nombre de particuliers, d'organisations et d'États-nations qui ont accès à des outils de pointe a connu une croissance exponentielle, avec les offres de services que les organisations criminelles ont conçus et optimisés. Les attaques lancées contre les services financiers ne se limitent pas aux cyberatteintes. Ces attaques peuvent rapidement évoluer vers des activités de fraude et de blanchiment d'argent, ce qui exerce une pression sur les talents et les ressources financières de n'importe quelle organisation. Ces préoccupations sont exacerbées par la pénurie de professionnels qualifiés dans l'ensemble des domaines relatifs aux crimes financiers. L'accès non autorisé à des systèmes de paiement, à des réseaux de transactions ou à des données de clients pourrait avoir des répercussions importantes sur l'économie.

Pensez un instant aux conséquences de ne pas être en mesure d'utiliser votre carte de débit ou votre carte de crédit pendant une journée ou même une semaine. Imaginez plus d'un million de Canadiens qui essaient de retirer de l'argent pour payer l'épicerie, l'essence ou les médicaments. De nombreux organismes de réglementation dans le monde estiment que la capacité de résilience des services financiers en cas de cyberincident est au sommet des priorités pour garantir la santé économique, comme en font foi les nouvelles exigences de sécurité adoptées à Hong Kong, au Royaume-Uni et à New York.

Les Canadiens veulent obtenir un meilleur accès aux services financiers au moyen de plateformes numériques comme le système bancaire ouvert. Nous devons donc envisager d'incorporer des principes de sécurité et de protection de la vie privée à l'étape de la conception d'une solution. Ce faisant, nous contribuerons à inspirer confiance aux clients, à encourager l'adoption de ces méthodes et à réduire de façon proactive le risque de devoir apporter des correctifs coûteux ultérieurement. La mise en place de mesures préventives comme la formation et la sensibilisation, la gestion de l'accès, l'hygiène informatique, la gestion du risque lié à des tiers et la gouvernance d'entreprise aura pour effet de réduire la surface d'attaque de ces plateformes de même que la maintenance nécessaire à leur soutien.

Le Canada a la possibilité de devenir un chef de file mondial en matière de sécurité et de protection de la vie privée, tout en demeurant un grand innovateur dans les technologies financières. En poursuivant les efforts de communication des renseignements et de développement des talents par l'éducation des jeunes et l'éducation continue, et en sensibilisant davantage le public aux cybermenaces menant aux crimes financiers, nous pouvons nous préparer à faire face à cette menace croissante.

Merci.

Le président: Je vous remercie, monsieur Davies.

Je tiens à faire remarquer à mes collègues la façon dont les exposés sont présentés dans les délais.

Monsieur Finlay, de Cybersecure Catalyst, nous vous écoutons.

M. Charles Finlay (directeur exécutif, Cybersecure Catalyst): Monsieur le président, mesdames et messieurs les membres du Comité, je vous remercie beaucoup de me donner l'occasion de parler avec vous aujourd'hui.

Cybersecure Catalyst est un nouveau centre d'activités de cybersécurité qui a été créé l'année passée par l'Université Ryerson. Il est installé en permanence à Brampton et c'est là qu'il ouvrira à la fin de l'année. Le centre va collaborer étroitement avec les gouvernements et les organismes gouvernementaux de tous les niveaux, avec les partenaires du secteur privé et avec d'autres établissements universitaires de partout au Canada afin de stimuler la croissance et l'innovation dans l'écosystème de cybersécurité du Canada.

Nous allons offrir des programmes reposant sur quatre piliers. Nous allons offrir de la formation en cybersécurité à l'intention des actuels professionnels de la cybersécurité, ainsi que de la formation de base en cybersécurité à l'intention de ceux qui sont nouveaux dans le domaine. Nous allons soutenir l'augmentation de la capacité des entreprises canadiennes de cybersécurité grâce à un programme unique d'accélérateur commercial. Nous allons soutenir les partenariats de recherche appliquée et de développement en cybersécurité entre des établissements universitaires et des partenaires du secteur privé. Enfin, nous allons offrir des activités d'éducation du public en matière de cybersécurité en mettant l'accent sur les particuliers et les petites entreprises.

Au moment de concevoir le mandat de Cybersecure Catalyst, l'Université Ryerson a entrepris un long processus de consultation auprès de l'industrie et du gouvernement, entre autres, auprès de plusieurs institutions financières. Je pense que les résultats de ce processus de consultation sont importants pour notre discussion sur la cybersécurité dans le secteur financier comme enjeu de sécurité économique nationale. Quand nous avons demandé aux grandes institutions financières et à d'autres organismes du secteur privé de nous préciser ce qu'un centre universitaire de cybersécurité pouvait faire de plus utile pour eux, ils n'ont pas parlé d'un outil technologique particulier ou de progrès précis dans les sciences. Ils ont répondu massivement qu'il leur fallait plus de gens. D'autres personnes venues témoigner devant le Comité aujourd'hui vous ont dit la même chose. En particulier, des institutions financières ont indiqué qu'il fallait mettre à niveau les compétences de leur personnel existant pour répondre aux menaces émergentes, et qu'il fallait que plus de gens fassent leur entrée dans le secteur pour qu'ils puissent doter les postes de premier échelon au sein de leurs organisations. Toutes les grandes institutions financières au Canada ont de nombreux postes à doter dans le domaine de la cybersécurité.

Les données empiriques confirment ce que notre processus de consultation a révélé. Comme vous l'avez déjà entendu de la part d'autres témoins, en juillet 2018, Deloitte et la Toronto Financial Services Alliance ont publié un rapport qui estimait que la demande en personnel de cybersécurité au Canada augmente de 7 % par année et qu'il faudrait doter 8 000 postes en cybersécurité d'ici 2021.

Il est important de souligner que cette pénurie n'est pas qu'un problème de sécurité; c'est un problème de développement économique. Le manque de personnel de cybersécurité qualifié crée des problèmes de dotation pour les activités régulières de ces institutions financières, mais cela a également des répercussions sur la capacité des institutions de créer de nouveaux produits et services sûrs pour les marchés national et international. Ce qui est crucial, c'est que le manque de personnel qualifié a de graves répercussions sur la capacité de croissance des petites et moyennes entreprises canadiennes de cybersécurité.

Il y a une façon intéressante de voir le problème du manque de travailleurs en cybersécurité au Canada, et c'est de se rendre en Israël. Ce pays est généralement reconnu pour posséder le plus solide écosystème technologique en matière de cybersécurité dans le monde. Le gouvernement israélien a récemment créé un grand centre d'activités de cybersécurité dans une petite ville du désert du Néguev appelée Beersheba, à environ une heure en voiture de Tel-Aviv. En janvier, je suis allé à Beersheba non pas pour rencontrer des représentants de sociétés israéliennes, mais des représentants d'institutions financières canadiennes qui ont établi des bureaux là-bas parce qu'il leur est beaucoup plus facile de trouver des talents en cybersécurité en Israël qu'au Canada.

C'est là la mauvaise nouvelle. La bonne nouvelle, c'est que ce problème est bien compris et que des efforts sont déployés pour le résoudre. Les montants que le gouvernement fédéral a consacrés dans son budget de 2018 à la cybersécurité étaient considérables, surtout en ce qui concerne le Centre canadien pour la cybersécurité. Le centre agit déjà comme un partenaire et une voix d'importance pour le secteur de la cybersécurité au Canada. Dans le budget de 2019, qui a été rendu public récemment, le présent gouvernement a fait de la cybersécurité une priorité en allouant 80 millions de dollars aux institutions postsecondaires afin qu'elles accroissent le bassin de talents en cybersécurité au Canada, entre autres mesures.

Bien sûr, il y a toujours plus à faire. À notre avis, les programmes de formation devraient se concentrer sur deux cohortes clés: les jeunes de la maternelle à la 12e année, et les groupes démographiques qui sont gravement sous-représentés dans le secteur de la cybersécurité. Les jeunes n'ont pas nécessairement tendance à voir la cybersécurité comme un domaine d'études intéressant ou excitant ou comme une option d'emploi futur, mais cela peut changer avec la bonne stratégie de mobilisation.

● (1610)

Nous n'arriverons pas à résoudre le problème de la pénurie de personnel de cybersécurité des institutions financières ou de n'importe quel autre type d'institutions si nous n'ouvrons pas le secteur de la cybersécurité de manière à avoir plus de femmes, de membres de groupes racialisés, de nouveaux Canadiens, d'Autochtones, de vétérans et de personnes qui ont perdu leur emploi dans des secteurs existants. Il faut déployer des efforts afin d'offrir aux personnes de ces groupes des occasions de formation et de placement dans l'industrie, et c'est là-dessus que nous allons nous concentrer à Cybersecure Catalyst.

Enfin, à mesure que notre économie poursuit sa transformation, nous voyons des possibilités excitantes de réorienter des talents de secteurs d'où les travailleurs ont été déplacés vers le secteur de la cybersécurité, où le besoin de personnel qualifié est en croissance.

Je vous remercie beaucoup.

Je serai ravi de répondre à vos questions.

Le président: Merci, monsieur Finlay.

Monsieur Gordon, vous avez sept minutes.

M. Robert Gordon (directeur exécutif, Échange canadien de menaces cybernétiques): Merci, monsieur le président.

Je remercie le Comité de me donner l'occasion aujourd'hui de parler de la cybersécurité dans le secteur financier.

Je suis directeur exécutif de l'Échange canadien de menaces cybernétiques, l'ECMC. Je vais mettre en lumière le travail de l'ECMC parce que je crois qu'il a une incidence directe sur l'orientation actuelle des enquêtes de ce comité.

L'ECMC est un organisme à but non lucratif établi par le secteur privé et ayant deux vastes mandats. Premièrement, nous effectuons un échange de renseignements sur les menaces cybernétiques pour informer nos membres. Deuxièmement, nous offrons un centre de collaboration pour mettre en commun les pratiques exemplaires des professionnels de la cybersécurité. Notre organisme est relativement nouveau, puisqu'il a atteint la capacité opérationnelle de base il y a seulement deux ans. Je vais faire quelques autres observations sur nos services dans une minute.

Les principes fondateurs de l'ECMC le rendent unique. Premièrement, notre objectif est d'attirer des membres venant de tous les secteurs de l'économie, pas seulement des infrastructures essentielles. À l'heure actuelle, nous avons notamment des membres de cabinets comptables, du secteur de la santé, d'entreprises de construction, d'entreprises de divertissements, d'administrations aéroportuaires et d'entreprises de haute technologie.

Deuxièmement, les grandes entreprises qui ont fondé l'ECMC ont clairement indiqué que l'ECMC ne pouvait pas servir uniquement les grandes organisations. Nous devons attirer des PME. Dans tous les secteurs de l'économie, des organisations de toutes tailles subissent des cyberattaques. Nous sommes passés des neuf premiers membres fondateurs à un peu moins de 60 membres aujourd'hui, et d'autres demandes d'adhésion sont traitées toutes les semaines.

En janvier dernier, nous avons changé la composition et les barèmes tarifaires de notre organisme de manière à rendre l'adhésion plus attrayante pour les PME. Ces changements ont été bien reçus. Les petites organisations représentent maintenant 28 % de notre effectif, et nous déployons des efforts pour que ce nombre augmente considérablement. À mesure que nous augmentions le nombre de petites organisations, nous avons mis au point des rapports et des services adaptés aux besoins des propriétaires de petites entreprises.

Je vais souligner brièvement deux secteurs de prestation de services.

Nous exploitons un centre de mise en commun de renseignements sur les cybermenaces. L'information sur les menaces est fournie par les organisations qui participent. L'information qui est obtenue ainsi ne contient pas de renseignements personnels, et la source est anonyme.

L'ECMC reçoit aussi de l'information sur les cybermenaces de la part du nouveau centre de cybersécurité. Nous sommes heureux d'être la première organisation à avoir signé un accord de collaboration avec le nouveau centre. C'est un partenariat important pour l'ECMC et le gouvernement. Nous pensons que nous allons tirer parti de la pleine capacité du gouvernement en matière de cybersécurité, et le gouvernement profitera de l'élargissement de la portée de ses efforts auprès de petits segments de l'économie qu'il ne dessert plus, notamment à l'extérieur de l'infrastructure essentielle de base.

L'ECMC offre aussi à ses membres l'occasion de fournir au gouvernement de l'information liée aux menaces, tout en conservant leur anonymat. À mesure que nous prenons de l'expansion, nous allons permettre au gouvernement de mieux comprendre comment les cybermenaces ont des répercussions sur l'économie canadienne dans son ensemble.

Des témoins ont déjà mentionné à votre comité l'importance du développement de l'effectif dans le domaine de la cybersécurité pour défendre l'économie canadienne. L'ECMC joue un rôle en aidant le secteur privé à perfectionner et à tenir à jour les compétences nécessaires. Notre capacité à collaborer entre secteurs procure diverses façons de rassembler les professionnels de la cybersécurité pour mettre en commun leurs pratiques exemplaires et leurs idées. Les praticiens se réunissent pour discuter de nouveaux sujets, comme les nouvelles techniques utilisées par les pirates, les nouvelles technologies et stratégies de défense ainsi que les changements au paysage juridique que les entreprises devraient connaître. Nous offrons cette capacité au moyen de webinaires mensuels et d'activités de collaboration de vive voix. Le temps que les employés consacrent à ces activités contribue à leur maintien en poste et à leurs certifications professionnelles.

Les institutions financières comprennent l'importance de la collaboration, ce qui explique pourquoi les grandes banques du Canada font partie de l'ECMC. Les banques reconnaissent que la collaboration leur permet d'améliorer leurs moyens de défense et de rendre plus coûteuses les démarches des pirates. Nous offrons un forum unique d'échanges intersectoriels. À titre d'exemple de la relation bénéfique et unique de l'ECMC, du travail se fait au moyen de notre portail entre les institutions financières et les entreprises de télécommunications pour contrer des cybermenaces très précises.

Les banques ont mis au point une impressionnante capacité à défendre leurs réseaux contre les cyberattaques, et elles lancent maintenant une nouvelle initiative par l'entremise de l'ECMC. Elles aimeraient faire part de leur expertise aux PME et travailler avec nous pour renforcer la maturité des PME dans tous les secteurs de la chaîne d'approvisionnement, pas que ceux liés aux services financiers. Chaque banque a cerné un domaine de compétence et préparé des exposés qui portent sur les besoins des PME. Nous nous penchons actuellement sur le mécanisme de mise en oeuvre de cette importante initiative.

● (1615)

La collaboration commence par l'établissement d'une relation de confiance. L'ECMC offre un environnement propice à la confiance. Nous créons une communauté où les membres n'ont pas à mener leurs activités en vase clos. Lorsqu'une crise se produit, ils peuvent se tourner vers cette communauté pour obtenir de l'aide. La création de cette organisation qui permet de signaler les menaces et de mettre en commun les pratiques exemplaires d'entreprises de toutes tailles dans l'ensemble des secteurs est un des principaux piliers pour atteindre le niveau de sécurité souhaité dans le but de protéger la prospérité économique du Canada. La collaboration signifie qu'on n'a pas à tout faire seul, car nul d'entre nous n'est aussi futé que nous tous réunis.

Je suis impatient de répondre à vos questions.

Le président: Merci, monsieur Gordon.

Sur ce, monsieur Spengemann, vous avez la parole pendant six minutes, s'il vous plaît.

M. Sven Spengemann (Mississauga—Lakeshore, Lib.): Monsieur le président, merci beaucoup. Je vais partager mon temps avec mon collègue, M. de Burgh Graham.

Ma question est pour M. Green.

Merci d'être ici pour nous faire part de votre expertise. Je vous remercie aussi de votre service antérieur en tant qu'officier dans l'armée américaine. Je siège aussi au Comité permanent de la défense nationale, et du point de vue de nos forces armées, je veux juste vous dire à quel point nous chérissons notre amitié et notre alliance avec les États-Unis.

● (1620)

M. Ron Green: Merci.

M. Sven Spengemann: Vous avez eu l'occasion de visiter le Centre canadien pour la cybersécurité. Je m'intéresse aux PME. Selon vous qui comptez des clients parmi les PME, dans quelle mesure la cybersécurité est-elle un obstacle structurel pour les entreprises en démarrage au Canada? Que peut faire de plus ou mieux faire le gouvernement du Canada afin de faciliter l'accès aux points d'entrée du marché pour ces entreprises axées sur les données qui dépendent de la cybersécurité?

M. Ron Green: J'ai visité de nombreuses petites entreprises en démarrage, et je peux vous dire que pour beaucoup d'entre elles, la sécurité n'est peut-être pas la principale préoccupation. Il faut que cela fasse partie de tout ce que nous faisons, non seulement dans les petites entreprises, mais aussi en tant que personnes.

Quand vous sortez de votre maison tous les jours, vous verrouillez la porte. Vous avez besoin d'un certain niveau quotidien d'hygiène cybersécuritaire. Pour les entreprises, surtout celles qui ont des données à leur disposition, il faut que cela fasse partie de ce qu'elles font maintenant. Nous sommes arrivés au point où nous devons les aider à cet égard, grâce à la mise en commun des pratiques exemplaires et à un accès aux experts. C'est une des raisons pour lesquelles nous dialoguons avec la Global Cyber Alliance. Nous faisons partie de nombreux groupes qui fournissent des pratiques exemplaires et des façons de faire. Il faut effectivement offrir des outils aux petites entreprises pour les aider à faire quelque chose, plutôt que se contenter de leur dire à quelles mesures elles devraient réfléchir. Donnez-leur les outils et l'accès à l'expertise.

Au centre de cybersécurité, on se penche sans aucun doute sur des façons d'informer les petites entreprises. Elles n'auront jamais d'organismes de renseignement comme moi, mais on peut certainement décortiquer suffisamment l'information pour les aider dans leurs démarches visant à accroître la sécurité.

M. Sven Spengemann: C'est très utile.

Je vais céder la parole à mon collègue.

M. David de Burgh Graham: Merci.

Monsieur Davies, monsieur Green, je ne sais pas lequel d'entre vous peut répondre. De quelle façon assume-t-on la responsabilité dans les institutions financières qui subissent des pertes liées à la cybersécurité?

M. Ron Green: Lors d'incidents ou d'atteintes à la cybersécurité, la victime peut être victimisée à deux reprises. Il y a les acteurs malveillants qui volent l'argent, et ensuite des causes au civil et au criminel. Parfois, selon l'entreprise, la victime est taxée davantage, ou dépense plus d'argent.

En ce qui nous concerne, nous travaillons avec un organe composé de nos avocats, les avocats de l'entreprise acquéreuse et les commerçants qui contribuent à l'émission. Les organisations touchées établissent une indemnisation raisonnable. C'est ainsi pour les atteintes liées aux cartes de paiement. Cela peut être différent lorsqu'il est question d'autres atteintes.

M. David de Burgh Graham: Les institutions financières ont-elles une assurance pour ce qui est de la cybersécurité? Y a-t-il une police distincte à cette fin?

M. Ron Green: Il y a une assurance pour la cybersécurité. Je suppose que cela dépend du pays où on se trouve et des polices qui sont offertes. Je procède à un examen annuel rigoureux avec nos assureurs pour être certain de maintenir un bon niveau de sécurité pour l'organisation, afin de tirer parti des possibilités que nous offre l'assureur.

M. David de Burgh Graham: La question est d'ordre plus général. Quand vous engagez des professionnels de la cybersécurité, à quel niveau de vérification procédez-vous? Ce n'est pas une entrevue d'emploi normale, n'est-ce pas? Procédez-vous à une vérification pour être certains de ne pas accroître la vulnérabilité plutôt que de la réduire?

M. Thomas Davies: Je peux répondre à celle-ci.

Nous faisons une évaluation technique de la plupart... dans notre communauté. C'est une petite communauté, et nous bénéficions habituellement du fait que nous connaissons les travailleurs du milieu. C'est un avantage et un inconvénient, mais nous examinons souvent les références et les environnements dans lesquels une personne a travaillé avant et la façon dont le travail s'est fait. Nous suivons ensuite un processus de vérification technique pour comprendre. C'est habituellement un long cycle, qui a aussi ses aspects négatifs, puisqu'il nous faut plus de temps pour embaucher un professionnel sûr dans ce domaine.

M. David de Burgh Graham: Nous parlons, monsieur Finlay, de la nécessité d'accroître le nombre de personnes dans le domaine de la cybersécurité. Nous essayons de veiller, alors que nous procédons à une expansion massive, à ne pas — comme nous l'avons vu en 1999 avec la bulle technologique — faire venir plein de personnes dont les intentions ne concordent pas nécessairement avec ce que nous voulons.

A-t-on l'intention à un moment donné d'offrir un diplôme en cybersécurité qui est distinct du diplôme en sciences informatiques?

M. Charles Finlay: Cybersecure Catalyst mettra l'accent sur la formation offerte à ceux qui sont déjà professionnels de la cybersécurité et sur une formation initiale pour introduire de nouveaux professionnels dans le secteur. Nous n'allons pas pour l'instant mettre l'accent sur un diplôme offert à la sortie de Cybersecure Catalyst. Des programmes en cybersécurité sont mis au point par de nombreux établissements postsecondaires. Un grand nombre de ces établissements, y compris Ryerson, offrent des cours de cybersécurité. Nous mettons surtout l'accent sur la formation professionnelle, car, en toute franchise, c'est là que nous pensons avoir un effet immédiat au cours des deux ou trois prochaines années. C'est donc là-dessus que nous nous concentrons.

D'un bout à l'autre du pays, des établissements offrent toutes sortes de programmes d'études différents.

● (1625)

Le président: Merci.

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

[*Français*]

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

Monsieur Green, ce que vous avez dit dans votre présentation m'a plu. Je vois que Mastercard a vraiment établi des priorités et des façons de faire quant à l'identification, la protection, la détection et la réaction. Je trouve également intéressante l'alliance que vous avez avec les différentes compagnies.

Dans votre présentation, vous avez aussi offert des conseils aux gouvernements. Vous avez parlé d'arrimage entre les différents pays. J'aimerais savoir à quel niveau le Canada se situe. Quels sont les points forts du Canada et, surtout, les points faibles auxquels il devrait remédier?

[*Traduction*]

M. Ron Green: Je pense, heureusement, que le Canada donne l'exemple dans le domaine du développement technologique lié à la cybersécurité. J'ai mentionné Ethoca. Nous avons aussi acquis une entreprise appelée NuData, qui fournit une grande partie des dispositifs de contrôle de sécurité que nous activons dans nos appareils mobiles. Je pense que nous avons l'occasion de poursuivre ces efforts pour mettre au point de nouvelles solutions en matière de sécurité qui pourront aider le marché, le secteur des technologies financières. Je crois que c'est une solide position pour la suite. Cela permet aussi, en étant en plein centre, d'être très ouvert à une collaboration avec le secteur privé, ce qui signifie qu'il est possible de mettre en commun des renseignements de sécurité.

Il y a des choses que nous pouvons aborder globalement que vos équipes pourraient trouver intéressantes, et les entendre parler de nouvelles menaces nous permet de prévenir des situations de manière plus proactive. Cela m'intéresse vivement.

[*Français*]

M. Pierre Paul-Hus: Il y a différentes menaces. Certaines viennent d'individus qui essaient de pirater un système, mais il y a aussi des attaques de nos systèmes qui sont faites par des États voyous, par exemple la Chine.

Comme entreprise privée, comment réagissez-vous à une attaque cybernétique de la part d'un État? Vous attendez-vous à ce que le gouvernement du Canada intervienne? Les ressources gouvernementales devraient-elles intervenir? C'est vous qui allez prendre les premières mesures, mais avez-vous des attentes à l'égard du gouvernement en cas d'attaque perpétrée par un État?

[*Traduction*]

M. Ron Green: Nous devons nous défendre contre tout le monde, des particuliers aux États-nations. Nous pensons à tous les acteurs malveillants possibles, et nous mettons en place des moyens de défense par couches pour éliminer les retards et pour prévenir la réussite de ces attaques. Cependant, si ces acteurs réussissent, nous dépendrions beaucoup de nos partenaires gouvernementaux pour nous aider à en atténuer les effets, mais aussi, selon le type d'attaque, à prendre d'autres mesures. Je ne fais qu'assurer une défense — c'est ma vie —, mais s'il faut faire quelque chose d'autre, il faudrait que ce soit avec un de nos partenaires gouvernementaux.

[*Français*]

M. Pierre Paul-Hus: D'accord, merci.

Monsieur Finlay, on voit maintenant qu'il est important que tous les intervenants travaillent ensemble: le gouvernement, le secteur privé et le secteur universitaire. En effet, on parle de formation de la main-d'œuvre dans le domaine de la cybersécurité.

Avez-vous un conseil à nous donner pour qu'on assure que tous ces intervenants travaillent ensemble? Comme tout va très vite en matière de cybersécurité, l'élément primordial dans ce domaine est la rapidité. On ne doit pas s'empêtrer dans des mesures administratives trop lourdes. Avez-vous un conseil à nous donner?

● (1630)

[*Traduction*]

M. Charles Finlay: Je crois sincèrement que la création du Centre canadien pour la cybersécurité est une amélioration fondamentale à la position du Canada en matière de cybersécurité et au regroupement de tous les partenaires.

Vous avez indiqué correctement que l'industrie, le milieu universitaire et le gouvernement doivent travailler ensemble.

J'ai parlé d'Israël dans ma déclaration liminaire. Ce qui m'intéresse dans cet écosystème, c'est la mesure dans laquelle ces trois piliers de la société civile, si je puis dire, vont ensemble pour régler le problème de la cybersécurité. Je pense qu'il est très important que le Centre canadien pour la cybersécurité ait un rôle catalyseur pour rassembler ces acteurs. À titre de conseil, je crois que le gouvernement et l'administration ont une importante occasion de suggérer à tous les acteurs de travailler étroitement, et qu'ils devraient en faire un thème récurrent, dans le cadre de vos discussions sur la cybersécurité, à savoir que tout le monde doit collaborer.

[*Français*]

M. Pierre Paul-Hus: Ma prochaine question s'adresse à tous les témoins.

Actuellement, la population canadienne en général est-elle naïve relativement à la cybersécurité, selon vous?

[*Traduction*]

M. Thomas Davies: Je ne dirais pas qu'elle est naïve. Je pense que nous sommes un peu plus insensibles aux incidents de cybersécurité que d'autres cultures. Nous laissons les choses aller un peu plus rapidement. C'est ce que je dirais.

Le président: Allez-y, monsieur Green.

M. Ron Green: Je pense à l'époque où nous avons adopté des choses comme l'automobile. Pendant un certain temps, personne ne comprenait ni ne savait ce que cela signifiait, et nous sommes tous très chanceux d'être en vie, car personne n'avait de sièges ou de choses du genre. Lorsqu'on compare les voitures d'aujourd'hui à celles construites il y a longtemps, on voit que les choses ont beaucoup évolué, qu'elles se sont beaucoup améliorées. Nous sommes dans le même genre de cycle. Nous ne sommes pas naïfs, mais juste inconscients par rapport à ces choses. Nous devons nous en occuper.

Le président: Merci.

Monsieur Dubé, vous avez six minutes.

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

Monsieur Green, tout le concept lié au fait de ne pas être un émetteur de cartes est une chose que des gens de votre entreprise m'ont récemment aidé à comprendre. Cela complique beaucoup, je crois, la façon dont ce processus fonctionne.

Je me demande juste si vous pouvez m'expliquer certaines choses.

Mastercard est responsable des paiements, des transactions proprement dites, et il y a ensuite une carte, un appareil ou un site Web, qui sont en quelque sorte des tiers lorsqu'on utilise Apple Pay ou d'autres applications du genre. Il y a ensuite la banque, qui serait l'émettrice de cartes.

Dans ce triangle, si je puis dire, qui assume la responsabilité pour ce qui est, par exemple, de mes renseignements? Autrement dit, si je me sers de mon téléphone pour payer quelque chose et qu'il y a un problème, la responsabilité revient-elle aux banques, aux émetteurs de cartes, à MasterCard ou à Apple, si le problème est attribuable à Apple Pay? Comment cela fonctionne-t-il?

M. Ron Green: Cela dépend beaucoup de l'incident, de qui est le plus responsable du problème qui survient. D'abord et avant tout, le pirate est la première personne. C'est lui qui a commis l'acte répréhensible, mais dans le modèle à quatre parties, il y a la banque émettrice, la banque acquéreuse, le commerçant et le titulaire de la carte.

Le titulaire de la carte s'adresse au commerçant et fait affaire avec lui, et je dirais que dans bien des cas, nous voyons des problèmes associés au commerçant à cause d'un problème de sécurité, de quelque chose qui n'a pas tourné rond. L'information peut être saisie ou volée à cette étape.

Nous prenons beaucoup de mesures pour éliminer, grâce à la transformation en jetons — la segmentation en unités —, la valeur des renseignements que le commerçant peut obtenir. Lorsqu'on se sert d'Apple Pay, il n'y a pas de NIP, de nombre à seize chiffres que vous connaissez bien. Nous fournissons un jeton qui ne peut être utilisé que d'une certaine façon. On ne peut pas le voler et s'en servir sur un autre appareil ou un ordinateur. Un jeton se trouve dans votre compte Apple Pay. Nous activons ce jeton dans Apple Pay. Nous nous servons de la transformation en jetons...

● (1635)

Le président: Monsieur Green, afin d'éclairer le président et possiblement d'autres membres du Comité qui n'ont peut-être pas entendu parler de la transformation en jetons, j'aimerais que vous expliquiez brièvement cette notion.

M. Ron Green: Les 16 chiffres qui composent votre carte sont ce que nous appelons un numéro d'autorisation personnel, ou NAP. Il s'agit d'un certain numéro que vous utilisez fréquemment — vous le connaissez et vous le voyez, car il est inscrit sur votre carte en plastique. Par contre, nous créons les jetons. Ils sont utilisés dans les systèmes, mais nous pouvons les créer et les éliminer, et les réutiliser ensuite... Ce n'est pas aussi rigide que le numéro à 16 chiffres.

Donc, lorsque nous créons un jeton, comme dans le cas d'un marchand qui... nous remplaçons les NAP et nous les utilisons pour placer des jetons. S'il y a une fuite et que quelqu'un vole les jetons, ce n'est pas un problème; nous créons simplement de nouveaux jetons. Nous éliminons la valeur du NAP — le numéro de la carte de crédit — et nous le remplaçons par un jeton, ce qui signifie que nous pouvons simplement créer d'autres jetons.

M. Matthew Dubé: C'est intéressant, car cela me fait penser à l'intelligence artificielle et à la biométrie.

Pardonnez-moi, mais je vais utiliser un langage de tous les jours. Vous autorisez, de façon temporaire, différentes méthodes de paiement. On peut donc se demander, si l'intelligence artificielle ou la biométrie est utilisée de différentes façons — pour comprendre les types de transactions effectuées par les gens, le moment où ils les effectuent ou ce qui se produit dans un appareil —, une connexion plus concrète n'est-elle pas inévitablement établie plutôt que ces processus temporaires?

Encore une fois, je tente d'aborder cette notion du point de vue d'un non-initié, car il me semble qu'une connexion plus solide s'établirait à ce moment-là si vous permettez ce type de collecte de données.

M. Ron Green: Il ne s'agit pas seulement de la collecte de données. Il s'agit d'avoir les bonnes données au bon moment.

Je ne veux pas trop compliquer les choses, mais à l'avenir, les répertoires de données d'identité seront moins importants que la capacité d'obtenir les renseignements sur l'identité au moment où on en a besoin.

Lorsque vous voulez effectuer une transaction, nous pouvons établir une connexion avec les répertoires de données d'identité afin d'y extraire les renseignements qui permettent de vous identifier, vous, Matthew, lorsque vous avez besoin d'effectuer une transaction. Ensuite, lorsque vous avez terminé, ces renseignements disparaissent. Il n'est pas nécessaire de les entreposer. Nous voulons simplement établir une connexion et veiller à ce que les renseignements soient disponibles lorsque vous en avez besoin.

M. Matthew Dubé: N'existe-t-il pas un endroit où toutes ces données aboutissent? Au cours d'une réunion précédente, un témoin nous a dit que c'était une drôle d'affirmation, mais que le nuage n'est pas un vrai nuage. Il existe un espace où ces données sont entreposées.

M. Ron Green: Oui, elles sont dans un ordinateur quelque part.

M. Matthew Dubé: Exactement. Ces données aboutissent quelque part.

Même si ce jeton, par exemple, offre une protection aux transactions effectuées avec Apple Pay, une transaction est tout de même effectuée et des données aboutissent quelque part et y restent, sans...

M. Ron Green: Ce processus peut être transitionnel, et les données sont entreposées pendant une certaine période. Elles ne le sont pas de façon permanente. Elles sont là lorsque vous avez besoin de faire ce que vous tentez de faire, et lorsque vous n'avez plus besoin de ces données, elles disparaissent.

M. Matthew Dubé: Je vais tenter de vous résumer les questions que j'ai posées aux représentants de l'association des banquiers lorsqu'ils ont comparu devant notre comité.

Si j'utilise une application bancaire sur mon téléphone pour payer le solde d'une carte de crédit, je le fais inévitablement par l'entremise de la banque, mais dans ce cas-ci, certains renseignements doivent être envoyés à la société de carte de crédit.

M. Ron Green: Les données qui composent la transaction sont le NAP — le numéro à 16 chiffres — la date, l'heure et les montants. Nous ne conservons pas les renseignements sur le titulaire de la carte. C'est la banque émettrice de la carte qui les conserve.

Tout ce que nous voyons, c'est que le numéro à 16 chiffres a fait quelque chose. Le marchand demande si le numéro à 16 chiffres peut effectuer le paiement. Nous demandons à l'émetteur de la carte. Nous ne connaissons pas le titulaire de la carte, mais l'émetteur le connaît. L'émetteur nous répond que le numéro à 16 chiffres qui appartient à Matthew peut effectuer le paiement. Nous transférons ensuite ce renseignement pour confirmer que le numéro peut effectuer le paiement. Ensuite, le montant est facturé.

Tous ces renseignements passent d'un côté à l'autre. Selon ce que vous demandez...

M. Matthew Dubé: Autrement dit, vous avez essentiellement le nom du marchand, le numéro de la carte et le montant de la transaction.

M. Ron Green: Oui.

M. Matthew Dubé: Ces données ne sont pas nécessairement entreposées au Canada; sont-elles protégées par les lois canadiennes?

M. Ron Green: Nous devons nous conformer aux lois canadiennes dans le cas des données des citoyens canadiens. Actuellement, la majorité des transactions s'effectuent à nos installations de St. Louis ou de Kansas City. D'autres installations dans d'autres endroits font également certaines tâches pour nous. Les données doivent demeurer locales. D'où je suis, je peux voir les auteurs de menaces tenter d'agir contre le système de paiement, peu importe où ils se trouvent. Mais plus les pays localisent ou tentent de localiser les données, ce qui empêche d'utiliser ces données ailleurs, plus ma capacité d'analyser la situation et de suivre les mouvements des auteurs de menaces diminue.

Les auteurs de menaces ne se soucient pas des frontières. Ils sont prêts à s'attaquer à l'Amérique latine, à l'Europe, au Canada ou aux États-Unis. Si je peux les voir mener une attaque en Amérique latine, mais que je ne suis pas autorisé à utiliser ces renseignements pour aider à protéger un autre pays, l'attaquant peut mener une autre attaque ailleurs sans que je puisse utiliser ce que j'ai appris pour protéger sa prochaine victime. Les attaquants peuvent donc continuer d'attaquer de nouveaux endroits sans que je puisse utiliser les renseignements recueillis pour aider à protéger ces endroits.

● (1640)

Le président: Merci.

Monsieur Picard.

[*Français*]

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

Monsieur Davies, vous offrez des services de consultation à des institutions financières. En affaires, l'un des défis est de bien gérer l'investissement en matière de sécurité et le risque associé à ce domaine. C'est une question d'équilibre. Quand vient le temps d'investir dans des mesures de sécurité, il faut voir si le remboursement d'éventuels dommages coûterait moins cher ou aussi cher que l'investissement en matière de sécurité.

Pendant longtemps, il y a eu cette perception selon laquelle les institutions financières limitaient leur investissement dans la sécurité et choisissaient de payer les dommages subis à la suite d'incidents, parce que cela était plus avantageux. Rencontre-t-on encore ce genre de résistance ou le marché a-t-il évolué sur la question de la sécurité?

[*Traduction*]

M. Thomas Davies: Je dirais qu'elles investissent massivement dans les mesures de protection dans le domaine cybernétique. En effet, leur marque et leur réputation sont à risque. Même si dans la communauté, nous disons qu'il ne faut pas se faire concurrence en matière de sécurité, je crois que les institutions financières se font concurrence pour gagner la confiance des clients.

Le plus gros problème auquel font face les institutions financières aujourd'hui, c'est que les personnes sont nécessaires pour déployer le capital. Elles ont de solides budgets et elles réservent le financement adéquat, mais elles ont de la difficulté à réaliser leurs nombreux projets en raison des pénuries de main-d'oeuvre qualifiée.

[*Français*]

M. Michel Picard: Il faut dire que les tierces parties qui ont accès aux institutions financières n'ont peut-être pas les moyens financiers ou les outils nécessaires pour se protéger des risques. De ce fait, elles peuvent présenter un risque d'accès au système financier. Les investissements dans la sécurité faits par l'industrie permettent-ils quand même de protéger le marché?

[*Traduction*]

M. Thomas Davies: On considère que les tierces parties qui fournissent des services aux institutions financières représentent l'un de leurs plus grands risques. Les institutions financières mettent au point un programme de sécurité rigoureux, mais ce programme peut être affaibli par un intervenant extérieur. Ainsi, les institutions financières prennent très au sérieux le risque lié aux tierces parties.

Je crois que l'un des problèmes qui se posent, c'est que les gens croient que la cybersécurité est un domaine trop complexe. Toutefois, un grand nombre de fuites est attribuable à la méconnaissance des éléments fondamentaux. Je crois qu'une formation appropriée sur la nature des éléments fondamentaux et sur la façon de les renforcer pourrait réduire considérablement ce risque. C'est pourquoi les institutions financières commencent à exiger que les tierces parties mettent en oeuvre un minimum de vérifications dans leurs contrats et qu'elles présument qu'il y a un certain risque. Au Canada, le BSIF régit les banques. Si la fuite est attribuable à une tierce partie, le BSIF ne veut pas le savoir. L'organisme tient tout de même la banque responsable, et les banques prennent donc cet enjeu très au sérieux et mettent en oeuvre de grands programmes liés aux risques pour contrer ce problème.

[*Français*]

M. Michel Picard: Ma prochaine question concerne les ressources humaines et s'adresse à MM. Davies et Green.

Du côté consultatif, on regarde le recrutement, alors que, du côté du client, par exemple chez Mastercard, on regarde le risque que présentent les ressources humaines.

J'ouvre ici une parenthèse pour vous raconter une anecdote. Il y a plusieurs années, j'ai rempli en bonne et due forme un formulaire de demande de carte de crédit — je ne dirai pas laquelle. Quand j'ai reçu la carte, la limite de crédit prévue avait déjà été dépassée. Évidemment, j'ai contacté le service qui s'occupait de la sécurité. Le problème n'était pas attribuable à moi, mais au service de la sécurité, au moment de la délivrance de la carte. Cela venait donc de l'intérieur.

Dans une autre vie, j'ai assisté à des réunions de l'Association des banquiers canadiens où il était question de terminaux de paiement qui étaient, disait-on, impossibles à pénétrer. Or, ils avaient été décodés en trois semaines. On pense qu'il y a encore des risques qui viennent de l'intérieur.

Comment gère-t-on ce risque lié aux ressources humaines, qui semble mener à un cul-de-sac, tant chez le client que chez le consultant?

● (1645)

[*Traduction*]

M. Ron Green: Nous menons une vérification approfondie des antécédents de nos employés avant de les embaucher, mais nous avons également des programmes de surveillance des menaces internes. Nous connaissons le comportement approprié ou habituel, et nous cherchons des anomalies. J'ai eu l'occasion de démontrer aux membres de mon conseil d'administration les outils dont nous disposons dans notre programme de surveillance des menaces internes, mais nous avons des moyens de détecter les comportements anormaux.

Lorsque ces comportements sont détectés, mon équipe lance une enquête pour vérifier si l'employé agit d'une façon qui va à l'encontre de l'intérêt supérieur de l'entreprise.

De plus, certains de nos employés jouent des rôles à risque élevé. Leur travail leur pemet de construire ou de détruire des machines, etc.

Nous exerçons une surveillance accrue et mes employés surveillent donc ce qu'ils font. Tout cela se déroule en arrière-plan, mais tout se déroule pour veiller à ce qu'ils fassent ce qu'ils sont censés faire. Si ce n'est pas le cas, nous intervenons.

M. Thomas Davies: J'aimerais ajouter que la menace interne est la plus grande préoccupation de la plupart des agents principaux de gestion des risques en raison de l'ampleur d'un tel incident lorsqu'il se produit. Vous savez, on discute souvent de l'affaire Edward Snowden dans le milieu de la sécurité nationale. La notion selon laquelle un initié a accès à des renseignements confidentiels est toujours préoccupante.

On parle d'exercer une surveillance accrue à l'égard de ce que nous appelons les utilisateurs qui ont beaucoup de pouvoir, c'est-à-dire des personnes qui — pour revenir au point de M. Green — jouissent de grands privilèges au sein de l'organisme, afin de veiller à réduire les risques.

Donc, lorsqu'un compte est la cible de fraude, c'est un risque réduit, et il faut avoir un certain degré de tolérance au risque à l'interne. En effet, on ne peut pas garantir que personne ne posera de gestes inappropriés, mais on peut réduire les effets d'un tel incident au minimum et offrir une formation de base pour sensibiliser les gens.

Lorsque j'étais membre de Scotiabank, les formations sur le code de déontologie, sur la conduite professionnelle, sur la façon de connaître ses clients et sur la lutte contre le blanchiment d'argent étaient obligatoires. Il est important de rendre cette formation obligatoire et d'au moins donner à tous l'impression que nous sommes là pour faire ce qu'il faut.

Le président: Merci.

Monsieur Motz, vous avez quatre minutes.

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Merci, monsieur le président. J'aimerais également remercier les témoins d'être ici.

Monsieur Gordon, des témoins précédents nous ont dit que des pays comme l'Australie et Israël disposaient de réseaux d'échange de renseignements plutôt efficaces entre les industries, le gouvernement et les universités. Nous n'avons pas nécessairement entendu parler de l'existence de tels réseaux au Canada. Le Canada pourrait-il s'améliorer à cet égard et si c'est le cas, que devrions-nous faire?

M. Robert Gordon: Je pense que nous nous améliorons. Je crois que l'une des étapes importantes que nous avons franchies était la création du nouveau centre cybernétique à cette fin. C'est l'une des raisons pour lesquelles nous collaborons aussi étroitement avec eux pour établir ce lien entre les activités du secteur privé et celles du gouvernement dans ce domaine.

En fait, nous travaillons avec certains organismes australiens pour créer, en Australie, un organisme semblable à l'ECMC, afin d'obtenir cet élément intersectoriel. C'est l'un des moyens qui permettent de regrouper toutes les entreprises, quelles que soient leur taille ou leurs activités, et de les préparer à interagir avec le gouvernement.

Le gouvernement s'occupera du centre cybernétique, qui représente une très petite partie de l'infrastructure essentielle — c'est ce qu'il mettra à l'échelle — et il compte sur nous pour étendre cela aux secteurs et aux domaines qui ne seront pas visés par ses activités. Le gouvernement peut offrir des conseils généraux, mais il faut en grande partie qu'une personne prenne ces conseils et se rende compte qu'il faut faire quelque chose sur le plan technologique, et qu'elle se demande comment y arriver au sein de son entreprise.

Cela revient un peu au développement des compétences dont parlait M. Finlay. Nous tentons d'intégrer cela, c'est-à-dire que nous communiquons les connaissances fournies par le gouvernement à des personnes qui utiliseront la technologie, afin qu'elles puissent réfléchir à la façon de réaliser certaines de ces choses.

● (1650)

M. Glen Motz: La plateforme de votre organisme est maintenant plus accessible aux petits marchés et aux petites et moyennes entreprises, et elles en profitent.

Avez-vous déjà observé des attaques menées contre des entreprises en démarrage ou des petites entreprises qui ont ensuite été menées ailleurs?

M. Robert Gordon: Pas contre nos entreprises, mais cela arrive.

De nombreux exemples sont liés à de petites entreprises. Une partie de la chaîne d'approvisionnement est le point de départ qui mène à la cible suivante, c'est-à-dire des organismes beaucoup plus importants. C'est l'une des raisons pour lesquelles — et on l'a dit plus tôt — les banques souhaitent tellement examiner leurs tierces parties, afin de déterminer ce qu'elles peuvent faire pour tenter d'améliorer leur résilience cybernétique, car elles sont toutes connectées à leurs systèmes.

Cela va plus loin, car on retrouve ce phénomène dans pratiquement tous les secteurs. Par exemple, les propriétaires de gros immeubles qui s'inquiètent maintenant au sujet des locataires de leur immeuble qui pourraient se connecter à leurs systèmes sont seulement protégés au niveau de leur maillon le plus faible. Tous les secteurs font face à ce problème.

M. Glen Motz: Un témoin précédent nous a dit que le Canada était souvent la première victime des attaques, et que c'est en partie attribuable au fait que nous avons moins de ressources que nos voisins du sud.

Avez-vous constaté que c'était le cas dans le cadre de vos discussions avec les alliés?

M. Robert Gordon: Que nous sommes attaqués en premier ou...?

M. Glen Motz: Vous avez beaucoup d'interactions avec nos alliés.

Avez-vous constaté que le Canada est parfois le premier pays attaqué de cette façon comparativement à certains de ses alliés?

M. Robert Gordon: Oui. Les attaquants choisissent certains pays pour diverses raisons.

Dans certains cas, nous pouvons être la seule cible d'une attaque à venir et dans d'autres cas, nous servons de tremplin pour d'autres attaques qui seront ensuite menées ailleurs. Nous pouvons aussi être le deuxième pays sur la liste, c'est-à-dire que l'attaque commence ailleurs et est ensuite dirigée contre le Canada. Nous sommes visés dans les trois cas.

M. Glen Motz: Parfait.

Monsieur Davies, à votre avis, quelles sont les lacunes les plus importantes en matière de cybersécurité dans le secteur financier au Canada?

M. Thomas Davies: Le plus gros problème est lié aux anciens systèmes et il est toujours extrêmement difficile d'entretenir ces systèmes. En effet, il n'existe pas vraiment d'outils liés à la sécurité dans le cas de nombreux systèmes plus anciens, et on doit construire ce qu'on appelle un enclos pour les protéger. C'est toujours le problème le plus important. On doit lui consacrer beaucoup de temps.

M. Glen Motz: J'aimerais poser une question de suivi, car c'est important dans le cadre de cet enjeu.

Vous avez raison. Si vous êtes aussi vieux que John et moi...

Le président: Merci beaucoup.

M. Glen Motz: Nos données bancaires sont vieilles. Les institutions financières, plutôt que de tenter de construire, comme vous l'avez dit, un enclos ou des protections, ne devraient-elles pas transférer ces données dans des logiciels ou des mécanismes qui pourraient mieux assurer leur sécurité, plutôt que de se contenter de les protéger dans le système dans lequel elles se trouvent?

M. Thomas Davies: Oui. Les banques adoreraient simplifier cet environnement. C'est difficile, car certains de ces anciens systèmes sont toujours nécessaires pour le réseau d'une succursale ou pour d'autres systèmes de leur réseau global. Les banques souhaitent certainement faire quelque chose à cet égard, mais c'est extrêmement difficile et cela demande énormément de ressources.

Le président: Merci.

Madame Sahota, vous disposez de quatre minutes.

Mme Ruby Sahota (Brampton-Nord, Lib.): Merci, monsieur le président.

Notre comité entend beaucoup parler de la collaboration nécessaire entre l'État, le secteur privé et les universités.

Monsieur Finlay, vous avez parlé de votre visite en Israël et de la nécessité, pour nous, de nous préparer à donner le type de formation qui se donne là-bas. Pouvez-vous expliquer un peu plus ce qu'est Cybersecure Catalyst, comment ça se compare, sur certains points, à la formation donnée en Israël et quelles sont, entre les deux, les similitudes et les différences?

M. Charles Finlay: On observe un certain nombre d'éléments intéressants dans la formation que donne à ses gens l'écosystème israélien de cybersécurité. Cette formation présente manifestement une caractéristique de service national unique en son genre: en effet, en Israël, le service militaire est différent de ce qui peut lui ressembler au Canada.

L'un de ses points forts et intéressants est qu'elle commence à un jeune âge, celui de la maternelle à la 12e année. Nous croyons nous attaquer très énergiquement à la racine du problème du marché du travail en cybersécurité, en intéressant beaucoup les jeunes à la cybersécurité et en les attirant dans des carrières de ce domaine. Ryerson, en partenariat avec la Banque Royale du Canada et l'Université Carnegie Mellon, l'une des chefs de file de la cybersécurité aux États-Unis, ont organisé, en 2018, un hackathon appelé CanHack. C'est un jeu en ligne dans lequel des élèves d'écoles secondaires exécutent sous surveillance et sous supervision, donc sans risque, des tâches de sécurité informatique. Le nombre d'élèves participants, que nous prévoyions, a doublé.

Les perspectives sont extraordinaires. D'abord, l'événement s'adresse aux jeunes. Ensuite, il mobilise un groupe démographique sous-représenté dans le cyberespace et parmi les travailleurs déplacés des secteurs traditionnels. Voici que se présente l'occasion d'accueillir des travailleurs déplacés de secteurs dont les effectifs diminuent, pour les former pour celui de la cybersécurité au niveau de débutant. C'est très emballant.

Voilà deux des objectifs, analogues à ceux que nous avons vus atteindre dans d'autres pays, y compris Israël, que nous espérons réaliser.

● (1655)

Mme Ruby Sahota: Vous avez dit avoir rencontré des entreprises canadiennes, pendant que vous étiez là-bas, qui ont opéré un virage temporaire ou permanent pour recevoir ces types de services, de formation, pour leur personnel. De quelles entreprises ou de quels types d'entreprises parliez-vous, et envisagez-vous la possibilité qu'elles reviennent et que, peut-être, elles s'installent à proximité de Cybersecure Catalyst?

M. Charles Finlay: Oui. À Beersheba, on trouve d'importantes institutions financières canadiennes. Les grandes banques canadiennes y ont des bureaux et elles se trouvent là-bas parce que les talents y sont. Nous croyons pouvoir créer un écosystème pour la formation. L'industrie est présente pour acquérir ces talents, des entreprises prennent de l'expansion grâce au programme d'accélération, et des chercheurs universitaires collaborent aussi avec des entrepreneurs, avec les stagiaires et l'industrie. Ce que nous avons vu en Israël existe aussi ailleurs. Mais ce qui est là-bas remarquable, c'est la coordination entre l'industrie, les universités et l'État, et nous croyons que, chez Cybersecure Catalyst, elle créera cet écosystème.

Le président: Merci.

Monsieur Dreeshen, soyez le bienvenu au Comité. Vous disposez de quatre minutes.

M. Earl Dreeshen (Red Deer—Mountain View, PCC): Merci beaucoup, monsieur le président.

Je remercie aussi les témoins.

Seulement quelques idées qui me sont venues pendant que j'écoutais. Beaucoup d'institutions et d'entreprises ont été attaquées pour leurs données ou pour les empêcher de s'en servir. Diverses universités... ont été rançonnées. C'est important, pour la suite des choses dans les entreprises, mais la peur commence à s'installer dans les petites entreprises.

Je me demande quels genres d'enquêtes ont lieu et quel est leur taux de réussite contre ce problème. Beaucoup de petites entreprises s'inquiètent du genre d'attaques qu'elles pourraient subir et de la façon qu'elles pourraient être rançonnées.

M. Thomas Davies: Monsieur le président, je peux tenter une première réponse.

Aujourd'hui, on informe mal le public de la nature des intrusions. Le secteur bancaire ne dit rien, dans l'espoir de protéger chacun de ses membres contre la répétition du problème, mais, à part ça, les renseignements à ce sujet sont assez privés et ils peuvent avoir des conséquences graves sur les opérations et la réputation de l'entreprise. Voilà pourquoi on les divulgue peu.

Aux États-Unis, je crois que c'est le FBI qui possède un peu plus de détails sur la compromission du courriel d'affaires, d'autres rançongiciels et d'autres tentatives de fraude. Pour rassembler ces données au Canada, pour donner une idée des gens... les thèmes que nous abordons, nous pouvons en parler ici, ainsi que de gestion de l'accès, d'hygiène des systèmes et de formation et de sensibilisation, mais la preuve, avec de vraies données, serait utile.

M. Ron Green: Je pense aussi que les attaques de cryptoverrouillage ou les rançongiciels dont vous parlez sont en grande partie affaire de mesures d'hygiène de base. Si on apprenait à mettre les systèmes au niveau ou à appliquer des rustines, on s'épargnerait certainement beaucoup de problèmes. Un logiciel antivirus en préviendrait aussi. Il faut savoir éviter l'hameçonnage... D'après le rapport de Verizon sur les violations de données, 93 % des intrusions ont fait suite à un hameçonnage. Je peux vous assurer que nous, chez Mastercard, nous prenons le problème très au sérieux. Nous appliquons la règle des trois fautes. D'après mes statistiques de février sur l'hameçonnage, le taux d'échec était de 0,4, et considérez que 20 % sont à peu près la norme.

Il s'agit d'aider les petites entreprises à comprendre les rudiments de ce qu'il faut faire quand tout déraille, à sauvegarder leurs données pour, en cas de verrouillage, les restaurer et surmonter le problème.

● (1700)

M. Earl Dreeshen: On peut encaisser beaucoup d'argent en propageant la peur. Ça me rappelle le bogue de l'an 2000 et l'inquiétude générale pour les systèmes informatiques et ainsi de suite. Beaucoup d'entreprises se sont enrichies à essayer de résoudre un problème — vous, messieurs, savez peut-être s'il était grave — mais beaucoup d'autres croyaient que c'était un canular.

Vous pouvez faire des observations à ce sujet, mais je suppose que je m'inquiète aussi de la protection de la propriété intellectuelle, la crainte de faire tout ce travail de développement... puis de voir d'autres acteurs, individus, pays ou entreprises... Comment trouver la meilleure protection ou essayer de se protéger soi-même?

Les intéressés peuvent aussi parler du bogue de l'an 2000.

Le président: Dans ce cas, il faudra être très bref.

M. Robert Gordon: Dans ce cas, je passe sur le bogue.

L'une des difficultés, pour les entreprises, est de déterminer les renseignements essentiels dans leurs systèmes, à protéger absolument. Impossible de les protéger tous si on ne sait pas desquels il s'agit. Alors, on commence par les associer aux éléments importants. On peut ensuite commencer à contrôler l'accès à ces données.

Beaucoup d'entreprises, les petites notamment, et c'est intéressant en ce qui concerne particulièrement les rançongiciels, croient habituellement ne pas posséder de secrets commerciaux importants, qui exciteraient la convoitise.

Les rançongiciels n'ont pas le vol pour objectif, mais seulement celui d'empêcher d'accéder à un bien précieux pour son propriétaire. Pour beaucoup de petites entreprises, il suffit, pour prévenir le problème, d'un petit changement de mentalité, parce que, ensuite, elles peuvent comprendre pourquoi elles doivent s'intéresser aux rançongiciels, à la fois pour défendre leur bien — des solutions existent — et pour, après une attaque, savoir comment revenir à la normale.

Le président: Merci.

Madame Dabrusin, vous disposez de quatre minutes.

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

Monsieur le président, je suis aussi inscrite pour la prochaine intervention de sept minutes, ce qui m'en fait dix. Je pourrais les partager avec quelqu'un. Pouvez-vous me conseiller?

Le président: Je pensais que l'efficacité des témoins avait déteint sur celle de nos membres. Disposant donc d'une demi-heure, nous avons fusionné l'intervention. Je prévoyais que, après les trois dernières minutes de M. Dubé, la présidence pouvait exercer sa prérogative et poser quelques questions, mais nous sommes disposés à essayer des interventions de trois minutes pour le temps qui reste.

Mme Julie Dabrusin: Merci.

Tantôt, sur le site de Cybersecure Catalyst, j'ai lu que le taux annuel de croissance de la demande de professionnels formés en cybersécurité, au Canada, était de 7 %.

D'où vient ce chiffre? Est-ce une tendance pluriannuelle que vous avez constatée? Prévoyez-vous qu'elle se maintiendra?

M. Charles Finlay: Oui. Le taux provient d'un rapport de 2018, de Deloitte et de la Toronto Financial Services Alliance, qui l'ont estimé à 7 % par année.

Mme Julie Dabrusin: Nous avons parlé de la nécessité de former des gens et de posséder des effectifs qualifiés pour cette tâche. Quelle est la durée de cette formation? À un diplômé du secondaire que la cybersécurité intéresse, combien de temps faut-il pour terminer tous les programmes de formation qui lui permettraient d'être embauché?

● (1705)

M. Charles Finlay: Excellente question. Beaucoup de facteurs entrent en jeu. Nous sommes dans la formation continue. Essentiellement, nous collaborons avec des employeurs, pour augmenter les compétences de leur personnel. Les échéanciers dépendent exactement de l'ensemble de compétences dont ces employés ont besoin. C'est un problème particulier en cybersécurité, parce que les menaces et les conditions techniques évoluent continuellement. Cela concerne les rudiments de l'éducation des cadres supérieurs.

Pour le stage d'initiation des cohortes sous-représentés, nous visons un programme de six mois. D'après nous, un programme intensif de six mois peut conduire un candidat possédant une formation technique assez limitée à un poste de débutant qui le rendra admissible à des stages pour débutant et à des détachements dans l'industrie. Ensuite, on offre des programmes de premier cycle en cybersécurité et en informatique, après les cours habituels de premier cycle. Un programme de premier cycle en cybersécurité pourrait prendre trois ans, quatre avec spécialisation. Ce sont des parcours différents. On offre toutes sortes de programmes de formation continue en cybersécurité de différentes longueurs.

Mme Julie Dabrusin: J'essaie seulement de comprendre, au cas où je devrais expliquer les échéanciers à des jeunes qui terminent leurs études secondaires avec un diplôme en poche. Ils doivent y réfléchir. S'ils songent à des prêts d'études et à tout ce qu'il faut mettre de côté pour s'instruire, si nous leur disons que c'est une carrière emballante, que la demande est forte, nous nous rendons utiles si nous pouvons au moins leur donner un aperçu de ce que l'avenir leur réserve. C'est l'aide que j'espère de l'un des membres de votre groupe de témoins. Qu'est-ce que je leur dis sur la durée des études, les diplômes exigés pour se faire embaucher dans ce secteur?

M. Ron Green: Mon point de vue est celui d'un embaucheur. Certains membres de mon équipe ne sont allés ni au collège ni à l'université. Ils ressentaient seulement un intérêt très vif et, pendant leurs études secondaires, ils ont passé beaucoup de temps à travailler avec des ordinateurs, à en comprendre le fonctionnement et à éprouver un sentiment de sécurité. Ils se démarquent dans nos entrevues et nos tests, et nous pouvons pressentir qu'ils seront un bon apport dans notre équipe. Du point de vue technique, ils possèdent des atouts, mais ils finissent par être bloqués, faute d'antécédents en gestion.

Actuellement, il est difficile de trouver des diplômés de collèges en cybersécurité. Je cherche un diplômé en technologie que je peux former à la sécurité dans mes centres d'opérations de sécurité. Je peux le former sur le tas. Ce qui est rare et que nous recherchons particulièrement pour beaucoup de postes, c'est l'expérience. Nous cherchons des candidats qui ont un diplôme collégial. Ils peuvent avoir une maîtrise en cybersécurité, mais en plus, ils possèdent une expérience pratique, comme les militaires ou des personnes qui ont défendu des réseaux importants. Ils sont très peu nombreux. Il m'a fallu deux ans pour combler certains postes, tant les candidats sont difficiles à trouver.

Le président: Merci.

Monsieur Dubé, vous avez trois minutes.

M. Matthew Dubé: Merci, monsieur le président.

Monsieur Green, pardonnez mon rabâchage. J'essaie seulement de comprendre. Quand nous nous sommes quittés, tout à l'heure, vous commenciez à m'éclairer.

Vous parliez de l'incapacité de reconnaître, localement, une menace qui fait fi des frontières. Je suppose que les motifs de préoccupation peuvent englober l'accessibilité de ce type d'information pour, disons, les organismes chargés de la sécurité nationale ou la police. L'exemple précis qui me vient à l'esprit a été soulevé par notre commissaire à la protection de la vie privée, ici, au Canada. Par exemple, des Canadiens pourraient désormais, en toute licéité, se procurer de la marijuana avec leur carte de crédit. Comme, à l'échelon fédéral, aux États-Unis, c'est illégal, si la Patrouille frontalière des États-Unis en avait l'envie, ce renseignement pourrait leur fermer les portes des États-Unis.

Si ce renseignement se trouve quelque part, pour le meilleur ou pour le pire, le risque existera toujours qu'on s'en serve. Je comprends seulement mal la responsabilité, attribuée par la loi ou d'autres moyens, de l'information stockée, dans un serveur aux États-Unis ou n'importe où ailleurs, sur mes opérations de citoyen canadien avec une banque canadienne.

● (1710)

Le président: Ce n'est pas une question personnelle.

Des voix: Oh, oh!

M. Ron Green: D'abord, quelques précisions. Ce n'est pas vous que nous stockons; nous connaissons un nombre à 16 chiffres qui appartient à une banque émettrice. La banque canadienne pourrait en fait comprendre qui est Matthew; tout ce que nous savons, c'est un nombre à 16 chiffres. Nous n'avons rien d'ouvert... nos données sont accessibles à...

M. Matthew Dubé: Désolé de vous interrompre, j'interviens seulement pour comprendre. Je viens de déménager et j'ai fait changer mon adresse. J'ai dû en subir les conséquences, parce que l'actualisation n'avait pas été faite dans le système. C'est le système de qui? Est-ce le vôtre ou celui de la banque, qui est l'émettrice de la carte?

M. Ron Green: Quelle est la cause du problème? Le code postal ou quelque chose comme ça?

M. Matthew Dubé: J'essayais de confirmer un paiement pour un achat en ligne. On m'a demandé le nom du détenteur de la carte, qui paraît sur la carte, les trois chiffres au verso de la carte et l'adresse. Comme l'adresse avait changé le jour même, il a finalement fallu que j'appelle la ligne d'assistance où on m'a dit que je devais attendre que le système corrige l'adresse pour pouvoir fonctionner. Est-ce la faute de l'émetteur?

M. Ron Green: Avez-vous appelé au numéro qui se trouve à l'arrière de la carte?

M. Matthew Dubé: Oui, c'est le numéro de l'émetteur de la carte, n'est-ce pas?

M. Ron Green: Oui, c'est le numéro de l'émetteur, c'est-à-dire votre banque.

M. Matthew Dubé: Si j'utilise PayPal, par exemple, et que je paie avec une carte de crédit, je dois inscrire le numéro et l'adresse. Le numéro vous est transmis pour la validation et l'adresse, le nom, etc., du détenteur de la carte sont transmis à la banque.

M. Ron Green: C'est exact, et nous utilisons le numéro lorsque nous communiquons avec l'émetteur. S'agit-il d'une information qui nous permet d'autoriser la transaction? On nous transmet le numéro à 16 chiffres, que nous transmettons à notre tour à l'émetteur — c'est-à-dire votre banque, qui vous connaît — qui peut vérifier si vous avez les fonds nécessaires. Ensuite, nous faisons savoir au marchand que le détenteur dispose des fonds nécessaires et qu'il peut procéder à la transaction. Par la suite, le montant est transmis à l'émetteur.

L'information que nous utilisons pour que la transaction s'effectue est le numéro à 16 chiffres.

Le président: Je vous remercie.

J'ai quelques questions à poser, et ensuite, M. de Burgh Graham et M. Paul-Hus disposeront chacun de trois minutes, et d'autres pourront aussi intervenir. Cela devrait nous mener à la fin de la réunion. Aucune question pour M. Motz — c'est de l'âgisme.

Vous savez que cette étude a été entreprise en partie à cause de la controverse entourant le 5G, et particulièrement la controverse entourant le 5G en ce qui a trait à Huawei, Nokia et Ericsson. Vous êtes tous les trois en particulier sur la ligne de front, alors j'ai une question pour vous. Si ce réseau est lancé — et il le sera — comment vous préparez-vous à cela, ou est-ce que vous vous y préparez, et dans quelle mesure cette préparation changerait ce que vous venez de dire aujourd'hui, si effectivement elle changeait ce que vous venez de dire?

Nous allons commencer par M. Green et continuer par la droite.

M. Ron Green: Peu importe le réseau — mobile, 5G, Wi-Fi ou même connecté — lorsque nos employés utilisent ces réseaux, nous leur fournissons une voie de transmission sécurisée. Qu'il s'agisse d'un réseau 5G ou d'un réseau mobile, nous sécurisons les données transmises. Le réseau que nous utilisons est un réseau privé. Nous n'avons pas recours à Internet. Les transactions commerciales s'effectuent sur un réseau très privé que nous contrôlons. Si j'utilise un réseau 5G, je vais fournir à mes employés une voie sécurisée pour communiquer les données de manière sûre. Le réseau que nous utilisons pour faire notre travail est notre propre réseau privé.

Le président: Alors toutes les transactions Mastercard dans le monde s'effectuent sur un réseau privé?

M. Ron Green: Oui, c'est un réseau privé. C'est pourquoi il est difficile de faire ce que nous faisons; il nous a fallu du temps pour mettre en place ce réseau privé.

Le président: Monsieur Davies.

M. Thomas Davies: Nous nous concentrons sur la protection des données d'un bout à l'autre. Pendant la transmission des données, personne ne devrait être en mesure de lire les données. C'est l'objectif, mais tout dépend de la technologie dont disposent certaines personnes pour intercepter, modifier, etc... C'est une technologie de pointe. C'est possible, mais comme M. Green vient tout juste de le dire, il faut qu'une seule entité puisse lire et transmettre les données, et une fois qu'elles sont rendues à destination, on peut les décoder et les lire. Cela peut se faire grâce à un réseau privé ou un réseau public, mais c'est ce sur quoi nous nous concentrons.

● (1715)

Le président: Vos clients n'ont pas de réseau privé, n'est-ce pas?

M. Thomas Davies: Tout dépend des types de systèmes qu'ils utilisent. Par exemple, les banques utilisent des réseaux privés pour les messages SWIFT et les virements télégraphiques, et elles utilisent des réseaux publics pour traiter avec leur clientèle.

Tout dépend aussi du degré d'importance des données. Par exemple, dans bien des cas, ils utiliseront un réseau privé avec leurs fournisseurs de services tiers.

Le président: Une personne du milieu de la sécurité nous a expliqué que c'était sécurisé aux deux extrémités, et que c'était comme une boîte de carton entre les deux.

Est-ce qu'un certain nombre de vos clients sont confrontés au fait que ce n'est pas sécurisé à une extrémité ou à l'autre ou entre les deux?

M. Thomas Davies: Améliorer cela, c'est notre objectif. C'est comme lorsqu'on transmettait des messages dans des langues autochtones durant la guerre pour éviter qu'ils soient lus pendant la transmission. Nous faisons la même chose aujourd'hui. Lorsqu'un message est transmis, on essaie de faire en sorte qu'il demeure codé le plus possible, et une fois qu'il est rendu à destination, quelqu'un possède une clé pour déverrouiller l'information et la lire.

Le président: Monsieur Gordon, voulez-vous ajouter quelque chose?

M. Robert Gordon: Du point de vue de notre organisation, cela n'a pas d'importance parce que la responsabilité appartient à chacun de nos membres. Il y a des membres qui transmettront l'information par l'entremise d'institutions financières et d'autres le feront par l'intermédiaire d'un réseau public.

Le président: Pourquoi dites-vous que cela n'a pas d'importance?

M. Robert Gordon: Je ne surveille pas leurs réseaux, alors je ne vois pas tout ce que nos membres voient. Ce que je vois, c'est le résultat de ce qu'ils voient sur leur réseau, et lorsqu'ils voient des anomalies, c'est ce que je vois aussi. Je ne surveille pas constamment ce qui se passe sur leurs réseaux.

Le président: Je vous remercie.

Monsieur Graham, vous disposez de trois minutes.

M. David de Burgh Graham: Monsieur Green, je vais terminer la question de M. Dubé. PayPal a son siège aux États-Unis. Je pense que le point qu'on a tenté de faire valoir c'est que, même si vos réseaux sont privés, si les données passent par les États-Unis, elles sont soumises à la Patriot Act de ce pays. Je crois que c'est la principale préoccupation.

Que faites-vous alors?

M. Ron Green: On ne peut pas identifier les personnes dans notre réseau.

M. David de Burgh Graham: Vous dites que vous recevez un numéro de 16 chiffres. Ce n'est pas difficile de décoder un numéro de 16 chiffres. Si quelqu'un met la main sur ce chiffre pour connaître l'identité de la personne, s'il découvre comment entrer dans votre système pour obtenir ce numéro, il découvrira l'identité de la personne. Alors, je n'accepte pas nécessairement votre argument. Comprenez-vous le point que je veux faire valoir?

M. Ron Green: Vous dites que si on trouve une autre façon de faire de l'ingénierie inverse pour obtenir le numéro à 16 chiffres... il faudrait qu'il s'agisse d'un processus légal. Nous n'allons pas tout simplement permettre au gouvernement américain d'entrer dans notre réseau lorsqu'il le souhaite et d'examiner ce qui s'y trouve. Nous ne faisons pas cela.

M. David de Burgh Graham: Mais c'est dans cette boîte de carton dont John aime parler que fonctionne votre réseau virtuel privé. Je présume que c'est un réseau virtuel. Vous avez parlé de votre réseau privé. Vous n'avez pas votre propre fibre optique partout dans le monde, alors il s'agit d'un réseau virtuel, n'est-ce pas?

M. Ron Green: C'est exact.

M. David de Burgh Graham: Mais vous utilisez des câbles d'accès public.

M. Ron Green: C'est codé, toutefois. Ce n'est pas ouvert... Nous avons le module de sécurité matériel le plus important après celui du ministère de la Défense, alors il y a beaucoup de cryptage dans notre réseau.

Il est vrai qu'un réseau privé peut passer par une tierce partie, mais tout demeure codé et les transactions sont également codées.

Le cryptage n'est pas une chose sans importance. Il est possible qu'un État-nation dispose de moyens pour décoder l'information et intercepter ce qui est transmis, mais je n'en connais pas.

M. David de Burgh Graham: Monsieur Gordon, lorsque j'ai obtenu mon premier mot de passe d'administrateur il y a environ 22 ans, il y avait le site Web rootprompt.org. Vous vous en souvenez peut-être. C'était un site Web qui faisait en fait ce que votre organisation fait maintenant, c'est-à-dire surveiller les vulnérabilités et les communiquer pour que les administrateurs de systèmes puissent demeurer à l'affût. Un jour, ce site Web a été attaqué, et il a été fermé.

Quels sont les organismes dont vous ne voulez pas au sein de votre organisation? Quelles sont vos vulnérabilités? Que faites-vous à cet égard?

● (1720)

M. Robert Gordon: Quels sont les organismes dont je ne veux pas?

M. David de Burgh Graham: Oui, car vous avez dit que vous souhaitez que de nombreux organismes deviennent membres de votre organisation. Quels sont les organismes dont vous ne voulez pas?

M. Robert Gordon: Je veux des organismes qui font deux choses. Je veux des organismes qui souhaitent collaborer, communiquer ce qui se passe, respecter l'entente que nous avons et expliquer l'utilisation qu'ils feront de l'information. Je veux des organismes qui utiliseront l'information pour défendre leurs réseaux.

Si un organisme utilise l'information à d'autres fins, je préfère qu'il aille ailleurs.

Le président: Je vous remercie.

[*Français*]

Monsieur Paul-Hus, vous avez trois minutes.

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

Monsieur Green, comme Mastercard est une organisation internationale, votre réseau est relié à plusieurs banques de différents pays. Les banques canadiennes sont-elles bien équipées, comparativement aux banques européennes ou américaines? Vous êtes en relation directe avec les banques, car vous passez par elles pour vos transactions. Si on les compare aux banques des autres pays, les banques canadiennes sont-elles bien organisées?

[*Traduction*]

M. Ron Green: Je pense que les banques canadiennes sont dans une situation assez favorable comparativement aux banques américaines ou européennes. J'ai vu des banques dans d'autres pays que je ne...

[*Français*]

M. Pierre Paul-Hus: Notre étude porte sur le système bancaire canadien et sur le système des compagnies d'assurances. Votre entreprise est en relation directe avec les banques partout dans le monde. Selon vous, les banques canadiennes font partie des banques qui sont bien protégées en matière de cybersécurité. Est-ce bien ce que vous dites?

[*Traduction*]

M. Ron Green: Je pense qu'elles sont bien protégées. Nous échangeons beaucoup avec un certain nombre de banques. Nous voyons cela comme une occasion de nous assurer que nous travaillons tous ensemble. Je pense aux gnous. Lorsque nous sommes ensemble, nous sommes moins une cible. Si nous sommes seuls, nous sommes davantage une cible. Un certain nombre de banques canadiennes — et même la chaîne Canadian Tire — sont venues examiner notre centre de fusion, et elles travaillent et collaborent avec nous.

[*Français*]

M. Pierre Paul-Hus: J'ai une dernière question rapide.

Monsieur Green, Mastercard a-t-elle des stratégies de cyberdéfense pour se protéger d'attaques venant du Web clandestin?

Monsieur Finlay, du côté universitaire, s'agit-il de sujets sur lesquels on se penche régulièrement?

[*Traduction*]

M. Ron Green: Nous avons une équipe chargée du renseignement qui surveille les menaces sur le Web caché. Nous payons des consultants pour qu'ils surveillent différentes choses sur le Web caché. Nous avons aussi différents partenaires au sein du gouvernement qui surveillent aussi certaines choses sur le Web caché pour déterminer comment les pirates s'y prennent pour attaquer afin que nous puissions empêcher des attaques. Nous communiquons cette information à notre clientèle.

[*Français*]

M. Pierre Paul-Hus: Merci.

[*Traduction*]

Le président: Madame Sahota.

Mme Ruby Sahota: Tout cela est très fascinant, mais comme je suis députée de Brampton, je m'intéresse particulièrement au centre Cybersecure Catalyst, qui a déjà amorcé en partie ses activités et qui est en voie d'atteindre sa vitesse de croisière grâce à Ryerson. Je suis heureuse de voir que dans le budget de 2019 on a prévu des fonds pour Cybersecure Catalyst.

J'aimerais savoir, plus particulièrement, quels types de titres de compétence vous accorderez dans le cadre de la formation. S'agit-il de titres de compétence reconnus à l'échelle internationale? Est-ce que vos programmes de formation sont comparables à d'autres programmes offerts dans d'autres pays? Aussi, combien de personnes vont se recycler ou se perfectionner selon vous, et combien de cours d'introduction prévoyez-vous être en mesure de donner lorsque vous aurez atteint votre vitesse de croisière?

M. Charles Finlay: En ce qui concerne les titres de compétence, notre objectif est d'accorder des titres reconnus à l'échelle internationale au terme de formations données par des organismes de formation en cybersécurité bien établis. Il s'agit d'organismes bien connus dans le marché. Il s'agit notamment de SANS, EC-Council et Palo Alto. Il y a de nombreux organismes qui offrent ces formations, et nous travaillons assez activement à établir des partenariats avec SANS et EC-Council pour offrir les cours en question.

Nous faisons cela parce que Cybersecure Catalyst est une entreprise axée sur l'industrie. Nous souhaitons vivement soutenir le secteur canadien de la cybersécurité grâce aux partenariats que nous voulons établir avec des universités et, bien entendu, grâce à la collaboration avec le gouvernement. Le secteur canadien de la cybersécurité a le potentiel de devenir le meilleur au monde, et il peut l'être. Nous allons travailler d'arrache-pied pour favoriser cela. Nous cherchons à offrir des titres de compétence utiles pour l'industrie.

Je peux vous donner quelques chiffres. Nous avons établi un plan quinquennal en ce qui concerne les cours d'introduction. Nous voulons aller chercher des groupes démographiques qui sont sous-représentés dans le secteur de la cybersécurité. Nous visons environ 500 personnes. En ce qui a trait aux formations offertes en collaboration avec nos partenaires du secteur privé, il s'agira de plusieurs milliers de personnes. Nous espérons aussi aller chercher des dizaines de milliers de jeunes. La cybersécurité est un grand problème, et nous devrons former de nombreuses personnes pour avoir une incidence importante.

Voilà ce que nous visons.

● (1725)

Mme Ruby Sahota: Je vous remercie.

Le président: Chers collègues, il nous reste quatre minutes avant de devoir quitter la salle, car il y aura ensuite une réunion d'un sous-comité.

Comme je suis gentil à l'égard de M. Motz, malgré son commentaire sur l'âgisme, je vais permettre à M. Picard de partager son temps de parole avec lui.

Vous avez chacun deux minutes.

Monsieur Picard.

M. Michel Picard: J'ai une seule question à poser.

Monsieur Davies et monsieur Green, quelle est votre compréhension des systèmes bancaires ouverts et quel est votre point de vue en ce qui concerne la sécurité?

M. Ron Green: Les systèmes bancaires ouverts offriront beaucoup de nouvelles possibilités, mais nous devons veiller à assurer la sécurité de la nouvelle technologie qui y est associée; des nouveaux fournisseurs. Je crois que le gouvernement peut aider en veillant à ce qu'ils respectent de bonnes normes lorsqu'ils déploient des capacités.

Le président: Monsieur Motz, la dernière question vous appartient.

M. Glen Motz: Je veux qu'on poursuive dans la même veine.

Michel, je vous remercie, c'était une excellente question.

J'aimerais que M. Davies y réponde.

Le président: Oh, je suis désolé. Est-ce que j'ai coupé la parole à quelqu'un? Pardonnez-moi.

M. Thomas Davies: Non, il n'y a pas de problème.

Je sais que le ministère des Finances travaille actuellement sur un document spécial qui porte sur les systèmes bancaires ouverts du point de vue la réglementation et de la sécurité. Comme M. Green l'a dit, il sera important de songer à la sécurité dès le début. Le Royaume-Uni est assez avancé en ce qui concerne les systèmes bancaires ouverts, alors il nous appartient d'examiner ce qu'il a fait et les leçons qu'il en a tirées.

Le président: Au nom du Comité, je remercie chacun de vous pour vos excellents témoignages. Ils ont été très instructifs.

La séance est levée.