Renforcement du cadre de la cybersécurité du Canada

Mémoire prébudgétaire présenté au Comité des finances de la Chambre des communes

Le 3 août 2018

Liste des recommandations pour surmonter les défis en matière de cybersécurité

- **Recommandation 1** : Adapter aux petites et moyennes entreprises les solutions de la cybersécurité.

- **Recommandation 2** : Harmoniser la réglementation en matière de cybersécurité, à l'aide d'un cadre de base.

- **Recommandation 3** : Établir les priorités du développement de systèmes d'établissement de l'identité et de vérification de l'identité à distance de la prochaine génération.

- **Recommandation 4** : Concevoir des normes pour améliorer l'interopérabilité ainsi que pour la détection et la prévention des cybermenaces, tout en éliminant la friction provenant du commerce.

- **Recommandation 5** : S'attaquer à la pénurie de personnel compétent dans le domaine de la cybersécurité.

- **Recommandation 6** : Envisager la mise sur pied d'un groupe de travail comprenant des représentants de l'industrie, du gouvernement et du maintien de l'ordre public, qui orientera les efforts en matière de cybersécurité.

Introduction

La cybersécurité est un des plus grands problèmes pour les gouvernements et les entreprises actuellement; il y a là des répercussions graves pour la sécurité nationale, la stabilité financière et la protection des consommateurs.

C'est également une priorité mondiale de premier ordre pour Mastercard parce que la sûreté et la sécurité sont des principes de base centraux pour chaque segment de notre entreprise ainsi que pour les plateformes technologiques innovatrices et les services que nous rendons possibles. Nous savons que des produits et services sûrs sont essentiels pour conserver la confiance que nous portent nos clients, nos détenteurs de cartes, nos commerçants et nos autres partenaires.

Afin d'aborder directement le thème de la consultation prébudgétaire de 2018, la cybersécurité est fondamentale pour la croissance économique et la compétitivité future du Canada. Un système de défense qui serait perçu comme faible pourrait avoir un effet négatif sur la réputation commerciale du Canada. Toutefois, un cadre réglementaire trop encombrant pourrait tout autant éloigner les investissements et affecter au respect de la conformité des ressources qui serviraient autrement à une défense réelle.

Le gouvernement fédéral devrait être loué pour ses efforts à ce jour dans le domaine de la cybersécurité, notamment pour l'adoption d'une législation créant le Centre canadien pour la cybersécurité et pour publier sa Stratégie nationale de cybersécurité. Les deux sont des initiatives qu'appuie Mastercard, et un certain nombre de points soulevés dans cette présentation sont en harmonie avec les priorités relevées dans la stratégie. Toutefois, notre message clé est que le temps presse de mettre en œuvre la stratégie.

À propos de Mastercard

Mastercard est une entreprise technologique dans l'industrie des paiements à l'échelle mondiale. Nous exploitons le réseau de traitement des paiements mondial le plus rapide, mettant en relation des consommateurs, des institutions financières, des commerçants, des gouvernements et des entreprises dans plus de 210 pays et territoires. Les produits et solutions de Mastercard facilitent les activités commerciales chaque jour – notamment le magasinage, les voyages, l'exploitation des entreprises et la gestion des finances – les rendent plus sécurisées et efficientes pour tous.

Mastercard n'émet pas de cartes de paiement de quelque nature que ce soit ni n'a de contrat avec les commerçants aux fins de l'acceptation de ces cartes. Dans le système de paiement de Mastercard, ces fonctions sont confiées aux institutions financières. Mastercard désigne par « l'émetteur » l'institution financière qui émet une carte de paiement portant la marque de Mastercard, puis par « l'acquéreur » l'institution financière qui signe un contrat avec un commerçant afin que celui-ci accepte les cartes de paiement portant les marques de Mastercard.

Mastercard est propriétaire de la gamme des marques Mastercard et accorde aux institutions financières des licences permettant d'utiliser ces marques lors de transactions de paiement. Mastercard fournit aussi des réseaux par lesquels ses institutions financières clientes peuvent interagir afin d'exécuter les transactions de paiement, puis détermine certaines règles liées à ces interactions, en vue de permettre au système de fonctionner avec efficience.

Lorsqu'un détenteur de carte présente à un commerçant sa carte de paiement portant l'une des marques de Mastercard afin d'acheter des marchandises ou services, le commerçant transmet une demande d'autorisation à son acquéreur; celui-ci achemine généralement la demande à Mastercard, et Mastercard achemine la demande à l'émetteur. L'émetteur approuve ou non la demande d'autorisation et transmet la décision au commerçant par les mêmes canaux. Le rôle de Mastercard est de faciliter les instructions de paiement entre les parties de la transaction; il y a aussi la détermination des règles qui permettent aux parties d'interagir avec efficacité et efficience.

Ce qui précède sert de contexte utile afin de comprendre pourquoi la cybersécurité est une priorité internationale absolue pour Mastercard.

Mastercard et la cybersécurité

Pour que Mastercard offre de la valeur aux émetteurs, aux commerçants et aux consommateurs qui se servent de son réseau, il lui faut offrir de la sécurité et de la sûreté. Nous ne pouvons nous permettre d'avoir toute interruption dans le fonctionnement de notre réseau. Lorsqu'un émetteur émet une carte Mastercard, lorsqu'un client sort celle-ci de sa poche ou lorsqu'un commerçant décide d'accepter Mastercard, chacune des parties prenantes doit avoir confiance que le réseau par lequel le paiement sera effectué est fiable et résistant.

Sur ce point, notre dossier est solide. Le réseau de Mastercard à des niveaux de cyberdéfense, conçus pour atténuer le risque et pour le protéger contre les pirates; de plus, nous renforçons continuellement la résistance, afin d'éviter des interruptions de service.

Au cours des trois dernières années, Mastercard a investi plus d'un milliard de dollars pour renforcer les cyberdéfenses de son réseau et pour trouver des solutions permettant de protéger les participants de l'écosystème de paiement, qu'il s'agisse des émetteurs, des acquéreurs, des commerçants ou des détenteurs de carte. Il a fallu pour cela prendre l'initiative dans la conception de nouvelles normes pour l'écosystème des paiements et du commerce, qui sont constamment révisées en se préoccupant de la sécurité.

Mastercard investit aussi dans l'innovation : en améliorant nos capacités internes; en acquérant des sociétés technologiques de pointe; en encourageant son groupe Start Path d'entreprises en démarrage, les reliant à nos partenaires émetteurs pour leur permettre de hausser leur chiffre d'affaires.

Pratiques exemplaires en gestion du risque relié à la cybersécurité

Il y a cinq éléments essentiels et largement acceptés en gestion du risque relatif à la cybersécurité. Voici les diverses façons dont Mastercard opérationnalise des éléments de ces pratiques exemplaires.

Identification. La priorité est d'authentifier l'identité des utilisateurs du réseau, et Mastercard fait des choses réellement intéressantes à ce sujet, notamment la vérification de l'identité de

Mastercard – ce qui est officieusement désigné par Selfie Pay – que les émetteurs canadiens ont été les premiers à commercialiser.

Protection. La sécurité de l'appareil est déterminante pour ce point. Avec un système en réseau, tout appareil peut être le point de départ d'une cyberattaque. À cette fin, en 2017, Mastercard a effectué l'acquisition de NuData Security, une société technologique canadienne innovatrice qui aide les entreprises à prévenir la fraude par des appareils mobiles et en ligne, à l'aide d'indicateurs comportementaux et biométriques. NuData améliore nos capacités, notamment en prévenant les cyberattaques à partir d'appareils de consommateurs, la prise de contrôle de comptes et en permettant des points de friction intelligents.

Détection. Cela est axé sur l'arrêt d'une attaque avant qu'elle commence, par l'utilisation d'analyses de données, en vue de mieux protéger la sécurité. Mastercard fait des investissements majeurs en intelligence artificielle, dont l'acquisition récente de Brighterion, un chef de file mondial de l'intelligence artificielle (IA), ce qui améliore la capacité de détecter des attaques complexes. Les solutions d'IA de Brighterion aident Mastercard à trouver l'aiguille dans une botte de foin lorsqu'il s'agit de filtrer d'énormes quantités de données.

Réaction. Afin de réagir efficacement face aux menaces, le partage d'information et la collaboration sont cruciaux entre les représentants du gouvernement et du maintien de l'ordre public, des partenaires de l'industrie et des institutions financières, tant au Canada qu'à l'étranger.

Rétablissement. Comme d'autres chefs de file de l'industrie, Mastercard dresse et améliore continuellement des plans de résistance, afin de nous assurer que nos plans de sauvegarde fonctionnent si jamais ils étaient nécessaires. Cela comprend des moyens automatisés machine à machine en temps réel, afin de réagir à une attaque. En outre, misant sur les solutions perfectionnées par Vocalink, nous sommes en mesure de suivre les mules qui transportent l'argent et d'aider les émetteurs à recouvrer des fonds.

Recommandations

Les recommandations suivantes devraient être considérées alors que le Canada perfectionne et met en œuvre la Stratégie nationale de cybersécurité.

Premièrement, dans un monde numérique réseauté et interconnecté, les **solutions en matière de cybersécurité doivent être adaptées aux petites et moyennes entreprises** (PME). Lors d'une attaque, les cybercriminels cherchent les points faibles du système au début de l'attaque. Par conséquent, nous devons offrir aux petites entreprises un cadre pour protéger leurs activités. À cette fin, Mastercard joue un rôle de chef de file dans la défense des PME, par l'entremise du Cyber Readiness Institute (CRI), qui se concentre sur l'utilisation pratique des outils, mais pour les PME.

Par exemple, le 1er juillet, le CRI a lancé le Cyber Readiness Program, un projet pilote conçu pour collecter les pratiques exemplaires en matière de cybersécurité des sociétés Fortune 500, afin de traduire ces pratiques en recommandations pour les entreprises qui n'ont pas les

ressources pour embaucher leur propre personnel de sécurité. Comme le disait le chef de la direction de Mastercard, Ajay Banga, au sujet du lancement : « Même si vous êtes une grande entreprise, vous êtes seulement aussi fort que le lien le plus faible avec lequel vous entrez en contact, car toutes nos réputations sont de concert à ce niveau. » [TRADUCTION]

Le CRI exhorte également les sociétés Fortune 500 à intégrer les principes de ce programme dans leur chaîne d'approvisionnement. Le projet pilote du CRI prend fin le 30 septembre; le CRI évaluera les points forts et les possibilités d'amélioration à ce moment avant de l'adapter sur une plus grande échelle.

Deuxièmement, **il faut que la réglementation en matière de cybersécurité soit harmonisée à l'aide d'un cadre de base**. Des entreprises mondiales telles que Mastercard sont souvent aux prises avec un ensemble de règlements dans le domaine de la cybersécurité, qui prend de l'ampleur et se chevauche sous divers régimes. D'énormes dépenses de temps et de ressources s'ensuivent pour assurer la conformité – c'est une notion très différente de celle de la défense contre une cyberattaque. Autrement dit, la conformité démontre le respect d'un ensemble de règlements à un moment donné; en revanche, la défense exige une concentration et une évolution constantes.

Troisièmement, des données probantes découlant de violations récentes suggèrent que les adversaires ont rattrapé le décalage du côté des normes de l'établissement de l'identité et de la vérification de l'identité à distance. L'établissement de l'identité sert à déterminer l'unicité et la validité de l'identité d'une personne, afin d'aider à se prévaloir d'un droit ou à obtenir un service. Les solutions antérieures, telles les vérifications sous forme de questions fondées sur le savoir, ne sont plus aussi utiles, car les violations ont permis aux attaquants d'obtenir suffisamment de données pour répondre aux questions que l'on croyait autrefois secrètes.

Le gouvernement devrai**t prioriser le développement de systèmes d'établissement de l'identité et de vérification de l'identité à distance**. Davantage d'investissement en R-D et dans les normes; du travail sur l'identité; la promotion de l'innovation en rapport avec l'identité; le leadership du gouvernement au regard de l'offre de nouveaux services numériques, afin de valider les attributs – en s'éloignant de l'approche reposant sur le papier – aiderait les gouvernements et le secteur privé à devancer d'un stade les pirates et à accélérer l'émergence de solutions de contrôle de l'identité supérieures.

Quatrièmement, avec l'Internet des objets, il y aura bientôt 30 milliards d'appareils connectés. Cela crée d'énormes opportunités pour l'économie numérique, mais augmente aussi les risques cybernétiques. Par conséquent, les gouvernements et le secteur privé devraient **élaborer des normes pour améliorer l'interopérabilité, la détection et la prévention des cybermenaces, tout en éliminant la friction pour le commerce**. L'analyse des données devrait servir à accroître la protection en matière de sécurité.

Cinquièmement, pendant qu'augmentent les cybermenaces, les gouvernements et le secteur privé ont **besoin de s'attaquer à la pénurie d'employés compétents dans le domaine de la cybersécurité**. Le monde a besoin de commencer à former la prochaine génération de cyberexperts, et la stratégie nationale mentionne cela à juste titre. C'est aussi un domaine dans lequel le CRI a déployé des efforts; ce devrait être également un facteur très important pour le

Canada, compte tenu du rapport récent de Deloitte qui souligne que la demande pour des travailleurs dans le domaine augmente de 7 % annuellement; de plus le Canada doit trouver 8 000 nouveaux cybertravailleurs d'ici 2022.

Enfin, et plus généralement, la collaboration, le partage de l'information et le regroupement de tous les intervenants autour de la table sont requis pour combattre le cybercrime, et nous espérons que le Centre canadien pour la cybersécurité devienne ce forum. Au sein de cette structure, le Canada **devrait envisager un groupe de travail comprenant des représentants de l'industrie, du gouvernement et du maintien de l'ordre public, afin de faire porter les efforts sur la cybersécurit**é. C'est un enjeu si fondamental pour l'avenir de notre économie et notre société qu'il lui faut de l'attention et du leadership aux plus hauts niveaux, et Mastercard est prête à fournir son expertise de toutes les façons possibles. Par exemple, aux États-Unis, le président Obama avait mis sur pied un groupe de travail consacré à la cybersécurité et le chef de la direction de Mastercard en faisait partie. Une série de recommandations a été formulée, et le CRI est une émanation directe de son insistance sur la sécurisation des PME.

Conclusion

Le Canada fait du très bon travail en matière de cybersécurité, mais nous ne pouvons nous payer le luxe d'attendre lorsqu'il s'agit des cybermenaces. Cet enjeu est décisif pour la croissance économique et la compétitivité futures du Canada, à la fois comme menaces et comme opportunités.

En ce qui concerne les menaces, comme il est souvent dit, ceux qui s'engagent dans la cyberdéfense doivent bien faire les choses dans 100 % des cas; tandis que les cybercriminels n'ont qu'à réussir qu'une seule fois pour causer une crise qui pourrait s'avérer énorme.

Quant aux opportunités, des sociétés telles que Mastercard investissent des milliards de dollars dans la cybersécurité. Si le Canada peut préparer les travailleurs qualifiés requis pour ce domaine, cela stimulerait la création d'entreprises innovatrices en cybersécurité telle que NuData; le Canada peut être un chef de file dans ce domaine, ce qui ouvre la porte à d'énormes opportunités économiques.

Nous encourageons fortement le gouvernement à mettre en œuvre rapidement la stratégie nationale, et nous espérons que nos recommandations seront utiles en ce sens. En particulier, nous aimerions que soient pris en considération le modèle qui existe déjà pour le Cyber Readiness Institute ainsi que le leadership dont a fait preuve le président Obama avec son groupe de travail sur la cybersécurité. Nous sommes prêts à discuter de nos constatations plus en détail, lorsque cela conviendra au Comité.