Stratégie de cybersécurité

2019-2021

Réduire les risques et renforcer la résilience

BANK OF CANADA
BANQUE DU CANADA

MESSAGE DU CHEF DE L'EXPLOITATION

La technologie moderne aide la Banque du Canada à tirer parti de l'innovation dans tout ce qu'elle fait.

Mais pour cela, il faut un engagement ferme et soutenu à l'égard de la cybersécurité.

La stratégie de cybersécurité de la Banque décrit l'approche institutionnelle à moyen terme : ***réduire les risques et renforcer la résilience***.

Il est important de prévenir les cyberattaques dans la mesure du possible, mais nous devons aussi être prêts à intervenir et à reprendre rapidement nos activités en cas d'atteinte à la cybersécurité.

Nous investissons dans des défenses de nature systémique pour que la Banque puisse exercer ses activités en toute sécurité.

De plus, nous avons l'intention de travailler en étroite collaboration avec nos partenaires du système financier pour renforcer la cybersécurité au pays et à l'étranger.

Le chef de l'exploitation,
Filipe Dinis

INTRODUCTION

La Banque du Canada est résolue à favoriser la stabilité et l'efficience du système financier. Dans un contexte où les cyberattaques sont plus fréquentes et plus graves dans le monde entier, la cybersécurité sera une priorité pour la Banque pendant de nombreuses années.

La stratégie de cybersécurité 2019-2021 énonce ce qu'entend faire la Banque pour réduire les risques et renforcer la résilience dans ses propres activités et dans les systèmes financiers canadien et international.

La vision de la Banque en matière de cybersécurité :

Renforcer la cyberrésilience du système financier canadien face aux menaces en constante évolution.

La mission de la Banque en matière de cybersécurité :

Favoriser l'efficience et la stabilité du système financier canadien grâce à de solides connaissances et capacités en matière de cybersécurité, à des efforts de collaboration et de mise en commun de l'information, et à un vaste processus de surveillance.

Les buts de la Banque en matière de cybersécurité :

1. **Renforcer** l'équipe chargée de la cybersécurité et les capacités connexes afin de permettre à la Banque d'exercer ses activités et d'innover en toute sécurité.
2. **Collaborer** avec les principaux partenaires en vue de favoriser la résilience et de réduire la fréquence et la gravité des atteintes à la cybersécurité.
3. **Réglementer** et promouvoir les normes de cybersécurité les plus élevées dans le cadre du rôle de surveillance de la Banque.

L'ENVIRONNEMENT DE CYBERSÉCURITÉ

Le secteur financier au Canada et à l'étranger utilise de nouvelles technologies novatrices pour améliorer les services, automatiser les tâches et réduire les coûts. L'infonuagique, l'informatique quantique, l'intelligence artificielle, l'Internet des objets, les technologies financières et d'autres ressources facilitent la transmission électronique efficace des transactions financières entre clients, fournisseurs, institutions et systèmes de paiement.

Cette interconnexion comporte certes de nombreux avantages, mais elle est devenue une source de vulnérabilité dans le monde actuel où les cyberattaques sont fréquentes et sophistiquées. Si un incident venait à altérer les données ou nuire aux opérations ne serait-ce que d'une seule institution financière, cet incident pourrait se répercuter sur les partenaires externes de cette institution et, à terme, perturber d'importants systèmes financiers nationaux et internationaux.

La valeur des transactions quotidiennes se chiffrant dans les milliards de dollars – et les pirates informatiques étant motivés dans bien des cas par l'appât du gain, il n'est pas étonnant de voir les institutions financières et les systèmes financiers subir davantage de cyberattaques. La Banque et d'autres participants du secteur investissent de façon importante et soutenue dans la protection des systèmes internes et des capacités de détection des cybermenaces, d'intervention et de rétablissement en cas d'incident.

Cela dit, mettre l'accent sur la sécurité interne ne suffit pas. La Banque et ses partenaires se soucient également de la possibilité qu'une attaque réussie mine la confiance dans le système financier. Il devient de plus en plus urgent d'intégrer les stratégies d'intervention et de rétablissement de l'ensemble des acteurs du secteur, et particulièrement des grandes institutions financières et des infrastructures de marchés financiers (IMF) essentielles.

IL DEVIENT DE PLUS EN PLUS URGENT D'INTÉGRER LES STRATÉGIES D'INTERVENTION ET DE RÉTABLISSEMENT

En tant qu'acteur clé au sein de l'économie canadienne, la Banque vise à réduire le risque que des cyberincidents « perturbent la prestation des services financiers essentiels aux systèmes financiers nationaux et internationaux, menacent la sécurité, ébranle la confiance et mettent en péril la stabilité financière »[1].

La Banque reconnaît sa responsabilité de travailler avec ses partenaires externes pour favoriser et renforcer la résilience du système financier. Les participants des secteurs public et privé se doivent de collaborer de manière efficace.

De même, dans le cadre de son rôle de surveillance, la Banque impose aux IMF l'utilisation d'outils et de pratiques de cybersécurité appropriés. Cette exigence contribue à la protection individuelle des IMF, et elle permet également de réduire les risques et de favoriser la résilience de l'ensemble du système financier.

LE PARCOURS DE LA BANQUE EN MATIÈRE DE CYBERSÉCURITÉ

En 2014, la Banque du Canada a publié des travaux de recherche soulignant le grand danger que revêtent les cyberattaques pour la résilience opérationnelle des institutions financières et des IMF au pays[2]. Pour la première fois, à la lumière d'une évaluation interne, la cybersécurité était considérée comme un risque d'échelon 1 pour les activités de la Banque.

Depuis, la Banque a fait de la cybersécurité une priorité absolue. Le Plan à moyen terme 2016-2018 prévoyait d'ailleurs des investissements dans les nouvelles technologies, les processus et l'effectif pour faire face aux cyberrisques actuels et émergents. La Banque a adopté une approche proactive en matière de cyberdéfense en vue de limiter ou de maîtriser l'incidence d'un éventuel cyberincident.

La Banque s'est employée à mieux comprendre l'incidence de la cybersécurité sur la stabilité financière

La Banque collabore depuis bon nombre d'années avec le gouvernement du Canada et d'autres partenaires des secteurs public et privé, au pays et à l'étranger, pour réduire ou atténuer les cyberrisques auxquels est exposé le système financier. À titre d'exemple, citons notamment sa participation à l'élaboration des lignes directrices du Comité sur les paiements et les infrastructures de marché (CPIM) et de l'Organisation internationale des commissions de valeurs (OICV) pour la cyberrésilience des IMF[3], lignes directrices sur lesquelles se fondent les exigences en matière de cybersurveillance.

Par ailleurs, le Comité de gestion conjointe des mesures favorisant la résilience des opérations a été créé pour permettre aux grandes banques, aux IMF et aux autorités publiques d'échanger de l'information sur les incidents porteurs de risque opérationnel et de mettre à l'essai des protocoles en matière de résilience. Cette instance est devenue le Groupe sur la résilience du secteur financier canadien pour refléter son nouveau mandat, qui prend désormais en compte explicitement les cyberincidents et la complexité croissante des besoins de coordination.

La protection contre les cyberattaques demeure un objectif, mais les efforts sont maintenant axés sur la préparation à intervenir et à assurer la reprise des activités en cas de cyberincident. Cette nouvelle orientation témoigne d'une meilleure compréhension de la nature des cybermenaces, car il n'est pas réaliste de croire que le système financier puisse être protégé contre tout risque d'attaque.

Dans cet esprit, la Banque a conclu, en 2018, un partenariat plus formel avec Paiements Canada et les six grandes banques canadiennes pour favoriser la continuité des opérations. Cette initiative vise à améliorer la coordination au pays et à rendre le système de paiement de gros plus résilient aux cyberattaques.

La Banque a investi dans les éléments fondamentaux de la cybersécurité

Renforcer sa posture de cybersécurité est une priorité pour la Banque, qui a élaboré des directives et des normes pour établir un niveau de référence à cet égard. Ces travaux l'ont amenée à perfectionner son modèle de gouvernance afin de tenir compte de l'accroissement de la taille et de la portée de ses programmes de cybersécurité et des responsabilités communes à plusieurs départements.

En outre, la Banque a adopté un cadre de gestion des cyberrisques pour guider les évaluations de sa posture de cybersécurité et mesurer les progrès réalisés en la matière. Elle a aussi élaboré une « stratégie relative aux employés » dans le but d'attirer, de fidéliser et de développer des personnes compétentes dans le domaine de la cybersécurité, y compris des étudiants et de nouveaux diplômés.

En 2018, le poste de chef de la sécurité de l'information a été créé afin d'assurer l'harmonisation et la coordination des programmes et des activités de cybersécurité, au sein de la Banque comme à l'extérieur. Sous la supervision du chef de la sécurité de l'information, une méthode d'établissement des priorités en fonction des risques est appliquée, et ajustée selon les résultats des tests, des audits, des évaluations et des expériences opérationnelles.

La Banque a donné la priorité à la protection des activités et des actifs essentiels

La Banque a examiné soigneusement ses activités et actifs essentiels les plus importants – ses piliers – pour comprendre de quelle façon ils peuvent être ciblés par les pirates informatiques. Dans un souci de protection de l'institution et de détection des menaces, des contrôles propres à chaque actif ont été ajoutés ou renforcés dans le but d'atténuer les risques les plus probables.

En particulier, la Banque a amélioré les mécanismes de contrôle liés à son environnement du système de paiement SWIFT[4], par lequel elle communique avec des institutions financières partout dans le monde.

Elle a également porté une attention particulière aux systèmes qui facilitent les opérations bancaires cruciales qu'exécute le département de la Gestion financière et des Opérations bancaires.

De plus, un programme intégré des tests de sécurité a été mis en œuvre pour détecter les vulnérabilités du personnel, des systèmes et des processus, et y remédier. Les résultats de ces tests servent à améliorer les principaux processus et plans d'intervention en cas de cyberincident, par exemple un rançongiciel.

Pour assurer ses services de sécurité, la Banque a adopté une approche axée sur les personnes

Comme la plupart des cyberattaques réussies surviennent par l'intermédiaire de personnes, la Banque a amélioré sa capacité de contrer les cyberattaques qui exploitent ce maillon faible.

Un programme de sensibilisation des utilisateurs a été mis sur pied afin d'informer les utilisateurs réguliers ou privilégiés des systèmes de la Banque au sujet des risques liés à leur travail, y compris l'hameçonnage et le vol de justificatifs d'identité.

En outre, des mesures ont été adoptées pour assurer la protection et la gestion des mots de passe de la Banque, notamment ceux des personnes qui ont un accès privilégié aux systèmes déterminants et essentiels. Un logiciel a aussi été déployé sur les serveurs et ordinateurs portables de la Banque pour permettre de détecter les activités malveillantes et d'intervenir rapidement.

La Banque a investi dans des initiatives clés afin d'accroître la résilience

Le renforcement de l'infrastructure de rétablissement pour assurer la résilience opérationnelle faisait partie des grandes priorités de la Banque dans le dernier plan à moyen terme.

Les initiatives comme le Programme d'amélioration de la reprise des activités et le Programme relatif à la résilience des opérations sur les marchés et des opérations bancaires ont amélioré la capacité de la Banque d'éviter un préjudice potentiel ou de s'en remettre si ses ressources ou services sont compromis pour quelle que raison que ce soit. Elles ont jeté les bases d'une meilleure cyberrésilience.

La protection ne suffit pas : la Banque doit être prête à intervenir en cas d'attaque et pouvoir reprendre ses activités

La Banque a renforcé ses capacités globales en matière de résilience et de cybersécurité, mais elle doit en faire davantage. Elle continuera donc à adapter ses activités internes et externes à l'environnement de cybersécurité en évolution rapide.

La stratégie de cybersécurité 2019-2021 s'appuie sur les réalisations passées, elle concorde avec le Plan à moyen terme[5] et le goût du risque de la Banque (voir l'annexe) et tient compte des défis de notre écosystème financier.

LE PARCOURS SE POURSUIT : 2019-2021

La stratégie de cybersécurité 2019-2021 définit la nouvelle approche globale de la Banque en matière de cybersécurité. Le rôle essentiel que remplit l'institution au sein du système financier est maintenant pris en compte dans ses opérations de cybersécurité internes.

Partant du postulat que les cyberincidents sont inévitables, la stratégie souligne l'importance de détecter les cyberintrusions qui peuvent survenir, d'intervenir et d'assurer la reprise des activités.

La stratégie décrit également la contribution de la Banque à la cyberrésilience globale du système financier canadien, notamment sa participation à d'importantes activités de collaboration avec des partenaires des secteurs public et privé, et l'exercice de son mandat de surveillance des IMF, qui lui est conféré par la loi.

Partout à la Banque, des leaders ont été consultés au sujet de l'élaboration de la vision, de la mission et des buts stratégiques. Ces trois volets tiennent compte de la diversité des intérêts de la Banque en matière de cybersécurité et de la concordance avec son énoncé sur le goût du risque. (Voir l'annexe.)

La vision de la Banque en matière de cybersécurité :
Renforcer la cyberrésilience du système financier canadien face aux menaces en constante évolution.

La mission de la Banque en matière de cybersécurité :
Favoriser l'efficience et la stabilité du système financier canadien grâce à de solides connaissances et capacités en matière de cybersécurité, à des efforts de collaboration et de mise en commun de l'information, et à un vaste processus de surveillance.

La sections qui suivent décrivent les buts, objectifs et résultats stratégiques qui contribueront à la réalisation de la vision et de la mission de la Banque.

BUTS POUR 2019-2021

BUT 1 — Renforcer l'équipe chargée de la cybersécurité et les capacités connexes afin de permettre à la Banque d'exercer ses activités et d'innover en toute sécurité.

Indicateurs de succès

- La Banque est en mesure d'attirer et de retenir des talents de haut niveau en cybersécurité qui sont novateurs et bien outillés.
- Les divers secteurs d'activité de la Banque connaissent les cyberrisques auxquels ils sont exposés, et les gèrent en amont selon le goût du risque de cybersécurité.
- La posture de cybersécurité de la Banque est optimale; elle permet à l'institution de garder une longueur d'avance sur les menaces et lui procure des solutions sûres et novatrices.

BUT 2 — Collaborer avec les principaux partenaires en vue de favoriser la résilience et de réduire la fréquence et la gravité des atteintes à la cybersécurité.

Indicateurs de succès

- La Banque met régulièrement à l'épreuve ses capacités d'intervention et de rétablissement avec ses partenaires, en vue d'accroître l'efficacité des cyberdéfenses et de renforcer la cyberrésilience globale du secteur.
- La Banque collabore et échange de l'information de manière efficace avec les parties externes, y compris les autres banques centrales, les organisations homologues et les services canadiens de sécurité et de renseignement du gouvernement du Canada.
- La Banque contribue à la conception et à la mise en œuvre des stratégies de cybersécurité des systèmes financiers canadien et international.

BUT 3 — Réglementer et promouvoir les normes de cybersécurité les plus élevées dans le cadre du rôle de surveillance de la Banque.

Indicateurs de succès

- Les IMF gèrent les cyberrisques auxquels elles sont exposées conformément aux lignes directrices de la Banque, qui se fondent sur les pratiques exemplaires internationales.
- La Banque collabore efficacement avec ses partenaires canadiens et étrangers pour améliorer les mesures législatives, réglementaires et de surveillance liées à la cybersécurité.
- La Banque assure une surveillance prudentielle rigoureuse du processus de gestion des risques entrepris par les IMF, y compris les cyberrisques auxquels elles sont exposées.

CE QUI NOUS ATTEND – OBJECTIFS, RÉSULTATS ET MESURES INTERNES

La Banque a amélioré ses capacités globales en matière de cybersécurité et de cyberrésilience dans le cadre de son plan à moyen terme précédent, mais il lui faudra déployer encore de grands efforts pour se préparer aux cyberrisques qui se présenteront dans les années à venir et pouvoir intervenir efficacement.

La taille et la portée du programme de cybersécurité ont été élargies pour favoriser l'atteinte des objectifs stratégiques de la Banque. Outre les projets importants et les travaux d'envergure liés à des systèmes d'exploitation qui ont été amorcés dans le plan à moyen terme précédent et qui se poursuivront, de nouvelles initiatives seront entreprises au cours des trois prochaines années pour s'attaquer aux priorités naissantes. Les activités de détection, d'intervention et de reprise des opérations, auxquelles la Banque compte s'attacher davantage, font partie de ces initiatives.

La feuille de route, les objectifs et les résultats attendus du programme ont été regroupés par fonctions, selon le cadre de cybersécurité du National Institute of Standards and Technology. (Voir l'annexe.) Ce cadre facilite le suivi et l'évaluation des mesures prises par la Banque pour mettre en place des mécanismes de contrôle de la cybersécurité et réduire les risques.

IDENTIFIER ET GÉRER | **PROTÉGER** | **DÉTECTER** | **INTERVENIR** | **RÉTABLIR**

Gérer efficacement les personnes, les risques, les ressources et la gouvernance pour faire face aux cyberrisques

La Banque aura la structure de gouvernance et l'information nécessaires pour gérer et surveiller les cyberrisques.

Résultats attendus

- Les processus de gouvernance et de gestion des risques permettent de gérer et de surveiller efficacement les cyberrisques et de prendre des décisions fondées sur les risques.
- Les cyberrisques liés aux opérations essentielles, y compris ceux auxquels sont exposés des tiers, sont compris et évalués adéquatement.
- La Banque a accès, en temps voulu, aux compétences et aux talents nécessaires dans le domaine de la cybersécurité.

Mesures stratégiques pour 2019-2021

Pour obtenir ces résultats attendus, la Banque continuera de développer son cadre de gouvernance et de gestion des risques pour y inclure :

- un énoncé sur le goût du risque et des paramètres à jour, qui faciliteront la prise de décisions fondée sur les risques, par exemple les principaux indicateurs de risque, les principaux indicateurs de rendement et les cibles de mise en œuvre;
- des outils de déclaration perfectionnés assurant une surveillance efficace du programme;
- les rôles et responsabilités clairement définis des trois lignes de défense;
- des évaluations cohérentes et rigoureuses des risques associés aux tiers, tout au long des étapes de la relation;
- la planification des effectifs, afin de disposer des ressources nécessaires pour répondre aux futurs besoins de compétences et de talents dans le domaine de la cybersécurité.

Adopter une posture proactive contre les cyberattaques

La Banque donnera la priorité à la protection des actifs numériques déterminants et essentiels, appelés piliers.

Résultats attendus

- L'accès aux actifs et aux systèmes est géré de manière efficace et se limite aux utilisateurs autorisés et à l'usage permis.
- Les vulnérabilités sont identifiées rapidement, leur incidence est comprise et les mesures d'atténuation appropriées sont appliquées.
- Les données sont catégorisées et protégées de manière adéquate.
- La sensibilisation des employés de la Banque à la cybersécurité dépasse celle des employés d'organisations homologues.
- Les services de cybersécurité sont actualisés et la sécurité fait partie intégrante de la conception des systèmes.

Mesures stratégiques pour 2019-2021

Pour obtenir ces résultats attendus, la Banque :

- améliorera sa capacité de gestion de l'identité et de l'accès en y intégrant un mécanisme de contrôle centralisé et efficace des identités privilégiées ainsi qu'une application sécurisée pour la gestion de l'accès à ses systèmes par des partenaires externes;
- poursuivra le développement du Programme des tests de cybersécurité pour assurer des évaluations plus systématiques de l'efficacité des cyberdéfenses (personnes, processus et technologies) ainsi que l'identification des vulnérabilités et des maliciels;
- perfectionnera les outils et processus de catégorisation des données de nature délicate et les mesures de prévention et de détection des pertes de données, pour ainsi réduire les risques associés à la sécurité des données;
- peaufinera son Programme de sensibilisation à la cybersécurité en veillant notamment à y intégrer une formation, la mise à l'essai de mesures préventives (p. ex., la gestion efficace des mots de passe) et de nouvelles capacités de détection des cyberattaques (p. ex., celles qui sont perpétrées au moyen de courriels malveillants) et d'intervention;
- mettra en place des services de cybersécurité de la prochaine génération (p. ex., un processus de gestion centralisée des pare-feu) en vue d'accroître la résilience et à la sécurité de tous les environnements du Programme d'amélioration de la reprise des activités (PARA).

Renforcer les systèmes pour identifier les cyberincidents

La Banque élargira ses capacités de cyberdéfense pour repérer les problèmes qui surviennent.

Résultats attendus

- Les cyberattaques sont détectées rapidement et gérées de manière appropriée.
- Les paramètres de sécurité sont appliqués et surveillés systématiquement.
- La communication de renseignements à jour sur les menaces favorise la gestion efficace des cyberincidents.

Mesures stratégiques pour 2019-2021

Pour obtenir ces résultats attendus, la Banque :

- mettra en place des outils et processus de surveillance de la sécurité de la prochaine génération, comme des analyses en temps réel et des analyses de comportements, dans le but de détecter rapidement les activités malveillantes et de comprendre l'incidence potentielle des incidents;
- effectuera régulièrement des tests de cybersécurité pour mettre à l'épreuve les cyberdéfenses et les capacités de détection et d'évaluation;
- développera les processus et procédures de détection, par exemple elle élargira les capacités de détection au niveau des points d'accès et d'exploration de données;
- mettra en place des normes rigoureuses pour la configuration de la sécurité et surveillera en continu les changements de configuration;
- améliorera les processus de traitement des renseignements sur les menaces et mettra sur pied des activités de recherche des menaces pour détecter les activités malveillantes.

Renforcer les mesures pour limiter l'incidence d'un cyberincident potentiel

La Banque s'assurera de disposer des ressources dont elle a besoin pour intervenir efficacement en cas d'incident.

Résultats attendus

- Les plans et processus de cyberdéfense et d'intervention sont régulièrement mis à l'essai.
- Les mesures d'intervention en cas d'incident sont gérées en permanence et automatisées si les circonstances le justifient.
- Les enquêtes judiciaires sont menées efficacement.
- Les activités d'intervention sont coordonnées efficacement avec les parties prenantes internes et externes.

Mesures stratégiques pour 2019-2021

Pour obtenir ces résultats attendus, la Banque :

- augmentera encore la fréquence et la portée des tests de cybersécurité pour exercer ses capacités de cyberdéfense en cas d'incident. Elle veillera notamment à élargir ses plans d'intervention et ses activités de mise à l'essai au moyen d'une approche concertée avec les parties prenantes externes, comme les participants au système financier et le gouvernement fédéral. Cette initiative concorde avec les objectifs externes décrits à la section suivante;
- améliorera ses outils et processus pour être en mesure de limiter l'incidence d'un cyberincident, de façon automatisée;
- mettra en place des outils et processus améliorés, et s'assurera les services d'experts judiciaires et techniques dans le domaine de la cybersécurité pour mener des enquêtes efficaces. Elle devra notamment sensibiliser son personnel à l'information à fournir à l'appui des enquêtes.

Accroître la résilience pour assurer la reprise des activités après un cyberincident

La Banque s'assurera de pouvoir reprendre ses activités normales.

Résultats attendus

- Des tests de reprise des activités en cas de cyberattaque sont effectués régulièrement et les plans connexes sont constamment améliorés.
- Le rétablissement à la suite d'un cyberincident se fait dans un délai convenable, et la communication avec les parties internes et externes est adéquate.

Mesures stratégiques pour 2019-2021

Pour obtenir ces résultats attendus, la Banque :

- testera sa capacité de rétablissement en cas de cyberincident avec les parties prenantes internes et externes (les participants au système financier, le gouvernement fédéral, etc.) pour s'assurer que les approches sont suivies uniformément dans tous les contextes. Il s'agit d'un élément important des objectifs externes décrits ci-après. Des processus d'intervention en cas d'incident seront établis ou mis à jour;
- gérera efficacement les problèmes de cybersécurité en assurant la coordination et la communication avec les parties prenantes touchées. Elle utilisera des guides et des exercices de simulation sur le rétablissement en cas de cyberincident pour vérifier son état de préparation et la vitesse à laquelle elle est capable de reprendre ses activités. En particulier, la Banque améliorera et mettra à l'épreuve sa capacité de faire face à une attaque perpétrée au moyen d'un rançongiciel et de s'en rétablir.

CE QUI NOUS ATTEND – OBJECTIFS, RÉSULTATS ET MESURES EXTERNES

La Banque s'emploie, avec des partenaires du secteur public, les autorités de réglementation et les institutions financières, à concevoir et à mettre en œuvre des politiques et des normes qui contribuent à la stabilité du système financier canadien et qui étayent solidement la croissance économique du pays.

La collaboration et la coordination entre les secteurs public et privé, au Canada et à l'étranger, est essentielle à la cybersécurité. L'échange d'informations contribue à l'élaboration de stratégies efficaces en matière de détection, d'intervention et de rétablissement des opérations.

À l'échelle internationale, la Banque participe aux travaux liés à la cybersécurité effectués par le G7 et le Comité sur les paiements et les infrastructures de marché, entre autres. À l'échelle nationale, elle collabore avec des partenaires fédéraux du secteur financier, d'autres organismes de sécurité du secteur public, le secteur financier et les commissions provinciales des valeurs mobilières dont les responsabilités comportent des cyberrisques.

Les activités de cybersécurité internes et externes de la Banque sont de plus en plus interreliées, particulièrement dans le cas des systèmes déterminants et essentiels, comme les systèmes de compensation et de règlement des paiements, d'adjudication des titres et de gestion des réserves de change.

En 2018, la Banque s'est associée aux grandes banques canadiennes et à Paiements Canada en vue d'accroître la résilience du système de paiement de gros. Ce partenariat prévoit des exercices de simulation conjoints, des protocoles de communication coordonnés, l'amélioration de la cyberdétection et des solutions conjointes relatives à la résilience et au rétablissement des opérations. À l'avenir, c'est le nouveau Groupe sur la résilience du secteur financier canadien qui les gérera.

La Banque surveille les IMF désignées dont les responsabilités de compensation et de règlement des paiements jouent un rôle important dans la stabilité du système financier. La Banque effectue des évaluations des risques des IMF selon ses propres normes, fondées sur les Principes pour les infrastructures de marchés financiers (PIMF) établis par le CPIM et l'OICV. Ces normes couvrent entre autres les risques financiers, opérationnels et d'activité.

Objectif externe 1

Renforcer la résilience du système financier

La Banque continuera d'accroître la cyberrésilience du système financier canadien.

Résultats attendus

- Les exigences réglementaires en matière de cybersécurité sont définies en fonction des objectifs de surveillance de la Banque.
- Les IMF désignées sont résilientes aux cyberincidents majeurs.

Mesures stratégiques pour 2019-2021

Pour atteindre ces résultats, la Banque :

- s'emploiera, avec des partenaires du secteur public et les autorités de réglementation, à définir les exigences de cybersécurité relatives aux cybersystèmes canadiens essentiels, conformément à la stratégie nationale de cybersécurité du gouvernement du Canada[6];
- poursuivra son partenariat avec Paiements Canada et les institutions financières canadiennes en vue de moderniser les systèmes de paiement de gros du Canada et d'en accroître la résilience;
- améliorera les outils et les données servant à l'analyse, à l'évaluation et à la communication des cybermenaces et des cybervulnérabilités pour le système financier afin d'en accroître la compréhension.

Objectif externe 2

Renforcer la collaboration et les partenariats

La Banque travaillera en étroite collaboration avec des partenaires clés des secteurs public et privé pour développer de l'expertise, mettre en commun des pratiques exemplaires et collaborer à des stratégies, à des politiques et à des projets de réglementation visant à atténuer les cyberrisques.

Résultats attendus

- Des initiatives visant à renforcer la cyberrésilience des systèmes sont en place à l'échelle nationale.
- Des protocoles de mise en commun de l'information sont en place avec des instances de discussion et des homologues internationaux.

Mesures stratégiques pour 2019-2021

Pour atteindre ces résultats, la Banque :

- collaborera avec des partenaires pour trouver des moyens d'améliorer la qualité des services de cybersécurité utilisés sur le marché canadien;
- améliorera la mise en commun de l'information et la coordination avec les instances de discussion et les organismes homologues de cybersécurité à l'échelle nationale et internationale.

Objectif externe 3

Renforcer les pratiques de cybersécurité des IMF

La Banque remplira le mandat qui lui a été confié par la loi, qui consiste à favoriser la stabilité du système financier par la surveillance des IMF.

Résultats attendus

- Les attentes des autorités de réglementation en matière de cybersécurité sont exposées clairement aux IMF.
- Les mécanismes de cybersécurité des IMF et les cybermenaces auxquelles elles sont exposées sont bien compris.
- Les IMF ont des plans d'intervention et de rétablissement efficaces en cas de cyberincident.

Mesures stratégiques pour 2019-2021

Pour atteindre ces résultats, la Banque :

- précisera les attentes à l'endroit des infrastructures de marchés financiers quant au respect de ses normes de gestion des cyberrisques;
- travaillera avec des spécialistes et des partenaires externes afin d'évaluer les cyberrisques et les cybermenaces auxquels sont exposées les IMF;
- collaborera avec des partenaires pour renforcer la capacité des IMF d'intervenir et de reprendre leurs opérations en cas de cyberincident – des guides et des exercices de simulation seront utilisés pour vérifier l'état de préparation des IMF et la vitesse à laquelle elle peuvent rétablir leurs opérations.

Objectif externe 4

Améliorer la cybersurveillance

La Banque travaillera avec le gouvernement du Canada et ses organismes pour accroître les initiatives législatives, réglementaires et de surveillance en lien avec la cybersécurité.

Résultats attendus

- Le rôle de surveillance de la Banque du Canada en matière de cybersécurité est intégré aux obligations découlant de la *Loi sur la compensation et le règlement des paiements*.
- Des cyberressources sont en place pour appuyer le rôle de surveillance.

Mesures stratégiques pour 2019-2021

Pour atteindre ces résultats, la Banque :

- élaborera des plans pour respecter ses nouvelles obligations législatives relatives aux cybersystèmes canadiens essentiels;
- mettra en œuvre un plan de formation et de perfectionnement en matière de cybersécurité pour les personnes prenant part aux activités de surveillance du système financier canadien.

Stratégie de cybersécurité 2019-2021 – Résultats internes

OBJECTIFS	IDENTIFIER ET GÉRER	PROTÉGER	DÉTECTER	INTERVENIR	RÉTABLIR
RÉSULTATS	Les processus de gouvernance et de gestion des risques permettent de gérer et de surveiller efficacement les cyberrisques et de prendre des décisions fondées sur les risques. Les cyberrisques liés aux opérations essentielles, y compris ceux auxquels sont exposés des tiers, sont compris et évalués adéquatement. La Banque a accès, en temps voulu, aux compétences et aux talents nécessaires dans le domaine de la cybersécurité.	L'accès aux actifs et aux systèmes est géré de manière efficace et se limite aux utilisateurs autorisés et à l'usage permis. Les vulnérabilités sont identifiées rapidement, leur incidence est comprise et les mesures d'atténuation appropriées sont appliquées. Les données sont catégorisées et protégées de façon adéquate. La sensibilisation des employés de la Banque à la cybersécurité dépasse celle des employés d'organisations homologues. Les services de cybersécurité sont actualisés et la sécurité fait partie intégrante de la conception des systèmes.	Les cyberattaques sont détectées rapidement et gérées de manière appropriée. Les paramètres de sécurité sont appliqués et surveillés systématiquement. La communication de renseignements à jour sur les menaces favorise la gestion efficace des cyberincidents.	Les plans et processus de cyberdéfense et d'intervention sont régulièrement mis à l'essai. Les mesures d'intervention en cas d'incident sont gérées en permanence et automatisées si les circonstances le justifient. Les enquêtes judiciaires sont menées efficacement. Les activités d'intervention sont coordonnées efficacement avec les parties prenantes internes et externes.	Des tests de reprise des activités en cas de cyberattaque sont effectués régulièrement et les plans connexes sont constamment améliorés. Le rétablissement à la suite d'un cyberincident se fait dans un délai convenable et la communication avec les parties internes et externes est adéquate.
FEUILLE DE ROUTE 2019-2021	Goût du risque, seuils et cibles Normes, politiques et processus améliorés Stratégie relative aux employés	Catégorisation et protection des données et de l'information Gestion élargie des vulnérabilités Sensibilisation accrue à la cybersécurité Programme de gestion de l'identité et de l'accès	Perfectionnement des outils de cybersécurité Gestion de la configuration de la sécurité Programme d'évolution de la surveillance de la sécurité Amélioration des renseignements sur les menaces	Programme des tests de cybersécurité Amélioration des enquêtes judiciaires	Exercices sur le rétablissement en cas de cyberincident Plan de rétablissement et mesures correctives, élaboration de guides et exercices d'intervention en cas d'incident

Stratégie de cybersécurité 2019-2021 – Résultats externes

OBJECTIFS EXTERNES	RENFORCER LA RÉSILIENCE DU SYSTÈME FINANCIER	RENFORCER LA COLLABORATION ET LES PARTENARIATS	RENFORCER LES PRATIQUES DE CYBERSÉCURITÉ DES IMF	AMÉLIORER LA CYBERSURVEILLANCE
RÉSULTATS	Les exigences réglementaires en matière de cybersécurité sont définies en fonction des objectifs de la Banque. Les systèmes de paiement sont résilients aux cyberincidents majeurs.	Des initiatives visant à renforcer la cyberrésilience des systèmes sont en place à l'échelle nationale. Des protocoles de mise en commun de l'information sont en place avec des instances de discussion et des homologues internationaux.	Les attentes des autorités de réglementation en matière de cybersécurité sont exposées clairement aux IMF. Les mécanismes de cybersécurité des IMF et les cybermenaces auxquelles elles sont exposées sont bien connus. Les IMF ont des plans d'intervention et de rétablissement efficaces en cas de cyberincident.	Le rôle de surveillance de la Banque du Canada est intégré aux obligations découlant de la *Loi sur la compensation et le règlement des paiements*. Des cyberressources sont en place pour appuyer le rôle de surveillance.
FEUILLE DE ROUTE 2019-2021	Résilience des systèmes de paiement de gros Planification des cybersystèmes essentiels Mise en œuvre d'un régime de réglementation fédéral en matière de cybersécurité	Programme de certification en matière de cybersécurité Mise en œuvre d'un programme externe de cybersécurité Coordination des plans de gestion de crise et trousse d'outils	Lignes directrices pour la cyberrésilience des IMF Exercices d'intervention et de rétablissement des opérations en cas d'incident Définition de scénarios de menace pour les systèmes	Planification de la surveillance des IMF Plan de formation et de perfectionnement relatif au système financier, à la stabilité financière et à la cybersécurité

CONCLUSION – RÉALISER LA VISION EN MATIÈRE DE CYBERSÉCURITÉ

« Réduire les risques et renforcer la résilience » est le thème sous lequel la Banque du Canada compte aborder la cybersécurité à moyen terme.

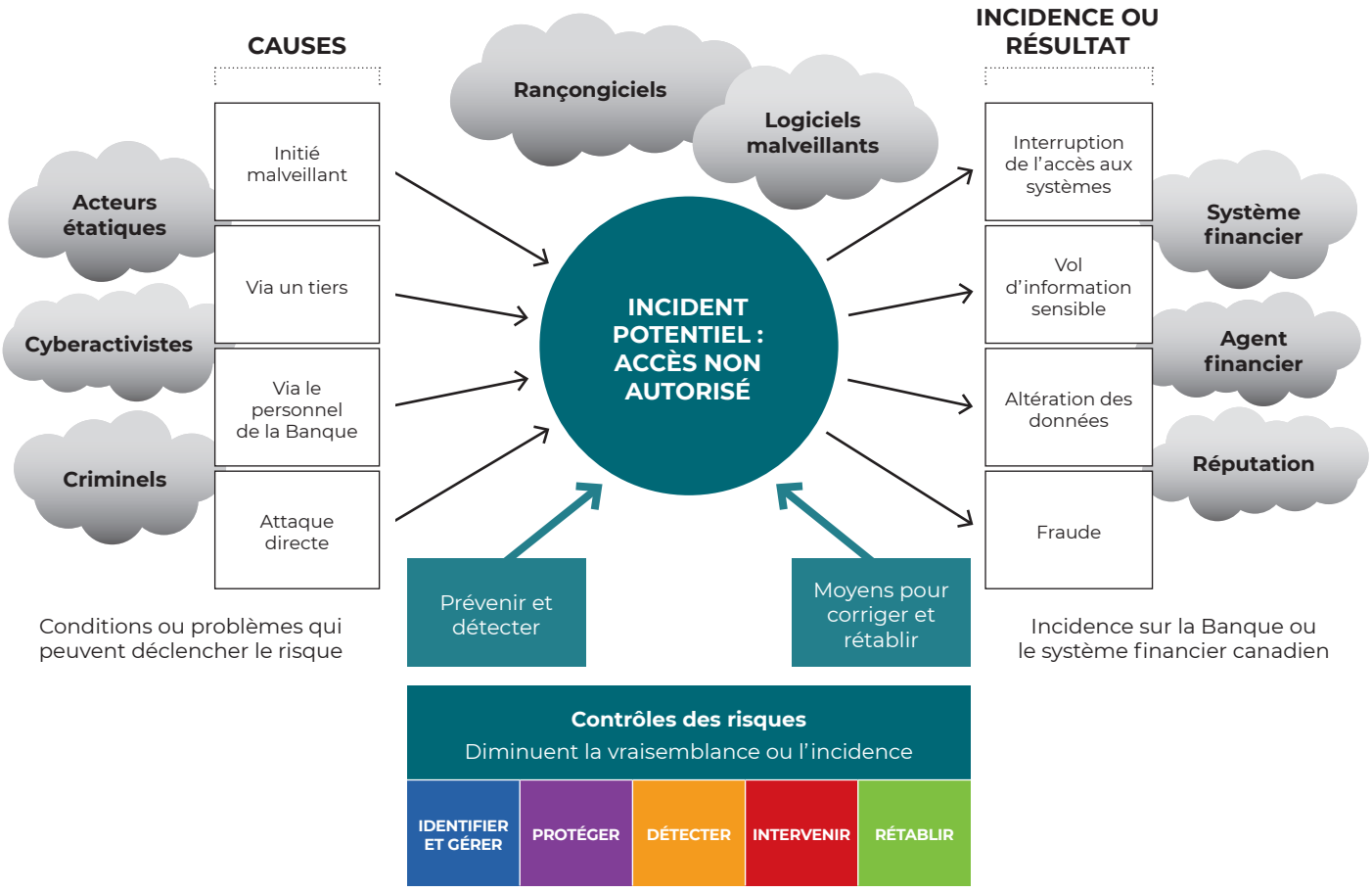
La Banque favorisera la résilience de ses propres activités et contribuera à renforcer les systèmes financiers canadien et international. Pour ce faire, ses efforts déployés à l'interne et à l'externe en matière de cybersécurité seront étroitement intégrés grâce à sa collaboration avec les parties prenantes et partenaires publics et privés du système financier.

La vision, la mission, les buts et les résultats attendus sont délibérément ambitieux en raison de la nature critique de la cybersécurité. S'appuyant sur les assises solides de la Banque en matière de cybersécurité, la stratégie définit la méthode d'intervention adoptée pour faire face aux défis que poseront les cybermenaces dans l'avenir.

La Banque élaborera un cadre de mesure pour permettre le suivi et le compte rendu des progrès, y compris des tests de cybersécurité et des évaluations de la posture en la matière.

La stratégie de cybersécurité aidera la Banque à réaliser sa vision, sa mission et ses objectifs en matière de cybersécurité.

ANNEXE – GESTION DES RISQUES ET NIST



L'évaluation de l'efficacité et de la résilience des programmes et de l'infrastructure de cybersécurité repose sur la politique et le cadre de la Banque du Canada en matière de gestion des risques d'entreprise.

La stratégie de cybersécurité cadre avec les deux grands principes de l'Énoncé sur le goût du risque de la Banque, soit :

1. limiter et gérer l'incidence des risques qui pourraient nuire à la capacité de l'institution d'accomplir son mandat;
2. prendre des risques calculés afin de favoriser l'innovation, de faire progresser nos recherches et l'élaboration de politiques, et d'améliorer nos opérations et nos pratiques organisationnelles.

La vision, la mission et les objectifs de la stratégie de cybersécurité témoignent de l'intention de la Banque de limiter les cyberrisques tout en favorisant l'innovation par la mise en commun de l'information et la collaboration. Les comportements à l'appui du goût du risque sont intégrés aux indicateurs de succès de la stratégie.

Cadre de gestion des cyberrisques

La Banque a élaboré un cadre de gestion des risques pour guider l'évaluation des cyberrisques. Ce cadre est fondé sur un ensemble de normes, de lignes directrices et de pratiques exemplaires du National Institute of Standards and Technology (NIST), qui sont axées sur la gestion des cyberrisques.

Les cinq fonctions du NIST – identifier, protéger, détecter, intervenir et rétablir – ont servi à guider les discussions et les analyses des cybermenaces ainsi qu'à définir les mesures de contrôle appropriées pour gérer les principaux risques.

La stratégie de cybersécurité présente l'approche et les mesures qu'adoptera la Banque pour faire face aux risques existants et aux nouveaux risques, ainsi que pour prévenir les cyberattaques et favoriser la résilience qui permettra d'intervenir et de rétablir les opérations en cas d'accès non autorisés.

NOTES

1. Voir le communiqué de la réunion des ministres des Finances et des gouverneurs des banques centrales du G20 (Allemagne), mars 2017. Citation du rapport du Comité de Bâle sur le contrôle bancaire : *Cyber-Resilience: Range of Practices*, Banque des Règlements Internationaux. https://www.bis.org/bcbs/publ/d454.htm

2. Banque du Canada (2014), « Résilience du système financier canadien : l'apport de la cybersécurité », *Revue du système financier*.
https://www.banqueducanada.ca/wp-content/uploads/2014/12/rsf-decembre14-morrow.pdf

3. Comité sur les paiements et les infrastructures de marché, Conseil de l'Organisation internationale des commissions de valeurs (2016), *Guidance on Cyber Resilience for Financial Market Infrastructures*, juin.
https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

4. SWIFT (Society for Worldwide Interbank Financial Telecommunication) est le principal fournisseur de services de messagerie de paiements pour les institutions financières du monde entier. https://www.swift.com/

5. *Plan à moyen terme 2019-2021 de la Banque du Canada : Chef de file dans la nouvelle ère*
https://www.banqueducanada.ca/sujet-banque/direction-gouvernance/plan-moyen-terme-2019-2021-chef-file-nouvelle-ere/

6. Gouvernement du Canada, *Stratégie nationale de cybersécurité : Vision du Canada pour la sécurité et la prospérité dans l'ère numérique*.
https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-fr.aspx