BANQUE DU CANADA
BANK OF CANADA

Discours prononcé par Filipe Dinis
Chef de l'exploitation de la Banque du Canada
Association canadienne de la technologie de l'information
Toronto (Ontario)
12 novembre 2019

Cybersécurité : lever les obstacles

Introduction

Bonjour. Quel plaisir d'être parmi vous, ici à Toronto! Je remercie sincèrement l'Association canadienne de la technologie de l'information de m'avoir invité.

Je profiterai de cette tribune pour parler du travail de la Banque du Canada dans le dossier de la cybersécurité, ainsi que du rôle des spécialistes en technologies de l'information et des professionnels du secteur comme vous. Ce sera l'occasion d'ouvrir le dialogue sur nos objectifs communs.

D'ailleurs, saviez-vous que les objectifs de l'ACTI ressemblent beaucoup à ceux de la Banque? Vous aidez le Canada à devenir une société numérique qui donne l'exemple à l'international – une société à la fois prospère et compétitive sur le marché mondial. Quant à elle, la Banque favorise la prospérité économique et financière du Canada, comme le veut la *Loi sur la Banque du Canada*.

L'ACTI et la Banque cherchent donc à atteindre un même résultat, soit assurer la prospérité, la stabilité et la sûreté de l'économie pour le bien du pays et de ses citoyens. Et la cybersécurité est certainement l'un des principaux facteurs qui déterminent notre capacité à y arriver.

À la Banque, protéger le système financier contre les cyberattaques est un rôle que nous prenons très au sérieux. Mais nous n'accomplirons rien si nous travaillons en vase clos. Nous devons joindre nos efforts à ceux des acteurs du secteur financier, voire de tous les secteurs de l'économie, pour lutter contre ces menaces bien réelles. Et même si nous avons innové afin de collaborer plus souvent – et plus efficacement – avec nos partenaires nationaux et internationaux, la partie est loin d'être gagnée.

Pour entrer dans le vif du sujet, j'aimerais maintenant vous parler un peu plus de ce que fait la Banque pour assurer la résilience du système financier canadien.

Le rôle de la Banque du Canada

Vous vous doutez bien qu'en 1935, les fondateurs de la banque centrale du pays n'avaient jamais entendu parler de cybersécurité. Tant mieux pour eux; ce n'était pas encore une réalité à ce moment-là.

À l'époque, les banques centrales et les institutions financières n'avaient qu'à se préoccuper de la sécurité physique, sans égard aux cyberrisques auxquels nous

faisons face à l'heure actuelle. En effet, l'or a longtemps été le bien le plus précieux des banques centrales; aujourd'hui, ce sont les données.

Dans les 84 années d'existence de la Banque, ses priorités sont restées sensiblement les mêmes. Cependant, ses façons de faire ont considérablement évolué.

Par exemple, l'une des principales responsabilités de la Banque consiste à favoriser la stabilité et l'efficience du système financier. De nos jours, vu l'augmentation constante de la portée et de la gravité des cyberattaques à l'échelle mondiale, nous devons prêter une plus grande attention à ce type de menace. Dans la *Revue du système financier* de 2019, qui dresse le bilan des vulnérabilités du système financier, nous avons insisté à la fois sur le fait que les cyberattaques sont de plus en plus fréquentes, graves et sophistiquées à l'échelle du globe et sur la possibilité qu'elles causent des perturbations généralisées.

Au pays, les cybermenaces sont aussi une préoccupation de premier plan pour les spécialistes de la gestion du risque qui travaillent dans le secteur financier. Deux fois par année, la Banque invite ces experts à participer à une enquête sur le système financier. Au printemps dernier, les cyberincidents étaient encore, selon eux, le plus grand risque pour le système financier canadien. Les résultats de l'enquête de l'automne seront publiés la semaine prochaine, et nous nous attendons à ce que la cybersécurité figure encore parmi les préoccupations du secteur.

Et ce n'est pas pour rien. Les cyberincidents se multiplient, se raffinent et menacent de façon bien réelle la stabilité du système financier. Selon les informations obtenues auprès d'Advisen, une agence spécialisée en données, près de 5 000 cyberattaques ont perturbé le secteur financier mondial entre 2014 et 2018. En tout, plus de 550 millions de dossiers ont été compromis, ce qui a entraîné des pertes directes de plus de 4 milliards de dollars américains, d'après les données rapportées.

Ces chiffres alarmants viennent appuyer la nécessité pour la Banque de se doter de cyberdéfenses suffisamment solides pour protéger ses actifs de valeur (avoirs financiers, données) et son personnel. Dans les cinq dernières années, notre institution a réalisé d'énormes progrès en cybersécurité et investi des sommes considérables dans l'amélioration de sa résilience globale.

Par exemple, grâce au Programme d'amélioration de la reprise des activités, nous avons renforcé la résilience de nos centres de données, de nos infrastructures réseau et technologiques, et de nos systèmes opérationnels. Ce programme aidera la Banque à résister aux bouleversements de toutes sortes, comme les mauvaises conditions météo et, vous l'aurez deviné, les cybermenaces.

Au printemps dernier, nos investissements dans les effectifs, la planification, les infrastructures et la formation ont donné lieu à la mise en service du Site des opérations de Calgary, dont les employés font partie intégrante de l'équipe responsable des opérations bancaires et des opérations sur les marchés basée à Ottawa. À partir de ce nouveau site, le personnel pourra prendre la relève et assumer les fonctions essentielles des marchés sans délai en cas d'incident

opérationnel majeur. C'est là une avancée de taille dans nos efforts pour renforcer la résilience de la Banque.

De plus, l'an dernier, nous avons créé le poste de chef de la sécurité de l'information à la Banque. Cette décision était le fruit de notre modèle de gouvernance fondé sur des pratiques exemplaires visant à harmoniser et à coordonner les programmes et activités de cybersécurité.

Voilà quelques exemples des mesures prises à l'interne pour améliorer la cybersécurité. Mais la Banque a aussi le mandat de faire avancer la cybersécurité en dehors de ses murs. À ce chapitre, l'été dernier, j'ai eu le plaisir de présenter et de publier en ligne la stratégie de cybersécurité 2019-2021 de la Banque : une autre étape importante de notre « cyber-évolution ».

Dans cette stratégie, nous reconnaissons non seulement l'excellent travail accompli jusqu'ici, mais aussi tout ce qu'il reste à faire pour remplir ce mandat d'améliorer la cybersécurité à la grandeur du système financier.

Dans cette optique, nous n'arrêtons pas d'innover et de rehausser la sécurité dans la conduite de nos propres activités.

En outre, nous collaborons avec des partenaires externes dans le but de renforcer notre résilience individuelle et commune. Par exemple, il n'y a pas très longtemps, nous avons fait appel à une entreprise spécialisée en cybersécurité pour voir si l'apprentissage automatique pourrait nous permettre de détecter les anomalies à même nos infrastructures et d'atténuer le risque de cyberincidents.

Enfin, nous nous faisons les champions de l'adoption de normes de cybersécurité robustes dans le secteur financier, normes qui contribueront à protéger ce secteur contre les cyberrisques, tant au pays qu'à l'étranger.

Aux grandes vulnérabilités, les grands moyens

À la Banque, nous abordons les enjeux dans une perspective globale, qu'il soit question de la politique monétaire, du système financier ou de la cybersécurité. Et quand nous parlons de cybersécurité avec les institutions financières et autres participants au marché, nous devons nous assurer qu'ils mettent de côté leurs instincts compétitifs et voient eux aussi la situation dans son ensemble. Pourquoi? Parce que les interventions doivent être à la mesure des vulnérabilités.

Par le passé, la plupart des entreprises, y compris les banques, ont eu tendance à limiter leur réflexion sur la cybersécurité aux répercussions qui les toucheraient directement. Pour un gestionnaire, évaluer le risque lié aux rançongiciels et aux attaques ciblées de cyberactivistes n'a rien de bien compliqué : il n'a qu'à calculer ce qu'il en coûterait de réparer les dégâts causés à l'entreprise et le montant qui suffirait à la protéger contre ce risque. Il s'agit d'une simple dépense d'exploitation.

Les choses se corsent si ce même gestionnaire tient compte des implications pour les principaux fournisseurs et partenaires de son entreprise. Malgré cela, il passe encore à côté de la possibilité d'un cyberincident systémique, c'est-à-dire un incident pouvant s'étendre aux institutions financières, aux réseaux, aux infrastructures et aux marchés. Le problème pourrait être déclenché par une

faille de sécurité dans un logiciel largement utilisé, des vulnérabilités venant des infrastructures, voire un gouvernement hostile.

N’oublions pas que nous vivons dans une société toujours plus interconnectée, ce qui amplifie le risque d’un cyberincident systémique. Le nombre d’appareils branchés à Internet s’accroît de façon exponentielle. Bien entendu, cette interconnexion a toutes sortes d’avantages. Mais imaginez qu’une institution financière est victime d’un piratage qui compromet non seulement ses propres données et opérations, mais aussi ceux de ses partenaires externes. Voilà le genre de scénario qui nous donne des cauchemars; un incident majeur qui perturbe les systèmes financiers nationaux et internationaux.

Cette interconnexion fait qu’il est très difficile de mesurer le risque d’un cyberincident systémique. Il est donc probable que les entreprises évaluent mal les ressources nécessaires pour s’en prémunir. Certaines pourraient sous-estimer l’investissement requis, faute d’internaliser le coût des effets systémiques du risque, et d’autres le surestimer. Quoi qu’il en soit, à mon avis, une meilleure collaboration pourrait donner une meilleure issue pour tous, et ce, sans faire monter les coûts. Personne ne perdrait au change; c’est là la beauté de la collaboration.

J’apprends beaucoup en travaillant jour après jour avec des économistes. Je me suis même familiarisé avec leur jargon. Par exemple, devant ce genre de problématique, ils parleraient sans doute de la « tragédie des biens communs ». Je vous explique. Dans une société où chaque personne doit mettre une ressource non renouvelable à la disposition des autres, règle générale, les gens subviendront tout d’abord à leurs propres besoins, sans beaucoup d’égard au bien commun. Le problème? Si chacun n’agit que dans son intérêt personnel, les ressources mises en commun s’épuiseront et tout le monde en souffrira.

Là où je veux en venir, c’est qu’il existe certaines situations où les gouvernements doivent intervenir pour le bien commun. Replongez-vous il y a une dizaine d’années, en pleine crise économique mondiale. Avant cela, la réglementation sur les banques était pensée en fonction de chaque institution, sans aucune perspective systémique et avec peu de considération pour les risques visant le système financier dans son ensemble. Souvent, les banques prenaient des risques sans réfléchir aux conséquences pour le reste du système financier.

Depuis la crise, les gouvernements ont adopté une perspective systémique et investi beaucoup d’énergie, au pays et à l’étranger, pour établir des conventions favorisant la sûreté du système financier.

Les parallèles entre bien commun et cybersécurité sont clairs. D’ailleurs, favoriser le bien commun est l’un des objectifs du Centre canadien pour la cybersécurité. Son mandat consiste à orienter les actions de l’État lors d’incidents de cybersécurité en veillant à une vaste collaboration entre fonctionnaires, universitaires et représentants du secteur privé pour régler les problèmes de cybersécurité complexes.

À plus grande échelle, mais toujours avec le même objectif, le gouvernement canadien a mis sur pied la Stratégie nationale de cybersécurité. En fait, dans le

budget fédéral de l'an dernier, il s'est engagé à injecter plus d'un demi-milliard de dollars supplémentaires dans la cybersécurité.

Heureusement, les grandes institutions financières canadiennes ont montré qu'elles reconnaissent le besoin d'élargir leur perspective. Elles comprennent qu'une attaque portée contre une seule institution peut vite s'étendre à toutes les autres.

Dans cet ordre d'idées, la Banque a fait appel aux six plus grandes banques canadiennes, ainsi qu'aux principaux fournisseurs de systèmes de paiement, de compensation et de règlement du pays, pour collaborer au Programme de résilience du système de paiement de gros. Cette initiative marque un grand pas en avant, et j'applaudis l'esprit de coopération et la transparence dont font preuve nos partenaires.

Tout récemment, nous avons mis sur pied le Groupe sur la résilience du secteur financier canadien, qui réunit d'importants acteurs du système financier, ainsi que des représentants du ministère des Finances Canada et du Bureau du surintendant des institutions financières. Son mandat : gérer tout éventuel incident opérationnel systémique, notamment en mettant à l'épreuve des protocoles de résilience et en cherchant des moyens d'améliorer l'échange d'information entre les participants.

Jusqu'à présent, nos efforts collaboratifs ont permis de renforcer la confiance entre les institutions financières du pays. Mais la confiance se perd plus vite qu'elle ne se gagne. Ainsi, il est impératif de ne pas la tenir pour acquise et de continuer à lever les obstacles qui se présentent si nous voulons mieux travailler et mieux collaborer.

Une réglementation efficace

Comment peut-on lever de tels obstacles à la collaboration? Peut-être devrions-nous tirer des leçons de nos « adversaires », les pirates informatiques, qui sont des as dans ce domaine. Bien sûr, ils n'ont pas à rendre de comptes à des avocats, des organismes de réglementation et des actionnaires. C'est bien dommage, mais leur collaboration est récompensée. Le fait est que nous devons sortir des sentiers battus pour éliminer les obstacles à la mise en commun de l'information.

Il arrive que des cadres réglementaires conçus pour protéger les institutions et les clients nuisent à la collaboration. Par exemple, les institutions ont parfois déclaré que la loi les empêchait de fournir des renseignements au sujet de la cybersécurité.

Traditionnellement, la réglementation a été axée sur la protection de la vie privée et la promotion de la concurrence. Ce sont des objectifs importants, mais il faut s'intéresser davantage à la résilience du secteur financier. Ainsi, nous devrions envisager d'actualiser les règlements qui n'ont pas encore été revus, et réfléchir aux compromis nécessaires pour y parvenir.

Qu'est-ce que j'entends par « compromis »? Par exemple, face à la menace terroriste, certains pays comptent sur l'utilisation généralisée de la télévision en circuit fermé et les avancées de la technologie de reconnaissance faciale pour améliorer la sécurité. Ces technologies soulèvent évidemment des enjeux de

protection de la vie privée, mais ces pays ont décidé que le compromis en valait la peine pour le bien commun.

De la même manière, tous ceux qui interviennent dans le domaine de la cybersécurité doivent se demander quel type de réglementation permet d'atteindre un bon équilibre entre confidentialité et concurrence, tout en offrant une protection globale contre les cybermenaces.

Notre cadre réglementaire doit certainement favoriser la coopération et la mise en commun de l'information, de façon à réduire le risque qu'une cyberattaque soit fructueuse. À tout le moins, un tel cadre ne doit pas nuire à la collaboration.

À mon avis, nous avons besoin d'une approche en deux volets qui tient compte tant de l'hésitation à divulguer de l'information que de la nécessité d'investir adéquatement dans la cybersécurité.

Il serait possible de renforcer notre cadre réglementaire en créant des canaux fiables et sûrs pour transmettre des renseignements délicats, de manière à protéger la réputation des institutions et à ne pas accroître leurs vulnérabilités.

De plus, les gouvernements pourraient envisager de resserrer les exigences minimales de cyberrésilience, et d'imposer des tests sectoriels et intersectoriels qui obligeraient les institutions à régler les problèmes soulevés.

Je ne pense pas que nous allons concevoir la réglementation parfaite aujourd'hui. Cependant, selon moi, il est possible d'améliorer notre cadre réglementaire actuel qui s'appuie – mais pas exclusivement – sur des sanctions financières. Après tout, si la direction d'une entreprise est incapable d'évaluer précisément le risque qu'un cyberincident systémique se produise, elle pourrait bien se dire que l'amende imposée en cas de non-conformité à la réglementation est un coût qu'il vaut la peine de payer.

Les autorités doivent donc réfléchir à la meilleure façon de concevoir des cadres s'appuyant sur des mesures qui incitent les organisations à coopérer et à mettre l'information en commun, et faire en sorte que la loi protège celles qui le font.

Il faut veiller à la neutralité technologique de la réglementation, afin que celle-ci reste adaptée aux changements qui surviendront inévitablement. Nous devrions aussi viser des réformes législatives compatibles avec les normes internationales, et qui utilisent des approches et un vocabulaire communs. Cela encouragera la collaboration transfrontière et réduira les possibilités pour les entreprises de profiter du fait que certains territoires appliquent des règles moins strictes en matière de cybersécurité.

Les administrations nationales doivent non seulement promouvoir des mesures de protection à l'intérieur de leurs frontières, elles doivent aussi coopérer entre elles afin de favoriser la cybersécurité à l'échelle mondiale. En effet, aucun mur n'empêche les cyberattaques de se propager d'un pays à l'autre. Étant donné les interconnexions entre les institutions financières internationales, la Banque est également tenue de collaborer avec des partenaires d'autres territoires de compétence.

Plus tôt cette année, le G7 a organisé un exercice de simulation de cybercrise auquel des ministères des Finances, des autorités de surveillance bancaire et

des banques centrales ont participé. Les participants ont alors eu l'occasion d'examiner les outils dont leur pays dispose pour réagir à un tel événement. L'exercice a aussi soulevé d'importantes questions concernant la façon et le moment de communiquer avec les partenaires internationaux si une cybercrise devait survenir.

La collaboration et la voie à suivre

En plus de nous efforcer d'améliorer les cadres réglementaires, nous nous engageons à tenir régulièrement des tests réalistes et rigoureux qui mettent à l'épreuve les cyberdéfenses de l'ensemble du système financier canadien, ce qui n'est pas sans rappeler l'exercice du G7. Cette approche consolidera l'esprit de collaboration des institutions financières, optimisera la capacité de protéger le système et réduira au minimum les délais de reprise des activités.

Il est tout aussi important que l'esprit de collaboration ne se limite pas au secteur financier et qu'il se répande à d'autres secteurs constituant une partie de l'infrastructure essentielle de notre pays, comme les télécommunications, l'énergie et les services publics, ainsi que le transport. Il nous faut accroître sans tarder la collaboration dans toute l'économie canadienne. Nous devons inciter les entreprises à participer régulièrement à des exercices complexes qui mettent à l'épreuve leurs cyberdéfenses et leur capacité d'intervention. Même la conception de scénarios de risque peut aider les entreprises à déterminer les sources potentielles de risque.

Le secteur privé a également un rôle à jouer. Je suis ravi de constater que des entreprises collaborent pour établir des pratiques de cybersécurité exemplaires. En particulier, je suis heureux que l'ACTI se soit associée au Conseil stratégique des DPI dans le cadre de l'initiative sur les technologies responsables. Comme vous le savez, un des objectifs de cette initiative consiste à accroître la collaboration, l'expertise et les connaissances dans tous les secteurs. Je suis convaincu que l'ACTI peut aider à souligner l'urgence de ces objectifs sur le plan de la cybersécurité.

Tous ces efforts ont suscité la participation d'acteurs clés et permis d'établir des objectifs communs. Toutefois, ils ont aussi montré que des défis importants demeurent, et qu'il faut agir rapidement et avec fermeté pour les relever. Après tout, la technologie et les menaces à notre sécurité évoluent à une vitesse incroyable. Alors, quelles sont les prochaines étapes?

Permettez-moi de suggérer quelques voies à explorer. D'abord, des groupes sectoriels pourraient collaborer avec des autorités publiques, y compris des organismes de réglementation et de renseignement, pour concevoir et mettre en œuvre le type d'exercices nationaux de cybersécurité dont j'ai parlé plus tôt, notamment des tests d'intrusion.

Ces exercices peuvent aider les entreprises à mieux réagir et à approfondir les relations nécessaires pour repousser les attaques. Il est maintenant temps de créer des tests plus exigeants et réalistes destinés à plusieurs secteurs, afin de mettre à l'épreuve la cybersécurité de notre économie.

Un autre moyen non négligeable de renforcer la résilience passe par une meilleure communication. Il faut instaurer des mécanismes qui accroîtront

considérablement la mise en commun de l'information sur les cybermenaces et des pratiques exemplaires de cyberdéfense entre les organisations des secteurs public et privé. Cela est particulièrement important pour les petites entreprises qui disposent de moins de ressources à consacrer à la cybersécurité.

Nous devrions également songer aux possibilités de concevoir des méthodes et des systèmes sectoriels – plutôt qu'individuels – de cyberdéfense, qui protégeraient un grand nombre d'organisations et optimiseraient leur résilience. Pensons aux fournisseurs de services infonuagiques, auxquels de nombreuses petites et moyennes entreprises confient des tâches précises pour ainsi se concentrer sur leurs activités principales.

Conclusion

Quelles que soient les avancées de la cybersécurité, il est évident que le secteur des technologies de l'information contribuera de manière importante aux solutions proposées. Pour terminer, j'aimerais dire quelques mots au sujet du rôle que les professionnels comme vous jouent dans l'amélioration de la cybersécurité pour tous.

Premièrement, en tant que membre de l'administration publique, j'estime qu'il est essentiel de tirer parti de votre expertise et de votre capacité d'adaptation pour élaborer des politiques de cybersécurité efficaces. Nous avons besoin de votre point de vue afin de protéger le système le mieux possible sans étouffer l'innovation et la créativité.

Deuxièmement, nous devons nous associer à vous pour découvrir des techniques qui permettront de résoudre les problèmes de cybersécurité les plus épineux. Quelle est la meilleure façon d'intégrer l'intelligence artificielle aux cyberdéfenses, y compris pour se prémunir contre les menaces internes? À quelle vitesse les machines peuvent-elles apprendre à détecter la fraude et s'adapter aux nouvelles techniques frauduleuses? Si l'informatique quantique est susceptible de rendre les méthodes actuelles de chiffrement des données obsolètes, quels nouveaux moyens permettraient de protéger nos données?

Je souhaite donc vous lancer un défi, si on peut dire. J'ai parlé de certaines des grandes questions de cybersécurité auxquelles nous sommes aujourd'hui confrontés. Je vous inviterais à tenter de trouver la réponse à ce type de questions cruciales pour la sécurité de l'économie canadienne. Et, bien entendu, les réponses seront extrêmement précieuses pour l'entreprise qui les trouvera!

J'aimerais vous remercier encore une fois de m'avoir invité à me joindre à vous aujourd'hui. J'espère avoir répondu à vos attentes, c'est-à-dire avoir su vous expliquer comment la Banque du Canada contribue à assurer la résilience et la sécurité du système financier.

J'espère aussi avoir réussi à faire valoir pourquoi il est essentiel de collaborer si nous voulons atteindre cet objectif important.

Enfin, j'espère vous avoir fourni des renseignements utiles sur les mesures de cybersécurité que nous avons prises jusqu'à présent, et sur tout ce qu'il reste à faire en la matière.

Je serais maintenant heureux de répondre à vos questions.