BANQUE DU CANADA
BANK OF CANADA

Discours prononcé par Filipe Dinis
Chef de l'exploitation de la Banque du Canada
Paiements Canada
Toronto (Ontario)
9 mai 2018

Renforcer nos cyberdéfenses

Introduction

Merci de cette invitation à prendre la parole devant vous aujourd'hui.

La possibilité de contrôler ses électroménagers à distance ou d'encaisser un chèque en quelques clics à partir de son téléphone n'a déjà plus rien de révolutionnaire. Ces innovations ont été introduites et adoptées à grande échelle en un temps record, et bien d'autres sont en chantier. De toute évidence, le rythme des changements technologiques n'est pas près de ralentir.

C'est ce que je constate dans ma propre famille. Je commençais à peine à me débrouiller avec les nouvelles méthodes de paiement que mes trois enfants – y compris ma fille de 12 ans – les qualifiaient de « complètement dépassées ».

Le projet de modernisation lancé par notre hôte, Paiements Canada, vise à renforcer les bases du système de paiement ainsi qu'à favoriser l'innovation et la concurrence dans l'écosystème du paiement de détail. Cependant, rien ne sert d'accroître la rapidité du système de paiement de détail si ses utilisateurs ne sont pas convaincus que les renseignements sur leurs comptes et leurs transactions seront mieux protégés.

Le maintien de la confiance des Canadiens est tout aussi essentiel lorsqu'il est question du système financier dans son ensemble. Il faut de solides mécanismes de protection au sein de chaque institution et d'étroites relations de collaboration entre les organismes publics et le secteur privé pour favoriser l'échange d'information sur les cybermenaces et renforcer nos défenses sur tous les fronts.

Toutefois, malgré tous nos efforts, il est inévitable que certaines attaques ne pourront être déjouées. Compte tenu de la fréquence et du raffinement des piratages informatiques, il est primordial que la population sache que si l'improbable devait se produire, des mécanismes de reprise sont déjà en place. Limiter les dommages et assurer un rétablissement rapide du système revêt une importance capitale.

Voilà le sujet dont j'ai choisi de vous entretenir aujourd'hui : les dispositifs de cybersécurité et les plans de reprise des activités. Dans un premier temps, je ferai un survol des cyberrisques, puis j'expliquerai le mandat de la Banque du

Je tiens à remercier Paul Chilcott, Ron Morrow, Grahame Johnson et Sylvain Chalut de l'aide qu'ils m'ont apportée dans la préparation de ce discours.

Canada et le rôle qu'elle joue en ce qui concerne la cybersécurité du système financier. Je décrirai ensuite ses trois grandes priorités à cet égard et présenterai les partenaires avec lesquels elle collabore, ici et ailleurs dans le monde. Je terminerai en passant en revue les mesures qui sont mises en œuvre.

Cybermenaces et risques systémiques

Pensez à toutes les façons dont vous pouvez accéder à vos comptes bancaires, hormis faire la queue en attendant qu'un caissier se libère. Vous pouvez utiliser votre montre ou votre cellulaire, une tablette, un guichet automatique ou un terminal de point de vente. Songez aussi à tous les commerçants ou créanciers qui acceptent des paiements électroniques. Toutes ces opérations se déroulent de manière relativement fluide, et le programme de modernisation rendra leur exécution encore plus efficace. En effet, grâce au système de paiement de détail en temps réel – l'une des composantes du programme –, les opérations seront finalisées, et les fonds, virés, en l'espace de quelques secondes, au lieu de plusieurs jours.

Or, sur bien des plans, ce n'est qu'un début. L'économie numérique est en plein essor, portée par des technologies émergentes telles l'intelligence artificielle, la robotique et la biométrie. Le nombre d'appareils électroniques donnant accès à Internet croît de manière exponentielle, et chacun multiplie les connexions entre les utilisateurs et les services disponibles.

Le secteur financier évolue au rythme de ces changements en investissant dans des innovations qui réduiront ses coûts et enrichiront l'expérience de ses clients. Si nous souhaitons tous des services plus rapides et de meilleure qualité, il faut savoir que l'adoption grandissante de nouvelles technologies et la constitution de mégabanques de renseignements sur les clients augmenteront d'autant les incitations à perpétrer des cyberattaques et les risques associés à celles-ci.

Les banques, les coopératives de crédit et d'autres acteurs du système financier canadien traitent quotidiennement des paiements en espèces d'une valeur de 175 milliards de dollars et des opérations sur actions et obligations totalisant plus de 500 milliards de dollars. Avec des chiffres pareils, on ne peut s'étonner que le système financier international soit devenu une cible de choix pour les cybercriminels[1].

Les institutions financières canadiennes se sont dotées de mécanismes de défense solides pour repousser les tentatives de vol d'argent ou d'information, ou simplement de perturbation de leurs opérations. Or, ce ne sont pas les institutions en tant que telles qui nous préoccupent, mais leurs interconnexions. Les protections mises en place par chaque institution constituent certes une excellente première ligne de défense, mais elles doivent s'accompagner de mesures efficaces à l'échelle du secteur étant donné qu'une intrusion réussie – quoique rare – dans un établissement pourrait rapidement engendrer une perturbation qui gagnerait l'ensemble du système financier.

---

[1] E. Kopp, L. Kaffenberger et C. Wilson (2017), *Cyber Risk, Market Failures, and Financial Stability*, document de travail nº WP/17/185, Fonds monétaire international.

J’aimerais maintenant aborder le rôle que joue la Banque du Canada dans le renforcement de la cybersécurité du système financier.

Atténuation des risques

Une des responsabilités de la Banque du Canada est de promouvoir la stabilité et l’efficience du système financier. L’ampleur et la gravité des cybermenaces ne cessant de s’accroître à l’échelle mondiale, notre institution consacre davantage de temps et d’attention aux menaces pesant sur la stabilité financière.

Comment la Banque contribue-t-elle à atténuer ces risques? Eh bien, son action s’articule autour de trois axes prioritaires.

Tout d’abord, elle investit et met tout en œuvre pour s’assurer de pouvoir faire face aux cybermenaces à son encontre.

Deuxièmement, elle veille à ce que les infrastructures de marchés financiers soumises à sa surveillance prennent des mesures adéquates pour atténuer les cybermenaces.

Et, troisièmement, elle collabore avec les participants du système financier ainsi qu’avec les organismes de réglementation et de surveillance nationaux et internationaux pour accroître la résilience du système financier.

Permettez-moi de vous donner quelques précisions au sujet de chacun de ces axes prioritaires.

Gestion des cybermenaces à l’encontre de la Banque

Dans l’un de ses récents discours, le gouverneur Stephen Poloz a mentionné que les cybermenaces étaient une des choses qui l’empêchaient de dormir la nuit. Si c’est vrai pour lui, je peux vous affirmer qu’il en est de même pour moi.

La Banque ne cesse d’investir dans son programme de cybersécurité et de l’améliorer afin de prévenir, de détecter et de contrer toute une gamme de cybermenaces en rapide évolution, qui sont susceptibles de compromettre la confidentialité, l’intégrité et la disponibilité de ses renseignements numériques. Les mesures de sécurité mises en place comportent plusieurs volets, respectent les normes internationales en la matière et sont constamment actualisées.

Dans le but de protéger ses systèmes internes, la Banque a soumis ses réseaux à des tests d’intrusion, amélioré ses processus de contrôle d’accès et déployé des outils de dépistage des vulnérabilités. Elle veille également au chiffrement de ses données et procède régulièrement à des mises à jour de sécurité.

De plus, la Banque informe périodiquement ses employés des pratiques optimales en matière de sécurité liée aux activités en ligne ou à la messagerie électronique afin de les sensibiliser au risque de cyberattaque et de favoriser les comportements appropriés. Même si elle a constaté une nette amélioration de la capacité de son personnel à repérer les courriels d’hameçonnage, la Banque est bien consciente qu’elle doit rester vigilante.

La Banque surveille également l’environnement extérieur pour détecter les cybermenaces et y réagir. Dans ce cadre, elle recueille et analyse des renseignements sur les menaces, procède à l’examen exhaustif des tierces parties avec lesquelles elle interagit, met en œuvre un programme rigoureux de

gestion des accès et voit à l'instauration de contrôles de sécurité plus rigoureux pour le système SWIFT.

En outre, la Banque investit beaucoup dans ses redondances opérationnelles de manière à renforcer la résilience de ses systèmes et de son personnel. Il est en effet crucial que ses fonctions essentielles soient maintenues en cas de perturbation majeure, que cette dernière résulte d'une cyberattaque ou d'une catastrophe naturelle.

Enfin, la Banque met en place des stratégies visant à limiter les dommages que de telles attaques pourraient causer et, le cas échéant, à lui permettre de reprendre rapidement ses activités. Je reviendrai sur ce point dans quelques instants.

La surveillance des infrastructures de marchés financiers

La Banque est responsable de la surveillance réglementaire des infrastructures de marchés financiers (IMF) qui ont, selon elle, atteint une masse critique faisant en sorte qu'une perturbation les touchant pourrait avoir des effets sur l'ensemble du système financier. On trouve parmi celles-ci le Système de transfert de paiements de grande valeur et le Système automatisé de compensation et de règlement, dont Paiements Canada est le propriétaire et l'exploitant. Les IMF servent de plateformes centrales pour les transactions financières, et les interconnexions qui existent avec elles garantissent la sûreté et l'efficience des échanges de fonds, de titres et d'autres produits financiers.

Compte tenu du rôle central que jouent les IMF dans le système financier, une interruption de service prolongée, une violation de l'intégrité des données ou une perte de confiance à leur égard pourraient avoir des répercussions considérables sur le système financier et l'économie réelle. Il est donc de la plus haute importance de les protéger contre les cybermenaces.

La Banque du Canada a contribué à la rédaction de lignes directrices internationales sur la cybersécurité. Elle s'en sert d'ailleurs pour s'assurer que les IMF qu'elle surveille prennent les mesures appropriées pour atténuer les cybermenaces. Les IMF évaluent leur propre cyberrésilience à l'interne, et elles font aussi appel à des experts de l'extérieur pour procéder à des évaluations indépendantes. La Banque étudie toutes ces évaluations, veillant ainsi à l'adéquation des outils et des pratiques de cybersécurité mis en œuvre.

L'un des sujets de préoccupation de la Banque concerne le risque opérationnel croissant lié à un groupe très concentré de tiers qui procurent au secteur financier la plupart des nouvelles technologies qui lui sont devenues indispensables. Certains de ces fournisseurs proposent des services cruciaux dans les domaines du traitement des données et de l'infonuagique, lesquels ne sont pas du ressort des instances de réglementation. Comme l'a souligné récemment le Conseil de stabilité financière, le fait de s'appuyer sur les mêmes fournisseurs, conjugué aux interconnexions entre les institutions, est susceptible de poser un risque pour l'ensemble du système financier. La gestion de ce risque systémique passe par une plus grande coordination à l'échelle internationale.

La Banque participe aussi activement au programme de modernisation de Paiements Canada. Elle entend ainsi veiller à ce que la cyberrésilience figure en tête des priorités pour la refonte des systèmes de paiement et de règlement.

Le gouverneur Poloz a récemment lancé un important projet – que je pilote – établissant un partenariat avec les six grandes banques canadiennes en vue de tester et d'améliorer la cyberrésilience de l'écosystème de paiement dans son ensemble. L'objectif est de faciliter un rétablissement rapide et collaboratif dans l'éventualité où un participant clé serait victime d'un cyberincident grave, comme la corruption de données cruciales entraînant une interruption de service prolongée.

Accroître la résilience par la collaboration

Compte tenu des interconnexions nationales et internationales du système financier, il importe de communiquer, de coordonner et d'harmoniser nos efforts avec ceux des autres participants.

Au pays, la Banque étudie et évalue les vulnérabilités et les risques qui pèsent sur le système financier. Dans sa livraison de novembre de la *Revue du système financier*, elle considère la possibilité de cyberattaques contre le système financier comme une grande source de vulnérabilité et explique qu'elle travaille de concert avec les participants du secteur, des instances internationales, ainsi que les autorités fédérales et provinciales tant pour optimiser la communication de l'information que pour améliorer les politiques en la matière.

La Banque veille à ce que les IMF canadiennes s'entretiennent avec les instances pertinentes en matière de sécurité, telles que le Centre de la sécurité des télécommunications (CST) et le Service canadien du renseignement de sécurité.

La stratégie nationale de cybersécurité exposée dans le plus récent budget fédéral est une avancée importante à cet égard. Le gouvernement allouera quelque 507 millions de dollars sur cinq ans, et près de 110 millions par an par la suite, pour mettre en place un écosystème cybernétique novateur et adaptable. Cette stratégie vise à appuyer un leadership et une collaboration efficaces entre les différents ordres de gouvernement, le milieu des affaires, le milieu universitaire et des partenaires internationaux de confiance.

La création d'un centre canadien pour la cybersécurité est un autre élément, tout aussi important, de cette stratégie. Le centre deviendra une source unifiée de conseils, d'orientations, de services et de soutien spécialisés concernant les questions opérationnelles liées à la cybersécurité. La Banque a hâte de mettre à profit les étroites relations qu'elle entretient déjà avec le CST et le nouveau centre.

En vue d'améliorer non seulement la préparation des IMF en cas de cyberattaque, mais aussi leur résilience opérationnelle et, au-delà, celle du système financier, la Banque a contribué à instaurer le Programme de gestion conjointe des mesures favorisant la résilience des opérations. Ce projet, qu'elle préside, est mené en partenariat avec le ministère des Finances, les IMF et les grandes banques canadiennes ainsi que l'Association des banquiers canadiens. Dans le cadre du Programme, il a été organisé l'an dernier un exercice de

simulation d'une journée et demie – mais qui a pris 20 mois à planifier –, auquel étaient associés plus de 180 participants dans trois villes distinctes. L'objectif était d'évaluer les protocoles de communication et de transmission de l'information aux paliers décisionnels supérieurs ainsi que les messages adressés au public à l'échelle nationale en cas de crise systémique. Pour ce faire, nous avons simulé la défaillance opérationnelle d'une IMF d'importance systémique, qui aurait interrompu les opérations sur les principaux marchés boursiers et obligataires canadiens pendant plus de 30 heures.

Ayant tiré plusieurs leçons essentielles de cet exercice, nous nous employons désormais à rehausser la capacité du secteur financier de coordonner les mesures à prendre dans l'éventualité où une interruption aussi grave se produirait.

L'enseignement sans doute le plus important a trait à la valeur que revêtent les partenariats et relations de confiance parmi les organismes de réglementation, les participants du système financier et d'autres secteurs. Les entreprises du système financier connaissent chacune leur métier, mais pas forcément tous les rapports qui existent entre elles. Elles risquent alors de prendre des décisions sans avoir la moindre idée des menaces qui pèsent sur le système.

Nous avons également découvert – et ce n'est certainement pas l'apanage de cet exercice – l'importance des protocoles en matière de communication et de coordination en cas de crise systémique. Dans de telles circonstances, confusion et ambiguïté sont à proscrire à tout prix. C'est pourquoi nous nous attachons maintenant à concevoir de meilleurs protocoles, qui permettront d'éviter ces écueils.

Au niveau international, la Banque fait partie d'organisations qui lui permettent de rester dans la course sur le plan stratégique. Il en est notamment ainsi de l'élaboration des politiques de réglementation et de supervision tout comme de la promotion de la résilience du système financier.

À titre d'exemple, la Banque participe aux travaux du groupe d'experts du G7 sur la cybersécurité, qui a été mis sur pied pour renforcer la cybersécurité au sein du système financier international. Comme les cybermenaces ne connaissent pas de frontières, nous coordonnons les échanges avec les membres de ce groupe sur les politiques à envisager dans des domaines tels que les risques associés aux tiers et les tests d'intrusion.

La Banque est aussi membre du groupe de surveillance international du réseau SWIFT, lequel voit à la cyberrésilience des services de messagerie SWIFT. Cette participation aide notre institution à améliorer tant son dispositif de cybersécurité que celui du système financier en général.

La Banque collabore enfin avec les représentants d'autres pays du G7, la Banque des Règlements Internationaux et de nombreuses banques centrales pour discuter des menaces émergentes, des réponses à y apporter, de la surveillance de la sécurité et de questions connexes.

Conclusion

Permettez-moi de synthétiser. Les cybermenaces ne sont pas près de disparaître, et nous devons constamment ajuster nos efforts en conséquence. De

fait, les menaces évoluent sans cesse, et l’économie numérique croît rapidement. Désormais, il ne suffit plus à chaque institution de maintenir son propre système d’alarme, quand bien même celui-ci procure un certain niveau de protection et de confort. Il faut maintenant investir dans des défenses de nature systémique.

Pour ce faire, une étroite collaboration entre les secteurs public et privé est nécessaire, au Canada comme à l’étranger, pour échanger des informations et élaborer des stratégies de détection, d’intervention et de rétablissement des opérations en cas de cyberincident.

Cela passe obligatoirement par l’établissement et le maintien de relations de confiance avec nos partenaires, qui savent que l’information qu’ils nous communiquent demeurera protégée.

Merci.