CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 146 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mercredi 30 janvier 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le mercredi 30 janvier 2019

● (1530)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Distingués collègues, la séance est ouverte. Il est déjà passé 15 h 30, et je vois que nous avons le quorum.

Ceci est la 146e réunion du Comité permanent de la sécurité publique et nationale. Nous amorçons une étude sur la cybersécurité dans le secteur financier comme un enjeu de sécurité économique nationale.

On nous a signalé que notre autre témoin est pris dans sa propre ligne de sécurité, mais je présume que cela sera éventuellement réglé.

Je vois que M. Kabilan est là. Je suis certain qu'il est au courant de nos procédures, alors, sans plus tarder, je vais lui demander de nous livrer sa déclaration liminaire de 10 minutes.

M. Satyamoorthy Kabilan (vice-président, Politiques, Forum des politiques publiques): Bonjour.

Merci beaucoup de m'avoir invité à comparaître. Le sujet que vous m'avez demandé de couvrir est la question de la cybersécurité et, plus particulièrement, son application dans le secteur financier.

Je pense qu'il serait utile de commencer par quelques renseignements généraux sur la cybersécurité, sur les raisons pour lesquelles le secteur financier présente un intérêt ainsi que sur les acteurs qui pourraient avoir un intérêt à s'y attaquer, à le compromettre ou à s'y introduire. Je vais aussi parler de certains des problèmes qui peuvent survenir lorsque l'on tente de protéger le système financier et expliquer pourquoi ces problèmes existent.

J'ai fourni mes notes d'allocution à l'avance. La couverture du document se contente de donner quelques chiffres, quelques très, très gros chiffres. Essentiellement, il s'agit du nombre d'infractions commises par jour. Il y en a des centaines, si ce n'est plus, et ce nombre n'arrête pas d'augmenter. Les gens voient un grand intérêt à attaquer les organisations par le biais des cybertechnologies ou de l'Internet parce que c'est facile. Cela peut se faire de partout dans le monde. En ce qui concerne ceux qui verraient un intérêt à s'attaquer au secteur financier, je les regrouperais en quatre catégories.

La première catégorie est facile à concevoir. Ce sont les gens qui aiment le défi. Je les appelle parfois les amateurs de sensations fortes. Sur le plan de la cybersécurité, les systèmes des institutions financières sont probablement les plus difficiles à percer. Par conséquent, ceux qui réussissent à le faire sont encensés par leurs pairs de la communauté des pirates informatiques. Bien souvent, ces interventions sont bénignes — comme le fait de changer l'interface graphique d'une page Web — et ne cherchent qu'à entacher la réputation de l'institution, mais il s'agit d'un groupe bien réel qui lorgne du côté du secteur financier.

Ensuite, il y a les hacktivistes, c'est-à-dire ceux qui défendent une cause sociale ou politique et qui voient dans le secteur financier — ou dans ceux qui sont soutenus par lui — une partie de la cause des problèmes qui les touchent. Le piratage les aide à faire avancer leur cause ou leur message. Encore une fois, je pense que c'est une catégorie qui est facile à concevoir. Tout le monde a entendu parler d'Anonymous, bien qu'ils ne soient plus très anonymes.

Troisièmement, il y a les criminels. Encore une fois, c'est quelque chose qui va de soi, à certains égards. Dans le système financier, les criminels peuvent faire des gains financiers directs, mais ce n'est pas la seule chose qui les intéresse, et je pense qu'il est très important de le souligner. Vous pourriez pirater un système et essayer de siphonner de l'argent, mais l'argent n'est pas la seule chose que le système renferme, il y a aussi l'information. Nommément, ce sont des renseignements personnels et des renseignements sur les transactions des entreprises qui peuvent tous être monnayés d'autres façons. Les criminels ne se limitent pas à une simple monétisation directe de leurs attaques. Ils s'intéressent aussi aux avantages indirects qu'ils peuvent en tirer.

Enfin — et je pense que c'est là où les choses se compliquent le plus —, il y a la catégorie des États-nations. Vous vous posez peut-être la question: pourquoi un autre État s'intéresserait-il à notre système financier? Pensez-y un instant. Compte tenu des problèmes auxquels nous devons faire face dans le monde d'aujourd'hui, la concurrence économique n'a jamais été aussi vive. Or, le fait de comprendre le système financier d'un autre pays — parce que tout passe éventuellement par lui — peut donner une très bonne idée de la situation qui prévaut dans ce pays, certes, mais aussi de celle de certaines des sociétés qui s'y trouvent.

Lorsqu'il s'agit d'avoir le dessus sur les autres nations sur le plan des problèmes économiques — je vais m'abstenir d'utiliser le mot « guerre » —, il devient très utile de comprendre la situation financière de ses rivaux. En poussant l'idée plus loin, je dirais que l'information recueillie lors de prises de contrôle parrainées par des États-nations est encore plus utile. Si vous vous posez des questions sur la nature de la guerre moderne et des menaces modernes, pensez au système financier. Étant donné que nos systèmes financiers sont littéralement fondés sur la confiance, quiconque est en mesure de s'y infiltrer et d'intervenir sur cette confiance aura une incidence sur nos marchés.

Nous avons vu à maintes reprises comment les marchés changent en fonction de ce que les gens croient qu'il arrivera. Pour ces États-nations qui cherchent des avantages — mais qui sont aussi à l'affût d'une nouvelle sorte de guerre hybride —, les systèmes financiers deviennent une cible de grand intérêt. Par conséquent, le fait de réussir à saper la confiance dans un système financier peut avoir des conséquences de taille.

En tenant compte de ces quatre catégories d'intervenants et de ce qui se passe dans l'ensemble du système financier, je crois que nous pouvons dégager cinq grands problèmes.

Tout d'abord— et je crois qu'on l'a mentionné à maintes reprises —, il y a le fait que nous envisageons les menaces dans une optique de réglementation et de législation. Nous croyons qu'avec les bonnes règles et les bonnes normes, nous allons être en mesure d'empêcher les mauvaises choses de se produire.

Je ne sais pas combien d'entre vous composent avec l'obligation de changer de mot de passe tous les 60 ou 90 jours. Eh bien, sachez que cette règle a été inventée à l'époque où, à partir du moment où un intrus aurait mis la main sur un mot de passe, il fallait entre 60 et 90 jours pour compromettre un compte. Il s'agit d'une norme ISO, et dans bien des entreprises, c'est une obligation.

● (1535)

D'abord et avant tout, les normes ont du mal à suivre. Quand une norme finit par entrer en vigueur, la réalité est déjà loin en avant. Je pense que le grand problème — surtout dans un secteur fortement réglementé comme le secteur financier —, c'est que nous mettons toute notre confiance dans des normes et des règlements qui ne peuvent pas suivre l'évolution de la menace. Pour moi, ces normes et règlements sont le strict minimum. Il faut aller beaucoup plus loin que cela.

Le deuxième problème — qui est assurément tout aussi pertinent dans le secteur financier, mais qui touche à tous les aspects de la cybersécurité —, c'est celui du partage de l'information. Supposons que je suis l'entreprise A et que quelqu'un tente de me compromettre en s'attaquant à un logiciel très spécifique et que personne ne le sait, on se retrouvera avec ce que l'on appelle une « vulnérabilité de jour zéro ». Personne ne sait encore que cette vulnérabilité existe, mais le reste du secteur financier — peut-être à 70 % — dépend du même logiciel. Or, vous savez sans doute ce qui se produit dans ces cas-là. C'est embarrassant d'admettre qu'on a été piraté, alors on choisit de ne le dire à personne. C'est un cliché en matière de cybersécurité. L'information sur ce qui s'est passé est rarement relayée ou rendue disponible, voire jamais. Or, la question ici n'est pas de mettre qui que ce soit sur la sellette. Ces renseignements peuvent être mis à la disposition d'autrui de manière anonyme. Certains pays comme l'Australie, par exemple, ont des exigences de plus en plus rigoureuses en ce qui concerne la divulgation d'informations en matière de compromissions ou d'attaques. L'échange d'informations a en fait un rôle crucial à jouer dans la cybersécurité, et c'est quelque chose que nous ne faisons pas encore correctement.

Le troisième problème, c'est qu'il faut comprendre que la cybersécurité n'est pas une question strictement technologique. Chaque fois que je dis « cybersécurité », quelqu'un sort son téléphone intelligent et dit: « Oui, il faut sécuriser ça. » En fait, si vous regardez les dernières statistiques du commissaire à la protection de la vie privée de l'Australie sur les atteintes à la vie privée et que vous les répartissez en fonction des différentes catégories utilisées là-bas, vous allez voir que plus de 60 % de ces atteintes sont commises par des humains qui font des erreurs — avec ou sans malveillance — ou sont le fait d'un piratage psychologique. C'est 60 % ou plus. Ce n'est pas seulement un problème technologique. C'est aussi un problème humain.

Permettez-moi ici d'ajouter ceci: si je voulais pirater votre banque, ce n'est pas elle que je viserais directement, mais bien vous. Il est beaucoup plus facile d'exercer un piratage psychologique sur quelqu'un que d'essayer de déjouer les dispositifs de protection qu'une institution financière ou une grande organisation peut avoir.

Le quatrième problème, qui est une sorte d'extension de ce premier élément concernant la technologie, c'est les utilisateurs. Je pense qu'il y a quelques semaines, un reportage a fait état d'un utilisateur qui a été compromis parce qu'il avait été victime d'une arnaque et qu'on lui faisait payer de grosses sommes. Malheureusement, comme un expert me l'a expliqué un jour, cette sécurité, c'est comme si on avait des véhicules blindés avec des agents armés qui feraient passer de l'argent entre deux boîtes en carton. Ce qui nous préoccuperait là-dedans, ce serait la boîte en carton en fin de processus, parce qu'il se peut que l'utilisateur au bout de la ligne ne soit pas aussi bien protégé que la banque, l'institution financière ou le fournisseur de services, ou qu'il ne comprenne pas les choses aussi bien qu'eux.

Mon plus grand cauchemar a été quand mon père s'est procuré un compte eBay et un compte PayPal. Tout le monde n'est pas familier avec le monde numérique et conscient du fait qu'ils peuvent être la cible d'attaques. Même si vous et moi pouvons les regarder en rigolant et dire que nous savons que ce sont des arnaques, ce n'est pas le cas de tout le monde. L'utilisateur au bout de la chaîne est donc un autre élément dont il faut tenir compte.

Pour en revenir à ce que je disais tout à l'heure, réfléchissez à l'incidence que cela pourrait avoir sur la confiance si un nombre névralgique d'utilisateurs — surtout s'ils ont commencé à prendre de l'âge — commençaient à subir de telles attaques, et ce, même sans que ce soit la faute de l'institution financière. Ils le diront à leurs amis, leurs amis le diront à leurs amis, et le bruit se répandra. Il y a un problème avec le système, mais ce n'est pas à cause du système. Tout bien compté, c'est à cause de l'utilisateur.

Le dernier élément est, à mon avis, un problème de taille, et c'est une question qui ne manque pas d'actualité. Il s'agit des chaînes d'approvisionnement. Cela peut sembler un peu étrange dans le domaine de la cybersécurité, mais regardez les choses sous l'angle suivant. Nous achetons de l'équipement, nous achetons des pièces de partout dans le monde et nous les intégrons à nos systèmes. Il y a probablement entre trois et vingt pays qui ont fourni quelque chose pour fabriquer les écouteurs que nous utilisons aujourd'hui pour la traduction simultanée, pour le système audio. Il y a une chaîne d'approvisionnement directe, mais ce n'est même pas dans l'équipement que nous utilisons directement. Certains d'entre vous se souviennent sûrement de la tristement célèbre brèche dont Target a été victime. Pour arriver à leurs fins, les pirates s'en sont pris à un sous-traitant de Target en chauffage, ventilation et climatisation, puis, de là, ils ont pu déjouer le système de sécurité et accéder aux données de Target.

Les chaînes d'approvisionnement sont devenues très complexes. Il ne s'agit pas seulement des pièces que nous achetons, mais aussi des organisations qui nous fournissent des services. Comme je le disais plus tôt, je n'attaquerais pas votre entreprise de front, mais je passerais par l'un de vos fournisseurs de services. Lorsque nous pensons à la cybersécurité, tous ces éléments s'additionnent pour former une image inquiétante. Quelle incidence cela peut-il avoir sur la confiance ? Si ces incidents continuent de se produire à un certain rythme, cela risque-t-il d'avoir une incidence sur la confiance, cette pierre d'assise de notre système financier? C'est la raison pour laquelle la cybersécurité dans le système financier est devenue et continue d'être une préoccupation de premier plan du monde actuel.

● (1540)

Le président: Merci beaucoup.

Apparemment, notre deuxième expert en cybersécurité est retenu à la sécurité, ce qui est un problème. Je propose que nous commencions nos questions. Quand il arrivera, nous pourrons interrompre l'interrogatoire pour entendre son témoignage.

Cela dit, nous allons laisser la parole à M. Spengemann, pour sept minutes.

M. Sven Spengemann (Mississauga—Lakeshore, Lib.): Monsieur le président, merci beaucoup.

Merci, monsieur Kabilan, d'être ici aujourd'hui.

L'un des angles que j'aimerais adopter pour examiner le sujet à l'ordre du jour, c'est la prémisse qui veut qu'une bonne cybersécurité soit bonne pour les entreprises canadiennes, bonne pour les investissements étrangers et qu'elle constitue un bien collectif. À votre avis, quelle est la situation du système canadien par rapport, disons, à celle de nos alliés du Groupe des cinq, dont nous parlons beaucoup? Vous avez mentionné l'Australie. Où en sommes-nous, et plus particulièrement en ce qui concerne le secteur bancaire? Selon vous, quels sont les problèmes concrets que le Comité devrait examiner?

M. Satyamoorthy Kabilan: D'abord et avant tout, sachez que je suis tout à fait d'accord avec l'affirmation selon laquelle une bonne cybersécurité est synonyme de bonnes affaires et de bonnes ouvertures pour le Canada. À une époque où les données sont devenues si importantes et où la capacité de fonctionner sur une base virtuelle est devenue l'élément central ou fondamental de presque toutes les organisations, c'est presque devenu une exigence infrastructurelle d'avoir des systèmes efficaces, robustes et sécuritaires.

Pour ce qui est de savoir où en est le Canada à l'heure actuelle, disons que c'est une chose qui est très difficile à évaluer. Je reviens à ce que j'ai dit au sujet du partage de l'information. Il y a certains éléments qui indiquent de manière éloquente que nous ne faisons peut-être pas aussi bien qu'ailleurs. La question du partage de l'information sur les atteintes à la cybersécurité est l'un de ces principaux éléments. Nous ne sommes pas tenus de le faire. Il y a eu des tentatives dans le secteur privé pour tenter de corriger cette situation — l'organisme Échange canadien de menaces cybernétiques en est un exemple — et je crois que Scott Jones vous en parlera plus tard. Néanmoins, je ne pense pas que nous réussissions très bien dans ce domaine.

Pour ce qui est d'agir, l'une des choses que nous devons examiner, c'est la façon dont nous pouvons diffuser cette information. Si vous avez fait l'objet d'une compromission ou si vous avez un problème, la divulgation de l'information ne sera pas utilisée pour vous mettre dans l'embarras ou vous causer des problèmes auprès des actionnaires. Tout ce que cela signifie, c'est que ces renseignements pourront être communiqués à la communauté. On pourra dire à tout le monde: « Il y a telle ou telle vulnérabilité, et voici ce que vous pouvez faire. » Il est difficile de juger où nous en sommes, mais, chose certaine, il n'y a pas de mécanisme robuste en place pour faire circuler ces informations de base et veiller à ce que toutes les organisations puissent y avoir accès.

M. Sven Spengemann: Voilà qui est très utile.

Croyez-vous que la tendance à sous-déclarer la cybercriminalité est seulement attribuable à la crainte de la stigmatisation qui pourrait découler du signalement d'une atteinte, ou y a-t-il d'autres facteurs dont le Comité devrait être informé?

M. Satyamoorthy Kabilan: L'embarras est certainement un facteur, mais le signalement de ces incidents peut aussi avoir des conséquences financières. Ces conséquences peuvent être directes — à savoir des amendes imposées pour la perte de données personnelles — ou indirectes, comme les atteintes à la réputation qui en découlent. Bien entendu, cela peut aussi avoir des répercussions directes sur les actionnaires en faisant chuter le prix des actions, par exemple. Ces incidents s'accompagnent d'un éventail de répercussions.

Dans le cadre de mon rôle précédent, nous avons rédigé un document portant sur l'échange d'information et de renseignements. Il y a un autre modeste élément que, selon moi, nous n'avons pas abordé, mais qui pourrait être utile — notamment les fausses impressions du public et du secteur privé quant aux renseignements qui peuvent être échangés et aux renseignements qui seront protégés. Par exemple, en tant que membre d'une entreprise privée, si je communiquais certains de ces renseignements au gouvernement du Canada, ces renseignements seraient techniquement considérés comme confidentiels et, en vertu de l'AIPRP, ils devraient être protégés contre toute divulgation. Je le répète, ces renseignements sont privés et ont des conséquences commerciales. Souvent, les gens ne comprennent pas bien où ces renseignements sont conservés et comment ils sont protégés.

En revanche, certains rapports examinent la difficulté qu'éprouvent les fonctionnaires à comprendre ce qu'ils peuvent communiquer à leur tour. En ce qui concerne les cotes de sécurité, voici la réponse que nous adresse constamment le secteur privé: « Bien que je détienne une cote de sécurité de niveau « secret », vous n'êtes pas, en fait, autorisé à me communiquer des données secrètes ou la teneur d'une conversation secrète ». Que vous déteniez ou non cette cote de sécurité, la circulation de l'information dépend tout de même grandement des relations que vous pourriez entretenir.

M. Sven Spengemann: Merci beaucoup. Je mentionne de nouveau que vos témoignages nous sont très utiles.

Vous parlez uniquement des institutions financières, des grands établissements qui sont la pierre angulaire de notre économie et qui ont la capacité de s'occuper de leur propre infrastructure de sécurité informatique. Je souhaite maintenant changer légèrement d'angle et vous demander ce que vous pensez des petites entreprises et des entreprises en démarrage. Le gouvernement actuel est très soucieux de créer un environnement qui encourage l'entrepreneuriat, le démarrage d'entreprises et l'innovation. Pour les petites entreprises, le coût d'établissement de leur propre infrastructure de sécurité informatique est...

Je vais vous céder la parole à ce sujet. Ce coût est-il prohibitif? Y a-t-il des difficultés particulières que nous devons examiner dans le cas des petites entreprises? Dans l'affirmative, quel rôle accru les gouvernements pourraient-ils jouer afin de leur fournir une plateforme satisfaisante de sécurité informatique?

● (1545)

M. Satyamoorthy Kabilan: Je ne dispose d'aucun résultat de recherches approfondies à ce sujet, mais, selon les quelques éléments que mon équipe a examinés dans le passé, je dirais que, bien que problématique, le coût de cette infrastructure n'est pas le premier problème que je réglerais. Certains travaux, comme celui de veiller à ce que vos systèmes soient à jour, occasionnent des coûts, mais il s'agit en grande partie d'une question d'éducation. Comment puis-je protéger mes systèmes? Quelles mesures sont requises, et comment puis-je quantifier le risque qui pèse sur mon entreprise? Les risques que je cours sont-ils liés au fait que je possède une cantine mobile et que j'accepte des cartes de crédit? Ces risques ressemblent-ils à ceux que je courrais si j'exploitais une boutique et que je recueillais des renseignements personnels dans le but de créer un programme de fidélisation? Les risques seraient-ils les mêmes? Ces données seront-elles envisagées de la même façon par les acteurs qui pourraient souhaiter s'attaquer à mon organisation?

Je pense que la grande difficulté n'est pas tellement le coût de cette infrastructure; le problème est plus fondamental. Il est lié à l'éducation et à la difficulté de faire comprendre aux petites entreprises les risques qu'elles courent et les mesures simples qu'elles peuvent prendre pour atténuer ces risques.

M. Sven Spengemann: J'aimerais simplement utiliser la minute et demie qui me reste pour vous demander quels sont, selon vous, les leviers dont dispose le gouvernement, outre la réglementation, et ce que vous pensez, le cas échéant, de l'idée d'établir des partenariats publics-privés afin d'élargir notre infrastructure de sécurité de base pour le secteur privé.

M. Satyamoorthy Kabilan: À mon avis, il est certain que la voie des partenariats publics-privés doit être envisagée, car aucun secteur n'a réponse à tout par lui-même.

Je précise de nouveau que des organisations comme l'Échange canadien de renseignements sur les menaces cybernétiques ont tenté d'accomplir cela. Elles ont fait appel au gouvernement et ont tenté de travailler avec le secteur privé. Mais le défi consiste à réunir ces deux groupes.

Certains organismes gouvernementaux, comme le Centre de la sécurité des télécommunications, ont des capacités à cet égard. Elles ont acquis des capacités et des connaissances remarquables mais, de même — et vous l'avez déjà mentionné —, les grandes institutions financières investissent dans la cybersécurité. Elles ont donc leurs propres connaissances et leurs propres capacités. Si ces éléments pouvaient être réunis, le tout serait beaucoup plus grand que la somme des actions des intervenants qui travaillent seuls.

M. Sven Spengemann: Merci. Je mentionne encore une fois que vos réponses nous sont extrêmement utiles.

Monsieur le président, me reste-t-il du temps?

Le président: Il vous reste 15 secondes.

M. Sven Spengemann: Je pense que je vais céder le temps qu'il me reste aux prochains intervenants.

Merci beaucoup.

Le président: Pendant ces 15 secondes, je vais poser une question. Lors de ma visite de l'OTAN la semaine dernière, un conférencier a parlé du modèle norvégien, dans lequel tous les renseignements proviennent d'un seul endroit. Êtes-vous prêt à formuler des observations à ce sujet?

M. Satyamoorthy Kabilan: Le modèle norvégien ne m'est pas complètement familier, mais si vous parlez d'un centre des communications où tout converge et tout est aseptisé ou protégé, je dirais que, dans ce cas, vous avez l'énorme avantage de pouvoir vous assurer que le centre contrôle tout. Le revers de la médaille, c'est que si ce centre tombe en panne, tout tombe en panne.

Le président: Bien. Merci.

Monsieur Motz, vous avez la parole pendant sept minutes.

J'espère que nos préposés à la sécurité ont une excellente raison à nous présenter pour expliquer l'absence de notre témoin.

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Je viens d'envoyer Sean en bas, et il a dit...

Le président: J'ai aussi dépêché mon Shawn en bas.

M. Glen Motz: D'accord. Sean et Shawn devraient être en mesure de gérer la situation. Il a dit que le témoin devrait être ici dans quelques minutes. Donc, avec un peu de chance...

Le président: Ces quelques minutes sont longues.

M. Glen Motz: Si vous me le permettez, monsieur le président, je peux commencer à poser mes questions. Je pourrais aussi adapter légèrement les questions destinées à M. Leuprecht.

Monsieur, je vous remercie de votre présence parmi nous.

Compte tenu de vos antécédents, l'une des questions que je souhaite vous poser est liée à la question de savoir si vous pouvez nous expliquer certaines des vulnérabilités que présente actuellement la technologie de l'IO, c'est-à-dire la technologie de l'Internet des objets. Je crois que les gens ne comprennent pas vraiment les vulnérabilités qui existent dans ce secteur. Pourriez-vous nous les expliquer?

M. Satyamoorthy Kabilan: L'Internet des objets est un phénomène plutôt intéressant. Pour récapituler un peu, je précise que ce phénomène est lié au fait qu'il est de plus en plus économique de doter les objets de micropuces...

Le président: M. Motz a gracieusement accepté de reporter pour le moment son intervention. Nous repartirons l'horloge de M. Motz une fois que M. Leuprecht se sera installé.

Je suis sûr que vous avez des commentaires négatifs à formuler à propos de notre niveau de sécurité.

M. Christian Leuprecht (professeur, Département de sciences politiques, Collège militaire royal du Canada, à titre personnel): Nous devons tous nous contenter des ressources dont nous disposons, n'est-ce pas?

Le président: Fort bien.

Vous êtes un témoin d'expérience qui a comparu devant notre comité ainsi que d'autres comités. Nous nous réjouissons à la perspective d'entendre ce que vous avez à dire pendant les 10 prochaines minutes.

M. Christian Leuprecht: La lecture de mon mémoire durerait plus de 10 minutes. Par conséquent, je vais me contenter de souligner quelques points. J'ai essayé d'assurer la distribution de mon mémoire avant mon exposé afin que nous puissions aborder d'autres questions.

[*Français*]

Comme toujours, je me ferai un plaisir de répondre à vos questions dans les deux langues officielles, mais je vais livrer ma présentation en anglais.

[*Traduction*]

Il y a cinq différents éléments qu'on m'a demandé de commenter en ce qui concerne l'éventail des cybermenaces qui pèsent sur le secteur financier.

Ici, en particulier, je souligne les menaces qui, de façon plus générale, découlent d'Internet, y compris les services bancaires en ligne et les transferts financiers, et, en particulier, les menaces au réseau SWIFT, c'est-à-dire la vulnérabilité de l'ensemble d'Internet et de tous les transferts électroniques, ainsi que la vulnérabilité des banques, en particulier lorsqu'il s'agit de détecter le blanchiment d'argent — de connaître son client — et les problèmes à grande échelle de blanchiment financier d'argent qui existent. Dans mon mémoire, j'énumère certains de ces problèmes. Il y a aussi les dangers qui découlent du réseau SWIFT, auquel le Canada est évidemment rattaché.

Vous trouverez ici quelques recommandations visant à appuyer les besoins en matière de cybersécurité des petites et moyennes institutions financières, en particulier; des besoins qui, à mon avis, sont souvent négligés, étant donné que nous nous soucions seulement des grandes organisations.

De plus, le Canada doit élaborer une politique pour reconstruire l'infrastructure technologique du système financier en cas de défaillance majeure. Je crois que nous n'avons pas tout à fait déterminé la relation qui existerait entre le gouvernement et l'industrie privée si le système en entier tombait en panne et qu'en fait, nous avions besoin d'une intervention gouvernementale et des compétences de certains de nos collègues d'Ottawa pour rétablir la totalité du système.

Nous devons avoir la capacité de publier des avis d'attaques de représailles possibles et de poursuivre les pirates informatiques de toutes les façons autorisées par le droit national et international, et, à mon avis, nous pourrions prendre toutes ces mesures de façon plus énergique.

Deuxièmement, je vais formuler brièvement des observations concernant les vulnérabilités et les efforts d'atténuation propres au secteur.

Le secteur bancaire, en particulier, est vulnérable aux actions des initiés. Cela s'applique non seulement aux menaces physiques que font peser les initiés, mais aussi aux gens qui permettent à ces menaces dans le domaine de la circulation et du blanchiment d'argent d'infiltrer l'organisation. On estime qu'environ 2,5 billions de dollars sont blanchis annuellement à l'échelle mondiale, dont une grande partie par voie électronique, y compris — comme vous le savez, compte tenu de notre propre affaire à Vancouver qui a été révélée récemment — une somme considérable d'argent blanchi dans notre propre pays.

Les banques doivent assumer la responsabilité pour les pertes des consommateurs, comme elles le font. Toutefois, elles ne sont pas grandement incitées à prendre toutes les mesures qu'elles pourraient. Lorsqu'elles doivent choisir entre la commodité et la sécurité, elles choisissent toujours la commodité, parce que c'est ce que désirent les clients. En outre, nous ne sommes pas convaincus que le gouvernement force les banques à prêter suffisamment attention au compromis à faire. À l'heure actuelle, lorsque des vols de banque sont commis à l'aide d'une cyberattaque, rien n'incite les banques à le faire savoir, ce qui signifie que tous les autres seront vulnérables au même genre d'attaque. Les banques courent aussi un risque d'atteinte à leur réputation.

Il est donc recommandé, entre autres, d'élaborer un cadre qui permettra d'atténuer les pertes des consommateurs liées à un comportement institutionnel ou personnel risqué; d'appuyer l'industrie naissante de la cybersécurité, dans laquelle le gouvernement peut intervenir davantage et devrait le faire; d'élaborer des politiques incitant les banques à analyser leurs données à des fins de cybersécurité; et d'encourager le gouvernement à collaborer davantage avec les organismes d'application de la loi, le CANAFE et les institutions financières, notamment en accordant au CANAFE une capacité d'application de la loi.

Troisièmement, des liens de dépendance liés aux infrastructures existent. Ils découlent du fait qu'Internet ne respecte pas les frontières. Par conséquent, les renseignements détenus par des entreprises comme les banques sont vulnérables aux pannes de données, aux atteintes à la sécurité des données et aux interruptions de communication provoquées accidentellement ou délibérément dans d'autres pays. Le réseau SWIFT, par exemple, a subi des pannes de plusieurs heures. Les institutions financières souhaitent conserver les données sur leurs clients et leurs opérations dans des répertoires nationaux, mais c'est difficile à accomplir compte tenu de la façon dont l'infrastructure est établie en ce moment. En raison de la mesure dans laquelle l'infrastructure est répartie, les données canadiennes sont vulnérables aux atteintes à la sécurité des données à l'étranger, où la réglementation est moins sévère.

L'infrastructure des systèmes de communication utilisés par les banques... En raison de la nature du système actuel et de toute extension considérable comme la technologie 5G, il est impossible d'éliminer ces vulnérabilités. On peut seulement les atténuer. Il est donc recommandé ici que le Canada mette en oeuvre une stratégie de localisation de données souveraines, renforcée par des incitatifs législatifs et fiscaux, qui obligerait les données essentielles à être conservées uniquement sur le territoire canadien, qui établirait des normes et des attentes claires pour la résilience des infrastructures de communication canadiennes, qui surveillerait cette résilience et qui imposerait des pénalités aux entreprises d'infrastructures de communication essentielles qui ne respectent pas les normes ou ne prennent pas les mesures nécessaires pour éliminer leur vulnérabilité.

● (1550)

Quatrièmement, il y a le rôle des fournisseurs de services de communications dans le secteur de la détection et de l'atténuation des menaces. C'est là que les télécommunications jouent un rôle particulièrement important. Je donne aussi l'exemple de l'inspection approfondie des paquets à laquelle le Centre de la sécurité des télécommunications, notamment, procède pour protéger l'infrastructure gouvernementale. Deux points préviennent la pleine exploitation de cette possibilité. Premièrement, comme ce niveau de détection est coûteux, les fournisseurs de services de télécommunication sont peu enclins à le fournir. Ensuite, ils jugent qu'une amélioration devient problématique sur le plan juridique une fois qu'elle est détectée. Une particularité intéressante est que les fournisseurs de services de télécommunications en Australie ont été beaucoup plus disposés à être proactifs, bien que leur régime législatif soit presque identique à celui du Canada. Selon moi, on doit se pencher davantage sur les résultats extrêmement différents qu'ont obtenus le Canada et l'Australie pour voir les leçons qu'on peut en tirer afin d'obtenir les mêmes résultats que l'Australie dans le cadre du même régime juridique.

La recommandation est que le gouvernement devrait préciser les possibilités et les obligations des fournisseurs de services de télécommunication sur le plan de la détection et de l'amélioration des communications qui pourraient causer du tort. Le gouvernement devrait investir davantage dans la recherche sur la cybersécurité. Nous avons déjà un certain nombre de capacités de calibre mondial, notamment en informatique quantique et en cryptographie, mais les besoins sont beaucoup plus grands. La demande de personnel hautement qualifié surpasse grandement l'offre. Contrairement à l'Australie, le Canada n'est pas doté d'une stratégie sur la façon de générer ce type de ressources humaines.

Enfin, il y a des questions liées aux entités participant à l'économie canadienne et aux infrastructures de télécommunication du Canada qui pourraient être assujetties à des directives extraterritoriales de la part de gouvernements étrangers. Deux parties des infrastructures de télécommunication comportent des vulnérabilités qui sont intrinsèquement impossibles à éliminer: les commutateurs réseau qui forment la base du Web et les dispositifs grand public eux-mêmes. Les commutateurs réseau voient forcément toutes les données qu'ils acheminent. Si ce flux de données est peu ou pas chiffré, ces commutateurs pourraient être en mesure de lire tout ce qu'ils acheminent. Même si le flux de données est fortement chiffré, il est impossible de dissimuler les habitudes de communication du commutateur. Cette analyse du trafic peut révéler beaucoup de renseignements. Les commutateurs peuvent aussi contrôler la façon dont ils gèrent la communication: ils peuvent la retarder, l'interdire complètement, ou détourner le trafic.

Le matériel et les logiciels qui forment un commutateur peuvent être analysés afin de repérer des vulnérabilités qui auraient pu être intégrées. Cependant, il faut être en mesure de mettre à jour les logiciels d'un commutateur de temps à autre. Par conséquent, chaque commutateur possède un mécanisme lui permettant de communiquer avec sa base à distance pour vérifier s'il y a des mises à jour et les télécharger. II est extrêmement difficile de surveiller ce mécanisme de mise à jour. La technique d'acheminement d'Internet se sert de tableaux qui indiquent à chaque commutateur le lien sortant à utiliser pour se rendre à chaque destination finale. Ces tableaux représentent une vulnérabilité, et il y a récemment eu plusieurs incidents où une grande quantité de données ont été mal acheminées dans le territoire d'un État particulier. Les dispositifs grand public comme les téléphones cellulaires comportent une vulnérabilité inhérente parce qu'ils doivent être en mesure de voir les touches appuyées et l'information affichée, même si ces données sont chiffrées pour le reste de leur existence. Les fabricants de tels dispositifs sont en position de voir tous leurs intrants et leurs extrants, même si l'espace de stockage d'un dispositif et toutes ses communications sont chiffrés. Puisque de tels dispositifs sont utilisés régulièrement pour effectuer des opérations bancaires, il est possible, en principe, de saisir des détails financiers et des opérations.

Voici les recommandations. Premièrement, le gouvernement devrait interdire à des fournisseurs de services de télécommunication comme Huawei de participer à la mise au point de l'infrastructure des réseaux 5G. Nous estimons — j'insiste ici sur le fait que j'ai rédigé ce mémoire avec un collègue en sciences informatiques et un autre en droit — que le gouvernement devrait exclure Huawei du développement de l'infrastructure mobile 5G du Canada. Par suite d'une modification législative récente, la Chine peut demander à toute entreprise chinoise, dont Huawei, de l'aider à appuyer les intérêts nationaux, y compris en matière de renseignement.

Une préoccupation connexe est que la Chine et ses industries sont soupçonnées de se livrer à de l'espionnage industriel à grande échelle à titre de moyen peu coûteux de faire des transferts de recherche et développement. De plus, Huawei et le Parti communiste au pouvoir semblent être imbriqués de bien des façons importantes, y compris par l'intermédiaire de subventions de l'État qui s'élèveraient à 10 milliards de dollars dans une seule année. Le vol systématique de propriétés intellectuelles et les énormes subventions de l'État font en sorte qu'il est impossible pour des concurrents comme Nortel Networks de faire concurrence, ce qui a fini par mener à la disparition de la principale société de haute technologie du Canada. Étant donné que les communications sont des infrastructures essentielles, le gouvernement devrait exclure systématiquement de l'ensemble des infrastructures de communications canadiennes toute entité étrangère soupçonnée d'avoir des liens avec tout pays pour lequel il existe de solides preuves de vol important de propriété intellectuelle ou de collecte de renseignements.

● (1555)

Pour le bien de la sécurité canadienne, de l'industrie canadienne et de la recherche canadienne, le Canada a un intérêt stratégique à appuyer ses alliés et à exclure les entités étrangères qui, selon eux, minent leurs intérêts en matière de sécurité nationale. Ce faisant, il se joindrait non seulement à ses partenaires du Groupe des cinq — les États-Unis, l'Australie et la Nouvelle-Zélande —, mais aussi à une liste croissante d'autres alliés qui ont déjà pris, ou cherchent activement à prendre, des mesures en vue d'exclure Huawei de leurs réseaux 5G et de leurs réseaux de communications, dont le Japon, la Corée du Sud, l'Allemagne, la France, la République tchèque et la Pologne.

De plus, le conseil d'évaluation du Huawei Cyber Security Evaluation Centre, établi conjointement entre l'entité en question et le GCHQ au Royaume-Uni, est devenu encore moins certain des répercussions en matière de sécurité de cette entité et de ses produits. Les fournisseurs de services de télécommunication au Royaume-Uni et en France remplacent activement cet équipement dans leurs infrastructures de communications essentielles.

Dans ce dossier, le Canada semble de plus en plus en décalage avec ses principaux alliés, et ses tergiversations risquent d'entacher sa réputation d'allié fiable et mettent en péril son intégration dans les infrastructures de communications de l'Amérique du Nord et des alliés. Le Canada a déjà exclu ce fabricant étranger des infrastructures gouvernementales essentielles il y a de nombreuses années. Il devrait en faire autant en ce qui concerne le réseau national.

● (1600)

Le président: Merci, monsieur Leuprecht.

Vous aviez 10 minutes pour faire votre exposé, mais compte tenu de vos frustrations à l'égard de la sécurité au pays, j'ai estimé que vous devriez avoir de la latitude.

Monsieur Motz, vous avez sept minutes.

M. Glen Motz: Merci, monsieur le président. Je vais revenir à la question que j'ai posée à M. Kabilan.

Pouvez-vous expliquer les vulnérabilités qui existent dans la technologie IdO?

M. Satyamoorthy Kabilan: Pour en revenir à ce que j'ai mentionné sur Internet, le réseau s'est développé de façon à ce qu'il soit de moins en moins coûteux de littéralement construire et placer un minuscule ordinateur dans n'importe quel objet. On peut donc avoir un réfrigérateur intelligent, ce dont je ne veux pas, car ma femme saurait la quantité de bière que je bois.

Des voix: Oh, oh!

M. Satyamoorthy Kabilan: Cependant, en fin de compte, c'est une question de coûts de production raisonnables, et la sécurité coûte cher. Si vous essayez de concevoir un produit pour qu'il coûte le moins cher possible, la sécurité est la première chose que vous aurez tendance à écarter.

Ces choses sont omniprésentes. On peut les obtenir n'importe où. Quand on y pense, lorsqu'un tas de très petits ordinateurs sont regroupés, ils ne peuvent pas faire grand-chose seuls, mais ils ne sont pas sécurisés. Il est très facile d'en prendre le contrôle. Comme ils surveillent votre maison, par exemple, ils sauront quand vous êtes là ou non. S'ils utilisent une caméra, ils pourraient connaître le mot de passe que vous tapez. Ajoutez cela au fait qu'une fois regroupés, ces petits ordinateurs forment soudainement un gigantesque super ordinateur.

Je crois qu'à l'automne 2016, une panne sur la côte Est a touché une partie des principales entreprises de médias sociaux comme Twitter et d'autres sites Web importants. Il s'agissait, en gros, d'une attaque entraînant un refus de service à grande échelle. Une entreprise s'était penchée sur tous ces appareils mal sécurisés, les a tous regroupés comme un marteau géant et a littéralement frappé ce qui était, essentiellement, un fournisseur d'adresses important sur lnternet, ce qui a causé une des plus grandes pannes de l'histoire. À ce jour, je crois que c'est toujours l'attaque entraînant un refus de service la plus sérieuse jamais vue.

En conséquence, les appareils bon marché compromettent la sécurité, mais c'est la même chose partout. C'est dans tout. Lorsqu'on les regroupe, ils peuvent être assez impressionnants et dangereux.

M. Glen Motz: Merci pour cette analyse.

Monsieur Leuprecht, je vous remercie de votre témoignage. Vous connaissez certainement l'étude conjointe réalisée par le U.S. Naval War College et l'Université de Tel Aviv, qui a révélé que la Chine réacheminait le trafic Internet du Canada et des États-Unis vers ses propres serveurs, au Canada et aux États-Unis, avant l'envoi des données. À ce jour, le gouvernement actuel s'est contenté de répondre qu'il ferait son possible pour soulever cette question auprès de la Chine. C'est ce qu'il nous a dit.

Comment qualifieriez-vous l'usage de ce type de pratique par une entité étrangère? Est-ce de l'espionnage? Est-ce une cyberattaque? Selon votre expérience, de quoi s'agit-il?

M. Christian Leuprecht: Ces interventions sont problématiques, car elles n'atteignent pas le seuil d'emploi de la force. Nous n'avons donc pas de régime international qui nous permette de les catégoriser. Elles constituent clairement une exploitation de notre réseau, et cela nous ramène au problème de sa vulnérabilité. Il s'agit d'un réacheminement du trafic via le recodage des serveurs DNS. Cela souligne la vulnérabilité du réseau dans son ensemble.

Le réseau fonctionne au moyen de commutateurs. Il n'y a qu'un nombre limité de commutateurs de premier niveau. Les fournisseurs de services de télécommunication n'en ont qu'un très petit nombre. Plus vous arrivez à vous approcher de ces commutateurs, plus vous serez en mesure de capter ou de réacheminer le trafic. Actuellement, nos adversaires essaient d'atteindre le niveau le plus élevé possible dans la structure des commutateurs, notamment en plaçant leurs propres serveurs dans les mêmes bâtiments que certaines grandes entreprises de télécommunications.

Nous espérons que les entreprises de télécommunications se montrent vigilantes à ce sujet, mais nous ne savons pas si elles s'assurent, par exemple, que nos adversaires ne louent pas l'étage situé au-dessous ou au-dessus de leurs locaux afin de se connecter physiquement à ces commutateurs.

Actuellement, le problème est que pour capter le trafic, vous devez utiliser un serveur qui capte le trafic entrant et sortant, ou réacheminer le trafic grâce à des serveurs DNS. Vous ne pouvez le faire que pendant un certain temps, car les gens finissent par se rendre compte de ce qui se passe. Vous devez donc agir stratégiquement et le faire lorsque vous essayez de capter des communications particulières.

Le problème est que si la technologie d'une entité adversaire se trouve dans le système même, cet adversaire n'a plus besoin d'atteindre les commutateurs de premier niveau parce que c'est l'ensemble du système qui est maintenant vulnérable. Contrairement au réacheminement du trafic, cette méthode leur permet de capter autant de trafic qu'ils le souhaitent.

● (1605)

M. Glen Motz: Nous avons entendu des comparaisons, et je m'adresse à vous, monsieur Leuprecht, entre l'état de cyberguerre actuel et ce que l'on appelait autrefois la guerre froide. Notre infrastructure essentielle subit des millions d'attaques — parfois tous les jours — qui, comme vous l'avez mentionné, n'atteignent pas le seuil justifiant des représailles conventionnelles. Elles nuisent toutefois aux personnes, aux sociétés et au gouvernement.

Pouvez-vous décrire la situation dans laquelle cela met le Canada et dire ce que nous devrions faire à ce sujet?

M. Christian Leuprecht: Il y a ici deux vulnérabilités, et je pense que nous nous rapprochons en réalité beaucoup plus d'une cyberguerre que certains ne le pensent, précisément à cause de ces vulnérabilités. L'une de celles-ci est que nos adversaires surestiment leurs capacités dans cet espace. Pour cette raison, et parce que leurs organismes du renseignement d'origine électromagnétique et autres leur disent qu'ils peuvent le faire, ils sous-estiment notre réaction. Les incertitudes comprennent donc, par exemple, les réactions possibles de l'adversaire et le ciblage de celles-ci. Ces armes de l'information peuvent facilement devenir incontrôlables et pénétrer d'autres types de systèmes.

Nous avons donc de la difficulté à déterminer à quel moment une cyberattaque devrait donner lieu à une intervention conventionnelle ou avoir un effet domino qui pourrait avoir des conséquences conventionnelles pour nous au Canada, et à quel moment nous pourrions, par exemple, décider qu'une cyberattaque justifie une intervention conventionnelle.

J'ai un autre document complet à ce sujet, que je me ferais un plaisir de transmettre au Comité, mais je pense en réalité que l'incertitude dans cet espace est très inquiétante, car elle crée toutes sortes de risques d'idées fausses et d'escalades, pour lesquelles nous n'avons aucun cadre international.

M. Glen Motz: Je pense qu'il serait bon que vous soumettiez ce document au Comité.

Le président: Si vous souhaitez soumettre ce document au Comité, je suis sûr qu'il n'y verra pas d'inconvénient.

Monsieur Dubé, allez-y, s'il vous plaît. Vous avez sept minutes.

M. Matthew Dubé (Beloeil—Chambly, NPD): Je vous remercie, monsieur le président.

Je voudrais revenir au concept de cyberguerre, cela semble être un grand mot, mais il a été évoqué, et au terme « guerre hybride », que vous avez, je pense, également utilisé. Je veux revenir un peu à la chaîne d'approvisionnement parce que, sans entrer dans les détails relatifs à chaque entreprise, etc., il y a la question de... en particulier parce que je pense que beaucoup d'entre nous, y compris les personnes présentes autour de cette table, ne comprennent pas vraiment les problèmes liés au 5G, et on en a beaucoup parlé.

L'un des problèmes est l'omniprésence des appareils tels que les téléphones intelligents et de toutes sortes d'objets de ce type. Vous avez utilisé l'exemple des réfrigérateurs. Ce problème se pose. Vous avez dit que vous n'attaqueriez pas la banque, mais la personne. Est-il donc possible que, par exemple, dans le cas des objets fabriqués en Chine, vous empêchiez le développement d'appareils équipés de la technologie 5G par une entreprise provenant de ce pays, mais qu'au bout du compte, ce pays participe tout de même à la fabrication du téléphone cellulaire, par exemple, même s'il s'agit d'un iPhone ou de quelque chose du genre?

Quels sont les problèmes liés au fait que les appareils se connectent au réseau? Peut-être que le réseau est protégé, mais pour ce qui est des appareils, ceux que nous allons maintenant utiliser chez nous, les véhicules autonomes et tous ces objets dont on parle actuellement et qui sont la raison pour laquelle la technologie 5G serait utile, nous n'avons actuellement aucun protocole de sécurité. J'aimerais vous poser la question à tous les deux, si vous me le permettez.

M. Satyamoorthy Kabilan: C'est ce qu'on appelle communément la sécurité des points terminaux. Littéralement, c'est le point d'extrémité d'Internet.

Faisons abstraction du fournisseur, pour quelques instants. Si ce qui se trouve au point terminal n'est pas sécurisé, vous vous trouverez à créer une faille majeure, peu importe la qualité de votre réseau. Si vous revenez à l'analogie que j'ai évoquée plus tôt concernant le transfert de fonds — les véhicules blindés avec des agents armés et les deux boîtes en carton —, c'est ce que cela donne. Vous aurez peut-être sécurisé le maillon de la chaîne où se trouve l'information, mais le problème, ce sont les failles aux deux extrémités.

Peu importe qui est le fournisseur — et des fournisseurs de partout dans le monde entrent dans cette catégorie —, on constate que cela n'est pas intégré, lorsqu'on pense à l'Internet des choses de façon plus générale, parce que la sécurité est une considération secondaire et coûteuse. Ce que vous avez décrit est tout à fait exact. Peu importe le degré de sécurité du réseau, cela crée immédiatement une faille qui pourrait permettre à quelqu'un d'infiltrer le système et entrer dans votre réseau à domicile, par exemple.

L'exemple classique est celui qu'un de mes amis, qui a travaillé pour le gouvernement américain, avait l'habitude de raconter. Il attendait toujours que quelqu'un achète la fameuse imprimante sans fil, qui était formidable. Il n'était pas nécessaire de s'y connecter. C'était il y a 20 ans, lorsque ces choses sont arrivées sur le marché. Toutefois, l'appareil émettait immédiatement un signal qui vous permettait d'infiltrer le système. Son travail consistait à protéger le gouvernement américain contre ce genre de menace, mais c'est ainsi qu'il le décrivait.

● (1610)

M. Matthew Dubé: Depuis, il a été révélé que ces imprimantes posaient problème...

M. Satyamoorthy Kabilan: Exactement.

M. Matthew Dubé: ... par exemple pour un cabinet d'avocats qui imprime des documents confidentiels dans le cadre de procédures judiciaires, etc.

Je veux entendre parler de l'autre aspect, mais j'aimerais aussi m'attarder brièvement sur votre commentaire sur le caractère abordable. Autrement dit, beaucoup de ces technologies sont coûteuses, mais lorsque c'est la seule option... Disons que vous voulez acheter une sonnette pour votre maison. Vous ne trouverez pas de sonnette ordinaire sur le marché, mais seulement une sonnette équipée d'une caméra liée à une application sur votre téléphone. On cherchera à réduire le prix le plus possible, ce qui mènera inévitablement à des problèmes de sécurité, si j'ai bien compris votre point de vue. Cette interprétation est-elle juste?

M. Satyamoorthy Kabilan: Oui, particulièrement si le prix devient le seul critère. Toutefois, certaines industries ou certains marchés ont réussi à régler certains de ces problèmes.

Pensez aux vols de véhicules. Comme mon accent le révèle, je suis Britannique. Au Royaume-Uni, pour régler ce problème, le gouvernement a notamment publié un tableau des véhicules les plus fréquemment volés. Cela a immédiatement changé la donne. La valeur du véhicule n'avait aucune importance. Cela signifiait que votre prime d'assurance augmenterait et que vous étiez plus susceptible de perdre le véhicule. Il était possible d'établir un classement.

Même si nous sommes engagés dans une course vers le bas, et ce n'est pas une question de dépense, il suffit parfois d'informer les gens pour modifier les comportements et avoir une incidence sur les choix des consommateurs. Le prix est certes un facteur, mais il ne doit pas être le seul pour juger si vous obtenez une sécurité de qualité ou non.

M. Matthew Dubé: Très bien.

Allez-y, monsieur.

M. Christian Leuprecht: Nous savons comment améliorer la sécurité des appareils et des téléphones. Il s'agit de prendre les choses en main et d'en faire une exigence. Je peux vous décrire tous les aspects techniques sous-jacents.

Je m'étonne toujours de voir que dans cette industrie, lorsqu'on télécharge une application et qu'on lit la longue description que personne ne lit jamais, on se trouve essentiellement à consentir à utiliser un appareil défectueux en exonérant le fabricant de l'appareil de toute responsabilité. Pour quelle autre industrie le gouvernement a-t-il décidé de laisser le fabricant se décharger complètement de toute responsabilité pour tout défaut de son produit, même les défauts connus, ou encore pour son incapacité ou son indisposition à déployer des correctifs pour ces appareils parce que les enjeux de sécurité sont plus... Et aussi parce que l'application pourrait ne plus fonctionner sur divers appareils, par exemple?

Je pense que c'est tout simplement irresponsable. Je pense que le gouvernement se doit d'intervenir et affirmer qu'on ne peut fabriquer des technologies en sachant qu'elles présentent des failles de sécurité et des défauts, mais en rendant les consommateurs responsables de leur utilisation.

M. Matthew Dubé: Je voulais parler brièvement de l'aspect du projet de loi C-59 lié à la cyberguerre, par exemple, et des cybercapacités actives du CST. Je crois comprendre que les lois internationales ne sont pas vraiment claires à cet égard. Certains pourraient-ils faire valoir que lorsqu'on attaque la souveraineté d'un pays... La souveraineté s'étend-elle aux données? Je pense qu'il y a des incertitudes à ce sujet actuellement.

Il y a un risque d'escalade, mais cela va-t-il dans les deux sens? Malgré l'annonce d'aujourd'hui, par exemple, concernant la lutte contre l'ingérence étrangère, risque-t-on de se faire des ennemis si nos organismes prennent des mesures proactives ou préventives pour contrer une perturbation quelconque afin de nous protéger avant qu'un acteur d'un État étranger ait agi?

M. Christian Leuprecht: Je pense qu'il y a quatre catégories auxquelles il faut réfléchir. Cela nous ramène à la question que vous avez posée plus tôt. Je dirais que le niveau le plus faible est celui de la propagande, qui est comparable à faire des graffitis sur un mur, comme fermer un site Web ou quelque chose du genre. Les autres sont la subversion, le sabotage et les attaques. Seules les attaques exigent la force.

Je pense que ces quatre niveaux différents, les trois qui sont sous les attaques... En tant que gouvernement ou État, nous n'avons pas vraiment réfléchi aux conséquences, notamment la façon de riposter, qui est responsable d'appliquer les représailles et qui décide du moment, de l'endroit et des conditions. Qui participe aux représailles? Devons-nous autoriser le secteur privé à riposter? Est-ce uniquement la responsabilité de l'État? Nous pouvons aussi définir clairement, ou assez clairement, ce qui distingue la propagande, la subversion et le sabotage.

● (1615)

Le président: Nous devons en rester là, monsieur Dubé. Merci beaucoup.

Madame Sahota, vous avez sept minutes.

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

Ma première question est pour vous, monsieur Leuprecht. Vous préconisez la mise en oeuvre d'une stratégie de localisation de données souveraines, ce qui exigerait que toutes les données essentielles soient conservées uniquement au Canada. Pouvez-vous définir ce que vous entendez par « données essentielles » et expliquer comment cela fonctionnerait?

M. Christian Leuprecht: Quatre stratégies distinctes s'offrent aux pays pour la question des données.

Je pourrais donner des explications dans un mémoire distinct, car cela prendra beaucoup de temps.

Mme Ruby Sahota: D'accord.

M. Christian Leuprecht: Les pays ont seulement quatre stratégies possibles. Je pense que nous avons une véritable possibilité de le faire beaucoup plus facilement que d'autres pays, étant donné les avantages disproportionnés du Canada, notamment en raison du nombre de centres de données qu'il héberge déjà. Nous avons un climat froid et beaucoup d'électricité relativement abordable, de sorte que beaucoup d'acteurs privés établissent déjà des centres de données au Canada. Cela ne signifie pas seulement que ces données seront alors assujetties aux lois canadiennes, mais que nous pourrons aussi imposer des exigences à l'industrie. Cela pourrait ensuite faire l'objet de vérifications, puisque ces données demeureront au Canada plutôt que d'être réparties dans le monde entier.

Mme Ruby Sahota: Donc, vous dites que nous avons certainement la capacité de le faire.

M. Christian Leuprecht: Nous en avons la capacité; c'est seulement une question de... Voilà pourquoi je dis que des règlements et des incitatifs fiscaux, par exemple, peuvent être utiles.

Mme Ruby Sahota: J'ai lu des commentaires concernant nos investissements en intelligence artificielle et sur le fait que le Canada est en train de devenir une superpuissance dans ce domaine. Le gouvernement actuel a certainement pris diverses mesures pour investir davantage. Ces derniers mois, le ministre Bains a annoncé diverses initiatives pour appuyer les technologies de l'IA et plusieurs entreprises. Pouvez-vous préciser vos propos?

M. Christian Leuprecht: L'intelligence artificielle n'est pas une sorte de chapeau extraordinaire et magique duquel on peut sortir un lapin. Ce n'est que des mathématiques, des mathématiques avancées et sophistiquées et leurs applications. Ironiquement, bien que le gouvernement ait investi des sommes considérables pour diverses applications dans le domaine, il n'a pas fait un seul investissement dans la cybersécurité liée à ces applications.

Nous produisons beaucoup de personnel hautement qualifié, ou PHQ, comme on les appelle dans le milieu universitaire, mais il y a un écart phénoménal entre la demande de personnel qualifié en cybersécurité et notre capacité de créer des programmes pour former ces gens dans les universités. Nous faisons beaucoup de recherches intéressantes et de qualité, mais elles ne visent pas à créer du talent dans le domaine de la cybersécurité.

Je reviens encore une fois à l'Australie, qui compte maintenant neuf centres consacrés à la cybersécurité. Au Canada, nous n'en avons aucun, essentiellement. Nous avons le Réseau intégré sur la cybersécurité, le SERENE-RISC, que nous avons créé avec un collègue de la diversité de Montréal, mais c'est à peu près tout. Je pense que nous devons en faire beaucoup plus. On peut acheter toute la technologie et faire tous les investissements qu'on veut, mais si nos adversaires n'ont qu'à voler le produit de nos investissements en R-D, ce qui représente des milliards de dollars par année, quelle est l'utilité d'investir en R-D? En outre, pourquoi une entreprise étrangère investirait-elle en R-D au Canada, ou dans le domaine de l'intelligence artificielle, sachant qu'elle risquerait de perdre la propriété intellectuelle qu'elle a créée?

● (1620)

Mme Ruby Sahota: Très bien.

Nous avons accueilli un témoin lors de notre dernière réunion. Le ministère de la Sécurité publique travaille à la création d'un centre de cybersécurité. Au ministère de la Défense, le ministre Sajjan a inauguré le Centre canadien pour la cybersécurité en octobre dernier, je crois. Je me demandais si je pouvais avoir vos observations à ce sujet, monsieur Kabilan. Je crois que vous avez mentionné que cela suscite beaucoup votre intérêt.

M. Satyamoorthy Kabilan: Certainement. Le centre pour la cybersécurité auquel vous faites référence, je crois, est celui qui sera éventuellement créé par le CST. Je crois savoir que M. Scott Jones viendra en parler dans la prochaine partie de la réunion. Lorsque j'ai discuté de cela avec le gouvernement, j'ai établi un rapprochement avec ce que le Royaume-Uni a fait avec le National Cyber Security Centre. Je constate, du moins d'après les mémoires et les diverses discussions qui ont eu lieu au sujet de ce nouveau centre canadien, qu'on tente de refléter en grande partie les activités du National Cyber Security Centre du Royaume-Uni.

En guise de contexte, j'ai mentionné plus tôt que l'éducation et l'information sont deux éléments clés de la cybersécurité. Le NCSC du Royaume-Uni a d'excellents résultats à cet égard. Il contribue à réduire les problèmes de communication des informations entre les secteurs public et privé, tout en rendant cela accessible à tous. Il donne des conseils aux particuliers et aux petites et moyennes entreprises, et cela va jusqu'aux échelons supérieurs. Je crois comprendre que le nouveau centre du Canada aura certaines des mêmes fonctions. Si on y parvient, surtout en ce qui concerne l'éducation et la communication des renseignements, le centre deviendra alors un outil extrêmement précieux pour accroître nos capacités et notre résilience aux menaces pour la cybersécurité.

Le défi est toutefois lié à l'enjeu que M. Leuprecht vient tout juste de mentionner, soit la question des compétences. Au Royaume-Uni, le NCSC organise des concours. À titre d'exemple, il invite de jeunes femmes à faire de l'encodage, ce qui contribue à combler l'écart entre les sexes. Je ne suis pas certain qu'on y trouve des éléments pour régler certains des enjeux soulevés par M. Leuprecht, non seulement pour la communication des renseignements, mais aussi pour la création d'une plateforme favorisant l'acquisition des compétences requises pour appuyer le développement de la cybersécurité au Canada. Il sera intéressant de voir comment cela évoluera.

Mme Ruby Sahota: Me reste-t-il du temps?

Le président: Vous avez une minute.

Mme Ruby Sahota: Concernant le développement des compétences, nous avons aussi entendu, lors de la dernière réunion, que pour certains emplois, le gouvernement préfère embaucher des Canadiens déjà formés en raison du niveau de sécurité requis. Comment pourrons-nous créer, en collaboration avec nos partenaires universitaires, plus de centres comme ceux de l'Australie et suivre l'exemple du Royaume-Uni, que vous avez en haute estime? Comment pouvons-nous y parvenir sans que le gouvernement se charge de tout?

Le président: Brièvement, s'il vous plaît.

M. Satyamoorthy Kabilan: Cela comporte plusieurs défis, mais je pense que dans un premier temps — et M. Leuprecht pourrait donner une réponse plus exhaustive —, il faut veiller à avoir une chaîne fonctionnelle à tous les échelons, du système d'éducation jusqu'au marché du travail. Nous avons de très bons exemples au Canada, notamment ici, à Ottawa. C'est le Collège Algonquin, qui produit d'excellents diplômés en cybersécurité grâce à son programme. Beaucoup d'entre eux sont directement embauchés par CGI.

Le président: Merci.

M. Satyamoorthy Kabilan: Donc, nous produisons des personnes qualifiées qui trouvent des emplois. L'idée est d'harmoniser les choses.

Le président: Merci, madame Sahota.

Monsieur Paul-Hus, les cinq dernières minutes sont à vous.

[*Français*]

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

Monsieur Leuprecht, vous avez beaucoup parlé de Huawei et des dangers que cette technologie pose pour la sécurité du Canada en raison de plusieurs facteurs. Le document que vous nous avez remis contient beaucoup de recommandations importantes pour le Comité. Il y est question du Huawei Cyber Security Evaluation Centre.

Est-ce un regroupement d'entreprises? Qu'est-ce exactement que ce centre d'évaluation? Qui en fait partie?

M. Christian Leuprecht: Ce centre est un effort de collaboration entre le Government Communications Headquarters, ou GCHQ, au Royaume-Uni, et Huawei. Il vise à renforcer les liens avec Huawei et à donner l'occasion au GCHQ de vérifier la sécurité de l'équipement de cette entreprise. Malgré cet effort de collaboration, un rapport public, que je pourrai transmettre au Comité, en arrive quand même à la conclusion que les produits de Huawei sont suspects.

M. Pierre Paul-Hus: Après avoir travaillé avec cette compagnie, le résultat a finalement été celui-là.

Un débat a cours actuellement au Canada sur la question de savoir si l'on doit continuer de faire affaire avec Huawei. Selon certains groupes d'intérêt, il est très important pour le Canada d'adopter la technologie 5G, car c'est une technologie supérieure, mais de votre côté, vous avez dit dans votre déclaration d'ouverture que cette technologie pose un risque pour la sécurité nationale.

Nous ne sommes pas des experts, mais nous en entendons beaucoup parler. Vous êtes professeur au Collège militaire royal du Canada et d'autres experts partout dans le monde disent la même chose que vous. Pouvez-vous nous expliquer en termes simples pourquoi il faudrait se départir de la technologie de Huawei?

● (1625)

M. Christian Leuprecht: Par souci de clarté, je vais répondre en anglais.

[*Traduction*]

Je pense qu'il y a deux risques importants. Il y a d'abord la structure pyramidale des commutateurs réseau dans Internet. Plus on se trouve près du sommet de la pyramide, plus il est possible d'extraire des données d'Internet. Actuellement, nos adversaires tentent de se rendre aux échelons supérieurs d'Internet pour extraire le plus de données possible. Sinon, ils redirigent le flux. Si la technologie était intégrée dans l'ensemble d'Internet, vous n'auriez plus aucun effort à faire pour accéder à ces commutateurs. Vous pourriez extraire l'ensemble des données directement à partir des infrastructures.

L'autre problème, c'est que même si nous pourrions tester la technologie,

[*Français*]

— et cette technologie nous semble entièrement sûre — il faut pouvoir mettre celle-ci à jour. Voilà le problème.

[*Traduction*]

Le fabricant ou un gouvernement adverse peuvent toujours exploiter cette technologie et, en utilisant le processus de mise à jour, y installer des vulnérabilités. Comme pour tout ce qui fait partie de la vie, c'est une police d'assurance que nous contractons.

Regardez le rapport publié par la commission du Congrès sur la défense commune, coprésidée par l'ambassadeur Edelman. Dans ce rapport, que vous pouvez télécharger sur le site de l'United States Institute of Peace, la commission conclut que si les États-Unis entraient aujourd'hui en guerre avec la Russie, la Chine ou les deux, les États-Unis en ressortiraient probablement perdants. Pourquoi? Parce que cette guerre commencerait par une attaque massive sur les points vulnérables de l'infrastructure critique du réseau national, de façon générale, et je ne fais pas seulement référence à l'électricité. Voilà qui créerait des vulnérabilités, un chaos et une instabilité tels que les États-Unis seraient incapables de réagir. Ce rapport a certainement permis aux États-Unis de prendre conscience de la situation. Des pays comme la Chine se réservent le privilège de la première frappe quand il est question du cyberespace. Cela s'inscrit dans la doctrine chinoise.

À quel degré de vulnérabilité et de risque notre pays est-il prêt à s'exposer? Si nous nous retrouvons dans une telle situation, alors il sera un peu trop tard pour faire machine arrière.

M. Pierre Paul-Hus: Merci.

Le président: Merci.

Je déteste mettre fin à cet échange, qui a été absolument fascinant. Je suis certain que nous pourrions continuer ainsi pendant longtemps.

En ce qui concerne le dernier point, permettez-moi de poser une brève question. Serait-il possible qu'une cyberattaque provoque une réaction de l'OTAN en vertu de l'article 5?

M. Satyamoorthy Kabilan: Cette possibilité fait l'objet d'un débat enflammé. L'Union européenne a tenu une session à ce sujet en 2017. La réponse, c'est qu'on ne le sait pas.

Le président: Voilà qui est réconfortant.

Sur ce, je pense que je vais devoir, à mon grand regret, mettre fin à la présente partie de la séance.

Nous suspendons la séance afin d'accueillir notre prochain groupe de témoins.

Au nom du Comité, je remercie de nouveau nos deux témoins.

● (1625)

(Pause)

● (1630)

Le président: Nous recevons de nouveau Scott Jones et Eric Belzile.

Monsieur Jones, votre dernière comparution a été fort populaire, et je prévois que celle-ci le sera également. Nous allons maintenant écouter votre exposé. Vous disposez de 10 minutes à vous deux.

Merci.

M. Scott Jones (dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Bonjour, monsieur le président et distingués membres du Comité.

Je suis enchanté de témoigner de nouveau, je pense. Je viens de traverser une bousculade: j'ai donc eu un aperçu de ce que vous vivez.

Comme vous le savez, je m'appelle Scott Jones et je suis à la tête du Centre canadien pour la cybersécurité; ma situation a donc changé depuis la dernière fois où j'ai comparu. Le lancement du Centre était alors imminent. Je suis accompagné aujourd'hui par Eric Belzile, directeur général de notre équipe de gestion des incidents et d'atténuation des menaces.

Lancé le 1er octobre 2018, le Centre canadien pour la cybersécurité est un nouvel organisme, qui jouit toutefois d'une riche histoire. Il réunit sous un même toit des experts de la cybersécurité de toutes les parties du gouvernement fédéral.

[*Français*]

En phase avec la Stratégie nationale de cybersécurité, le lancement du Centre canadien pour la cybersécurité marque un tournant vers une approche plus unifiée de la cybersécurité au Canada. Le Centre canadien pour la cybersécurité poursuit les efforts déployés par le Centre de la sécurité des télécommunications, ou CST, pour réaliser son mandat en matière de sécurité des TI. Il prodigue des conseils, des avis et des services aux ministères et organismes fédéraux concernant les systèmes d'importance pour le gouvernement du Canada.

Le Centre canadien pour la cybersécurité s'est donné pour mission de garantir la sécurité des Canadiens en fournissant de l'information pertinente sur les enjeux touchant à la cybersécurité. Suivant l'intégration de ressources provenant de Sécurité publique Canada et de Services partagés Canada, le Centre canadien pour la cybersécurité poursuivra les efforts déployés par ces ministères pour favoriser la collaboration avec les autres ordres de gouvernement, le secteur privé et le milieu universitaire.

[*Traduction*]

Nos partenariats avec l'industrie sont essentiels. Les gouvernements a l'échelle internationale n'arrivent pas à suivre la cadence rapide du secteur privé en matière d'innovation. C'est pourquoi le gouvernement du Canada ne peut renforcer la cybersécurité sans collaborer avec le secteur privé.

Cela m'amène au sujet qui nous intéresse aujourd'hui: la cybersécurité dans le secteur financier comme enjeu de sécurité économique nationale.

Les effets d'une perturbation substantielle sur le secteur financier pourraient avoir des répercussions qui se réverbéreraient sur l'ensemble de l'économie canadienne. Les effets d'une cyberperturbation peuvent être immédiats et entraîner des pertes financières. lls peuvent également se faire sentir à moyen ou long terme et miner lentement la confiance des consommateurs. Le risque de cybercompromission augmente à mesure que le secteur financier continue sa transition vers des services numériques et connecte plus de dispositifs à Internet.

Cette transformation a néanmoins le potentiel de créer d'immenses possibilités de croissance. En ne tirant pas parti des innovations de la technologie numérique, le Canada serait exclu de l'économie mondiale. Le retranchement n'est pas une option.

● (1635)

[*Français*]

Pour ce faire, le Canada doit demeurer vigilant et prendre les mesures nécessaires pour prévenir les cybermenaces contre le secteur financier et l'ensemble des secteurs de l'industrie canadienne, détecter ces cybermenaces et intervenir.

C'est pourquoi le Centre canadien pour la cybersécurité était fier de publier la première évaluation canadienne des cybermenaces nationales en décembre 2018. Cette évaluation donne un aperçu du contexte des cybermenaces au Canada. Elle vise à s'assurer que les Canadiens sont bien informés des cybermenaces qui pèsent sur le pays alors que les auteurs de cybermenaces cherchent de nouvelles façons d'utiliser le Web et les dispositifs connectés à Internet à des fins malveillantes. L'évaluation comprend plusieurs conclusions clés sur l'environnement des cybermenaces actuelles et traite notamment des cybermenaces visant le secteur financier du Canada.

[*Traduction*]

Selon nos observations, la cybercriminalité est la cybermenace la plus susceptible de toucher les Canadiens et les entreprises canadiennes en 2019. Même si toutes les entreprises sont à risque, le secteur financier est une cible fréquente des cybercriminels.

Dans le cadre d'une étude de l'impact de la cybercriminalité sur les entreprises canadiennes, les chercheurs de Statistique Canada ont découvert que près de la moitié des organisations canadiennes du secteur bancaire avaient été touchées par des cyberincidents de sécurité en 2017. Les cybercriminels peuvent cibler le secteur financier, comme les institutions bancaires, dans le but de tirer un gain financier immédiat. lls peuvent également cibler ce secteur pour exploiter les données des clients et des partenaires, ou pour obtenir des renseignements exclusifs. L'information volée fait souvent l'objet d'une demande de rançon. Elle peut aussi être vendue ou utilisée afin de tirer un avantage concurrentiel.

Ces incidents peuvent causer d'importantes pertes financières, porter atteinte à la réputation, entraîner une perte de productivité, mener au vol de propriété intellectuelle, donner lieu à des perturbations et entraîner des dépenses relatives à la récupération.

[*Français*]

Les auteurs de menaces plus sophistiquées, y compris les États-nations, pourraient aussi cibler le secteur financier, puisqu'il s'agit de l'un des secteurs d'infrastructures essentielles du Canada. Cependant, on considère pour le moment qu'il y a peu de risques que des auteurs de cybermenaces parrainés par des États cherchent à perturber volontairement les infrastructures essentielles du Canada. Bien que le secteur financier soit une cible intéressante pour les auteurs de cybermenaces, c'est aussi une cible relativement difficile.

[*Traduction*]

De fait, dans son sondage de 2017, Statistique Canada a révélé que les deux tiers des institutions bancaires avaient mis en place une politique pour gérer ou signaler les cyberincidents de sécurité. Le Centre canadien pour la cybersécurité joue également un rôle important en aidant à protéger les systèmes importants pour le gouvernement du Canada.

II mène des initiatives constantes et sur mesure avec ses partenaires du secteur financier du Canada. Par exemple, le Centre pour la cybersécurité transmet régulièrement des rapports sur les indicateurs de compromission aux fournisseurs d'infrastructures essentielles, y compris aux partenaires du secteur financier, dans le but de promouvoir l'intégration de la technologie de cyberdéfense.

Quand on examine ce que les Canadiens et les entreprises peuvent faire pour se protéger des cybermenaces, il est important de se rappeler que l'adoption des pratiques les plus élémentaires en matière de cybersécurité peut contribuer à contrer les auteurs de cybermenace. La cybersécurité est l'affaire de tous.

Merci. C'est avec plaisir que je répondrai à vos questions.

Le président: Merci, monsieur Jones.

Madame Damoff, vous avez la parole pour sept minutes.

Mme Pam Damoff (Oakville-Nord—Burlington, Lib.): Merci, monsieur le président.

Je vous remercie de votre exposé.

Je veux d'abord revenir sur une observation que vous avez faite, selon laquelle les deux tiers des institutions se sont dotées d'une politique pour signaler les incidents de cybersécurité. Est-ce bien ce que vous avez dit? Qu'en est-il de l'autre tiers?

M. Scott Jones: Le sondage de Statistique Canada a révélé que les deux tiers des organisations avaient instauré une politique indiquant comment faire des signalements, et je présume qu'elles ont été adoptées parce que les conseils d'administration posent plus de questions sur la cybersécurité et le cyberrisque auxquels ces organisations sont confrontées.

Mme Pam Damoff: Les institutions financières en particulier devraient-elles être obligées de signaler les incidents?

M. Scott Jones: Nous nous employons à établir la relation pour qu'elles se sentent à l'aise de nous approcher rapidement quand elles ne sont même pas encore sûres qu'un incident a eu lieu afin que nous puissions commencer à travailler ensemble dans le but de réagir. Nous tentons de les encourager à signaler précocement les incidents pour que nous puissions agir rapidement dans l'espoir de les aider avant que les données ne soient compromises.

En outre, plus elles signalent les incidents rapidement et plus les renseignements qu'elles nous transmettent sont pertinents, plus nous pouvons communiquer l'information à l'ensemble du secteur, et c'est vraiment important pour nous sur les plans de la gestion des incidents et de l'atténuation des menaces.

Mme Pam Damoff: À titre de membre du Comité, j'ai rencontré un certain nombre d'entreprises de cybersécurité qui conseillent des entreprises, des gouvernements et des institutions financières, et elles ont notamment parlé du nombre de sortes de comptes. Certains comptes restent ouverts quand les gens quittent l'entreprise. Il existe des comptes superflus créés par des gens lorsqu'ils entrent au service d'une organisation, mais qui restent inutilisés pendant des années. Les entreprises ne font même pas le bilan de leurs comptes. Certains comptes s'accompagnent probablement de plus de pouvoirs qu'ils ne le devraient. Les gens partent ou changent d'emploi.

Comment pouvons-nous enseigner aux entreprises à faire attention à la situation, puisqu'il semble qu'on puisse très aisément éliminer un grand nombre des vulnérabilités auxquelles elles s'exposent?

● (1640)

M. Scott Jones: Juste pour que je comprenne bien, parlez-vous des comptes informatiques que les gens utilisent pour se brancher au système, et non des comptes bancaires abandonnés?

Mme Pam Damoff: C'est cela: ce sont les comptes créés par de vrais employés qui ont peut-être accès à des renseignements secrets de très haut niveau, puis qui changent d'emploi ou de ministère alors que leur code d'accès demeure le même.

M. Scott Jones: C'est un point absolument essentiel. Parmi les 10 mesures prioritaires figurent la révocation des justificatifs d'identité au départ des employés. Il faut également veiller à ce que les pouvoirs correspondent aux besoins du poste quand le titulaire se branche au système.

Par exemple, quand j'accède à un système du Centre de la sécurité des télécommunications, je ne bénéficie d'aucun privilège administratif. Je ne peux même pas modifier l'heure parce que je n'ai pas à le faire dans le cadre de mon travail; nos administrateurs de système s'en occupent. Je ne peux pas installer de logiciels; nos administrateurs de système s'en chargent après avoir procédé aux essais appropriés. Il importe vraiment de gérer les justificatifs d'identité et d'en limiter le nombre le plus possible; quant aux employés dotés de privilèges supérieurs, ils devraient prendre d'autres mesures de protection.

Par exemple, si on est administrateur de système, il faut contrôler l'accès, ce que les employés peuvent faire, comment ils peuvent le faire et ce qu'ils peuvent accomplir avec leur compte. Nous donnons les exemples faciles suivants: ne lisez pas vos courriels et ne surfez pas sur Internet à partir de votre compte administrateur, car vous avez à ce moment-là des privilèges supérieurs. De simples précautions peuvent avoir une incidence considérable sur la cybersécurité.

Mme Pam Damoff: À qui prodiguez-vous ces conseils?

M. Scott Jones: Cela fait partie de nos conseils publics. Nous disons que cela fait partie de nos 10 conseils les plus importants. Nous avons certainement prodigué ces conseils au gouvernement au chapitre de la gestion des privilèges administratifs. Ce sont également des pratiques standards en matière de cybersécurité que l'on entend du SANS Institute ou d'autres organisations qui font la promotion d'une saine hygiène de cybersécurité.

Nous en parlons certainement. Le simple fait de mettre en application les 10, voire les quatre premiers conseils a un effet remarquable sur l'amélioration de la cybersécurité.

Mme Pam Damoff: Les organisations vous écoutent-elles?

M. Scott Jones: Dans bien des cas, elles le font certainement. Chose certaine, nous avons observé un changement considérable au sein du gouvernement fédéral, probablement depuis cinq ou six ans, car nous avons tenté de montrer les conséquences auxquelles on s'expose si on ne suit pas les 10 principaux conseils. Je pense en outre que les entreprises, les conseils d'administration et d'autres entités sont à l'affût de normes leur permettant d'évaluer leurs efforts en matière de cybersécurité. Ils utilisent donc nos 10 principaux conseils pour voir comment ils s'en tirent, examinant ces mesures une à une.

Mme Pam Damoff: D'accord. Merci de ces précisions.

Avez-vous une idée de ce que la cybercriminalité coûte à l'économie canadienne? Est-ce que quelqu'un s'est penché sur la question?

M. Scott Jones: Le sondage de Statistique Canada est probablement la meilleure enquête réalisée à ce sujet à l'heure actuelle. Le problème, c'est que la cybercriminalité est un des crimes les moins signalés; il est donc difficile de dire ce qu'il en est. Si quelqu'un se fait arnaquer en cliquant sur un lien ou payant pour quelque chose, le signalement ou le dépôt d'une plainte s'accompagnent de préjugés, et les gens ne savent où aller.

Je ne connais pas les chiffres. Je pense que le sondage de Statistique Canada est probablement ce qui se rapproche le plus de ce que vous cherchez. En collaboration avec l'Unité nationale de coordination de la lutte contre la cybercriminalité de la GRC, nouvellement mise sur pied, nous tentons d'encourager les gens à signaler les crimes à la police pour que cette dernière puisse intervenir. Nous incitons aussi les intervenants à commencer à recueillir des statistiques à ce sujet pour que nous puissions évaluer les répercussions du problème sur l'économie canadienne.

Mme Pam Damoff: Un des témoins précédents a proposé de réunir les données à un seul endroit au Canada. Voyez-vous un avantage à agir ainsi? J'ignore si vous avez entendu ou non ce témoin.

M. Scott Jones: De quel genre de données s'agit-il? Je ne l'ai pas entendu.

Mme Pam Damoff: Je pense qu'il parlait de... je ne sais pas. Il ne me reste qu'une minute.

Un de mes électeurs a communiqué avec moi pour me poser une question, que j'ai soumise à la GRC: si une banque canadienne faisait appel à une entreprise étrangère et qu'un incident de sécurité survenait, serait-il possible d'appliquer des sanctions? J'ai obtenu une réponse assez vague; ce ne serait probablement pas possible, mais peut-être pourrait-on le faire. Est-ce que le fait de conserver les données au Canada serait d'une aide quelconque à cet égard?

● (1645)

M. Scott Jones: Je pense qu'il est primordial d'étudier les risques dans la chaîne d'approvisionnement; c'est d'ailleurs un des points que nous avons soulignés dans le cadre de l'évaluation nationale de la cybermenace. Les entreprises doivent porter une attention particulière à la chaîne d'approvisionnement et aux entreprises avec lesquelles elles font affaire, et inclure de solides dispositions de cybersécurité dans leurs contrats pour pouvoir tenir les entreprises responsables et les obliger à leur signaler, comme il se doit, les atteintes à la sécurité et les autres incidents.

Nous affirmons toujours que le prix le plus bas n'est habituellement pas compatible avec la cybersécurité. Les entreprises doivent trouver la meilleure entreprise de cybersécurité, celle qui sera capable de protéger leurs données également.

Le président: Merci, madame Damoff.

[*Français*]

Monsieur Paul-Hus, vous avez sept minutes.

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

Bonjour, monsieur Jones. Nous nous sommes vus en septembre dernier. Tout le monde veut savoir ce que nous allons vous demander concernant vos impressions sur Huawei.

Avant de continuer, j'aimerais dire que, depuis 5 ou 6 mois, j'ai compris certaines choses et j'aimerais vérifier votre mandat. Depuis un certain temps, je comprends de nos conversations que votre organisme est davantage un centre d'information et qu'il n'est pas impliqué dans les tactiques et la stratégie. Je crois que votre rôle consiste plus à informer les Canadiens. Est-ce bien le cas?

M. Scott Jones: Je vous remercie de votre question.

[*Traduction*]

Je dirais d'abord que notre mandat consiste à conseiller et à guider les Canadiens, mais tout a commencé par le gouvernement fédéral. Nous fournissons donc des conseils pratiques en matière de sécurité. Nous sommes également mandatés pour veiller à ce que les Canadiens aient l'information dont ils ont besoin pour prendre eux-mêmes des mesures pour se protéger.

Depuis la création du centre pour la cybersécurité, notre mandat s'est élargi avec la fusion du Centre canadien de réponse aux incidents cybernétiques, qui jouait le rôle de l'équipe nationale d'intervention en cas d'incidents en informatique.

Notre objectif vise non seulement à fournir des conseils et de l'orientation, mais aussi à proposer des mesures pratiques que les gens peuvent appliquer.

[*Français*]

M. Pierre Paul-Hus: Actuellement, il y a tout un débat sur la compagnie Huawei. Les pro-Huawei appuient la technologie 5G. Ceux qui s'opposent à la compagnie, par contre, font valoir l'évidence des questions de sécurité nationale. Nos alliés du Groupe des cinq nous disent de ne pas toucher à cette compagnie.

Nous aimerions savoir si c'est vous qui donnerez l'avis définitif au premier ministre. Qui décide de ce qu'on doit faire au Canada avec cette compagnie?

[*Traduction*]

M. Scott Jones: À titre de membre de l'équipe et du gouvernement, notre rôle consiste à prodiguer des conseils en matière de cybersécurité. Une décision comme celle-là comporte d'autres facettes. Le moment était... le ministre Goodale a fait une sortie et a abordé la question hier. Je pense qu'il nous incombe avant tout de fournir les conseils que nous devons donner quant à la prochaine décision que prendra le gouvernement. À l'heure actuelle, nous appliquons la décision stratégique prise en 2013.

[*Français*]

M. Pierre Paul-Hus: Que répondez-vous à ceux qui disent que nous sommes en retard par rapport aux autres pays et que nous nous traînons les pieds? Vous avez entendu le témoignage de M. Leuprecht, professeur au Collège militaire royal du Canada, qui était très clair à ce sujet. Il n'est pas le seul, car des experts de partout semblent dire que c'est assez évident.

Comme je le disais, d'un point de vue technique, il nous est difficile de trancher cette question. Nous devons nous fier à des gens comme vous pour prendre une décision stratégique pour le Canada. Avez-vous assez d'information aujourd'hui? En septembre, vous disiez que vous étiez en mesure d'assurer la protection des Canadiens. Est-ce encore le cas aujourd'hui, le 30 janvier 2019?

[*Traduction*]

M. Scott Jones: Notre rôle consiste à fournir des informations et des conseils au gouvernement pour que ce dernier puisse prendre une décision éclairée. Par ailleurs, nous continuons de collaborer avec l'industrie afin de voir comment nous pouvons protéger les infrastructures du Canada aujourd'hui et demain, et prévenir les cybermenaces.

[*Français*]

M. Pierre Paul-Hus: Donc, pour l'instant, nous ne savons pas encore si le Canada peut faire confiance à Huawei.

Laissons maintenant cette compagnie de côté et passons au domaine financier, avec les banques. M. Leuprecht nous a également fourni des informations intéressantes concernant les transactions financières, qui peuvent provenir de partout puisqu'Internet est mondial.

Selon le CRTC, il est impossible de diffuser du contenu canadien à l'étranger. Quand on va aux États-Unis ou ailleurs, par exemple, on ne peut pas écouter TVA, car ce réseau n'est pas accessible. Il y a donc certaines barrières qui existent au niveau des communications. Pourquoi ces barrières n'existeraient-elles pas aussi pour les banques? Êtes-vous au courant de cela? Savez-vous pourquoi, d'un point de vue technique, il est possible d'avoir des barrières pour une activité, mais pas pour une autre? Je ne sais pas si vous avez le mandat de répondre à cela.

● (1650)

[*Traduction*]

M. Scott Jones: Je ne suis pas certain de bien comprendre la question. Je pense qu'essentiellement, quand on voyage, tout dépend si on peut accéder aux services, par exemple, en se connectant à sa banque. À moins que ce soit...

M. Pierre Paul-Hus: M. Leuprecht vient de nous dire qu'Internet est un espace ouvert, mais quand on voyage, on ne peut pas regarder la télévision canadienne. Pourquoi alors ne pourrait-on pas bloquer la communication entre les banques ou d'autres entités?

M. Scott Jones: Je pense que cela touche au coeur du problème. Cela sort légèrement de notre mandat, mais fondamentalement, le Canada a opté pour un Internet très ouvert où très peu de choses sont bloquées. En dehors du fait que les fournisseurs de services empêchent les gens de regarder NBC, par exemple, parce que les stations canadiennes possèdent des droits à cet égard, Internet tend à être très ouvert au Canada. Ce ne sont toutefois pas tous les pays qui adoptent la même approche, et certains choisissent de filtrer Internet et le contenu. Il s'agit simplement d'une décision que le Canada a prise.

Le président: Il vous reste une minute et demie.

[*Français*]

M. Pierre Paul-Hus: En terminant, j'aimerais parler de la Chine. C'est délicat actuellement. Nous sommes conscients qu'en diplomatie, il faut être prudent, mais du point de vue de la sécurité nationale, il faut savoir que la Chine a souvent des intentions malveillantes envers différents pays, dont le Canada.

Considérez-vous que la Chine est une menace potentielle pour la sécurité du Canada?

[*Traduction*]

M. Scott Jones: Pour notre part, nous indiquons dans l'évaluation de la cybermenace nationale qu'il faut se montrer vigilant à l'égard de chaque État-nation et que chaque État-nation a certainement des cybertechniques à sa disposition. Certains sont plus agressifs que d'autres.

Par le passé, le Centre de la sécurité des télécommunications s'est certainement vu demander d'attribuer des cyberactivités malveillantes à certains pays, et c'est une tâche que nous continuerons d'accomplir, conformément à la politique globale du gouvernement. C'est une situation que nous surveillons continuellement, mais à mon avis, nous ne nous défendons pas contre un seul pays, mais contre tout le monde. Si nous adoptons une approche pour chaque pays, nous mettrions l'accent sur...

[*Français*]

M. Pierre Paul-Hus: D'accord, mais pensez-vous que le Canada devrait avoir peur de la Chine?

[*Traduction*]

M. Scott Jones: Je pense que nous devrions nous montrer vigilants à l'égard de tous ceux qui ne partagent pas nos valeurs.

[*Français*]

M. Pierre Paul-Hus: Je vous remercie.

Le président: Merci, monsieur Paul-Hus.

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

M. Matthew Dubé: Merci, monsieur le président.

Messieurs Jones et Belzile, je vous remercie d'être ici.

Mme Damoff vous a posé des questions sur la politique des banques en matière de signalement des brèches ou des situations problématiques. De mon côté, je veux faire suite aux questions que j'ai posées lundi aux représentants de la GRC.

Ce n'est pas clair. Une mise à jour de la loi exige maintenant des entreprises qu'elles signalent les fuites d'information au commissaire à la protection de la vie privée. Ces représentants nous ont dit que le nouveau centre policier — j'ai moi aussi oublié les noms et les acronymes — n'a pas la même obligation et qu'ils tentent de travailler avec ces organisations. Y a-t-il un dédoublement des efforts? Si une banque vous rapporte un incident qu'elle considère comme suspect ou inquiétant, travaillez-vous par la suite avec la police pour qu'elle puisse entreprendre des démarches de ce côté?

[*Traduction*]

M. Scott Jones: Je pense que quelques éléments entrent en jeu ici. Je laisserai peut-être Eric traiter de certains points précis. Sachez tout d'abord que dans le cadre de notre collaboration avec la GRC, nous voulons nous assurer que nous ne nuisons jamais aux efforts que la police déploie pour mener des enquêtes et poursuivre les cybercriminels. Nous veillons donc à coordonner nos démarches.

Notre rôle auprès des banques et, de façon générale, des institutions financières consiste à déterminer comment nous pouvons lutter contre la cyberactivité de manière plus proactive. Nous voulons renforcer nos défenses et l'échange d'information pour pouvoir intervenir et protéger les données. Quand un incident survient, cependant, nous appliquons les protocoles de manière légèrement différente.

Je laisserai peut-être Eric...

[*Français*]

M. Eric Belzile (directeur général, Gestion des incidents et atténuation des menaces, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Voici ce que j'ajouterais à ce sujet.

Lorsqu'un incident nous est rapporté, nous travaillons en étroite collaboration avec les autres organismes. Un triage se fait, car il y a d'autres organismes que cela concerne, à savoir la GRC et le SCRS. Nous déterminons ensemble qui gérera l'incident. Nous collaborons afin que chaque organisme puisse exercer son mandat et ses fonctions, et nous nous assurons de ne pas empiéter sur le mandat des autres organismes. Cette collaboration est immédiate.

C'est ainsi que nous procédons depuis plusieurs années. Le fait de consolider le Centre canadien pour la cybersécurité et la mise sur pied du nouveau centre de cybercriminalité de la GRC nous aideront aussi à améliorer cette collaboration.

● (1655)

M. Matthew Dubé: D'accord.

Je sais qu'il peut être difficile de se prononcer sur des situations hypothétiques. Supposons qu'une entreprise vous signale une situation suspecte, mais qu'elle ne l'ait pas rapportée à la police pour toutes sortes de raisons, que ce soit lié aux relations publiques, à des conséquences financières ou à autre chose. S'il y a assez de preuves pour que vous soupçonniez qu'un geste criminel a été commis, transmettez-vous le cas à la police pour qu'elle entame une enquête officielle?

M. Eric Belzile: Généralement, nous consultons la victime pour déterminer la meilleure approche à adopter. Souvent, s'il y a des indices probants de cybercriminalité, nous conseillons aux victimes de rapporter l'incident à la police, de façon à ce que celle-ci soit au courant et qu'elle puisse exercer son mandat.

M. Matthew Dubé: D'accord.

Il a été question du rapport sur les menaces qui a été déposé. Dans votre présentation, vous avez dit ceci:

> Cependant, on considère pour le moment qu'il y a peu de risques que des auteurs de cybermenaces parrainés par des États cherchent à perturber volontairement les infrastructures essentielles du Canada.

Est-ce que le risque est peu élevé uniquement dans le secteur financier ou l'est-il également dans tous les secteurs d'infrastructures essentielles?

[*Traduction*]

M. Scott Jones: Je pense que le point principal auquel nous faisons référence au sujet des États-nations, c'est que ces derniers ont des objectifs précis. En l'absence de conflit international majeur, nous considérons que la menace de perturbation quant aux infrastructures canadiennes est très faible, mais certains États-nations s'intéressent aux informations privées et à d'autres renseignements. Certains d'entre eux recourent certainement à des outils de cybercriminalité pour générer des revenus, notamment pour contourner des sanctions et diverses mesures.

Nous devons toujours être vigilants. Ce qui importe pour nous, c'est de voir avec quelle rapidité nous pouvons obtenir et communiquer l'information pour pouvoir prendre des mesures contre ces cyberactivités malveillantes. Pour l'heure, toutefois, nous jugeons très faible la menace de perturbation, puisqu'il n'y a pas de conflit majeur. Si une perturbation survient, ce serait probablement un effet secondaire d'un outil de cybercriminalité, comme un rançongiciel, par exemple.

M. Matthew Dubé: J'aimerais aussi aborder un point ayant un lien avec l'annonce faite aujourd'hui sur les élections. Je sais que nous étudions le secteur financier, mais je m'interroge au sujet d'un autre point. Dans l'annonce qui a été faite, le SCRS semble prendre la direction des opérations avec le Centre de la sécurité des télécommunications, utilisant son mandat d'assistance pour fournir du soutien à cet égard. Le SCRS cherche à réduire les menaces, une question qui fait certainement l'objet d'un débat que nous continuerons d'avoir, mais pas nécessairement à ce moment-ci. Étant donné que nous étudions le secteur financier, je me demande...

Les élections ont lieu à un moment précis dans le temps. Or, les temps changent certainement, comme nous le savons tous. Cela étant dit, existe-t-il une tendance à cet égard? Est-il déjà arrivé que le SCRS prenne les devants et s'intéresse aux acteurs qui pourraient poser une menace à la cybersécurité, ou s'agit-il d'une mesure ponctuelle pour ces élections-là? Par exemple, si un effort concerté est déployé dans le secteur financier, sur lequel porte notre étude, ou dans un autre secteur, est-ce une mesure qui sera récurrente ou concerne-t-elle précisément les élections?

M. Scott Jones: Je pense que l'objectif consiste ici à tirer parti de l'approche d'Équipe Canada et à exercer les pouvoirs appropriés. À l'évidence, il incombe au Parlement de débattre de ces pouvoirs et de les attribuer aux organisations. Je ne me prononcerai donc pas sur la question.

Pour nous, l'important consiste à exercer le pouvoir approprié. Le Centre de la sécurité des télécommunications et le Centre canadien pour la cybersécurité ne ciblent pas les Canadiens dans le cadre de leurs activités; ainsi, si la menace émane du Canada, la GRC ou le SCRS sont mieux placés pour réagir.

M. Matthew Dubé: Très brièvement, dans les 15 secondes qu'il me reste, est-ce que cette structure et l'organisme responsable seraient différents si le projet de loi C-59 recevait la sanction royale aujourd'hui?

M. Scott Jones: Si la menace vient du Canada, cela ne change pas. La disposition stipule toujours que le Centre de la sécurité des télécommunications ne peut cibler de Canadiens dans le cadre de ses activités.

M. Matthew Dubé: Mais dans le cas présent, le SCRS s'intéresse à des acteurs étrangers. C'est ce que je comprends de l'annonce faite aujourd'hui. Est-ce exact?

M. Scott Jones: Nous utilisons l'outil qui convient au moment des faits. Si le projet de loi C-59 est adopté par le Sénat, reçoit la sanction royale et entre en vigueur, alors nous réévaluerions la manière dont nous abordons ces problèmes, au regard des nouvelles...

Le président: Merci, monsieur Dubé. Nous allons devoir nous en tenir là.

Monsieur Picard, vous disposez de sept minutes.

[*Français*]

M. Michel Picard (Montarville, Lib.): Je vous remercie, monsieur le président.

Messieurs, j'imagine que, lorsque des gens rapportent ou signalent des fraudes ou des attaques cybernétiques, ces informations confidentielles ne sont pas rendues publiques. Est-ce exact?

● (1700)

[*Traduction*]

M. Scott Jones: Oui. Comme nous l'avons indiqué à maintes reprises, nous avons tendance à pénaliser de nouveau les victimes de la cybercriminalité, les punissant en rendant l'affaire publique. Nous nous attendons à ce qu'elles assument leurs responsabilités et réagissent. Notre objectif consiste à les aider à se rétablir et à se défendre, puis à publier l'information à grande échelle.

[*Français*]

M. Michel Picard: D'après ce que je comprends, le fait que des compagnies rapportent un crime de nature cybernétique ne veut pas nécessairement dire qu'elles vont accroître leurs systèmes de sécurité ou de protection. Elles ne font que rapporter l'incident.

[*Traduction*]

M. Scott Jones: En effet. J'ai toutefois constaté que dans les entreprises et les conseils d'administration de grande envergure, le cyberrisque est en train de devenir le principal sujet de conversation. Je pense que c'est une tendance que nous commençons à observer. Les cyberrisques menacent non seulement leur réputation, mais aussi la poursuite de leurs activités; les organisations prennent donc la chose au sérieux.

M. Michel Picard: Examinons le risque du point de vue de l'entreprise et du président du conseil d'administration. Quand on se penche sur les dépenses relatives à la sécurité, il arrive un moment où on évalue les dépenses afférentes à la sécurité des systèmes et aux pertes causées par le risque relatif à la réputation, comparant le tout au montant à payer pour rembourser les victimes. Quand le remboursement s'avère moins élevé, on oublie la sécurité et on opte pour la voie la moins chère.

Discutez-vous de cette facette de la question avec les entreprises? Réalisent-elles que ce n'est pas qu'une question de perte financière, mais aussi de perte d'information?

M. Scott Jones: Lors de nos discussions et des échanges que j'ai eus avec de hauts dirigeants et des conseils d'administration d'entreprises, il est beaucoup question du tort causé à la réputation, dont il est difficile de calculer le coût. Nous avons certainement vu que les atteintes importantes à la sécurité survenues aux États-Unis ont mis à mal la réputation de certaines entreprises. Je pense que le problème principal pour nous, c'est que l'équipement que nous achetons n'est pas sécurisé par défaut; vous avez raison. L'équipement est de piètre facture, et cela va de mal en pis avec l'Internet des objets. Nous devons changer cette dynamique, et nous encourageons l'industrie à réclamer l'inclusion de dispositifs de sécurité dans l'équipement. Les entreprises ne devraient pas payer de suppléments à cette fin. Certains dispositifs de sécurité devraient être inclus dans n'importe quel équipement.

[*Français*]

M. Michel Picard: La plupart de nos discussions portent sur la technologie visant à accroître notre sécurité et à protéger notre information. Elles concernent l'outil comme tel. Un des problèmes qu'il est impossible de contourner — et vous me corrigerez si je me trompe — est le facteur humain. C'est le seul risque incontrôlable auquel fait face toute entreprise.

Est-ce à dire que, malgré l'importante technologie qui n'existe même pas encore, mais qui pourra être développée, il sera impossible de se protéger en raison du facteur humain?

[*Traduction*]

M. Scott Jones: Quand on examine la situation, on voit que vous avez absolument raison. Le facteur humain fait partie de la cybersécurité. Nous tendons parfois à ne pas accorder la priorité à la sécurité de nos produits si cela en complique l'utilisation. Tout est une question de convivialité.

Je pense que c'est aussi une question d'éducation, mais on ne peut se fier à cela. Par exemple, certains outils de cybercriminalité et stratagèmes d'hameçonnage personnalisé sont extrêmement raffinés. Même moi, je pourrais commettre une erreur, et ces problèmes sont mon pain quotidien. On peut fonder des espoirs sur l'éducation, mais on doit se fier à d'autres mesures mises en place dans le cadre d'une approche en matière de sécurité, car on fait fausse route en se fiant à une personne et certainement en punissant une personne. Il est très facile de faire l'erreur de cliquer trop vite, d'autant plus que certains pièges sont extrêmement bien structurés.

[*Français*]

M. Michel Picard: Ce que j'avais en tête était davantage que la simple erreur d'inattention. On connaît le principe des attaques indirectes, dans les logiciels. Notre problème est le piratage psychologique. La personne se trouve alors volontairement dans le système.

Par exemple, lorsque je siégeais à l'Association des banquiers canadiens, on nous a présenté un terminal de paiement électronique qui devait être incassable. Or il n'a fallu que trois semaines pour que cela se produise. Il ne s'agissait pas d'une erreur humaine, mais vraiment d'une mauvaise intention, à l'interne.

De quelles solutions disposons-nous pour gérer le facteur humain?

[*Traduction*]

M. Scott Jones: Je pense qu'il en existe quelques-unes. Habituellement, nous qualifierions ces manoeuvres de « menaces internes », quand quelqu'un fait...

On peut intervenir de diverses manières, notamment au chapitre des justificatifs d'identité dont nous avons parlé plus tôt. On peut s'assurer que les gens ne peuvent faire que ce qui est absolument nécessaire dans le cadre de leur travail du point de vue des TI.

On peut aussi se doter d'un programme pour surveiller ce genre d'activités et les irrégularités qui commencent à augmenter de façon marquée. Les entreprises tendent à considérer que la détection de la fraude concerne une menace venant de l'extérieur. La fraude vient aussi parfois de l'intérieur, cependant. Il se produit alors des pertes internes et des anomalies semblables. Il faut donc utiliser certains de ces outils au sein de l'entreprise.

Il existe un autre facteur concernant la menace interne, et certains collègues du gouvernement sont probablement mieux placés pour traiter de la question. Il s'agit de faire attention aux employés. Ainsi, s'ils se retrouvent dans des situations dans lesquelles ils se tournent vers la criminalité, il existe une meilleure solution pour eux. Il faut entre autres savoir comment leur offrir une autre issue quand les choses vont mal.

Du point de vue des informations et des activités internes du Centre de la sécurité des télécommunications, nous avons certainement passé beaucoup de temps à peaufiner notre programme de sécurité interne pour aider les employés pour qu'ils ne se retrouvent jamais dans pareille situation, et ce, pour gérer la menace interne. Il faut toujours se montrer vigilant à cet égard, et c'est habituellement un aspect qui est négligé. Nous n'aimons pas traiter nos employés comme s'ils étaient des criminels.

● (1705)

[*Français*]

M. Michel Picard: On nous a effrayés lundi dernier en nous disant que les moyens de certains États étrangers étaient nettement supérieurs à tout ce que le Canada pourrait investir pour être à la page en matière de haute technologie.

Si nous avons l'impression de ne pas pouvoir investir l'argent nécessaire pour disposer des moyens qui s'imposent, en sommes-nous au point de devoir convaincre les entreprises privées de faire partie de la solution en devenant en quelque sorte mandataires ou chiens de garde sur le marché?

[*Traduction*]

M. Scott Jones: À l'heure actuelle, la collaboration avec le secteur privé ne pose aucun problème. Les entreprises sont tout à fait disposées à collaborer avec nous, à signaler les incidents et à travailler en collaboration quand elles ou nous détectons quelque chose. Je pense que l'industrie canadienne tient à faire partie de la solution, mais comme vous l'avez souligné plus tôt, c'est onéreux. Il faut dépenser de l'argent. Si les marges sont serrées, alors il faut travailler ensemble pour assurer la cybersécurité à l'interne.

Il ne nous semble pas que l'industrie canadienne hésite à investir. Certaines entreprises ont la capacité de le faire, mais ce ne sont certainement pas toutes les organisations de cybersécurité qui sont capables de contrer le problème; elles font alors appel à des fournisseurs externes ou à des endroits où la sécurité est déjà assurée.

Le président: Nous allons devoir en rester là. Merci.

Monsieur Motz, vous disposez de cinq minutes.

M. Glen Motz: Merci, monsieur le président.

Je vous remercie tous les deux de témoigner.

Nous avons tous eu vent d'arnaques, que ce soit nous, nos voisins ou notre famille qui en avons été victimes. Elles viennent habituellement de l'étranger. Des électeurs m'ont affirmé — et j'ai certainement fait enquête sur la question au fil des ans — que lorsqu'ils menacent d'appeler la police, les malfaiteurs ont le culot de les envoyer paître, leur répondant qu'ils sont dans un pays étranger et que la police ne peut rien contre eux.

En vertu du nouveau mandat conféré au Centre canadien pour la cybersécurité, quel rôle jouez-vous pour aider la police? Quels outils lui offrez-vous afin de lui permettre d'intervenir ou d'atténuer le risque, non seulement pour appuyer la police et ses outils, mais aussi, espérons-nous, pour élaborer des stratégies plus agressives à l'intention des consommateurs pour qu'ils ne soient pas victimes d'arnaques?

M. Scott Jones: Si on examine le problème du point de vue des services de police, nous cherchons certainement à encourager les gens à s'adresser à la police quand ils sont victimes de ces genres d'arnaques pour que celle-ci puisse intervenir. Je pense que c'est une des premières choses à faire: convaincre les gens que la police ne va pas venir saisir leur ordinateur afin de les inciter à signaler les fraudes pour que la police puisse agir.

Il faut également faire de l'éducation. C'est le volet que nous dirigerions afin de tenter d'aider les Canadiens à comprendre de quoi ces menaces pourraient avoir l'air pour qu'ils soient vigilants à ce sujet. Le fait que l'électeur ait répliqué en disant: « un instant: c'est une arnaque et je vais appeler la police » montre qu'il savait que c'était une arnaque et qu'il ne devait pas tomber dans le piège. C'est une excellente chose.

Mon père raccroche le combiné. Il m'a fait promettre de ne pas faire référence à lui, mais il raccroche le téléphone, car il sait que c'est une arnaque et il ne croit plus rien. Je m'inquiète du jour où quelqu'un l'appellera à des fins légitimes, mais le fait est qu'il sait quoi faire.

Je pense qu'il est primordial de faire comprendre aux Canadiens qu'il n'y a pas de honte à être victime d'arnaque. Ce sont les plus vulnérables de la population qui tendent à tomber dans ce genre de piège. Il faut ensuite leur faire comprendre qu'ils doivent signaler la fraude et qu'ils peuvent prendre des mesures simples. Nous devons aussi voir comment nous pouvons collaborer avec l'industrie pour que nous soyons tous un peu plus résilients et assurions un certain degré de sécurité nationale. Si les gens ne reçoivent pas de pourriels parce que les entreprises canadiennes les bloquent, alors ils ne peuvent pas cliquer dessus.

Comment pouvons-nous commencer à travailler en vue d'atteindre ces résultats en interpellant l'industrie et en tirant parti du fait que notre secteur commercial souhaite également protéger ses clients?

● (1710)

M. Glen Motz: Quand vous parlez d'interpeller, faites-vous référence à la réglementation, oui ou non?

M. Scott Jones: À l'heure actuelle, nous parlons de partenariats. Nous adoptons une approche de partenariat.

M. Glen Motz: Quand il est question des divers niveaux de menace au Canada, un expert nous a indiqué qu'il faut évaluer la probabilité d'une attaque et les répercussions qu'aurait cette dernière. Juste avant que nous n'arriviez et auparavant, nous avons entendu dire que la probabilité qu'une banque soit piratée est faible et que celle qu'un particulier soit arnaqué est bien plus élevée, mais que les répercussions sont considérables dans les deux cas.

La compromission de nos réseaux de communication — je parle ici des systèmes qui transmettent nos renseignements personnels, gouvernementaux et bancaires — constitue-t-elle une des principales menaces à la sécurité du pays? Internet est-il le réseau le plus essentiel que nous ayons?

M. Scott Jones: Nous tendons à aborder la question en ne faisant jamais confiance aux systèmes sous-jacents à ceux avec lesquels nous travaillons. Par exemple, si Eric et moi communiquons par courriel, nous nous disons toujours que nous ne pouvons pas faire confiance au réseau, car en raison de la manière dont Internet fonctionne, ces messages pourraient faire le tour de la planète et traverser chaque pays; nous utilisons donc le chiffrement. C'est ainsi que nous protégerions la communication.

Nous cherchons toujours des moyens d'ajouter des couches de protection, en présumant que quelque chose d'autre n'est pas sécuritaire. Plus on porte attention à la question et plus on ajoute de couches de protection, comme le chiffrement, la sécurité et la gestion des justificatifs d'identité, plus la communication est sécuritaire.

À un moment donné, toutefois, il y a une limite à ce qu'on peut faire avant que le processus devienne si peu convivial que les gens changent de système ou contournent les mesures de sécurité. L'industrie doit trouver un juste équilibre à cet égard, mais je pense qu'elle doit améliorer sa sécurité. Les gens ne devraient pas devoir savoir comment sécuriser les dispositifs de base qui entrent chez eux. Ils ne devraient pas chercher à déterminer comment ils peuvent assurer la sécurité; c'est l'appareil qui devrait les aider à le faire d'entrée de jeu. À l'instant où on le démarre, il devrait indiquer comment l'utiliser de manière sécuritaire. Nous employons l'expression « sécuritaire par défaut ».

Le président: Merci, monsieur Motz.

Si le premier ministre téléphone au sujet de votre nomination au Sénat, c'est probablement une bonne idée de raccrocher.

Des voix: Ha, ha!

Le président: Madame Sahota.

Mme Ruby Sahota: Nous avons beaucoup parlé des entreprises et des individus qui préfèrent ne pas signaler des incidents, et ce, pour différents motifs. Les entreprises veulent projeter l'image d'une institution ou d'une organisation digne de confiance, alors que certaines personnes ressentent de la honte. C'est peut-être un peu la même chose dans les deux cas.

En novembre dernier, le gouvernement a établi une exigence obligatoire pour les organisations fédérales assujetties à la LPRPDE. Ces organisations sont ainsi tenues d'aviser le commissaire à la protection de la vie privée, les personnes pouvant être touchées ainsi que les tiers ou les ministères gouvernementaux susceptibles d'apporter leur aide. Si je ne m'abuse, il y a un critère permettant de déterminer si l'atteinte est suffisamment grave pour que l'exigence de signalement s'applique. Les amendes prévues peuvent atteindre 100 000 $.

Croyez-vous que cette mesure contribuera à faire en sorte que l'information soit transmise assez rapidement aux intéressés? Qu'en pensez-vous?

M. Scott Jones: Je ne veux pas parler au nom de la commissaire à l'information, mais nous estimons pour notre part qu'il serait préférable d'obtenir cette information bien avant que l'on soit capable de mesurer l'ampleur de l'atteinte à la vie privée. Nous voudrions que cela se fasse dès la première indication d'un risque de cybercompromission, le premier courriel d'hameçonnage ciblé ou la première tentative de piratage du système et d'utilisation d'authentifiants qui ne devraient plus être utilisés.

Nous pouvons travailler avec les entreprises. Nous souhaiterions obtenir cette information — et nous y parvenons — plus tôt dans le cycle d'exploitation de telle sorte qu'il nous soit possible de prendre les mesures qui s'imposent et d'aider d'autres organisations à faire le nécessaire avant d'être elles-mêmes touchées. Si nous concentrons nos efforts sur ce que nous appelons l'exfiltration de données, il est trop tard, car le mal est déjà fait.

Nous nous efforçons d'agir de façon proactive en intervenant plus tôt dans le processus. Je préférerais recevoir de la même entreprise 100 appels dont 99 fausses alertes — je ne suis pas certain que cela plairait beaucoup à Eric et son équipe — que de me retrouver dans une situation où l'entreprise ne communique pas avec nous lorsqu'il y a effectivement un problème et que nous aurions pu prendre les mesures nécessaires et aider le reste du secteur à se préparer en prévision d'une atteinte possible.

C'est un aspect que nous essayons d'améliorer. Nous tentons de collaborer avec les entreprises à cette fin.

● (1715)

Mme Ruby Sahota: Excellent. Je vous en félicite, mais reste quand même que nous entendons sans cesse... J'ai lu par exemple qu'Equifax a été victime d'une atteinte en raison de la défaillance de ses pratiques de cyberhygiène. Notre témoin précédent nous disait que les règlements et les normes appliqués par les entreprises sont totalement désuets, et que rien n'est fait pour les inciter à mettre à jour régulièrement ces normes et règlements en fonction des nouvelles menaces auxquelles elles peuvent être exposées.

Comment pouvons-nous inciter ces entreprises à prendre des mesures semblables en l'absence de réglementation et de sanctions en la matière?

M. Scott Jones: Je pense que c'est sans doute à vous qu'il incombe de déterminer quelle sera l'approche utilisée en matière de politiques et de réglementation. Pour nous, il importe que les organisations respectent les consignes de base. Je pense qu'il nous faut maintenant collaborer avec elles en nous efforçant de faire en sorte que les entreprises du secteur technologique apportent les améliorations qui s'imposent.

Le problème vient du fait que les dispositifs de sécurité doivent être inscrits dans la configuration du système. Lorsqu'une entreprise devient vulnérable, ce n'est pas nécessairement parce qu'elle a mal agi ou qu'elle n'a pas respecté les consignes de base. Il peut s'agir d'une simple erreur commise par l'administrateur du système. Votre sécurité ne devrait toutefois pas être mise en péril aussi facilement du simple fait qu'un administrateur a saisi la mauvaise commande. C'est tout à fait inacceptable.

C'est comme si les informaticiens et les ingénieurs construisaient un pont et que l'oubli d'un seul rivet provoquait son écroulement. Les ingénieurs ne s'y prennent pas de cette manière pour concevoir un pont. L'industrie doit trouver le moyen de s'assurer que la technologie n'est pas à ce point vulnérable en matière de cybersécurité.

Cela fait partie des principales mesures qu'il convient de prendre, mais je crois préférable de vous laisser déterminer si la réglementation est l'approche à privilégier. Dans mon rôle de fonctionnaire, je m'assurerai de donner consciencieusement suite aux directives qui nous seront données.

Mme Ruby Sahota: Nous essayons d'accumuler le plus d'information possible pour guider les recommandations que nous formulerons à l'issue de la présente étude. Certains témoins nous ont brossé un tableau plutôt effrayant de la situation alors que d'autres, comme vous, semblent nourrir davantage d'espoir.

Quels seraient selon vous les secteurs les plus vulnérables auxquels nous devrions nous intéresser de plus près?

M. Scott Jones: On peut prendre l'exemple du secteur financier qui investit des sommes considérables. On s'est ainsi donné d'excellentes capacités, notamment pour la détection de la fraude. C'est en fait l'un des domaines dans lesquels nous espérons tirer des enseignements de leur expérience d'utilisation de ce que j'appellerai l'intelligence artificielle ou l'apprentissage machine pour détecter des activités comme la fraude. Nous voulons ainsi tirer parti de leur expertise comme ils le font en partie pour celle que nous possédons en matière de cyberdéfense.

Il s'agit de secteurs qui ne se considèrent pas à la base comme de grands utilisateurs des technologies de l'information, mais il suffit de pousser les choses un peu plus loin pour voir ce qu'il en est. Nous nous assurons donc de travailler auprès des 10 secteurs faisant partie des infrastructures essentielles. Dans chaque cas, il y a un élément de technologie et de cybersécurité qui entre en jeu.

Le président: Nous devrons en rester là pour l'instant. Nous avons un peu dépassé le temps imparti.

Monsieur Eglinski, vous avez cinq minutes.

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

Je vous remercie tous les deux de votre présence aujourd'hui. Vous avez dit que le seul réseau sécuritaire est celui qui n'est pas utilisé. Bon nombre, si ce n'est la majorité, des atteintes à l'égard des réseaux gouvernementaux débutent par une forme quelconque d'hameçonnage ou autre stratagème d'individus mal intentionnés qui veulent avoir accès à des justificatifs d'identité valides. Bien que le National Institute of Standards and Technology ait indiqué qu'il n'était plus conseillé de procéder à des réinitialisations périodiques des mots de passe pour les réseaux, de nombreux services informatiques des ministères gouvernementaux ont maintenu en place un dispositif de réinitialisation automatique tous les 90 jours.

Ne serait-ce pas pour nous une façon très simple de commencer à mieux assurer la cybersécurité du gouvernement?

M. Scott Jones: Merci pour la question. Je crois que vous m'avez cité fidèlement, mais j'ai aussi indiqué que le meilleur moyen d'assurer la sécurité d'un réseau, c'est de le fermer complètement.

Je crois qu'il y a quelques éléments à prendre en compte.

La situation n'est plus du tout la même pour ce qui est des mots de passe. C'est justement pour cette raison que nous revoyons actuellement nos recommandations à ce sujet. Nous encourageons les gens à ne pas se contenter de changer leurs mots de passe. Ils devraient aussi utiliser un second facteur d'authentification, comme un dispositif générant une série aléatoire de chiffres. Certains reçoivent ainsi un message leur demandant de saisir un code donné lorsqu'ils ouvrent une session sur un nouvel appareil. L'utilisation d'un second facteur d'authentification est une mesure essentielle pour la cybersécurité. Si vous utilisez Twitter, Facebook ou d'autres plateformes de médias sociaux, vous devriez toujours vous connecter au moyen de votre second facteur d'authentification, et il en va de même de tous les systèmes gouvernementaux.

Il était tout à fait sensé de demander une réinitialisation périodique du mot de passe à une époque où chacun n'avait que deux systèmes à utiliser et deux mots de passe à retenir, voire un seul. J'utilise pour ma part une multitude de mots de passe pour mes activités personnelles et professionnelles. J'ai arrêté de compter à 90. Nous essayons de trouver le juste équilibre entre l'aspect sécuritaire et le côté pratique. En outre, les gens ont tendance à utiliser des mots de passe faciles à détecter lorsqu'ils en ont autant. C'est un aspect qu'il faut considérer.

● (1720)

M. Jim Eglinski: Dans votre exposé, vous avez parlé de la nécessité de mieux informer les gens au sujet des cybermenaces les plus susceptibles de toucher les Canadiens et leurs entreprises. Pouvez-vous me parler brièvement de quelques-unes des mesures que vous prenez pour sensibiliser les Canadiens à cet égard? Les derniers jours m'ont permis d'apprendre tellement de choses que j'ignorais auparavant, ce qui m'incite à me demander dans quelle mesure les Canadiens sont conscients de leur vulnérabilité lorsqu'ils utilisent Internet.

M. Scott Jones: Nous avons d'abord publié notre évaluation des cybermenaces nationales. Cet aperçu du contexte de la cybermenace s'accompagnait de notions élémentaires expliquant les termes techniques utilisés dans le langage le plus simple possible. Nous ne ménageons pas nos efforts.

M. Jim Eglinski: Comment les gens ont-ils pu y avoir accès?

M. Scott Jones: Nous avons publié un gazouillis avant d'afficher l'évaluation en ligne. J'ai fait une tournée des médias. Cet exercice médiatique était un peu étrange et irréel pour un fonctionnaire comme moi. Nous essayons de diffuser l'information de toutes les manières possibles. J'aimerais voir chaque député en faire autant. Nous tentons de mettre à la disposition de chacun des outils simples à utiliser.

M. Jim Eglinski: Merci. J'ai moi-même transmis cette information.

Pourquoi n'avez-vous pas fait appel aux journaux, plutôt qu'à l'Internet, pour informer les gens?

M. Scott Jones: Tout dépend de ce qu'il nous est possible de faire pour diffuser de l'information et des moyens que nous pouvons prendre, mais nous allons voir s'il est possible d'intégrer cela à notre stratégie de communication. Nous cherchons toujours à rejoindre le plus vaste public possible.

M. Jim Eglinski: Vous avez toutefois surtout recours à la publicité en ligne.

M. Scott Jones: C'est vrai. Nous pensons d'abord à la voie numérique.

M. Jim Eglinski: Est-ce qu'il me reste encore du temps?

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

M. Jim Eglinski: Existe-t-il dans notre pays des lois obligeant les entreprises canadiennes offrant des services de sécurité, comme les systèmes d'alarme pour les résidences, à être honnêtes envers leurs clients?

Je vais vous donner un exemple fort éloquent. Une firme de sécurité reconnue a installé un système d'alarme chez moi. On m'a dit l'automne dernier que l'on pouvait rendre ma résidence beaucoup plus sécuritaire en installant trois caméras. Personne ne pourrait plus circuler sur mon terrain ou pénétrer dans ma maison à leur insu. Tout cela m'apparaissait fort intéressant. J'ai voulu savoir combien cela me coûterait. C'était assez dispendieux, mais j'ai tout de même accepté. J'ai toutefois vérifié ensuite auprès de mon fournisseur de services qui m'a indiqué que le système ne disposait pas encore des capacités nécessaires pour accueillir une installation semblable. La firme m'avait assuré que je pourrais utiliser tous ces dispositifs, mais le service n'était pas accessible.

N'y a-t-il pas au Canada des exigences ou des lois obligeant ces entreprises à dire toute la vérité à leurs clients?

M. Scott Jones: Je ne connais pas la réponse à cette question.

Le président: Je pense que l'on peut considérer que votre temps est écoulé.

M. Jim Eglinski: J'avais une autre question, mais je vais y renoncer.

Le président: Merci.

Madame Dabrusin, vous avez cinq minutes.

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

J'ai été particulièrement frappée par le témoignage de M. Kabilan pendant la première partie de notre séance, et surtout par cette proportion de 60 % qu'il nous a citée. Je sais que vous avez déjà répondu à des questions à ce sujet, mais je crois qu'il a fait l'analogie avec un camion blindé qui ferait une livraison d'argent d'une boîte de carton à une autre. Nous discutons surtout de la situation du camion blindé, et il est important de le faire, mais si nous ne veillons pas à ce que les boîtes de carton soient également sécuritaires, nous avons vraiment un problème.

Vous nous avez donné l'exemple de votre père qui raccroche le téléphone, mais on nous a également parlé du Centre de cybersécurité du Royaume-Uni et des mesures de sensibilisation qui y sont prises. J'aimerais savoir dans quelle mesure vous comptez suivre ce modèle-là. Qu'est-ce qui pourrait fonctionner pour vous également, et que devriez-vous faire différemment?

M. Scott Jones: Nous travaillons en étroite collaboration avec le National Cyber Security Centre du Royaume-Uni. Nous essayons de mettre en pratique les enseignements tirés. Il faut notamment tenir compte du fait qu'ils ont une longueur d'avance. Notre cybercentre n'est en place que depuis 121 jours alors que le leur existe depuis plus de deux ans.

Nous essayons de voir comment nous pourrions améliorer les choses. Nous avons noté qu'ils prenaient différentes mesures... Parmi les initiatives en place au Royaume-Uni, je crois qu'il y a des programmes pour inciter les filles à faire de la programmation et d'autres visant à intéresser les plus jeunes. Nous avons parrainé des événements comme le Hackergal, et certains de nos professionnels s'y sont rendus pour servir de mentors. Il n'est pas nécessairement facile de refaire la même chose à plus grande échelle, simplement parce qu'il est difficile de déployer des gens un peu partout au Canada. Notre pays est gigantesque.

Avec qui pouvons-nous travailler en partenariat? Comment intéresser davantage de gens à l'aspect numérique? Nous explorons d'autres modes de communication. Parmi les campagnes recensées ailleurs dans le monde, il y en a une qui cible les aînés aux fins de la cybersécurité. On les invite à poser des questions à leurs petits-enfants. Cela semble fonctionner très bien. Nous attendons de pouvoir déterminer à quel point cela sera efficace, et nous tentons d'explorer d'autres mécanismes de rayonnement. Reste quand même que la sensibilisation est l'un des éléments essentiels.

Mme Julie Dabrusin: Vous serait-il possible de nous transmettre les liens pour certaines des initiatives auxquelles vous faites référence et pour les mesures qui sont déjà en place? Je consulte souvent le Citizen Lab qui offre un plan de sécurité et de l'information, mais il serait vraiment utile pour nous d'avoir accès aux meilleurs outils pouvant être déployés.

● (1725)

M. Scott Jones: Oui.

Mme Julie Dabrusin: J'ai lu un article du *Financial Post* où il était question du rôle du Bureau du surintendant des institutions financières (BSIF) pour la collecte de données sur différentes atteintes à la sécurité. Nous avons discuté de quelques modèles possibles pour la mise en commun de l'information. Comment le BSIF s'inscrit-il dans cette démarche?

J'essaie simplement de voir le rôle que peuvent jouer les différentes organisations.

M. Scott Jones: Nous collaborons certes avec le BSIF au sein de l'espace réglementaire, mais il importe de savoir que l'on peut s'adresser très tôt dans le processus à notre cybercentre, du fait que nous n'avons pas un rôle de réglementation. Nous sommes bien évidemment en faveur d'un gouvernement de plus large portée, ce qui nous amène à travailler avec le BSIF. Nous essayons de conjuguer nos efforts lorsqu'un incident se produit.

Il va de soi que la question de la confiance est l'une des principales à considérer, surtout dans le secteur financier. Nous devons nous assurer de maintenir la confiance des consommateurs quoi qu'il arrive. Nous pouvons apporter notre contribution, mais nous ne pouvons pas parler au nom du gouvernement pour les questions liées aux politiques monétaires ou financières.

Comment parvenons-nous à coordonner tout cela? Nous avons établi des partenariats. Si un incident se produit dans le secteur financier, le BSIF sera mis à contribution pour quelques-unes des mesures de gestion de crise mentionnées par Eric, car c'est l'une des principales parties prenantes.

Mme Julie Dabrusin: Le BSIF s'occupe des entités assujetties à la réglementation fédérale. Les prêteurs sur gages et tous ces petits établissements que l'on retrouve au coin des rues ont-ils également des exigences à remplir en matière de communication de renseignements? Qui surveille leurs activités?

M. Scott Jones: Nous espérons qu'ils vont communiquer avec nous. Ils ont accès à nos informations, mais rien ne les oblige pour l'instant à nous signaler quelque incident que ce soit.

Mme Julie Dabrusin: Très bien.

En fin de compte, nos renseignements personnels sont assujettis à différentes séries de normes et règlements, suivant l'institution avec laquelle nous faisons affaire, tout au moins pour ce qui est de la communication des renseignements.

M. Scott Jones: Pour autant que je sache, il n'y a aucune communication obligatoire pour les entreprises non assujetties à la réglementation. Nous recevons toutefois des signalements en provenance de firmes qui ont besoin d'aide.

Mme Julie Dabrusin: Une dernière question, car il me reste à peine 30 secondes. Les pouvoirs réglementaires du BSIF semblent également insuffisants du fait qu'il est possible pour les banques à charte fédérale de confier en sous-traitance une grande partie de leurs activités de sécurité à des firmes installées à l'extérieur du Canada. Qui surveille alors ces activités? Qui supervise les relations avec ces fournisseurs externes pour s'assurer que tout se déroule dans les règles?

M. Scott Jones: Nous avons notamment mentionné l'importance de l'évaluation de la cybermenace, mais nous travaillons aussi en étroite collaboration avec les entreprises pour déterminer comment elles s'y prennent pour appliquer les contraintes nécessaires en matière de sécurité tout au long de leur chaîne d'approvisionnement.

Pour une grande partie des incidents plus graves, l'atteinte se produit lorsqu'on va plus loin dans la sous-traitance. Généralement, le premier palier de sous-traitance n'est pas problématique; c'est au second que les choses se gâtent. Il faut s'assurer de mettre en place les exigences nécessaires en matière de sécurité et voir à ce qu'elles s'appliquent aux différents paliers. Il faut en outre que les entreprises sachent bien que le fait de confier en sous-traitance une activité ne signifie pas que l'on se départit de la responsabilité à l'égard de l'information correspondante. Je sais que différentes entreprises concentrent leurs efforts sur cet aspect que nous avons justement mis en lumière à cette fin dans notre évaluation de la cybermenace nationale.

Mme Julie Dabrusin: Merci.

Le président: Merci, madame Dabrusin

La dernière question reviendra à la présidence.

Lors de votre comparution précédente, monsieur Jones, vous avez indiqué que votre approche en matière de sécurité se décline en plusieurs couches successives. Vous avez parlé d'une forme d'ouverture auprès de certains fournisseurs qui vous permettent d'examiner différents éléments, y compris les codes. M. Leulprecht a parlé tout à l'heure d'un système d'interrupteurs et de tableaux ainsi que de l'évolution incessante de ces enjeux.

Estimez-vous encore que l'approche multicouches que vous préconisez convient aussi bien pour un réseau 5G que pour un réseau 3G, voire 4G?

M. Scott Jones: L'approche pour un réseau 5G est actuellement en cours d'évaluation au pays. Je suis tout à fait en confiance grâce aux relations que nous avons établies avec les fournisseurs de services de télécommunications au Canada et au travail que nous avons accompli pour améliorer les éléments de cybersécurité, quel que soit le réseau. Quoi qu'il advienne, nous devrons continuer de collaborer pour faire le nécessaire lorsqu'un incident se produit. Peu importe la technologie en cause, nous devons poursuivre la mise en place de multiples couches de sécurité.

Mon travail m'amène à ne jamais me fier à quoi que ce soit. Je présume que tous les éléments constitutifs d'un produit comportent des points vulnérables et je me demande comment il est possible d'ajouter de nouvelles couches de protection. Cela nous ramène à l'exemple de la boîte de carton pour recevoir des données. Plutôt qu'une boîte de carton, il faut que les données soient encryptées à destination pour assurer leur protection. Il ne s'agit pas d'ériger un mur autour du château; il faut plutôt s'assurer de disposer d'une véritable chambre forte pour que les renseignements confidentiels soient adéquatement protégés.

La sécurité de l'information évolue également à la faveur de l'amélioration des mécanismes de protection et d'encryptage. Il faut aussi commencer à s'interroger quant à la nécessité de conserver l'information pendant une période plus ou moins longue. Peut-être, n'est-il pas nécessaire de la garder aussi longtemps.

Nous utilisons donc une approche à plusieurs paliers, et il faut poursuivre dans le même sens.

Pour ce qui est des réseaux 5G, la question est actuellement à l'étude et des recommandations à ce sujet ne manqueront pas d'être formulées.

● (1730)

Le président: Je tiens à vous remercier tous les deux d'avoir été des nôtres aujourd'hui et de nous avoir transmis tous ces renseignements. Nous vous sommes reconnaissants encore une fois pour votre comparution.

La séance est levée.