CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 147 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le lundi 4 février 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le lundi 4 février 2019

● (1530)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Je déclare la séance ouverte.

Nous accueillons aujourd'hui Jobert Abma, fondateur de HackerOne, ainsi que Deborah Chang, également de HackerOne, puis à titre personnel, Steve Waterhouse.

Je suis certain que le personnel du Comité vous a informés de la procédure. Vous avez 10 minutes pour votre déclaration préliminaire, après quoi M. Waterhouse aura lui aussi 10 minutes pour un exposé et enfin, les députés vous poseront des questions.

Nos plans pour la deuxième heure sont tombés à l'eau, donc j'ai l'intention de dépasser le temps imparti, si nos témoins peuvent se le permettre.

Sur ce, je donne la parole aux représentants de HackerOne.

Mme Deborah Chang (vice-présidente, Politiques, HackerOne): Je remercie les membres du Comité permanent de la sécurité publique et nationale de la Chambre des communes de nous avoir invités à prendre la parole aujourd'hui. Je suis heureuse de pouvoir vous présenter notre point de vue sur la cybersécurité et les programmes de chasse aux bogues.

Je suis vice-présidente des politiques et du développement des affaires chez HackerOne, une entreprise établie à San Francisco et le plus grand fournisseur au monde de services de sécurité exploitant le potentiel des pirates informatiques. Je suis accompagnée de Jobert Abma, fondateur de HackerOne, qui a fondé l'entreprise à l'âge de 23 ans et fait du piratage informatique depuis l'âge de 13 ans.

HackerOne offre des programmes de chasse aux bogues, qui mettent des entreprises et des gouvernements en contact avec les meilleurs pirates éthiques au monde pour trouver et corriger les vulnérabilités d'un système avant que des acteurs malicieux ne les exploitent. En date de janvier 2019, plus de 300 000 pirates éthiques sont inscrits comme collaborateurs de HackerOne pour défendre les consommateurs — notamment le Département de la Défense des États-Unis —, et ils ont déjà réussi à éliminer plus de 80 000 vulnérabilités et à prévenir un nombre incalculable d'atteintes à la sécurité informatique.

Les méthodes de cybersécurité actuelles sont gravement dépassées compte tenu de la nature des cybermenaces auxquelles la société est confrontée de nos jours. Quand elle est exploitée à des fins criminelles, la plus petite vulnérabilité qui passerait relativement inaperçue peut créer des ravages, comme la fuite de données d'Equifax nous l'a brutalement rappelé en 2017. En 2018, beaucoup d'autres atteintes à la sécurité ont fait les manchettes, dont l'attaque au moyen du rançongiciel WannaCry.

Dans les institutions financières, la fraude en ligne et hors ligne a augmenté de plus de 130 % en 2018, causant du coup des pertes financières importantes qui ont beaucoup entaché leur réputation. Au Royaume-Uni, le nombre de cyberattaques à l'encontre de services financiers déclarées à la Financial Conduct Authority du pays a augmenté de plus de 80 % au cours de la dernière année. Il convient malheureusement de constater que dans l'univers numérique, la société n'arrive actuellement pas à offrir à ses citoyens ce pour quoi les sociétés ont été établies, soit la sécurité.

Je veux donc vous parler aujourd'hui des services de sécurité qui exploitent les compétences des pirates informatiques et leur grand nombre pour prévenir les cyberattaques dans la société dans son ensemble, y compris dans le secteur financier et dans le domaine de la sécurité nationale. Quels que soient les protections et les mécanismes de défense intégrés à nos actifs numériques — et nous devons en prévoir beaucoup —, il y a une façon de faire qui permet de déceler toutes les causes possibles d'intrusion. Il existe un système immunitaire qui abordera les actifs numériques comme leurs adversaires et les criminels, c'est-à-dire de l'extérieur. C'est un mécanisme qui, à grande échelle, peut permettre de détecter toutes les failles, les faiblesses et les vulnérabilités de sécurité d'un système ou d'un produit conçu par les humains.

C'est ce qu'on appelle souvent le piratage éthique. Le filet de sécurité qu'offre le piratage éthique englobe tous les services et toutes les formes d'automatisation destinés à accroître la cybersécurité produits totalement ou en partie par des experts de la sécurité indépendants. Ceux-ci viennent de l'extérieur de l'entreprise ou de l'organisation en question. Selon ce modèle, on invite les chercheurs externes et indépendants en matière de sécurité et les pirates éthiques à partir à la chasse aux vulnérabilités de systèmes informatiques. On parle ici de spécialistes ayant signé un engagement afin d'aider les entreprises et les organisations à détecter et à corriger leurs faiblesses en matière de sécurité.

La fonction la plus fondamentale des services de sécurité fondés sur le piratage éthique est l'établissement d'un programme de divulgation des vulnérabilités, c'est-à-dire de divulgation responsable ou coordonnée des vulnérabilités. En gros, ce type de programme équivaut, pour un logiciel, à la surveillance que peuvent exercer des voisins. La philosophie, c'est que si l'on voit quelque chose, on le dit. Concrètement, si un pirate éthique trouve une vulnérabilité de sécurité sur le site Web d'une entreprise ou d'une organisation gouvernementale, dans une application mobile ou un autre type de système informatique, il sera invité à divulguer la vulnérabilité trouvée au propriétaire.

La plupart des êtres humains sont prêts à aider leurs voisins, donc l'incitation à divulguer la vulnérabilité est énorme. Les questions de légitimité et de confiance, cependant, rendent la divulgation des vulnérabilités plus complexe que dans un contexte ordinaire de surveillance entre voisins. Pour résoudre ce problème, des entreprises de pointe se sont dotées de cadres stratégiques favorisant la divulgation des vulnérabilités décelées, tandis que d'autres sociétés se tournent vers des entreprises comme HackerOne pour organiser et coordonner ce genre de programme.

Quand une entité décide d'offrir une récompense financière à quiconque trouve une vulnérabilité, le programme de divulgation des vulnérabilités est alors qualifié de chasse aux bogues. Les programmes de chasse aux bogues existent depuis au moins 1983. C'est une méthode qui a été perfectionnée par Google, Facebook et Microsoft depuis cinq ou six ans.

● (1535)

Les services de sécurité fondés sur le piratage éthique ont fait leurs preuves si on les compare aux autres méthodes de détection des vulnérabilités. Il coûte plus cher d'embaucher des employés à temps plein, de retenir les services de fournisseurs externes ou d'acheter des produits pour effectuer des tests de vulnérabilité. Aucune autre méthode de validation des logiciels ou des produits de consommation n'affiche de résultats comparables à un prix unitaire aussi bas.

C'est un modèle qui repose sur la force du nombre. À l'heure actuelle, il y a plus de 300 000 pirates éthiques inscrits sur notre plateforme seulement, et au cours des prochaines années, nous espérons que leur nombre atteigne un million. Cette armée de pirates pourra alors s'attaquer à la tâche d'assurer la sécurité de tout l'univers numérique dans notre société.

Grâce à sa diversité et à son ampleur, la communauté des pirates éthiques arrive à trouver des failles que les détecteurs automatisés ou les équipes permanentes qui réalisent des tests de pénétration ne décèleront pas. Les modèles existants sont bons pour trouver les vulnérabilités prévisibles en matière de sécurité, mais il est encore plus important d'arriver à repérer les failles imprévisibles: l'inconnu des inconnus. Ainsi, si on lui en donne le temps, un groupe de pirates éthiques assez grand arrivera à détecter ces vulnérabilités.

Diverses entités ont des programmes de divulgation des vulnérabilités ou de chasse aux bogues de ce type, comme Adobe, AT&T, le Département de la Défense des États-Unis, Dropbox, Facebook, General Motors, Google, Microsoft, Nintendo, Starbucks, Shopify, Twitter et United Airlines. Dans le secteur financier, des entreprises comme American Express, Citigroup, JPMorgan Chase, ING et TD Ameritrade ont des programmes publics du genre.

Le Département de la Défense des États-Unis et HackerOne ont été des pionniers grâce à la mise en place du premier programme gouvernemental fédéral de chasse aux bogues. Depuis sa création, plus de 5 000 vulnérabilités de sécurité ont été résolues en toute sécurité dans les actifs de la Défense grâce au piratage éthique. Si la majorité de ces vulnérabilités ont été signalées au Département de la Défense des États-Unis sans indemnité financière, l'organisation a tout de même versé des centaines de milliers de dollars en récompenses lors d'exercices de chasse aux bogues.

On me demande souvent qui sont ces pirates. Il y a beaucoup de termes utilisés pour décrire ces spécialistes de la sécurité, comme pirate éthique, chapeau blanc, chercheur en matière de sécurité, chasseur de bogues et chercheur, tout court. Il y a un qualificatif qui brille par son absence dans cette liste, celui de criminel. Ces pirates ne sont pas des criminels. Il faut préciser que les programmes de chasse aux bogues n'offrent aucune rétribution à quiconque agit avec une intention criminelle. Au contraire, HackerOne compilera des données sur tous les pirates sur sa plateforme et ne les récompensera que s'ils respectent les règles. Pour ces raisons, les criminels vont ailleurs.

Les motivations qui habitent les pirates varient beaucoup, et ils sont nombreux à agir par altruisme. L'organisation de défense de la sécurité I Am The Cavalry résume ses motivations par le désir de protéger (pour rendre le monde plus sûr); le désir de résoudre des énigmes (par curiosité); le désir de prestige (par fierté ou pour se faire connaître) —; le désir de profit (pour gagner de l'argent) et le désir de protestation ou de patriotisme (qui se fonde sur l'idéologie et les principes). Selon une étude réalisée en 2016 par la National Telecommunications and Information Administration, qui relève du Département du Commerce des États-Unis, seuls 15 % des chercheurs en matière de sécurité s'attendent à une indemnité financière en contrepartie d'une divulgation de vulnérabilité.

Bref, non seulement le piratage éthique améliore-t-il la sécurité, mais il démocratise cet univers et offre un travail valorisant à quiconque a la motivation de faire oeuvre utile de cette façon. Beaucoup de pirates éthiques sont de jeunes adultes. Ils peuvent faire ce travail de n'importe où. L'argent qu'ils font grâce à cela leur sert à subvenir aux besoins de leur famille, à payer leurs études et à les propulser vers des carrières professionnelles épanouissantes.

Le piratage donne un sens et un mandat à des personnes dynamiques, d'où qu'elles viennent. Il a un effet sociétal positif pour le pays.

Bref, nous avons besoin des pirates éthiques. Nous devons aspirer à un Internet qui assure la confidentialité et protège les consommateurs. Nous ne pourrons pas y arriver sans l'aide des pirates éthiques pour préserver activement notre sécurité collective. Ils sont véritablement le système immunitaire d'Internet. Ils constituent une puissance positive dans la société. Nous devons leur donner les moyens d'agir en les encourageant à contribuer à notre sécurité. Il faut pour cela leur offrir un cadre juridique sûr et inciter tout le monde à divulguer les vulnérabilités qu'il détecte, quelles que soient les circonstances.

● (1540)

Pour terminer, je répéterai ce que de nombreux experts disent toujours, soit qu'il faut toujours le dire si l'on détecte une vulnérabilité, dans le but d'améliorer la cybersécurité pour les consommateurs. L'absence de mécanisme officiel pour envoyer des rapports de vulnérabilité à une entreprise affaiblit sa sécurité et l'expose à un risque inutile. Les entreprises et les gouvernements doivent être ouverts à toute information venue de l'extérieur sur leurs vulnérabilités potentielles en matière de sécurité. De même, le gouvernement canadien devrait encourager, voire même exiger ce comportement.

Je vous remercie de m'avoir fourni l'occasion de témoigner sur cet enjeu important.

Le président: Merci beaucoup.

Sur ce, nous entendrons maintenant M. Waterhouse.

M. Steve Waterhouse (ancien officier de sécurité des systèmes d'information, Ministère de la Défense nationale, à titre personnel): Je remercie le Comité de m'avoir invité à venir lui faire part de quelques problématiques perçues par nos concitoyens concernant l'accès à leurs revenus et à leurs économies et leur sécurité dans le contexte des technologies informatiques.

Je commencerai par vous présenter brièvement mon parcours. Après avoir travaillé au service des Forces armées canadiennes et du MDN pendant 23 ans, j'ai eu le privilège de faire partie des premiers cybersoldats du pays à gérer des systèmes d'information informatisés et mis en réseau, qui sont passés d'un réseau local d'environ 250 utilisateurs à un réseau métropolitain d'environ 5 000 utilisateurs sur divers sites, dans les différentes bases, aux premiers stades de l'intégration. Nous avions pour mandat de fournir toute l'information pertinente à la structure de commandement sur les processus papier, des simples tâches de bureau quotidiennes jusqu'aux activités d'enseignement que je menais au CMR Saint-Jean, en passant par toutes les autres opérations. Ces dernières années, je me suis plutôt consacré à l'instruction et à la formation de professionnels et des simples citoyens sur l'application des meilleures pratiques en matière de technologie d'information. Je leur explique, en termes simples (comme je le ferai aujourd'hui), ce qui se passe dans le cyberespace qui touche tout et tout le monde presque tous les jours avec les médias d'information. Je vous en présenterai d'ailleurs un aperçu maintenant.

[*Français*]

Il est minuit et quart. Telle est la situation.

Comme vous le savez, nous sommes au XXI^{e} siècle. Nous sommes plus connectés que jamais et l'automatisation est de plus en plus intégrée à nos vies. L'économie du pays repose en grande partie sur l'usage de la technologie, sur les PME et sur la grande entreprise. Même les services gouvernementaux ont pris un virage technologique. Cependant, la réalité nous rattrape de plus en plus.

Les quelques exemples énumérés dans le document que j'ai présenté au Comité démontrent que les problèmes se perpétueront dans le temps, mais ils sont néanmoins préoccupants dans le moment présent. Par exemple, les programmeurs et les spécialistes informatiques les plus futés conçoivent de mauvaises configurations pour se donner un avantage indu dans leurs transactions boursières.

N'importe quelle personne qui prend le temps de s'instruire sur la technologie qu'il est possible d'exploiter, voire de pirater, peut trouver sur Internet des techniques sur la façon de trouver les brèches et de contourner la sécurité. On peut utiliser les dernières techniques pour exploiter les lacunes, la plupart du temps pour mettre la main sur des informations qui mèneront à des gains financiers ou monétaires.

Au cours des dernières années, particulièrement en 2017 et en 2018, on a entendu parler de la persistance et de la virulence des rançongiciels, qui permettent de s'en prendre non seulement aux particuliers, mais également à n'importe quelle organisation, sans exception. Ce type d'arnaque est toujours présent, car les gens sont mal informés et incapables de repérer les menaces. Qui plus est, les malfaisants ont raffiné leurs méthodes, de sorte qu'il est de plus en plus difficile de repérer une arnaque dans un vrai message envoyé par courrier électronique.

Aujourd'hui, les institutions financières demandent à leurs clients, voire exigent d'eux, qu'ils effectuent leurs transactions financières seulement à partir de leur ordinateur personnel, de leur téléphone portable ou d'un autre moyen connexe. On s'attend à ce que les employés, les citoyens et les clients connaissent le fonctionnement de Windows 10 ou de la plus récente version de Microsoft Office.

Les gens ne sont pas formés ou ne connaissent pas bien les outils de base utilisés pour faire ces transactions. La plupart du temps, ces transactions sont effectuées alors que les mesures de sécurité ne sont pas optimales et que la connectivité est douteuse. La connexion au réseau WiFi public d'un hôtel ou d'un café Internet n'est pas du tout sécuritaire. Il y a aussi le cellulaire, mais même s'il est moins piraté, sa sécurité est tout aussi déficiente.

Le retard dans le déploiement de la connectivité haute vitesse promise dans les régions renforce le cynisme lié au manque d'accessibilité à une vitesse décente pour faire des transactions financières. Ce cynisme vient du fait que des commerces ou des résidences de Port-au-Prince, à Haïti, ont accès ou auront accès à la fibre optique dans les prochaines années, bien avant ceux situés dans un rayon de 50 kilomètres de Montréal.

● (1545)

[*Traduction*]

Que faut-il faire ou que pouvons-nous faire? Je dis toujours qu'il faut faire preuve de leadership et prêcher par l'exemple. C'est avec beaucoup d'enthousiasme que j'ai entendu parler de la mise en place du Centre canadien pour la cybersécurité en octobre dernier. Il fallait faire de la cybersécurité un enjeu distinct de la sécurité générale pour bien souligner son importance. Trop souvent, je vois des grandes entreprises et des conseils de gestion attribuer au premier venu la responsabilité de la « sécurité informatique ». C'est pour beaucoup un mal nécessaire, mais si le gouvernement fédéral lui-même a décidé de procéder de cette façon, il restera peu de raisons aux dirigeants d'entreprise pour négliger les questions de cybersécurité, et cela braquera les feux des projecteurs sur la question.

Les modifications apportées récemment au CCC grâce à l'injection de ressources dans la cybersécurité étaient plus que nécessaires depuis longtemps. Le Canada a longtemps été un pionnier en matière de télécommunications, mais nous avons depuis pris du retard par rapport au reste du monde, et nous essayons simplement de suivre la vague d'innovations technologiques. Nous avons autrefois été le pays du meilleur fabricant de matériel de télécommunications dans le monde, Nortel. Nous l'avons perdu. Le Canada a aussi été l'un des premiers pays à se démarquer comme chef de file de la sécurité quantique pour les réseaux informatiques. Nous avons récemment perdu la plus grande partie de nos effectifs de recherche à ce sujet.

Le renforcement des systèmes d'information du gouvernement a beaucoup aidé à assurer leur accessibilité. Tout le monde peut consulter ses renseignements n'importe quand. Comme vous le savez, la principale cible d'exploitation informatique est toujours le maillon le plus faible, et à ce jour, il s'agit de la composante humaine, particulièrement lorsqu'il s'agit du citoyen moyen, chez lui ou ailleurs.

Le but est de nous assurer d'une économie forte qui utilise les TI. Il faut pour cela utiliser la technologie de l'information et offrir de l'éducation en personne plutôt qu'en ligne pour enseigner l'utilisation de la technologie. Presque tout le monde utilise la technologie aujourd'hui. Cette façon de faire rassure le citoyen ou l'utilisateur et lui permet d'obtenir une rétroaction immédiate.

Tous les jours, monsieur et madame Tout-le-monde utilisent des logiciels et du matériel incomplets commercialisés sans garantie qu'ils fonctionneront — ou qu'ils ne présenteront pas de faille. Quand on vend des voitures au Canada, elles viennent avec toutes sortes d'approbations, et Transports Canada régit la sûreté des véhicules. On peut acheter des lumières de Noël n'importe où au Canada, et elles porteront le sceau d'approbation de la CSA. Industrie Canada assure le respect des normes et leur sécurité. Mais qui exerce les mêmes contrôles et la même forme de validation sur le code informatique ou le matériel électronique?

Ces appareils, dont nous dépendons chaque jour et qui constituent ce qu'on appelle aussi l'Internet des objets, abondent autour de nous, sans aucune forme de certification de sécurité. Les pompes à insuline en sont un bon exemple. Bien que l'importation et la vente de ces appareils semblent réglementées par Santé Canada, qui vérifie le code qui constitue ces appareils destinés à garder les gens en vie? Sont-ils adéquats? Est-ce la même chose pour les stimulateurs cardiaques? Je pense que oui.

Qui vient certifier le code informatique des guichets automatiques pour que les citoyens canadiens aient accès à leur argent quand ils en ont besoin? Et les poupées intelligentes? Il paraît qu'elles sont vendues en Amérique du Nord même si elles ont été déclarées appareils d'espionnage illégaux en Allemagne en raison de problèmes de respect de la vie privée des enfants. Qui est censé protéger la vie privée de nos enfants contre ces appareils immoraux, si ce n'est le commissaire à la protection de la vie privée?

Le code constituant le matériel électronique et les logiciels devrait être soumis à l'examen d'un organisme gouvernemental indépendant comme la CSA, par exemple. Idéalement, cet organisme aurait son mot à dire sur les appareils essentiels qui sont mis en marché et imposerait des sanctions strictes à tous les fabricants de produits non conformes ou les interdirait simplement d'accès sur le marché.

D'ailleurs, nous sommes confrontés à une nouvelle dynamique économique, c'est-à-dire à l'utilisation de données biométriques dans le domaine des affaires. En juillet dernier, le centre Chinook, à Calgary, s'est fait prendre à intégrer la reconnaissance faciale à des caméras de surveillance cachées dans ses panneaux interactifs. Il compilait ainsi des renseignements sur la clientèle sans que les clients n'en soient avertis d'aucune façon.

Des plaintes ont été déposées devant les commissaires à la protection de la vie privée du Canada et de l'Alberta. On attend toujours les rapports des enquêtes déclenchées en août 2018. De plus, je viens tout juste d'aller aux Promenades Gatineau, où j'ai remarqué la présence de panneaux comparables, mais d'une autre entreprise. Il y a des caméras cachées dans ces panneaux, sans que rien n'avertisse la clientèle que des renseignements sont recueillis à son sujet.

C'est la même chose à la Place Laurier, où quatre magasins utilisent ouvertement la reconnaissance faciale dans l'objectif de recueillir de l'information sur les impressions des clients grâce à leurs caractéristiques biométriques. Ce genre de surveillance se fait déjà par téléphone cellulaire et bien sûr, c'est la même chose avec les cartes de fidélité que les consommateurs utilisent dans les magasins.

Il serait sûrement bénéfique pour tous que l'OPC accorde des autorisations, après un processus d'accréditation en bonne et due forme, aux organisations et aux entreprises qui souhaitent utiliser les technologies biométriques. Il nous en coûterait ainsi moins cher en enquêtes, et cela rassurerait les citoyens, qui verraient que le gouvernement protège leur vie privée.

● (1550)

[*Français*]

Est-il trop tard? Non, je crois qu'il est encore temps de bien faire.

Comme c'est le cas pour n'importe quel outil, nous devons prendre le temps de lire le manuel avant de nous en servir. Qui d'entre vous a déjà utilisé ou lu le manuel de Windows 10, de Windows 7 ou de Windows XP? Je crois que personne d'entre vous ne l'a fait. C'est un document très volumineux. Les gens en ont peur et se sauvent. C'est là que l'aide d'un tiers devient nécessaire. Les humains qui utilisent des machines ont encore besoin d'humains pour les former et les guider.

Votre étude éclairée de cette question sera certainement appréciée et permettra d'améliorer ce qui fonctionne moins bien. Cela créera l'élan nécessaire pour que les différents intervenants contribuent à une meilleure économie et nous aidera à redevenir les meneurs que nous sommes fondamentalement.

[*Traduction*]

Je suis maintenant prêt à répondre à vos questions dans les deux langues officielles.

Merci.

Le président: Merci, monsieur Waterhouse, madame Chang et monsieur Abma.

La première députée à vous poser des questions sera Mme Dabrusin.

Vous avez sept minutes, s'il vous plaît.

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

Ce que vous avez dit ressemble beaucoup à ce que nous avons entendu la semaine dernière. J'ai vraiment été frappée par les témoignages de la semaine dernière. L'institution financière y était décrite comme un véhicule blindé entre deux boîtes de carton, soit entre les humains des deux côtés. Je pense qu'on nous a dit qu'environ 60 % des problèmes de cybersécurité étaient attribuables à l'humain, soit aux utilisateurs. C'est ce qui ressortait.

Vous nous avez demandé si nous lisons les manuels. Je ne pense pas que nous lisions tous les manuels, et je ne suis pas sûre qu'il soit vraiment raisonnable de s'attendre à ce que chacun le fasse.

Vous avez mentionné l'idée d'une certification gouvernementale pour les utilisateurs, d'une part, mais il y a aussi tout le volet éducation, d'autre part.

J'ai lu l'un des bulletins de HackerOne. Vous avez publié quelque chose sur le hameçonnage, un quiz. Il est très difficile.

Voici ma question: si vous deviez nommer trois choses pour nous aider à éduquer la population (parce que cela semble être l'un des principaux problèmes), quelles seraient-elles?

Commençons par vous, monsieur Waterhouse.

M. Steve Waterhouse: J'offre de la formation un peu partout au pays. J'offre de nombreuses conférences sur la cybersécurité. J'enseigne la chose professionnellement, et je peux vous dire qu'il est plus que nécessaire que les gens s'arrêtent pour prendre le temps de lire sur ce qu'ils font.

On rit du fait que personne ne lit jamais les manuels. C'est vrai, mais ils sont souvent précédés de déclarations de responsabilités juridiques et d'obligations qui décourageraient quiconque d'aller plus loin dans sa lecture. Les gens se disent qu'ils vont se débrouiller. L'interface graphique pour les utilisateurs est tellement conviviale que les gens utilisent le logiciel intuitivement, mais n'utilisent peut-être que 5 ou 10 % de sa pleine capacité.

J'ai vu la transition qui s'est opérée quand les secrétaires sont passées de WordPerfect 5.2 à Microsoft Word. Elles ont dû suivre des cours, parce que c'étaient deux logiciels très différents. Elles maîtrisaient WordPerfect, alors que personne n'a jamais vraiment maîtrisé Word par la suite.

Mme Julie Dabrusin: Vous nous dites donc qu'il faut lire les manuels.

M. Steve Waterhouse: Les gens ne pouvaient pas lire le manuel, il était bien trop compliqué. C'était un document tellement complet qu'il aurait fait l'objet d'un cours d'une semaine. Les secrétaires ont suivi des cours d'une semaine, mais elles ont été divisées en trois groupes selon le degré de difficulté: débutant, avancé et expert. On parle de secrétaires qui étaient expertes d'un logiciel. Quand le nouveau logiciel est arrivé, elles étaient de niveau débutant. Cela réduit l'efficacité de l'effectif et ralentit l'économie, selon moi.

Supposons que la version 15 de Windows sort l'an prochain. Combien de personnes sauront comment il fonctionne? La courbe d'adaptation est très abrupte.

Mme Julie Dabrusin: Je m'adresserai rapidement aux gens de HackerOne. Le quiz que vous avez publié sur le hameçonnage portait sur Google ou quelque chose du genre, mais il était difficile.

Avez-vous des idées de choses simples... Les gens ne veulent pas être des boîtes de carton.

M. Jobert Abma (fondateur, HackerOne): J'aimerais préciser que le comportement des consommateurs s'est transformé radicalement au cours des dernières années. En effet, jusqu'à il y a cinq ans, nos données étaient conservées par de grandes organisations qui avaient de grandes équipes qui pouvaient aider les consommateurs à se protéger contre les fuites de données en protégeant leurs renseignements personnels. Je crois que le comportement des consommateurs a changé pour que nous devenions responsables de nos propres renseignements personnels et, comme M. Waterhouse l'a souligné, nous n'assumons pas cette responsabilité dans la mesure dans laquelle il est nécessaire de le faire aujourd'hui.

J'aimerais toutefois ajouter que je ne crois pas qu'il devrait incomber au consommateur de garantir la protection de ses renseignements personnels. En effet, je crois que les organisations devraient aider les consommateurs et aider les organisations elles-mêmes à protéger les consommateurs et leurs propres utilisateurs de ces fuites de données.

Comme je l'ai dit plus tôt, maintenant que les utilisateurs sont responsables de leurs données, il est important que nous leur fassions remplir des questionnaires comme le test d'hameçonnage dont vous parliez plus tôt, afin de leur faire comprendre certains des risques auxquels ils s'exposent lorsqu'ils entrent leurs données dans un système ou dans une organisation. C'est un problème que nous devons aborder dans le cas des consommateurs et des organismes qui ont des copies de ces données.

● (1555)

Mme Julie Dabrusin: J'aimerais continuer de m'adresser à votre groupe. Vous avez notamment parlé de l'importance de pouvoir signaler les vulnérabilités, c'est-à-dire qu'un pirate informatique qui découvre une vulnérabilité doit être en mesure de la signaler. Vous avez mentionné qu'il y avait un problème sur le plan juridique dans ces cas.

Le problème juridique est-il que ces gens seront accusés d'infractions criminelles? De quelles protections juridiques avons-nous besoin pour permettre aux pirates informatiques de nous aider?

Mme Deborah Chang: C'est une excellente question. Dans les années 1980, les États-Unis ont adopté la Computer Fraud and Abuse Act qui indique qu'on ne peut pas s'introduire dans les biens numériques d'une entreprise sans son autorisation. Cette loi n'a pas été mise à jour depuis son adoption. Je crois que le Canada a aussi une version de cette loi.

Nous incitons le Canada à adopter une loi qui viserait à encourager toutes les organisations qui ont des biens numériques à adapter un type de politique pour inviter les gens — et il n'est même pas nécessaire de les appeler des pirates informatiques — à signaler tout problème et vulnérabilité qu'ils découvrent. C'est seulement pour les inviter à effectuer ces signalements, en précisant ce qui est autorisé et ce qui ne l'est pas, et en décrivant les vulnérabilités qu'ils pourraient rechercher. Ensuite, il serait important que les organisations offrent une voie de communication à l'intérieur de ce processus et qu'elles soient en mesure de recevoir ces renseignements et d'obtenir les ressources pour régler le problème.

En général, nous incitons donc le gouvernement à adopter une loi qui encouragerait ce type de comportement.

Mme Julie Dabrusin: Il me reste 20 secondes.

Supposons qu'une personne signale à une entreprise qu'elle a trouvé un problème, une faille ou une vulnérabilité informatique. Ensuite, on se rend compte qu'une série d'entreprises utilisent exactement le même type de logiciel ou de programme. Ces logiciels ou programmes présentent tous la même vulnérabilité. Comment pouvons-nous communiquer ces renseignements liés à la vulnérabilité aux différentes entreprises et organisations?

Le président: Veuillez être très bref.

M. Jobert Abma: Il existe un processus de coordination des vulnérabilités dans lequel on collabore avec les fournisseurs pour coordonner la divulgation de ces vulnérabilités à d'autres organisations qui utilisent le même logiciel.

Le président: Merci, madame Dabrusin.

[*Français*]

Monsieur Paul-Hus, vous avez la parole pour sept minutes.

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

Bonjour à tous. Ma première question s'adresse à M. Abma.

En septembre dernier, M. Scott Jones, qui est le dirigeant désigné du Centre canadien pour la cybersécurité, a dit à notre comité être convaincu qu'il existait au Canada suffisamment de garanties pour nous permettre de faire face aux risques de piratage ou d'espionnage des télécommunications par la Chine. Dans sa déclaration, M. Jones a conclu qu'il n'était pas nécessaire de suivre nos alliés du Groupe des cinq pour interdire une entreprise de nos réseaux 5G.

Pouvez-vous nous parler de la force du cyberespace canadien?

[*Traduction*]

M. Jobert Abma: À ce jour, aucun gouvernement n'est immunisé contre les menaces liées à la cybersécurité. Les États-Unis ont certaines des pratiques en matière de cybersécurité les plus sophistiquées au monde — tout comme le Canada, comme M. Waterhouse l'a souligné. C'est aussi le pays où s'installent les entreprises qui ont les pratiques en matière de sécurité les plus évoluées dans le monde. Mais même dans ces conditions, le piratage informatique peut se produire. Il faut donc toujours faire mieux.

L'Internet est un système très complexe auquel un grand nombre de gens contribuent. Tous ses éléments sont liés entre eux. Les systèmes et les réseaux changent ou contiennent des centaines de milliers de logiciels ou de composantes et des milliers de lignes de code. Chaque fois qu'un code est mis à jour, ce qui peut se produire plusieurs fois par jour, de nouvelles vulnérabilités peuvent apparaître. Il y aura toujours des variables inconnues et la seule façon de découvrir ces variables inconnues est d'inviter de bons pirates informatiques à tester les systèmes. Même dans le cas de systèmes dont la sécurité a été éprouvée, cela peut changer subitement en raison d'un changement interne ou externe, ce qui peut entraîner la création de vulnérabilités.

● (1600)

[*Français*]

M. Pierre Paul-Hus: J'aimerais savoir si, du côté américain, vos équipes et vos pirates informatiques sont prêts à gérer les menaces touchant les réseaux 5G.

[*Traduction*]

M. Jobert Abma: Les bons pirates informatiques se mesurent à de nouvelles technologies tous les jours. Ils devront se familiariser avec les nouvelles technologies afin d'être en mesure de trouver les vulnérabilités liées à la sécurité dans ces technologies ou dans les éléments qui sont construits pour des technologies comme 5G. Notre clientèle diversifiée offre de nombreuses occasions qui incitent les pirates informatiques à s'attaquer à ces nouvelles technologies. À mesure que la technologie 5G est utilisée à plus grande échelle, nous croyons qu'un plus grand nombre de personnes seront en mesure de vérifier la sécurité de ces éléments.

Actuellement, plusieurs clients de HackerOne lancent des composantes liées à la technologie 5G et exposent cette technologie à certains pirates informatiques, et nous croyons que c'est une bonne façon de découvrir certaines des vulnérabilités liées à la sécurité que nous ne connaissons pas encore ou qui sont inconnues aux États-Unis.

[*Français*]

M. Pierre Paul-Hus: Votre compagnie, HackerOne, a établi des relations avec des clients comme le Pentagone ou le département d'État américain. Comment avez-vous réussi à établir une relation de confiance avec ces clients, et comment pourrions-nous le faire aussi? Est-ce une pratique qui devrait être adoptée par le Canada?

[*Traduction*]

M. Jobert Abma: Tous les pirates informatiques qui ont participé aux programmes du département de la Défense des États-Unis ont été minutieusement choisis par le département de la Défense et par HackerOne, en raison de notre expertise et de nos antécédents. Nous complétons ce que nos consommateurs et le gouvernement accomplissent déjà. Nous avons fait nos preuves dans le domaine de l'amélioration de la sécurité à l'aide des pirates informatiques, et notre collaboration avec le gouvernement et le secteur privé renforce notre mission, qui est d'aider le monde à rendre Internet plus sécuritaire.

À ce jour, plus de 5 000 vulnérabilités ont été découvertes dans les systèmes du département de la Défense des États-Unis, et la majorité d'entre elles ont été signalées au département sans incitatif pécuniaire. Nous recommandons à tous les gouvernements de la planète de mettre en oeuvre un programme ou un processus de divulgation des vulnérabilités, afin d'assurer une collaboration avec la communauté des pirates informatiques fondée sur le principe « si vous voyez quelque chose de suspect, signalez-le ».

[*Français*]

M. Pierre Paul-Hus: Merci. Si cela intéresse le Comité, j'ai une photo de votre brochure montrant des pirates qui travaillent pour le département de la Défense. Ces gens-là ne veulent pas porter l'uniforme, mais ils sont les meilleurs.

J'ai maintenant une question pour vous, monsieur Waterhouse. Les institutions financières en font-elles assez actuellement pour protéger les citoyens au quotidien?

M. Steve Waterhouse: Les institutions financières répondent « oui ». De mon point de vue de client d'une institution financière, par contre, je réponds « non ». Souvent, le client se présente à son institution financière, laquelle lui impose des outils dont elle certifie qu'ils sont sécuritaires. Le client retourne à la maison ou au travail avec cet outil d'accès au système ou cette application, mais ne sait vraiment pas comment cela fonctionne. Tout le risque lui retombe sur les épaules: s'il commet une erreur, c'est sa faute et pas celle de l'institution financière, qui le prouve facilement.

C'est cela qui est dommage. Je faisais un peu l'apologie du besoin de connaître son système d'exploitation. Le prochain téléphone Android suffira-t-il à la tâche? Les gens ne sauront pas plus comment l'utiliser. La formation va se concentrer sur une seule application et les gens devront s'adapter lorsque l'application va changer d'apparence et de convivialité. C'est ce que nous impose le marché depuis une trentaine d'années: dès que l'apparence d'une application change, il faut déployer des efforts pour s'adapter. Il n'y a pas de mise à jour, et personne ne nous prend par la main pour nous aider à nous familiariser avec la nouvelle application.

● (1605)

M. Pierre Paul-Hus: D'accord.

[*Traduction*]

Le président: Il vous reste 20 secondes.

[*Français*]

M. Pierre Paul-Hus: Quel est le meilleur moyen de les sensibiliser?

M. Steve Waterhouse: Les institutions financières devraient s'investir un peu plus dans la formation du citoyen ou du client. Les séances de formation ne devraient pas se faire au moyen de vidéos sur Internet, que l'on consomme distraitement.

Ce devrait être de la formation interactive, pour permettre de savoir si le client a bien compris. Lorsqu'on fait une formation avec quelqu'un à l'écran, surtout en différé, le client peut appuyer sur le bouton « Pause » puis recommencer, ce qui est fantastique. Sinon, le client peut aussi décider d'appuyer sur le bouton « Jouer » et d'aller faire autre chose ailleurs pendant ce temps. On ne saura jamais s'il a bien compris l'information. La case sera cochée, mais on ne saura pas si la matière a bien été assimilée.

Le président: Merci, monsieur Paul-Hus.

Monsieur Dubé, vous avez sept minutes.

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

[*Traduction*]

J'aimerais poser une question aux représentants de HackerOne, étant donné que l'exemple que j'utiliserai se fonde sur la situation actuelle aux États-Unis.

La NSA américaine a mis en oeuvre ce qu'elle appelle un « vulnerabilities equities process », c'est-à-dire un processus pour déterminer si la vulnérabilité doit être divulguée. Il y a probablement environ un an, un journaliste m'a posé des questions sur ce processus, car notre organisme équivalent — ce n'est pas vraiment un organisme équivalent, car ce n'est jamais exactement la même chose —, le Centre de la sécurité des télécommunications, le CST, n'a pas le même type de processus transparent.

J'aimerais que vous nous précisiez si ce processus — à votre avis, étant donné les travaux que vous menez — a réussi à accroître la transparence lorsque les organismes eux-mêmes découvrent des vulnérabilités dans un logiciel qui pourrait potentiellement être utilisé pour recueillir toutes sortes de renseignements sur les gens.

M. Jobert Abma: Oui, je serai heureux de répondre à cette question.

Le gouvernement américain a dépensé beaucoup d'argent et de temps pour assurer la sécurité de ses propres systèmes. Nos données révèlent qu'après l'établissement d'un processus transparent pour travailler avec la communauté des pirates informatiques, plus de 5 000 vulnérabilités liées à la sécurité ont été cernées, et on a offert des centaines de milliers de dollars pour encourager ces pirates informatiques à examiner davantage ces systèmes.

Le nombre de vulnérabilités découvertes par la communauté des pirates informatiques est beaucoup plus élevé que le nombre de vulnérabilités cernées par le gouvernement américain. Le grand nombre de vulnérabilités démontre que la collaboration avec la communauté des pirates informatiques représente l'approche appropriée pour découvrir d'autres vulnérabilités liées à la sécurité.

M. Matthew Dubé: C'est un point intéressant, car cela m'amène à une autre question que je souhaitais poser — mais permettez-moi d'abord de revenir un peu en arrière. Si un organisme d'application de la loi souhaite déverrouiller, par exemple, un iPhone pour avoir accès à l'information qu'il contient, il existe manifestement un processus pour qu'il puisse le faire après avoir obtenu un mandat. Ces processus varient évidemment dans chacun de nos pays, mais je crois que leur fondement est assez semblable pour que nous puissions en discuter. Voici donc ma question. Si un pirate informatique souhaite agir à titre de pirate éthique, il peut croire que c'est une bonne chose de fournir des renseignements au gouvernement, mais ces renseignements ne seront pas nécessairement communiqués à l'entreprise concernée par la suite et des gens seront vulnérables, car l'organisme en question pourrait avoir intérêt à conserver cette vulnérabilité. Pensez-vous qu'on devrait adopter un type de loi ou de règlement qui appliquerait aux organismes de sécurité nationale le même juste équilibre des pouvoirs qu'on applique à la police lorsqu'elle obtient un mandat pour déverrouiller un téléphone? Ces lois et règlements indiqueraient qu'un organisme qui souhaite utiliser une vulnérabilité doit se soumettre au même processus auquel se soumettent les organismes de protection de la loi, afin de protéger la vie privée des gens.

M. Jobert Abma: C'est un dilemme éthique qu'il est très important d'aborder, selon moi. Le problème que nous avons observé jusqu'ici, c'est que les gouvernements achètent des vulnérabilités de jour zéro, c'est-à-dire des vulnérabilités qui ne sont pas connues du fournisseur qui est là pour les corriger. Elles sont utilisées pendant une guerre pour extraire des renseignements qui sont actuellement inconnus. En ne divulguant pas cela aux fournisseurs, on fait également courir un risque aux consommateurs ou aux citoyens.

Nous croyons que les vulnérabilités de jour zéro devraient être signalées au fournisseur dans tous les cas, mais nous abordons cet enjeu sous un angle différent. Nous abordons cet enjeu en ayant recours à la communauté des pirates informatiques pour découvrir les mêmes vulnérabilités qui ont été découvertes par les gouvernements ou les criminels, et ces vulnérabilités seront ensuite directement divulguées aux fournisseurs. C'est notre façon de veiller à ce que les fournisseurs soient au courant de ces vulnérabilités.

À mon avis, il serait formidable que le gouvernement adopte également une telle loi, car je ne crois pas que cela justifie le risque couru par vos citoyens. Cependant, je crois que nous sommes loin de l'adoption d'une telle loi.

● (1610)

M. Matthew Dubé: Je vous suis reconnaissant de votre réponse.

[*Français*]

Ma dernière question s'adresse également à vous, monsieur Waterhouse.

[*Traduction*]

C'est la question du rôle essentiellement joué par les médias et le fait que certaines de ces vulnérabilités sont signalées. J'ai un exemple en tête. Je ne me souviens plus si j'ai vu cela aux nouvelles ou si quelqu'un m'a raconté cette histoire, et je pourrais donc me tromper, mais la semaine dernière, lorsque la vulnérabilité liée à FaceTime sur les iPhone et les iPad a été découverte, l'entreprise Apple a demandé à la personne qui avait involontairement découvert cette vulnérabilité de démontrer son processus — comme si cette personne cherchait une vulnérabilité sans être un pirate informatique. Je suis donc préoccupé au sujet des cas dans lesquels des vulnérabilités sont découvertes par accident et signalées ensuite dans les médias. Quelles sont les répercussions sur la vulnérabilité elle-même et sur les efforts en vue de tenter de la corriger?

[*Français*]

Monsieur Waterhouse, vous pouvez émettre des commentaires à ce sujet.

[*Traduction*]

M. Steve Waterhouse: Cela continuera pendant le reste de notre vie. En effet, les logiciels sont tout à fait incomplets. Actuellement, nous avons des milliards de lignes de code dans toutes sortes d'applications, surtout dans des systèmes d'exploitation, et il est presque impossible de... Puisque la concurrence est féroce sur le marché, les entreprises distribuent tout simplement leurs logiciels incomplets et tentent ensuite de corriger les erreurs à mesure qu'elles apparaissent. C'est l'une des raisons pour lesquelles nous avons ces types de découvertes de temps en temps.

Dans le cadre d'une analyse technique, les intervenants de l'entreprise se disent que personne ne pensera à faire cela. Mais vous savez quoi? Dans le monde réel, les gens tentent de trouver ce qui les intéresse. Et, oui, ils trouvent ces vulnérabilités par accident, comme nous les appelons aujourd'hui. La divulgation de ces vulnérabilités devrait-elle être obligatoire? Bien sûr.

Le jeune et ses parents ont divulgué la vulnérabilité en toute légalité. Ils ne souhaitaient pas exploiter la situation, ils tenaient simplement à signaler la vulnérabilité, mais même l'entreprise a refusé de les écouter.

Je suis certainement d'accord avec vous sur cette question. Il devrait exister une loi qui obligerait les entreprises à écouter toute personne qui leur fournit des renseignements et à prendre rapidement les mesures nécessaires pour corriger la situation. Si l'entreprise ne fait rien, elle devrait être tenue de payer une amende.

M. Matthew Dubé: Je crois qu'il me reste 30 secondes si vous souhaitez formuler des commentaires.

Mme Deborah Chang: J'aimerais formuler des commentaires. Je crois que la protection de la vie privée est un élément fondamental de cette discussion.

Lorsque j'ai lu au sujet de cette situation... À notre avis, le droit à la vie privée est un droit fondamental, et la protection des données personnelles est aussi un droit fondamental. Les entreprises devraient être fortement encouragées à protéger ces droits. Dans ce cas-ci, je crois que la mère a communiqué avec Apple à quelques reprises. Elle protégeait son droit, le droit de son fils et le droit de sa famille. Le fait qu'il n'y ait aucune politique de divulgation de vulnérabilités ou processus en place pour gérer ces situations représente une violation des droits liés à la protection de la vie privée.

[*Français*]

Le président: Merci, monsieur Dubé.

Monsieur Picard, vous avez la parole pour sept minutes.

[*Traduction*]

M. Michel Picard (Montarville, Lib.): Ma question s'adresse aux représentants de HackerOne. Lorsque vous présentez votre rapport sur les vulnérabilités aux fournisseurs de services financiers, quel type de rétroaction obtenez-vous à la suite de vos recommandations? Les mettent-ils en oeuvre immédiatement ou évaluent-ils les coûts de la mise en oeuvre comparativement aux coûts de courir le risque de ne pas les mettre en oeuvre?

M. Jobert Abma: Au bout du compte, un organisme mature sur le plan de la sécurité est un organisme au sein duquel tout risque ou vulnérabilité découverte, peu importe sa source, fait l'objet des investissements nécessaires pour protéger l'organisme contre la menace signalée.

Nous avons observé que de nombreux organismes, y compris des organismes financiers, avaient mis en oeuvre différents moyens de défense fondés sur les vulnérabilités qui avaient été signalées, afin d'éliminer des catégories entières de vulnérabilités ou de protéger les clients contre les menaces liées à la sécurité. Par exemple, l'authentification à deux facteurs est souvent utilisée pour ouvrir une session dans un compte bancaire.

Il est habituellement assez facile pour les entreprises de régler les vulnérabilités liées à la sécurité les plus communes, mais surtout, avec les données que nous avons recueillies, nous pouvons aider un organisme à accorder la priorité aux moyens de défense en profondeur, afin de mieux protéger cet organisme à long terme.

● (1615)

[*Français*]

M. Michel Picard: Monsieur Waterhouse, concernant les produits utilisés par les services financiers, j'aimerais savoir si les points vulnérables rapportés à leur sujet sont pratiquement de niveau débutant, sans importance, ou si les logiciels sont maintenant à ce point sophistiqués qu'il reste malgré tout quelques points vulnérables exigeant encore un niveau de précision ou d'expertise extrêmement élevé.

Dans quelle position sommes-nous présentement?

M. Steve Waterhouse: Monsieur Picard, les deux extrêmes du spectre sont à l'oeuvre. La semaine dernière, par exemple, des renseignements personnels des 500 millions de clients de la plus grande banque de l'Inde ont été révélés au grand public parce que le serveur contenant ces renseignements n'était pas sécurisé et qu'il n'y avait aucun mot de passe. À l'intérieur du réseau de cette mégabanque, un système était tout simplement vulnérable. Il s'agissait là d'une erreur de base, que j'appellerais pour ma part une erreur de débutant.

Aujourd'hui, les institutions financières canadiennes utilisent le meilleur équipement qu'elles peuvent trouver. Elles ont suffisamment de ressources pour se le permettre. Il reste que ce sont des produits commerciaux offerts à n'importe quelle compagnie dans le monde et qui comportent le même genre de vulnérabilité. Il faut donc des équipes capables de faire des vérifications et des contre-vérifications afin de déterminer si l'installation est toujours bonne et valide, et ce, de manière constante, selon un cycle perpétuel. Or la majorité des PME font faire des installations, se disent qu'elles sont munies d'un pare-feu, croient qu'elles sont à l'abri et ne s'inquiètent plus. Malheureusement, certains de ces équipements sont vulnérables. Il faut donc constamment faire des vérifications.

[*Traduction*]

M. Michel Picard: En ce qui concerne la stratégie, un fournisseur de services financiers peut décider de diviser ses données le plus possible, afin de compliquer l'agrégation des données dans le but d'en tirer des renseignements. Mais aussi, dans le cas d'un système bancaire ouvert, il peut centraliser toutes ses données sur un seul serveur pour optimiser le rendement et l'efficacité. Quelle stratégie semble la plus appropriée? Ces jours-ci, nous discutons de ces deux stratégies.

M. Jobert Abma: L'un des problèmes que nous avons observés, surtout dans les cas les plus récents de fuites de données, c'est que la centralisation des données est en train de devenir un problème. L'entreprise a plus de facilité à se protéger contre certains risques, car elle a seulement une composante à défendre. Toutefois, le problème, c'est que lorsque les choses tournent mal, que ce soit à cause d'une mauvaise configuration effectuée par l'organisme — comme cela s'est produit en Inde — ou à cause d'une négligence ou d'une vulnérabilité dans un logiciel fourni par une tierce partie, les conséquences sont habituellement trop importantes pour être contrôlées. Par contre, la décentralisation est beaucoup plus difficile à entretenir. En effet, il y a beaucoup plus d'éléments en mouvement, mais du point de vue de la protection des données, il semble que ce soit la bonne méthode ou la bonne stratégie à adopter.

Lorsque vous parlez des renseignements qui peuvent être tirés d'un système central, je vous répondrais qu'on peut accomplir la même chose avec des systèmes multiples et avec des systèmes décentralisés, mais au lieu d'utiliser les données, on extrapole des données ou des renseignements de ces données et on les utilise pour formuler des recommandations ou pour mener l'analyse de données requise. De plus, de nombreux organismes commencent à utiliser l'infonuagique, ce qui revient essentiellement au même problème auquel font face les grands organismes, car ils ont centralisé une grande partie de leurs données. Nous observons une augmentation du nombre de fuites, car les gens ne connaissent pas les conséquences qui peuvent suivre l'entrée de données dans un système qu'ils ne comprennent pas bien. Cela revient également au point que faisait valoir M. Waterhouse selon lequel les consommateurs ne lisent pas les manuels, mais parfois, même les organismes eux-mêmes ne comprennent pas la menace à laquelle ils s'exposent en adoptant de nouvelles stratégies.

M. Michel Picard: Il me reste seulement une minute.

[*Français*]

Nous avons des logiciels qui sont vulnérables et nous commençons à considérer l'utilisation de l'intelligence artificielle pour nous aider à contrôler ce que ces mêmes logiciels ne font pas bien.

Devons-nous mettre notre confiance dans un système de façon aveugle? L'intelligence artificielle est quand même programmée par des humains.

M. Steve Waterhouse: Monsieur Picard, c'est le même concept pour les logiciels d'aujourd'hui. Ce sont des programmeurs qui produisent des systèmes d'exploitation incomplets auxquels sont attachés des logiciels pour faire du traitement de l'information qui sont eux-mêmes incomplets.

Vous me demandez si l'intelligence artificielle sera meilleure. On me confie qu'il existe des mesures de sécurité qui se veulent avant-gardistes pour prévenir ce genre de comportement. Toutefois, je ne crois pas que ces nouveaux logiciels soient à l'abri de toute faille.

● (1620)

[*Traduction*]

M. Michel Picard: Une dernière intervention à ce sujet, HackerOne?

M. Jobert Abma: D'après moi, l'intelligence artificielle est une technologie très importante, que nous devons répandre et utiliser le plus possible. En fin de compte, nous croyons que là où il y a des humains, il survient des erreurs. L'intelligence artificielle ne nous protégera pas davantage contre ces menaces. Quand on peut s'en servir pour mieux se protéger, c'est la chose à faire, mais elle n'offre pas une solution ou une protection permanentes contre les menaces pour la sécurité.

Le président: Merci, monsieur Picard.

Monsieur Motz, vous disposez de cinq minutes.

Oh! Attendez. Il y a confusion.

Monsieur Paul-Hus.

[*Français*]

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

Je veux remercier nos invités d'être ici, cependant j'aimerais prendre un peu de temps pour aborder la situation qui existe actuellement au Comité permanent de la citoyenneté et de l'immigration. Ma collègue vient de déposer une motion. J'aimerais donc...

[*Traduction*]

Le président: Pardon, mais ça ne peut pas attendre la fin de la séance?

[*Français*]

M. Pierre Paul-Hus: Je vais procéder rapidement, monsieur le président.

[*Traduction*]

Le président: Procéder rapidement pour une motion, ça n'existe pas.

[*Français*]

M. Pierre Paul-Hus: Je vais lire ma motion rapidement et le Comité pourra en décider.

[*Traduction*]

Le président: D'accord. Personnellement, je préférerais la fin de la séance, mais si vous insistez, je dois le défalquer de votre temps, ce qui est regrettable, parce que j'aime bien les questions de M. Motz. D'accord.

[*Français*]

M. Pierre Paul-Hus: Moi aussi, c'est ce que j'aurais préféré, mais je risque de ne pas être disponible à 16 h 30. Je vais donc continuer, monsieur le président. Je suis désolé.

Je vais lire ma motion, à l'intention de mes collègues:

> Que, conformément aux articles 108(1)a) et 108(2) du Règlement, le Comité se réunisse conjointement avec le Comité permanent de la citoyenneté et de l'immigration pour étudier si des lacunes ont été créées dans le processus de vérification de sécurité des personnes qui sont entrées au Canada ces trois dernières années, aux points d'entrée officiels et entre les points d'entrée, pour identifier les causes et les effets de ces lacunes et pour proposer des solutions potentielles; que des responsables ministériels et les ministres de l'Immigration, des Réfugiés et de la Citoyenneté ainsi que de la Sécurité publique et de la Protection civile soient présents à au moins une rencontre; que des responsables et des représentants élus du Congrès et du Sénat des États-Unis soient invités à être présents; que ces rencontres aient lieu avant le vendredi 1er mars 2019; que le Comité présente ses conclusions à la Chambre; et que, conformément à l'article 109 du Règlement, le gouvernement présente une réponse exhaustive aux conclusions du Comité.

[*Traduction*]

Le président: Bien.

L'avis de la motion est dans les règles, comme le dépôt de la motion. J'aurais préféré un autre moment, mais c'est comme ça. Je suppose que quelqu'un a des observations.

Madame Damoff. Encore une fois, toutes nos excuses aux témoins.

Mme Pam Damoff (Oakville-Nord—Burlington, Lib.): Merci, monsieur le président. Moi aussi, je présente mes excuses aux témoins pour le temps qu'on leur enlève.

Je suis déçue, mais pourquoi m'étonner. Cette motion est caractéristique de l'évolution du style conservateur à la Harper-Scheer en politique. Il s'agit d'effrayer les Canadiens et, encore une fois, en choisissant les nouveaux venus comme boucs émissaires.

[*Français*]

M. Pierre Paul-Hus: Monsieur le président, j'aimerais intervenir.

[*Traduction*]

Le président: Oui?

[*Français*]

M. Pierre Paul-Hus: J'ai tout simplement déposé une motion selon les règles de la Chambre des communes. Ce n'est pas approprié de la part de ma collègue de commencer à faire de la politique à la table, ici.

[*Traduction*]

Le président: Si nous pouvions faire taire l'esprit de parti sur une motion partisane, la présidence serait beaucoup plus heureuse.

Madame Damoff, vos observations sur la motion, s'il vous plaît.

Mme Pam Damoff: En fait, monsieur le président, les Canadiens peuvent et devraient se sentir en sécurité, sachant que notre frontière est sûre et que nous possédons un système de filtrage de sécurité efficace. Jamais leur sécurité n'a été et ne sera compromise. Nous n'appuierons donc pas cette motion.

Le président: D'autres interventions? Il ne semble pas. Je mets donc la motion aux voix.

(La motion est rejetée.)

Le président: Monsieur Motz, il vous reste deux minutes.

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Je vous remercie, monsieur le président.

Ma première question est pour HackerOne. Vous avez essentiellement dominé le secteur du piratage éthique aux États-Unis. Avez-vous des idées de pratiques exemplaires pour le Canada et de moyens à employer ici pour se doter de ce genre de réputation avec le volet privé du piratage éthique dans notre pays?

M. Jobert Abma: Nous croyons que la sécurité avec le concours de pirates informatiques est la clé d'un Internet plus sûr grâce à tous. Le recours aux pirates informatiques bien intentionnés est l'un des éléments d'une organisation chargée de la sécurité qui a atteint la maturité. HackerOne diffuse des données pour aider les entreprises à se doter d'une telle organisation et à assujettir les éléments à améliorer à un ordre de priorité. Nous encourageons tout le monde à au moins établir une politique de divulgation des vulnérabilités pour, grâce à la collaboration avec le milieu des pirates informatiques, découvrir ce qu'il y a de plus inconnu dans leurs systèmes, les vulnérabilités de leur sécurité.

● (1625)

M. Glen Motz: Merci.

Dans le peu de temps que j'ai, je tiens à demander à M. Waterhouse quelles pourraient être les répercussions d'une attaque par impulsion électromagnétique au Canada sur les institutions financières. De quoi s'agit-il, et quelles sont nos vulnérabilités sur ce plan?

M. Steve Waterhouse: Bien sûr. C'est un fait établi que des États-nations s'affairent à mettre au point une telle arme.

Cette arme grillera toute composante électronique, sinon l'ensemble du réseau électrique. Notre société reviendra 100 ans en arrière. C'est arrivé à quelques reprises. Il y a eu la tempête solaire des années 1850. En 1989, une impulsion électromagnétique d'origine solaire a complètement paralysé le réseau d'Hydro-Québec pendant plus de huit heures.

Nous sommes à même de constater l'évolution de sa mise au point, particulièrement aux États-Unis. Personne ne s'en cache, parce que ce ne sont pas des armes cinétiques classiques létales. Elles ne font que neutraliser l'environnement électrique. Cela étant dit, les sinistrés privés d'électricité peuvent devenir fous furieux. J'en ai été le témoin pendant la tempête de verglas de 1998, qui a privé toute la population pendant 22 jours au moins d'électricité, de liquidités et ainsi de suite.

C'est donc une menace directe contre notre mode de vie contre laquelle très peu d'organisations sont prémunies ou préparées.

Le président: Merci, messieurs.

Madame Sahota.

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

Tous peuvent répondre.

Avant tout, je suis réellement fascinée par ce scénario de chasse au bogue. Je sais que cela a déjà été soulevé, que vous encouragez les organisations, dans votre témoignage, à y recourir et peut-être les gouvernements aussi. Je pense que c'est établi que le gouvernement canadien n'y a pas recours, mais des entreprises canadiennes le font. Shopify en est une sur qui j'ai lu, et diverses entreprises y ont eu recours.

Pourriez-vous expliquer un peu plus le facteur de confiance et de quelle manière une entreprise encourage la chasse au bogue, c'est-à-dire par de plus en plus de pirates informatiques, que leurs buts ou leurs actions soient légitimes ou non, pour exposer leurs vulnérabilités pour se protéger et protéger les renseignements personnels. Comment pouvez-vous en être sûr? Comment pouvez-vous le vérifier? À l'embauche d'un employé, vous vérifiez ses antécédents et vous lui faites confiance en raison de la relation établie avec lui. Des inconnus pourraient accéder à vos systèmes et peut-être aux renseignements qui s'y trouvent. Même vous, HackerOne, comment savez-vous que vos pirates vous communiquent tous les renseignements qu'ils ont trouvés et qu'ils ne les utilisent pas à d'autres fins?

M. Jobert Abma: Je peux répondre. Merci pour votre question.

Nous croyons en la force des nombres. Ça signifie que les personnes bien intentionnées sont majoritaires. Manifestement, il y en aura toujours de mal intentionnées, mais HackerOne ne permet pas à ces criminels d'agir par son intermédiaire. S'ils étaient mal intentionnés, ils auraient déjà agi. Ce que nous ouvrons, c'est la possibilité, pour des personnes bien intentionnées, de se servir d'HackerOne pour faire de la recherche pour certaines des raisons que ma collègue Debbie a exposées.

Mme Ruby Sahota: Je le comprends. Bien sûr, certains pourraient rechercher et obtenir ces renseignements eux-mêmes, de leur propre initiative, mais, par ce scénario, ne les encouragez-vous pas essentiellement à le faire? Vous les encouragez à accéder à la base de données d'une organisation. Comment vous assurez-vous que les gens qui travaillaient pour HackerOne sont crédibles, dignes de confiance?

● (1630)

M. Jobert Abma: Tous nos collaborateurs doivent nous communiquer des renseignements. Par exemple, nous avons besoin de renseignements d'ordre fiscal pour les rémunérer. Certains de nos clients exigent la vérification de leurs antécédents. À l'instar du ministère de la Défense des États-Unis, nous faisons ces vérifications partout dans le monde pour établir leur identité avant de leur donner l'accès à certains systèmes. En fin de compte, comme la plupart des systèmes des organisations sont accessibles au public, n'importe quel internaute peut déjà les attaquer.

Pour revenir à ce que je disais tout à l'heure, pour chaque personne mal intentionnée, il y a des dizaines et des milliers bien intentionnées. Si nous les encourageons autant que les criminels à trouver les vulnérabilités, nous croyons que pour chaque personne étrangère à HackerOne qui trouve une vulnérabilité sans la divulguer, un nombre suffisant trouvera exactement la même et la signalera directement au distributeur.

Mme Ruby Sahota: Vous avez effleuré l'idée d'encourager l'adoption d'une loi qui autoriserait cette mesure. Je suppose que c'est parce que vous estimez que certains ne se sentent pas encouragés par les vieilles lois en vigueur. Comment l'expliqueriez-vous? À quoi cette loi ressemblerait-elle et comment la soutiendrait-on?

Mme Deborah Chang: Simplement quelques détails pour que vous sachiez, nous avons fait une étude chez nos propres pirates. Le quart d'entre eux a trouvé à un certain moment une vulnérabilité mais ne l'a pas signalée, faute, pour l'entreprise, de posséder une voie de communication pour en permettre la divulgation. Comme Jobert le disait, ils sont indéniablement nombreux les pirates, un sur quatre, dans notre bassin, qui veulent faire plus, mais ne le peuvent pas sans une sorte de sauf-conduit.

Nous collaborerons volontiers avec l'éventuel législateur, mais la loi n'autoriserait généralement qu'une politique de divulgation des vulnérabilités. La loi autorisant le piratage du ministère de la Sécurité intérieure de 2018 vient d'être adoptée en janvier et ceux qui ont besoin du concours de ce ministère pour se doter d'une politique de divulgation des vulnérabilités à la faveur d'un programme pilote de chasse au bogue... Et le libellé — je tiens à préciser que le texte tient en six ou sept pages — autorise donc la création d'un programme de communication volontaire de renseignements dans une telle opération pilote dans cet organisme. Plus tôt cette année, le Congrès a déposé le projet de loi sur le piratage du Département d'État. Il existe donc des textes, mais nous pouvons certainement aider à en rédiger.

Mme Ruby Sahota: Merci.

Le président: Monsieur Motz, vous disposez de cinq minutes.

M. Glen Motz: Monsieur Waterhouse, revenons à notre question antérieure, sur l'attaque par impulsion électromagnétique.

D'après vous, où croyez-vous que notre pays se situe sur l'échelle décrivant notre degré de préparation et notre capacité de réagir, non seulement à une attaque contre nos réseaux de transport d'électricité, mais contre toute autre cible possible?

M. Steve Waterhouse: J'ai été témoin de l'évolution de la guerre froide et des préparatifs auxquels elle a donné lieu. En effet, pendant les années 1970 et 1980, les systèmes informatiques des forces armées de tous les pays étaient vulnérables à ce genre de menaces. Les centres de traitement des données étaient construits de manière à résister à de telles attaques. Au fil du temps et dès la fin de la guerre froide, on a considéré que ces précautions étaient trop coûteuses. Nous — je veux dire différentes entreprises... Nous avons donc commencé à nous procurer des ordinateurs du commerce prêts à l'emploi. C'est ce qui explique la vulnérabilité d'aujourd'hui.

À moins de se trouver dans un local prévu pour résister à une attaque par impulsion électromagnétique, les systèmes sont vulnérables. L'infrastructure des télécommunications est vulnérable; vulnérables aussi les voitures dont le fonctionnement doit beaucoup à l'électronique.

Nous sommes donc, je regrette de le dire, condamnés si une bombe explose à 400 kilomètres au-dessus de l'Amérique du Nord. Ce sera la chute du continent, et nous retournerons 100 ans en arrière, en nous chauffant au bois et en communiquant par des signaux de fumée.

Des députés: Oh, oh!

Le président: ... et par pigeons voyageurs.

● (1635)

M. Glen Motz: ... effectivement.

D'après certaines questions de mes collègues et des observations de HackerOne, nous pouvons faire plus pour augmenter dans notre pays la participation des experts en la matière dans cette industrie particulière.

D'après nous, que peut faire le gouvernement pour accroître nos capacités de nous en occuper, d'après le point de vue d'un pirate éthique?

M. Steve Waterhouse: Je ne suis pas sûr de comprendre.

M. Glen Motz: Notre pays possède une capacité limitée, un nombre limité de spécialistes en la matière pour suivre les États-Unis, compte tenu du nombre de pirates éthiques qu'on y trouve là-bas.

D'après vous, comment le gouvernement peut-il mieux nous préparer?

M. Steve Waterhouse: Actuellement, des organismes comme le Centre de sécurité des télécommunications et le centre de cybersécurité lancent des initiatives pour favoriser des festivals ou des marathons de programmation ou de codage dans tout le pays ou des conférences à cette fin.

Par exemple, j'ai assisté à celui de Québec, en novembre, qui, depuis 10 ans, est parrainé par le Centre de sécurité des télécommunications. Ces manifestations permettent d'avoir un aperçu de l'actualité grâce aux pirates informatiques les plus réputés et les plus à la pointe de leur domaine, qui viennent montrer leur savoir-faire en employant tous les moyens techniques dont ils disposent. On peut puiser dans ce bassin pour recruter l'élite, la crème. Il y a la Conférence sur la sécurité de la région de l'Atlantique, ou « AtlSecCon », tandis qu'il s'en tient d'autres dans le pays, notamment une en Colombie-Britannique. Ainsi, les organismes peuvent activement se tenir au courant au fur et à mesure de l'évolution.

Je crois que le Centre canadien pour la cybersécurité étant ce qu'il est aujourd'hui — je veux dire qu'il existe —, il s'investira davantage. J'y vois un signe positif: le fait de pouvoir compter sur la présence constante d'un organisme de l'État pour faire connaître à la communauté que des gens sont...

À Québec, au marathon de codage, la ministre Gould a annoncé que le Canada voulait compter sur l'aide d'un plus grand nombre de pirates informatiques pour neutraliser les ingérences dans la prochaine campagne électorale. Cette première a sidéré tout le monde. C'était un bon signe, que le gouvernement annonce sa volonté de profiter de l'effort général pour éviter ce qui est arrivé aux États-Unis.

M. Glen Motz: Une dernière question, et j'ignore combien il me reste de temps.

Au fil des ans, le coût des tests de pénétration pour nos entreprises a toujours été élevé. La réaction des entreprises a toujours été de dire qu'il était inabordable. C'est presque le contraire: elles ne peuvent pas ne pas se le permettre.

Les prix ont-ils baissé? Existe-t-il une incitation non pécuniaire qui permet à HackerOne d'offrir à des entreprises privées — petites et même à nos grandes — la possibilité de savoir qu'elles peuvent au moins résister à une attaque de l'extérieur?

M. Jobert Abma: Avant que je ne fonde HackerOne, j'étais testeur de pénétration. L'un des motifs de sa fondation était d'abord que nous croyions que nous avions besoin d'un modèle évolutif qui pouvait s'appliquer à toute organisation de notre planète et qui serait également abordable pour tout le monde. Comme vous l'avez fait remarquer, les tests de pénétration, ce sur quoi on nous consulte, coûtaient très cher.

Nous croyons que plus l'entreprise a de choses à protéger, le plus elle a besoin de sécurité. Voilà pourquoi chacun de nous devrait pouvoir mettre sur pied son propre programme de divulgation de ses vulnérabilités. À HackerOne, nous offrons des services gratuits aux organismes communautaires et faisant la promotion des logiciels libres. Nous offrons de l'aide ou des produits à ceux qui veulent établir ce processus pour leur organisation, même sans encouragement sur la plateforme même. De cette manière, nous croyons que nous permettrons à toutes les organisations de la planète d'améliorer leurs défenses contre une atteinte à la protection des données.

Le président: Merci, monsieur Motz.

Monsieur Spengemann, vous disposez de cinq minutes.

M. Sven Spengemann (Mississauga—Lakeshore, Lib.): Ça arrive on ne peut plus parfaitement à point nommé. Je poursuis sur la lancée de M. Motz. Je pense que ça intéresse particulièrement les petites entreprises que de se faire rappeler les obstacles à la mise au point d'une bonne cyberinfrastructure. Beaucoup de nos jeunes entreprises utilisent des masses de données, dont la protection a beaucoup d'importance dans les premiers temps de leur existence, mais dont le coût à supporter est hors de proportion par rapport à celui que supportent nos grandes banques.

À part les États-Unis et le Canada, y a-t-il d'autres pays où des partenariats ont été établis entre des entreprises comme la vôtre et le secteur public pour établir les niveaux de base de la sécurité, pour le bien commun des petites entreprises, qui pourraient inspirer d'autres modèles, adaptés à la croissance de ces entreprises et à la spécialisation de leurs demandes en matière de cybersécurité?

Répond qui veut.

● (1640)

M. Jobert Abma: Je peux répondre.

Le problème en ce qui a trait aux petites entreprises, c'est qu'il y a toujours un compromis à faire sur le plan des risques. Il existe des listes de vérification, ou des documents sur des politiques, qui indiquent aux petites entreprises ce qu'elles doivent faire. Malheureusement, il leur appartient de mettre en oeuvre certaines des pratiques exemplaires qui ont été établies. Certaines entreprises, particulièrement les plus petites, prennent cela au sérieux, particulièrement, comme vous l'avez dit, lorsqu'elles gèrent un grand volume de données.

Cependant, nous ne sommes pas encore en mesure de dresser une liste de vérification fondée sur les données relatives aux vulnérabilités que nous avons observées au niveau des plateformes, mais nous nous attendons à pouvoir le faire d'ici quelques années.

M. Sven Spengemann: Avant que nous passions à M. Watherhouse, dites-moi s'il y a quelque chose que le secteur public pourrait offrir? Si vous aviez une liste de souhaits à transmettre au secteur public, peu importe le territoire, que comporterait-elle? Qu'est-ce que le secteur public pourrait fournir pour faciliter votre travail?

M. Jobert Abma: Nous serions ravis de collaborer avec des tierces parties pour établir cette liste. Je n'ai pas une réponse plus concrète à vous donner pour l'instant.

M. Sven Spengemann: Je pense à la wikinomie pour assurer un niveau de sécurité de base au sein des petites entreprises, ou à un programme de surveillance, peu importe le modèle qu'on souhaite appliquer. On a déjà abordé cela.

Monsieur Watherhouse, avez-vous des commentaires?

M. Steve Waterhouse: Oui, monsieur.

Il y a déjà de la documentation qui existe, notamment celle de la NISC aux États-Unis, qui a été diffusée à l'échelle internationale et qui constitue un bon point de départ pour n'importe quelle entreprise. Cette documentation a été conçue pour de très grandes entreprises ainsi que pour des PME.

Si une PME prend au sérieux la question de la protection de ses données, elle se servira de cette documentation. Toutefois, comme je viens du milieu des PME, je sais que ces entreprises n'ont pas de temps à consacrer à cela. Ce qu'il faudrait, c'est un guichet unique. Les entreprises pourraient payer pour le strict minimum et obtenir une liste des vérifications obligatoires à faire qui seraient satisfaisantes pour elles. Mais qu'en est-il de cette satisfaction? Est-ce qu'elles seraient satisfaisantes pour l'industrie des cartes de paiement? Est-ce qu'elles seraient satisfaisantes pour la protection des renseignements personnels? Il n'existe pas de lignes directrices claires qui permettraient au propriétaire d'un petit café de s'assurer qu'il n'y a pas de problème sur le plan de la sécurité pour son entreprise et ses clients. Si ce café offre un service d'accès à Internet à ses clients, le propriétaire ne sait pas exactement quoi faire dans ce cas-là.

Je suis souvent sur la route, et j'ai la mauvaise habitude de vérifier la sécurité dans ces petits cafés. La plupart du temps, je me rends compte qu'on peut avoir accès à la caisse enregistreuse et au disque dur qui contient toutes les copies de sauvegarde ainsi qu'à Internet. C'est ce que je fais. Les propriétaires de ces PME souhaitent simplement que ça fonctionne, car elles n'ont pas tellement les moyens de faire appel à des ressources.

M. Sven Spengemann: Est-ce que les représentants de HackerOne ou M. Watherhouse ont des commentaires à faire au sujet de la main-d'oeuvre au Canada dans le domaine de la cybersécurité? Qu'en est-il des programmes et de la formation, que ce soit dans le secteur public, au sein des Forces canadiennes ou dans le secteur privé? Y a-t-il suffisamment de main-d'oeuvre pour pouvoir en faire davantage dans ce domaine au sein du gouvernement?

M. Steve Waterhouse: Je vais commencer par la première question. Comme vous avez pu le constater, de nombreuses statistiques indiquent qu'il y a un manque d'expertise en matière de cybersécurité. À preuve, je donne moins de cours et de formation dans ce domaine. Une des raisons est que les coûts augmentent depuis quelques années, mais il y a aussi le fait que les gens ne sont pas intéressés à s'engager dans ce domaine. C'est un travail très exigeant qui nécessite beaucoup de connaissances. Il faut connaître de nombreux systèmes d'exploitation antérieurs et être en mesure de s'adapter aux nouveaux systèmes et aux plus importants qui font leur apparition.

Cela étant dit, certaines universités offrent de bons programmes pour former ces gens. Je viens de terminer un microprogramme en cybersécurité au niveau de la maîtrise à l'Université de Sherbrooke. Nous étions 15 étudiants dans la classe. C'est un excellent programme, mais nous étions seulement une quinzaine. J'aurais aimé que nous soyons 115, car ceux qui étaient là étaient très enthousiastes. Ils voulaient accroître leurs connaissances — ce sont des professionnels dans le domaine — et c'était une des rares occasions pour eux d'enrichir leurs connaissances.

Jadis, en 2003, je fréquentais l'Université de Winnipeg, et c'est à cette époque que le premier programme menant à un certificat a été créé. Ce n'est pas répandu. Ce n'est pas aussi présent que dans d'autres pays, où cela fait partie des programmes scolaires.

Le président: Je vous remercie, monsieur Spengemann.

Monsieur Dubé.

● (1645)

M. Matthew Dubé: J'aimerais revenir à la question de la nouvelle génération de réseaux 5G, qui font encore l'objet de recherches, et à la métaphore utilisée par Mme Dabrusin. On a parlé de boîtes de carton entre lesquelles circule un camion blindé, mais je crois qu'il faut aussi parler des appareils. Lors de la dernière réunion, nous avons eu une conversation intéressante à propos du nombre d'appareils qui vont être ciblés par la prochaine génération de réseaux, plus rapides, comme des robots utilisés lors de chirurgies et des drones pouvant être utilisés en agriculture.

Je vais m'adresser d'abord aux représentants de HackerOne, et ensuite à M. Waterhouse.

On m'a dit que le prix n'est pas le seul facteur. À mesure que le marché tente de concevoir des appareils abordables pour les maisons intelligentes et tout ce à quoi vous pouvez penser, est-ce qu'il y a un risque à un moment donné qu'il y ait un nivellement par le bas, que la sécurité soit sacrifiée? On a beau avoir les réseaux les plus sécurisés, mais, au bout du compte, si les gens utilisent des micrologiciels ou des appareils médiocres, cela ne sert à rien.

Est-ce une préoccupation? Que pourrions-nous faire?

M. Jobert Abma: C'est un des problèmes auquel nous n'avons pas encore trouvé de solution. Je dis « nous » en parlant de la planète. Nous voyons qu'il y aura un grand problème si des entreprises vendent des micrologiciels qui comportent des vulnérabilités sur le plan de la sécurité, mais cela pourrait ne pas avoir d'importance si elles ne subissent pas de conséquences.

Grâce aux changements récents que nous avons observés, les entreprises qui sont négligentes en ce qui concerne la sécurité subissent davantage de conséquences, et je crois que c'est une bonne chose. Les consommateurs exigent des normes élevées, surtout pour certains produits. Je crois aussi que, vu les modifications apportées à la réglementation, qui permettent au gouvernement d'exiger des entreprises qu'elles respectent certaines normes, il sera très important pour nous de veiller à ce que les entreprises ne puissent pas vendre des micrologiciels qui n'ont pas fait l'objet de tests. J'espère que cela permettra en effet d'éviter un nivellement par le bas.

M. Matthew Dubé: Avant que nous entendions la réponse de M. Waterhouse, je vais vous demander si vous pensez que l'obsolescence programmée a un rôle à jouer dans tout cela. Nous voyons, par exemple, des appareils qui ne sont plus compatibles avec de nouveaux micrologiciels.

Je me demande si nous n'incitons pas les consommateurs à mettre à niveau leurs appareils au détriment peut-être de la sécurité des réseaux, entre autres. On pense que mettre à jour un micrologiciel est une bonne chose, mais d'un autre côté, sans vouloir être complètement déconnectée, une personne pourrait souhaiter continuer d'utiliser une technologie moins récente. Ce pourrait être plus sûr d'une certaine façon.

Je ne sais pas si j'ai raison ou s'il y a des préoccupations à cet égard.

Mme Deborah Chang: Il y a des préoccupations, et je crois que les États-Unis et le Royaume-Uni ont adapté certaines normes dans le domaine de l'Internet des objets. Ils ont notamment dressé une liste. Le Royaume-Uni a dressé une liste de 10 recommandations dans le domaine de l'Internet des objets, et l'élaboration de politiques de divulgation des vulnérabilités est la deuxième recommandation.

Aux États-Unis, la Federal Trade Commission joue un rôle très actif en exigeant certaines choses dans ce domaine, à l'instar de la FDA en ce qui concerne des appareils médicaux. La FDA a publié l'année dernière un plan d'action pour les appareils médicaux en ce qui a trait à la sécurité, qui exige un certain nombre de choses, même relativement au cycle de vie ou au lancement d'un nouvel appareil.

Je crois que toutes ces lois et ces normes sont établies parce que tout le monde doit faire la même chose, car tout est interexploitable et connecté. Je crois que toutes ces politiques et ces normes visent l'uniformité, comme les normes du NIST, dans ces différents domaines.

M. Matthew Dubé: Je vous remercie beaucoup.

[*Français*]

Monsieur Waterhouse, en terminant, avez-vous des commentaires à formuler?

[*Traduction*]

M. Steve Waterhouse: Comme vous l'avez dit, c'est en quelque sorte voué à l'échec, car de nombreux appareils ont littéralement envahi le marché sans qu'ils aient fait l'objet de vérifications, alors ils sont...

On met ces appareils entre les mains des gens en pensant qu'ils vont faciliter leur vie et améliorer leur environnement. Ces appareils se vendent. Prenons l'exemple d'un thermostat à 250 $, qui enregistre vos habitudes de vie et qui transmet cette information à cette entreprise qui s'appelle Google puisque c'est un produit de cette compagnie. Alors, oui, vous serez en mesure de régler à distance le chauffage dans votre maison et de le programmer, mais en même temps, cet appareil enregistre vos allées et venues.

À mon avis, il aurait fallu tenir compte de cela avant d'autoriser la mise en marché de ce type d'appareils. La plupart des gens ne se rendent même pas compte que ces appareils enregistrent leurs habitudes de vie. Pour ce qui est des appareils qu'on trouve dans les voitures, et il y en a de plus en plus, ils peuvent être piratés parce que les logiciels ont des lacunes.

● (1650)

Le président: Officiellement, nous sommes rendus à la fin de la période des questions, mais je vois que mes collègues sont très enthousiastes. J'espère que les témoins sont prêts à rester un peu plus longtemps. J'ai l'intention qu'on poursuive jusqu'à 17 heures, mais je vais exercer ma prérogative en tant que président et poser une question à propos de la cryptomonnaie.

Dans les médias ce matin, on parlait d'une entreprise qui s'appelle QuadrigaCX. C'est une entreprise de cryptomonnaie dont la valeur s'élève, semble-t-il, à environ 250 millions de dollars. Le propriétaire a à peu près le même âge que M. Abma, et il est décédé. Son ordinateur portable contient tous les mots de passe. Je trouve plutôt bizarre qu'une entreprise de 250 millions de dollars ne puisse plus fonctionner parce que personne ne peut avoir accès aux mots de passe qui se trouvent dans un ordinateur portable.

J'aimerais savoir premièrement si cela représente un défi pour HackerOne.

Des députés: Oh, oh!

Le président: S'agit-il, à première vue, d'un mépris total envers la sécurité?

Ma deuxième question concerne la chaîne de blocs. Même si nous pouvions obtenir les mots de passe, est-ce que la technologie de la chaîne de blocs fait en sorte que même HackerOne, avec toutes ses compétences, ne pourrait rien faire compte tenu de la sécurité de cette technologie?

Je m'excuse pour ces questions mal formulées, mais cela m'apparaît comme une situation où nous sommes censés étudier la sécurité des institutions financières alors que nous sommes confrontés à un important échec technologique. Il pourrait s'avérer que la technologie de la chaîne de blocs ne puisse pas causer des torts qui ne peuvent pas être réparés. Ai-je raison ou pas?

M. Jobert Abma: Je suis au courant de cette situation. Il y a deux problèmes en ce qui concerne la technologie de la chaîne de blocs que j'aimerais souligner.

Premièrement, les ordinateurs actuels ne sont tout simplement pas assez rapides, alors même si nous voulions décrypter des codes utilisés par la technologie de la chaîne de blocs, nos ordinateurs ne sont tout simplement pas assez puissants pour le faire. Il faudra de nombreuses années pour que les ordinateurs deviennent assez puissants pour le faire.

Deuxièmement, parce que la technologie de la chaîne de blocs est nouvelle, les consommateurs ont accordé une grande confiance à ces entreprises qui valent des centaines de millions de dollars, mais ils n'ont aucune idée des mesures de protection qui ont été mises en place, ou si ces mesures sont trop nombreuses. Dans ce cas-ci, on se fie à une seule personne.

D'une certaine façon, les technologies sont fantastiques et je crois que le fait de les expérimenter constitue une bonne façon de découvrir leurs applications. Cependant, je ne suis pas d'avis que l'application de la technologie de la chaîne de blocs dans le secteur financier, comme on l'a fait jusqu'à maintenant avec le bitcoin et d'autres cryptomonnaies, soit l'application qui convienne.

Cette technologie est très puissante et elle peut et devrait être utilisée pour régler certains des problèmes que nous avons observés, notamment le fait qu'une seule personne soit responsable de 250 millions de dollars qui appartiennent à d'autres personnes.

● (1655)

Le président: Ne trouvez-vous pas cela plutôt absurde qu'un seul ordinateur portable permette d'avoir accès au système?

M. Jobert Abma: Oui. Cela ne devrait jamais être le cas.

Le président: D'accord.

Si une des cryptomonnaies ne peut plus être utilisée — et corrigez-moi si j'ai tort — dois-je présumer que toutes les personnes qui négocient des cryptomonnaies et qui ont cette cryptomonnaie en particulier dans leur portefeuille seront touchées? On parle de beaucoup d'autres personnes que simplement les clients de Quadriga. Est-ce exact ou non?

M. Jobert Abma: Ce qui est une bonne ou une mauvaise chose à propos de la chaîne de blocs ou des cryptomonnaies, c'est qu'il existe une seule copie d'un bloc ou d'une monnaie en particulier, selon le type de cryptomonnaie, ce qui signifie que, si une entreprise n'a plus accès à ce qu'on appelle des « portefeuilles », l'argent est essentiellement perdu, car il est impossible mathématiquement de récupérer ces portefeuilles, et encore moins d'y avoir accès.

Le président: Vraiment?

M. Glen Motz: Nous devrions leur demander de s'entretenir avec les gens qui négocient des bitcoins.

Le président: En dernier lieu, j'ai une question à propos d'un autre point. Comme Mme Sahota l'a dit, votre entreprise est aussi forte que son plus faible maillon. Il peut y avoir 20 000 ou 30 000 pirates informatiques qui travaillent, semble-t-il, pour HackerOne, mais une de ces personnes pourrait découvrir une vulnérabilité qu'il serait plus profitable financièrement de ne pas divulguer. Comment alors protégez-vous vos clients contre ces personnes que vous avez choisies, qui travaillent pour vous et en qui vous avez confiance?

M. Jobert Abma: C'est une excellente question.

C'est pourquoi j'estime que la sécurité assurée par des pirates est si utile. Si un grand nombre de personnes ont les mêmes motivations, nous croyons qu'il y aura toujours davantage de personnes qui seront en mesure de trouver la même vulnérabilité. Si une de ces personnes, qu'il s'agisse d'un criminel ou non, décide de ne pas divulguer cette vulnérabilité en matière de sécurité, elle court le risque que d'autres personnes décèlent cette même vulnérabilité et la divulgue à l'entreprise.

Nous n'avons jamais essayé de concurrencer le marché noir où, essentiellement, des vulnérabilités aux attaques du jour zéro ont fait l'objet d'échanges avec des gouvernements ou des entreprises privées. Les programmes bug bounty ont certes créé une motivation inverse chez les pirates à chapeaux noirs, qui cherchent à déceler ce type de vulnérabilités, car les prix augmentent simplement parce que la probabilité que des gens bien intentionnés découvrent ces mêmes vulnérabilités augmente en flèche de nos jours.

Le président: J'aimerais poursuivre dans cette veine, mais mes collègues ont également des questions à poser et il nous reste seulement quelques minutes

M. Spengemann ou M. Picard?

M. Michel Picard: Oui, j'ai une brève question à poser.

● (1700)

[*Français*]

Je vais m'adresser à M. Waterhouse en premier.

Si le gouvernement canadien souhaite utiliser les services de pirates informatiques ou de chercheurs en sécurité — pour les qualifier de façon positive —, doit-il passer par un processus de reconnaissance ou de légalisation de tels services? Faut-il qu'il y ait des cours légitimes sur des sujets légitimes pour pouvoir avoir la même expertise que celle des pirates informatiques par définition?

M. Steve Waterhouse: Si je comprends bien votre question, monsieur Picard, vous me demandez si le gouvernement pourrait recourir aux services d'un pirate informatique reconnu ou non.

M. Michel Picard: C'est cela.

M. Steve Waterhouse: Les contrats que conclut Services publics et Approvisionnement Canada doivent être en bonne et due forme. Ils doivent contenir un chapitre consacré à la sécurité. Une enquête de sécurité doit être faite. Si un individu ou un groupe d'individus travaille sur des systèmes d'information du gouvernement, il doit avoir reçu l'autorisation légale appropriée pour pouvoir faire le travail.

M. Michel Picard: Il y a un autre aspect important.

[*Traduction*]

Je vais maintenant m'adresser aux représentants de HackerOne.

Je crois savoir que vous avez commencé à faire du piratage à un jeune âge. À cette époque, ce n'était peut-être pas aussi légal que cela aurait dû l'être, mais vous avez réussi à créer une entreprise légale qui se porte assez bien. Vous avez maintenant une entreprise légitime qui a une bonne réputation. Comment vous y êtes-vous pris pour acquérir votre réputation et collaborer avec le gouvernement?

Le président: Est-ce que vous demandez des conseils professionnels?

M. Michel Picard: Non, je veux que cette entreprise ouvre une filiale au Canada.

M. Jobert Abma: Voulez-vous une réponse d'un point de vue personnel ou du point de vue d'une entreprise?

M. Michel Picard: Disons du point de vue d'une entreprise.

M. Jobert Abma: Nous sommes notamment très fiers de l'amélioration que les gens ont pu constater grâce à la mobilisation du milieu des pirates informatiques dans le cadre d'une entreprise bien établie dans le domaine de la sécurité. Nous observons d'ailleurs que, malgré notre expertise dans ce domaine, il y a toujours des problèmes qui sont décelés par d'autres personnes plus intelligentes ou plus créatives que nous.

Notre modèle fonctionne. Grâce à nos rapports avec le milieu des pirates informatiques, nous sommes en mesure de créer des produits qui aident les entreprises à établir un lien avec ce milieu, et nous agissons comme intermédiaires si c'est nécessaire. Notre succès repose entièrement sur la réussite des pirates informatiques et le type de vulnérabilités qu'ils ont su déceler pour le compte de nos clients.

M. Michel Picard: J'ai une préoccupation. D'un point de vue pratique, c'est fantastique. Par contre, d'un point de vue juridique, puisque nous sommes un État qui respecte la primauté du droit, nous devons nous assurer de ne pas faire affaire avec des « délinquants », pour ne pas légitimer une activité illégale pour notre propre intérêt et notre propre bien. Nous ne pouvons pas faire cela. Nous devons agir en toute légalité pour pouvoir justifier nos actions. Avez-vous eu à obtenir une certaine reconnaissance ou à supprimer d'anciens dossiers ou quelque chose du genre?

Mme Deborah Chang: En ce qui concerne le département de la Défense, nous avons dû respecter des exigences supplémentaires. Les pirates ont dû respecter certaines exigences imposées par le département de la Défense. Le gouvernement canadien peut faire la même chose que le gouvernement américain, c'est-à-dire ouvrir au public des programmes du type Hack the Pentaqon. Le gouvernement américain a invité un grand nombre de pirates informatiques à pirater la plateforme. Cela a permis de faire accepter l'idée qu'on peut découvrir parmi ces pirates des personnes talentueuses qu'on ne connaissait peut-être pas.

Dans le cadre de certains programmes, des pirates signent un accord de non-divulgation directement avec le client, ou bien certains clients veulent uniquement des pirates qui sont citoyens d'un pays en particulier, comme les États-Unis par exemple. Certains clients veulent uniquement des pirates qui sont citoyens américains. Nous voyons avec le client ce qu'il souhaite, puis nous choisissons les pirates qui conviennent le mieux.

Le président: Je vais laisser le dernier mot à M. Waterhouse.

M. Steve Waterhouse: Monsieur Picard, il existe déjà au pays des entreprises qui oeuvrent dans le domaine du piratage éthique. Ce sont des entreprises légitimes. On n'y trouve aucun criminel. Après l'université, les gens acquièrent une expérience pratique comme je l'ai fait moi-même au cours de ma carrière. Elles constituent une solution fiable, comme HackerOne.

À Montréal, il y a l'entreprise GoSecure, qui a une bonne réputation. Elle embauche des personnes qui viennent d'obtenir leur diplôme universitaire. Ce sont des gens très professionnels, comme cette dame et ce monsieur de HackerOne.

● (1705)

Le président: Je tiens à vous remercier tous au nom du Comité, mais aussi personnellement. Nous avons passé une heure et demie fascinante. La cybersécurité devient de plus en plus complexe. Nous nous en rendons compte à mesure que nous étudions le sujet.

Je suis certain que nos amis en Californie ont droit à du temps beaucoup plus clément que nous ici aujourd'hui.

La séance est levée.