Résilience du système financier canadien : l'apport de la cybersécurité

Harold Gallagher, Wade McMahon et Ron Morrow

- Les cyberattaques sont une source potentielle de risque systémique, car elles sont susceptibles de perturber les opérations des principaux participants au système financier canadien.
- La résilience opérationnelle des principaux participants — à savoir les grandes institutions financières et les infrastructures de marchés financiers auxquelles elles participent — se trouve au cœur même de la résilience globale du système financier.
- Les menaces qui planent sur les différentes composantes du système financier canadien émanent de groupes hétérogènes disposant d'habiletés et de moyens très variés.
- Les institutions financières et les infrastructures de marchés financiers du Canada se sont montrées proactives en renforçant leur défense et en collaborant de façon dynamique entre elles et avec le gouvernement fédéral, afin de combattre les cyberattaques.

Introduction

La bonne tenue du système financier dépend de la résilience opérationnelle collective des institutions financières et des systèmes de règlement et de compensation des paiements qui facilitent leurs transactions. Ces systèmes, désignés par le terme générique « infrastructures de marchés financiers » (IMF), font office de plateforme centrale pour les transactions et assurent un lien entre les institutions financières. La résilience des relations entre les institutions et les IMF est essentielle à la sûreté et à l'efficience du système financier. Toutefois, ces relations peuvent aussi servir de canaux de propagation des chocs. L'impressionnante résilience opérationnelle qui caractérise les activités du secteur financier depuis bon nombre d'années ne doit pas conduire au relâchement. Une grave interruption des transactions et des services causée par un incident opérationnel, telle une cyberattaque, risquerait de créer des perturbations à l'échelle du système financier.

Pour remédier à ces vulnérabilités, les institutions financières et les IMF canadiennes mobilisent des ressources et fournissent des efforts considérables de manière à mettre leurs activités à l'abri d'un large éventail de perturbations (catastrophes naturelles, pannes de courant, attentats, etc.). Cependant, la montée en puissance des cyberattaques soulève toute une gamme de nouveaux défis en matière de résilience opérationnelle. Les cyberattaques sont des actes malveillants commis par un individu ou un groupe dans le but de compromettre l'intégrité des systèmes et dispositifs technologiques d'une institution, ou encore d'y accéder clandestinement. À l'échelle du globe, le nombre moyen de cyberattaques à l'endroit des institutions financières a grimpé de 169 % entre 2012 et 2013 (PricewaterhouseCoopers, 2013). Les IMF sont moins souvent ciblées, mais leur forte utilisation de technologies peut les exposer à des cyberattaques déstabilisantes.

Le présent rapport étudie l'importance grandissante que revêtent les cyberattaques en tant que source potentielle de risque systémique, les différents acteurs qui les commettent ainsi que les méthodes qu'ils utilisent. Après un examen des risques associés aux cyberattaques, nous décrirons certaines des mesures prises par les organisations internationales, les institutions financières, les IMF et le gouvernement fédéral pour renforcer la cybersécurité.

Les infrastructures de marchés financiers essentielles

Les IMF favorisent la sûreté et l'efficience des échanges de fonds, de titres et d'autres produits financiers entre des institutions financières, comme les banques, et les

maisons de courtage. Ces entités sont tributaires des IMF, car celles-ci facilitent les transactions nécessaires à l'exercice de leurs activités. Au Canada, les IMF sont à même de traiter quotidiennement des paiements en espèces de l'ordre de 150 milliards de dollars, ainsi que des opérations sur actions et obligations totalisant plus de 450 milliards de dollars.

Il est possible que des défaillances opérationnelles touchant les IMF aient une incidence sur le risque systémique. Plus particulièrement, l'incapacité d'une institution à s'acquitter de ses obligations de paiement ou de règlement auprès d'une IMF pourrait empêcher d'autres participants de satisfaire à leurs propres obligations, ce qui déclencherait des défaillances à la chaîne dans l'ensemble du système financier. Comme les IMF sont susceptibles de présenter un risque systémique, elles sont soumises à la surveillance de la Banque du Canada, dans le but d'assurer le bon fonctionnement du système financier canadien (**Encadré 1**).

Encadré 1

Les IMF assujetties à la surveillance de la Banque du Canada

Les infrastructures de marchés financiers (IMF) sont des systèmes qui facilitent la compensation, le règlement et l'enregistrement de paiements, de titres et de produits dérivés ou d'autres transactions financières entre les entités participantes. Les IMF permettent aux consommateurs et aux entreprises d'acheter des biens et des services, de procéder à des placements et de virer des fonds de manière sûre et efficiente.

Certaines IMF sont dites « d'importance systémique », car elles peuvent présenter des risques qui menacent l'ensemble du système financier. De fait, l'incapacité d'un participant de remplir ses obligations de paiement ou de livraison envers ce genre d'IMF pourrait empêcher d'autres participants de s'acquitter de leurs obligations, ce qui entraînerait la diffusion de risques à l'échelle du système financier, par effet de contagion. Pour que le risque systémique soit bien maîtrisé, il est donc essentiel de doter ces IMF de mécanismes de contrôle appropriés. Le gouverneur de la Banque du Canada a désigné plusieurs IMF comme étant d'importance systémique pour le système financier canadien, les soumettant ainsi à la surveillance de la Banque (**Tableau 1-A**)[1]. Cette surveillance vise, d'une part, à faire en sorte que le fonctionnement des IMF d'importance systémique soit assorti d'une gestion adéquate des risques et, d'autre part, à accroître l'efficience et la stabilité du système financier canadien.

1 Pour en savoir davantage sur la surveillance exercée par la Banque du Canada, voir son site Web, à l'adresse http://www.banqueducanada.ca/grandes-fonctions/systeme-financier/surveillance-systemes-designes-compensation-reglement.

Tableau 1-A : Activités menées par les IMF d'importance systémique en 2013

	Volume	Valeur (milliards $ CAN)
Système de transfert de paiements de grande valeur		
▪ Traitement de gros paiements à délai de règlement critique		
▪ Exploité par l'Association canadienne des paiements		
▪ Nombre moyen et valeur moyenne des transactions en dollars canadiens réglées chaque jour :	30 000	150
CDSX		
▪ Règlement d'opérations sur actions et titres à revenu fixe		
▪ Exploité par la Caisse canadienne de dépôt de valeurs limitée		
▪ Nombre moyen et valeur moyenne des transactions en dollars canadiens réglées chaque jour :	1 372 000	452
Service canadien de compensation de produits dérivés		
▪ Compensation d'opérations de pension et de produits dérivés		
▪ Exploité par la Corporation canadienne de compensation de produits dérivés	--	20
▪ Valeur moyenne des opérations de trésorerie et de pension compensées chaque jour :		
▪ Valeur moyenne (encours notionnel) des produits dérivés négociés en bourse compensés chaque jour :	--	101
Système de la Continuous Linked Settlement Bank		
▪ Règlement des opérations de change		
▪ Exploité par la CLS Bank		
▪ Nombre moyen et valeur moyenne des transactions en dollars canadiens réglées chaque jour :	27 000	126
SwapClear		
▪ Compensation de swaps de taux d'intérêt négociés de gré à gré		
▪ Exploité par LCH.Clearnet Limited		
▪ Valeur moyenne des swaps en dollars canadiens compensés chaque jour :	--	30

Source : Banque du Canada (2014)

Les cyberattaques et leurs auteurs

Les cyberattaques dirigées contre les institutions financières et les IMF canadiennes constituent une source de préoccupation croissante pour le gouvernement et le secteur financier. Les services offerts sur le Web, même s'ils sont ceux que le public connaît le mieux, ne représentent qu'une petite portion des technologies dont disposent les grandes institutions financières complexes. Or, des efforts considérables sont déployés pour empêcher les intrus de se servir des services en ligne comme d'un point d'accès aux réseaux, systèmes et données internes qui sous-tendent les activités de ces institutions. S'agissant des IMF, les systèmes internes sont habituellement séparés des applications Web, ce qui en fait des cibles plus difficiles à atteindre. Les IMF doivent néanmoins adapter leur cyberdéfense aux tactiques employées par les pirates, qui évoluent sans cesse et sont de plus en plus perfectionnées.

Les cyberpirates forment un groupe hétérogène, et la gravité de la menace qu'ils représentent dépend de leurs motivations et de leurs moyens (**Tableau 1**). Les répercussions des cyberattaques peuvent varier considérablement, mais la principale source potentielle de risque systémique provient des cyberpirates qui cherchent à entraver les opérations des institutions financières ou à affecter les fonctions essentielles des IMF (**Tableau 2**).

Les adversaires de haut rang sont des groupes de pirates bien organisés, dotés de ressources financières appréciables et possédant les capacités de nuisance les plus développées. Ils sont mus par des motifs autres

Tableau 1 : Les cyberpirates : catégories et capacités

Cyberpirates	Définition
Crime organisé	Groupes de pirates, principalement motivés par l'appât du gain, qui s'en prennent à des cibles mal protégées. Ils se servent de techniques utilisées par des cyberpirates mieux outillés.
Cybermilitants	Pirates dont les capacités s'apparentent à celles du crime organisé, mais qui sont mus par des motifs idéologiques plutôt que par l'appât du gain.
Adversaires de haut rang	Groupes de pirates disposant de moyens financiers et techniques suffisants pour mener des attaques de longue haleine; leurs motivations sont d'ordre économique, financier et politique.
Agents internes	Employés mécontents qui trahissent la confiance qui leur a été accordée en utilisant leur accès aux systèmes internes pour lancer des cyberattaques.
Tierces parties	Concurrents ou fournisseurs tentant d'accéder à des renseignements exclusifs ou de vendre sur le marché noir des informations à d'autres cyberpirates concernant les vulnérabilités d'un système.
Pirates solitaires doués	Individus qui cherchent à exploiter les vulnérabilités de leurs cibles afin d'acquérir une certaine notoriété ou de recevoir de l'argent.

Tableau 2 : Cartographie du risque : notation des cyberpirates selon leur incidence potentielle

	Incidence						
Cyberpirates	Vol ou fraude de nature financière	Vol d'actifs intellectuels liés aux plans stratégiques	Perturbation des opérations	Destruction d'infrastructures essentielles	Atteinte à la réputation	Menaces à la vie et à la sécurité	Retombées d'ordre réglementaire
Crime organisé							
Cybermilitants							
Adversaires de haut rang							
Agents internes							
Tierces parties							
Pirates solitaires doués							

Très élevée Élevée Modérée Faible

Nota : Ces cotes s'inspirent d'une évaluation des risques pesant sur les institutions financières qui a été menée par Deloitte.
Source : Deloitte Center for Financial Services (2014)

que le simple appât du gain. À titre d'exemple, il a été rapporté que des adversaires de haut rang avaient infiltré la bourse NASDAQ et avaient réussi à accéder à des renseignements confidentiels, vraisemblablement pendant plusieurs années, sans se faire repérer. Après la découverte de l'intrusion, les enquêteurs ont avancé l'idée que les pirates, compte tenu des moyens à leur disposition, auraient été en mesure de saboter les opérations des cibles infectées, ce qui va bien au-delà du cyberespionnage (Riley, 2014). Les conséquences de cette cyberattaque se sont apparemment limitées au vol de renseignements exclusifs, mais si les malfaiteurs avaient exploité toute l'étendue de leurs possibilités, les perturbations occasionnées auraient pu causer un risque de nature systémique.

L'attaque contre la bourse NASDAQ a montré que les pirates avaient profité des défauts de l'architecture informatique pour accéder aux systèmes internes. Les failles Heartbleed et Shellshock sont des exemples de vulnérabilités analogues. Elles pourraient permettre à des pirates d'exploiter les faiblesses des logiciels courants pour s'emparer de données de nature délicate, modifier le contenu de sites Web ou compromettre l'intégrité des ordinateurs d'internautes (Symantec, 2014). Une autre technique largement utilisée est le « harponnage »; elle consiste à envoyer des messages électroniques personnalisés aux employés d'une organisation. L'ouverture de ces courriels déclenche l'installation de logiciels malveillants qui permettent à des intrus de pénétrer les systèmes internes.

Les activités des institutions financières et des IMF peuvent également faire l'objet d'attaques plus fréquentes, mais de moindre ampleur, de la part de groupes aux capacités moins développées. Ces attaques sont souvent le fait de cybermilitants qui cherchent davantage à nuire aux opérations d'une organisation qu'à s'enrichir. Les attaques par saturation, un exemple d'activité menée par ces activistes du cyberespace, consistent à submerger les réseaux d'une société en manipulant ou en redirigeant le trafic Internet. Les institutions financières sont souvent la cible d'attaques quotidiennes de ce type, qui ont, dans certains cas, causé la paralysie de sites Web et l'interruption des services en ligne de grandes banques internationales (Nguyen, 2013; Crosman, 2014). De telles attaques, lorsqu'elles aboutissent, posent un risque d'atteinte à la réputation en raison des pannes temporaires qu'elles occasionnent dans les services en ligne. Elles ne compromettent toutefois pas l'intégrité des systèmes internes.

Par ailleurs, de nombreuses cyberattaques sont motivées par l'appât du gain. C'est plus particulièrement le cas des vols de données exclusives et d'informations financières (cyberespionnage), qui peuvent être commis par différents groupes de cyberpirates, notamment par des concurrents, des tierces parties ou des agents internes (des membres du personnel d'une organisation). Il est particulièrement difficile de se prémunir contre les menaces provenant d'agents internes, puisque ceux-ci disposent de droits d'accès aux systèmes. Le cyberespionnage ne touche pas que les institutions financières ou les IMF : des organes publics peuvent également en être victimes (Perlroth, 2014; Weston, 2011). Bien que ce genre d'attaques n'entrave pas nécessairement le fonctionnement des établissements, l'incapacité des institutions financières ou des IMF à protéger la confidentialité de leurs transactions pourrait miner la confiance portée au système financier.

Les cyberattaques destinées plus directement à générer des profits, par des vols ou des fraudes, sont elles aussi susceptibles d'ébranler la confiance dans le système financier. Des groupes liés au crime organisé ont récemment commencé à employer des techniques et des outils plus diversifiés qui étaient auparavant l'apanage des cyberpirates les plus sophistiqués. Parmi les attaques les plus médiatisées, mentionnons le vol, en 2013, de 45 millions de dollars américains, retirés à des guichets automatiques dans plus d'une vingtaine de pays, et coordonné par des pirates qui avaient réussi à manipuler les limites de retrait de cartes de crédit (Santora, 2013).

L'appât du gain et l'importance des institutions financières dans l'économie continueront de motiver des acteurs de tout acabit à entreprendre des cyberattaques. Il n'est pas étonnant que, selon des sources du milieu, 15 % de toutes les cyberattaques recensées dans le monde visent le secteur financier, ce qui en fait la branche d'activité la plus touchée (Mandiant, 2014). Les IMF sont ciblées moins souvent que les institutions financières, mais elles doivent néanmoins rester vigilantes et prendre les précautions qui s'imposent.

Les risques potentiels

La compréhension des canaux par lesquels les effets des cyberattaques pourraient se propager dans le système financier constitue un volet important de l'évaluation du risque systémique éventuel représenté par ces menaces.

La gravité potentielle d'une attaque dépend des perturbations opérationnelles qui en résulteraient. Une cyberattaque visant à subtiliser des informations financières ou des données exclusives ne bouleverse pas les fonctions principales d'une institution financière ou d'une IMF. En revanche, les atteintes à la réputation découlant d'une telle violation peuvent avoir des conséquences négatives sur la perception qu'ont les investisseurs de la rentabilité future de l'entité touchée (Sharf, 2014). Il n'est

pas impossible qu'une perte de confiance dans le bon fonctionnement d'une institution financière ou d'une IMF ait des implications plus importantes du point de vue du risque systémique. En effet, les participants au système financier pourraient interrompre leurs opérations ou retirer leurs fonds en réponse à une intrusion. Toutefois, l'expérience montre que les incidences des atteintes à la réputation peuvent être éphémères et tributaires de plusieurs facteurs, notamment le type d'intrusion et la taille de l'entité concernée (Acquisti, Friedman et Telang, 2006).

Une cyberattaque qui déstabilise des activités peut poser directement un risque systémique selon le type de services perturbés et la durée de la suspension des opérations. Par exemple, une panne touchant les fonctions essentielles d'un établissement financier ou d'une IMF aura sans doute des répercussions plus graves que des attaques par saturation interrompant uniquement les services en ligne d'une institution.

Les perturbations pourraient avoir des conséquences encore plus graves si des données et des systèmes vitaux étaient corrompus. L'impossibilité de se fier à l'intégrité de l'information et des systèmes pourrait entraîner une longue interruption de service avant le rétablissement des systèmes. La probabilité de se trouver devant un risque de nature systémique augmenterait également si les participants perdaient confiance dans l'exactitude des données relatives à leurs transactions et positions financières (CPIM, 2014). Les institutions et les IMF reconnaissent les risques associés aux cyberattaques dirigées contre les systèmes internes et ont pris des mesures, à titre individuel et collectif, pour y faire face.

La riposte aux cybermenaces

Conscientes des risques, les entreprises aux quatre coins du monde investissent beaucoup pour protéger leurs activités contre les cybermenaces. C'est tout particulièrement le cas des exploitants d'infrastructures essentielles de divers secteurs, qui comptaient consacrer, à l'échelle du globe, jusqu'à 46 milliards de dollars américains à la cybersécurité en 2013 (Rubenfeld, 2013). Ciblées par les cyberattaques, les institutions financières et les IMF ont renforcé leur sécurité en investissant dans de multiples chantiers. Leur première ligne de défense est la protection des systèmes internes. Leurs stratégies, outils et technologies comprennent des tests d'intrusion effectués sur les réseaux, des processus rigoureux de contrôle des accès aux systèmes internes, des outils de dépistage des vulnérabilités, le chiffrement des données, ainsi que des mises à jour de sécurité périodiques (BSIF, 2013). Cependant, on considère désormais que la mise en place de systèmes de protection périphérique inviolables ne constitue plus un objectif réaliste ni suffisant pour gérer adéquatement les risques liés à la cybersécurité (Kochan, 2014). Une stratégie proactive doit inclure une activité de veille afin de repérer les cybermenaces dans l'environnement externe, et faire appel à des outils tels que les moyens de surveillance réseau pour détecter les violations des systèmes informatiques lorsqu'elles surviennent. Il importe aussi que les institutions financières et les IMF élaborent les processus et procédures appropriés pour riposter aux cyberattaques et en surmonter les conséquences le cas échéant (National Institute for Standards and Technology, 2014).

Aux actions entreprises par les institutions financières et les IMF s'ajoute le rôle des autorités, qui doivent tenir à jour les cadres de surveillance en fonction des différentes menaces à la cybersécurité (Bin Ibrahim, 2014). Au Canada, des efforts sont déjà faits dans ce sens, et ils visent à faire en sorte que les intervenants de la cybersécurité intègrent à leurs pratiques les éléments nécessaires pour parer à des menaces plus graves. Le Bureau du surintendant des institutions financières (BSIF) a publié des conseils sur la cybersécurité afin d'aider les institutions financières sous réglementation fédérale à évaluer l'adéquation de leurs pratiques et à déterminer les changements requis pour adopter les pratiques exemplaires de l'industrie (BSIF, 2013). De même, la Banque du Canada a exigé que les IMF d'importance systémique évaluent leurs propres pratiques en regard de normes favorisant une approche de la cybersécurité fondée sur la gestion des risques.

Les actions en cours au Canada sont à l'image des mesures déployées ailleurs. De fait, la cybersécurité est considérée comme un enjeu public d'envergure mondiale. Aux États-Unis, le ministère de la Sécurité intérieure a adopté, au début de 2013, un décret-loi sur le renforcement de la cybersécurité des infrastructures essentielles. Dans le même ordre d'idées, la Commission européenne a publié en 2014 une stratégie de cybersécurité pour les membres de l'Union européenne, dont l'évaluation des pratiques relatives à la protection des infrastructures essentielles constitue un élément central. Ces grands chantiers concernent les infrastructures vitales dans chaque secteur d'activité et sont les fondements de la réglementation du secteur financier dans ces pays.

Des organisations internationales s'emploient également à revoir leurs cadres de politiques afin de tenir compte de l'évolution des risques posés par les cybermenaces. Le Comité sur les paiements et les infrastructures de marché a récemment publié un rapport sur les pratiques actuelles des IMF en matière de cybersécurité (CPIM, 2014). La Banque du Canada a adopté les principes généraux de gestion des risques énoncés par le Comité

(CSPR-OICV, 2012) et en a fait sa norme pour les IMF désignées. Elle a la ferme intention d'y incorporer toute indication supplémentaire sur la cybersécurité.

La coopération au service de la cybersécurité

À elles seules, les mesures de protection rigoureuses adoptées par les institutions financières et les IMF ne suffisent pas à atténuer les risques susceptibles de concerner toutes les composantes d'un système financier du fait des interdépendances. Étant donné les répercussions qu'une cyberattaque de grande ampleur pourrait avoir, il est nécessaire qu'une collaboration efficace s'installe entre les IMF, les institutions financières et l'administration fédérale. Des liens avec d'autres secteurs importants (p. ex., télécommunications et énergie) s'imposent également afin d'assurer la résilience collective des opérations.

Sécurité publique Canada est chargée de mettre en place la stratégie de cybersécurité du pays. Celle-ci est destinée à protéger les systèmes gouvernementaux, à favoriser les collaborations en vue de sécuriser les systèmes non gouvernementaux et à aider la population à se protéger en ligne[1]. Cette stratégie fait appel à une panoplie d'outils et se fonde sur une approche proactive, plutôt que réactive, de la réduction des cybermenaces. Une dimension importante de cette stratégie consiste à consolider les partenariats entre les secteurs et entre ceux-ci et l'État. Les projets de coopération qui facilitent la mise en commun de l'information renforcent la cybersécurité en créant un espace de discussion propice à l'échange de pratiques exemplaires et de renseignements sur les menaces, ainsi qu'à l'établissement de réseaux de confiance intersectoriels. Ces projets marquent une transition. En effet, ils permettent de passer de stratégies tournées vers la mobilisation des ressources internes d'une seule entité à des stratégies qui tirent parti de l'expertise de différents partenaires, et ce, dans le but de réduire la probabilité des cyberattaques et de faciliter la mise en place de mesures d'atténuation des risques plus efficaces.

Des initiatives comme la création du Centre canadien de réponse aux incidents cybernétiques (CCRIC) de Sécurité publique Canada, dans lequel les institutions financières et les IMF canadiennes collaborent activement, illustrent bien les avantages associés à la mise en commun de l'information. Le CCRIC est une plateforme d'échange de renseignements : les informations clés sur les cyberattaques signalées par les participants des secteurs privé et public sont combinées aux analyses fournies par les organismes chargés de l'application de la loi, afin de produire un savoir pertinent pour toutes les parties intéressées. La réception en temps utile de renseignements sur les menaces peut mener à des solutions aptes à prévenir la matérialisation de cyberattaques. En outre, le CCRIC continue de travailler avec les institutions financières canadiennes pour chercher des façons encore plus optimales d'échanger de l'information.

Les IMF et les institutions financières participent également à des structures de coopération axées sur l'échange de pratiques exemplaires et l'élaboration de stratégies de lutte à long terme. Ces structures constituent des moyens efficaces pour diffuser les expériences acquises et formuler des stratégies qui permettront de remédier aux vulnérabilités communes. Pour l'heure, les entités participantes en retirent d'importants avantages, mais il faudra inclure d'autres partenaires stratégiques aux réseaux existants. L'administration fédérale, les institutions financières et les exploitants d'IMF s'efforcent de trouver de nouvelles façons de mettre en place des protocoles d'échange de renseignements, entre eux et avec d'autres secteurs clés.

Grâce à l'échange d'informations, les entités ne travaillent plus en vase clos et sont à même d'élaborer ensemble de meilleures stratégies de cybersécurité que celles qu'elles auraient élaborées individuellement. Pour parvenir à un renforcement significatif de la résilience opérationnelle du secteur financier, il est essentiel qu'un consensus se dégage parmi les institutions, car celles-ci tendent à s'attaquer aux problèmes en se présentant avec leurs propres priorités et méthodes.

La cybersécurité mise à l'épreuve

Malgré les actions individuelles et collectives de lutte contre les menaces, une cyberattaque de grande envergure peut toujours survenir. L'Association des banquiers canadiens dispose d'un cadre d'intervention coordonnée pour gérer les incidents opérationnels majeurs touchant plus d'une institution financière. Son cadre comprend un comité sur les incidents cybernétiques formé de spécialistes de l'informatique. Les IMF canadiennes ont de leur côté prévu des procédures et des mesures d'urgence en cas de grave perturbation de leurs activités. Toutefois, la portée des dispositions prises par ces deux groupes est trop limitée pour qu'ils puissent faire face à un incident de dimension véritablement sectorielle. En mettant en relation les grandes banques canadiennes, les IMF et l'administration fédérale, le Programme de gestion conjointe des mesures favorisant la résilience des opérations permet d'orchestrer les interventions en vue de surmonter une perturbation majeure.

1 Pour de plus amples renseignements, voir le site Web de Sécurité publique Canada, à l'adresse http://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-fra.aspx.

À cet effet, les participants au Programme ont réalisé une série d'exercices sur table visant à évaluer les capacités des secteurs public et privé dans une situation de crise au moyen de plusieurs scénarios fictifs. Ces simulations peuvent permettre d'apprécier les principaux risques, de déterminer la meilleure façon de faire remonter les incidents jusqu'aux décideurs et de coordonner les stratégies de réduction des risques.

L'exercice de 2014, qui a été mené récemment, comportait une cyberattaque dirigée contre une IMF, causant des retards et des perturbations dans le déroulement des services de post-marché des institutions financières. Cette simulation avait pour objectif de clarifier les rôles et les responsabilités de chacun pendant un incident opérationnel d'envergure sectorielle. L'élaboration d'un cadre de définition des paliers d'intervention a été un volet central du test et a contribué à la mise sur pied d'un protocole d'échange de renseignements et de coordination des actions en cas d'attaque. Les observations et leçons tirées de cette simulation serviront à perfectionner les procédures de gestion de crise au sein du secteur financier.

Les exercices effectués gagneront en complexité et feront intervenir de plus en plus d'acteurs afin qu'une simulation à grande échelle touchant l'ensemble du secteur soit menée en 2016. Celle-ci exigera des efforts de planification et de coordination comparables à ceux déployés par la Securities Industry and Financial Markets Association (SIFMA) des États-Unis[2] et la Banque d'Angleterre[3] pour des exercices similaires.

En ce qui concerne l'évaluation des vulnérabilités et des capacités en matière de cybersécurité, une collaboration soutenue permettra d'accroître la complexité des simulations. S'agissant des tests auxquels sera soumis le secteur, de nombreuses avenues pourraient être explorées. Par exemple, les autorités financières du Royaume-Uni se sont concentrées sur un cadre de mise à l'essai alimenté par des renseignements précis sur les cybermenaces, de façon à ce que les tests reflètent aussi fidèlement que possible les menaces réelles en constante évolution[4].

Conclusion

En plus des menaces habituelles qui planent sur leurs activités, les institutions financières et les IMF sont confrontées à des défis grandissants dans le domaine de la cybersécurité. Leur forte dépendance à l'égard des technologies, combinée à l'étendue de leurs liens, accentue la vulnérabilité du secteur financier aux cyberattaques. C'est pourquoi les intervenants des secteurs public et privé ont reconnu qu'ils devaient unir leurs forces pour corriger ces faiblesses potentielles.

Les progrès accomplis grâce à des partenariats public-privé, semblables à ceux qui ont abouti à la création du Centre de réponse aux incidents cybernétiques et du Programme de gestion conjointe des mesures favorisant la résilience des opérations, ont permis d'accroître la résilience des entités du secteur financier face aux nouvelles cybermenaces. Cependant, les institutions financières et les IMF canadiennes, et leurs interlocuteurs du secteur public, doivent continuer de tirer parti des plateformes de coopération existantes afin de mieux renforcer les initiatives liées à la cybersécurité.

2 Le 18 juillet 2013, la SIFMA a effectué un deuxième exercice (Quantum Dawn 2), dont l'objet était de simuler une cyberattaque d'envergure systémique contre le système financier américain. Ainsi, les acteurs du domaine ont eu l'occasion de mettre à l'épreuve leur riposte.

3 Le 12 novembre 2013, la Banque d'Angleterre a réalisé un deuxième exercice (Waking Shark II) conçu pour mettre à l'essai la réaction coordonnée des entreprises offrant des services bancaires de gros, y compris les banques d'investissement et les principales IMF, afin de mieux comprendre et d'atténuer l'incidence des cyberattaques dans ce secteur.

4 Voir « An introduction to CBEST » sur le site Web de la Banque d'Angleterre, à l'adresse www.bankofengland.co.uk/financialstability/fsc/Documents/anintroductiontocbest.pdf.

Bibliographie

Acquisti, A., A. Friedman et R. Telang (2006). *Is There a Cost to Privacy Breaches? An Event Study*, 27e conférence internationale sur les systèmes d'information, Milwaukee (Wisconsin).

Banque du Canada (2014). *Activités de surveillance menées en 2013 par la Banque du Canada en application de la* Loi sur la compensation et le règlement des paiements.

Bin Ibrahim, M. (2014). *Demystifying Cyber Risks: Evolving Regulatory Expectations*, discours prononcé dans le cadre du sommet sur la cybersécurité organisé par les banques centrales de l'Asie du Sud-Est (SEACEN), Kuala Lumpur (Malaisie), 25 août.

Bureau du surintendant des institutions financières (BSIF) (2013). *Conseils sur l'autoévaluation en matière de cybersécurité*, 28 octobre.

Comité sur les paiements et les infrastructures de marché (CPIM) (2014). *Cyber Resilience in Financial Market Infrastructures*, novembre.

Comité sur les systèmes de paiement et de règlement et Comité technique de l'Organisation internationale des commissions de valeurs (CSPR-OICV) (2012). *Principes pour les infrastructures de marchés financiers*.

Crosman, P. (2014). « DDoS Attacks Are Still Happening — and Getting Bigger », *American Banker*, 28 juillet.

Deloitte Center for Financial Services (2014). *Transforming Cybersecurity: New Approaches for an Evolving Threat Landscape*.

Kochan, N. (2014). « Taking the Strategic View of Cyber Security », *Risk.net*, 22 juillet.

Mandiant (2014). *MTrends 2014: Beyond the Breach*.

National Institute for Standards and Technology (NIST) (2014). *Framework for Improving Critical Infrastructure Cybersecurity*, 12 février.

Nguyen, L. (2013). « TD Online Banking Services Hit by Cyber Attack », *The Globe and Mail*, 21 mars.

Perlroth, N. (2014). « JPMorgan and Other Banks Struck by Hackers », *The New York Times*, 27 août.

PricewaterhouseCoopers (PwC) (2013). *Defending Yesterday: Key Findings from the Global State of Information Security Survey 2014*, septembre.

Riley, M. (2014). « How Russian Hackers Stole the Nasdaq », *Bloomberg Businessweek*, 17 juillet.

Rubenfeld, S. (2013). « Cybersecurity Spending Set to Rise to $46 Billion », *Risk and Compliance Journal, The Wall Street Journal*, 17 juillet.

Santora, M. (2013). « In Hours, Thieves Took $45 Million in A.T.M. Scheme », *The New York Times*, 9 mai.

Sharf, S. (2014). « Target Shares Tumble as Retailer Reveals Cost of Data Breach », *Forbes*, 8 mai.

Symantec (2014). « 2014 Internet Security Threat Report », *2013 Trends*, vol. 19, avril.

Weston, G. (2011). « Foreign Hackers Attack Canadian Government », *CBC News*, 16 février.