GROUPE DES SEPT – ÉLÉMENTS FONDAMENTAUX POUR LA CYBERSÉCURITÉ DU SECTEUR FINANCIER

De plus en plus sophistiqués, fréquents et persistants, les risques cyber deviennent plus dangereux et diversifiés, menaçant de perturber nos systèmes financiers mondiaux interconnectés et les institutions qui exploitent et prennent en charge ces systèmes. Pour faire face à ces risques, les éléments fondamentaux qui figurent ci-après constituent un texte de haut niveau sans valeur réglementaire; ils s'adressent aux entités privées et publiques du secteur financier et peuvent être déclinés en fonction de leur environnement opérationnel et des menaces qui s'y rapportent, de leur rôle dans le secteur ainsi que de leurs obligations légales et réglementaires.

Les éléments ont vocation à fournir les blocs constitutifs à partir desquels une entité peut concevoir et mettre en œuvre sa stratégie de cybersécurité et son cadre opérationnel, selon son approche en matière de gestion et de culture du risque. Les éléments présentent également les étapes d'un processus dynamique à l'aide duquel l'entité peut réévaluer systématiquement sa stratégie et son cadre de cybersécurité au fur et à mesure de l'évolution de l'environnement opérationnel et des menaces. Les autorités publiques, au sein d'une même juridiction ou entre plusieurs juridictions, peuvent en outre se servir des éléments pour orienter leurs actions de politique publique, de réglementation et de supervision. En s'appuyant sur ces éléments et en unissant leurs efforts, les entités privées et publiques, ainsi que les autorités publiques peuvent contribuer à renforcer la cybersécurité et la résilience globales du système financier international.

Élément 1 : Stratégie et cadre de cybersécurité
Établir et tenir à jour une stratégie et un cadre de cybersécurité qui soient adaptés aux différents cyber-risques et prenne correctement en compte les normes et lignes directrices internationales, nationales et professionnelles.

La stratégie et le cadre de cybersécurité visent à préciser comment identifier, gérer et réduire efficacement les cyber-risques d'une manière intégrée et exhaustive. Les entités du secteur financier devraient établir une stratégie et un cadre de cybersécurité adaptés à leur nature, leur taille, leur complexité, leur profil de risque et leur culture. Prenant en compte le contexte des cyber-menaces et des vulnérabilités, une autorité compétente nationale peut aussi établir une stratégie et un cadre de cybersécurité sectoriels qui décrivent la coopération entre les entités et les autorités publiques dans le secteur financier, ainsi qu'avec d'autres secteurs dont dépend le secteur financier, ou avec toute autre autorité compétente nationale concernée.

Élément 2 : Gouvernance
Par souci de responsabilisation, définir les rôles et les responsabilités du personnel assurant la mise en œuvre, la gestion et la surveillance de l'efficacité de la stratégie et du cadre de cybersécurité ; faciliter l'exécution de ces rôles et responsabilités; fournir les ressources adéquates, accorder le niveau d'autorité approprié et un accès aux instances dirigeantes (par exemple, le conseil d'administration ou les hauts fonctionnaires des autorités publiques).

Des structures de gouvernance efficaces renforcent la responsabilisation en ce qu'elles formulent clairement quelles sont les attributions de chacun, ses lignes de rattachement et les processus d'escalade en cas de désaccord. Une gouvernance efficace permet aussi de concilier des objectifs concurrents et de favoriser la communication entre les unités opérationnelles et les fonctions liées

aux technologies de l'information, aux risques et au contrôle. Conformément à leurs missions et à leurs orientations, les conseils d'administration (ou les organes de surveillance similaires dans le cas des entités ou autorités publiques) devraient déterminer la tolérance aux cyber-risques de leur entité et superviser la conception, la mise en œuvre et l'efficacité des programmes de cybersécurité qui y sont relatifs.

Élément 3 : Évaluation des risques et des contrôles
Déterminer les fonctions, les activités, les produits et les services – y compris les interconnexions, les dépendances et les tiers –, hiérarchiser leur importance relative et évaluer leurs cyber-risques respectifs. Déterminer et mettre en œuvre des moyens de maîtrise – y compris par des systèmes, des politiques, des procédures et de la formation – afin de se protéger contre ces risques et les gérer selon le degré de tolérance établi par l'autorité gouvernante.

Idéalement, dans le cadre d'un programme de gestion des risques internes, les entités devraient évaluer le cyber-risque intrinsèque (c'est-à-dire le risque brut, sans prise en compte de mesures visant à le maîtriser) que présentent les personnes, les processus, les technologies et les données sous-jacentes qui soutiennent chaque fonction, activité, produit et service particulier. Les entités devraient alors déterminer et évaluer l'existence et l'efficacité des moyens de réduction du cyber risque pour le ramener à un niveau résiduel. Les mécanismes de réduction peuvent comprendre le fait d'éviter le risque ou de l'éliminer en ne se livrant pas à une activité déterminée. Ils peuvent aussi comprendre l'atténuation du risque à l'aide de dispositifs de maîtrise, ou encore le partage ou le transfert du risque. En plus d'évaluer les cyber-risques d'une entité propres à ses fonctions, ses activités, ses produits et ses services, les évaluations des risques et des mesures de maîtrise devraient tenir compte de tout cyber-risque que l'entité peut faire courir à d'autres et au secteur financier dans son ensemble. Les autorités publiques devraient identifier les fonctions économiques essentielles de leur système financier dans le cadre de leurs évaluations des risques et des mesures de maîtrise, et ce, afin de connaître les points uniques de défaillance et le risque de concentration. Les fonctions économiques essentielles du secteur comprennent la réception des dépôts, les prêts et les paiements, ainsi que les échanges, la compensation, le règlement et la conservation de titres.

Élément 4 : Surveillance
Établir des processus de surveillance automatisés destinés à déceler rapidement les incidents de cybersécurité et évaluer périodiquement l'efficacité des mesures de maîtrise du risque, y compris par la surveillance des réseaux, des tests, des audits et des exercices.

Une surveillance efficace aide les entités à se conformer au degré de tolérance au risque qui prévaut et, en temps opportun, à améliorer les contrôles existants ou à remédier à leurs lacunes. Les protocoles de tests et d'audits offrent des mécanismes d'assurance essentiels aux entités comme aux autorités publiques. Selon la nature d'une entité, son profil de cyber risques et son environnement de maîtrise des risques, les fonctions de tests et d'audits devraient être adéquatement indépendantes du personnel responsable de la mise en œuvre et de la gestion du programme de cybersécurité. À l'aide d'enquêtes, de contrôles sur place et d'autres moyens de supervision, d'une analyse comparative des résultats des tests des entités et d'exercices publics-privés conjoints, les autorités publiques peuvent mieux comprendre les cyber menaces et les vulnérabilités de l'ensemble du secteur, ainsi que le profil relatif de risques et les capacités d'entités données.

Élément 5 : Intervention

En temps opportun : a) évaluer la nature, la portée et l'incidence des incidents de cybersécurité ; b) limiter l'incident et en atténuer l'impact ; c) notifier les parties prenantes internes et externes (comme les forces de l'ordre, les autorités de réglementation et autres autorités publiques, ainsi que les actionnaires, les prestataires de service externes et éventuellement les clients) ; et d) coordonner les activités d'intervention conjointes en tant que de besoin.

Dans le cadre de leurs évaluations des risques et des mesures de maîtrise associées, les entités devraient mettre en œuvre des politiques d'intervention ainsi que toute autre mesure de maîtrise afin de faciliter une intervention efficace en cas d'incident. Entre autres choses, ces mesures devraient clarifier quelles sont les responsabilités dans la prise de décision, définir les procédures d'escalade et établir des processus pour communiquer avec les parties prenantes internes et externes. Faire l'exercice d'un mode opératoire d'intervention au sein et entre des entités et autorités publiques contribue à rendre les interventions plus efficaces. Faire de tels exercices permet également aux entités et autorités publiques de déterminer l'incidence de leurs décisions éventuelles sur leur capacité à maintenir leurs activités et services critiques ou non-critiques.

Élément 6 : Rétablissement
Reprendre les opérations de façon responsable tout en permettant de continuer la remise en état, y compris a) en mettant fin aux effets néfastes de l'incident; b) en rétablissant les systèmes et les données à la normale et en confirmant le retour à l'état normal; c) en relevant et en remédiant à toutes les vulnérabilités qui ont été exploitées; d) en corrigeant les failles afin de prévenir des incidents semblables; et e) en communiquant de manière appropriée en interne et en externe.

Une fois que la stabilité et l'intégrité opérationnelles sont assurées, le rétablissement rapide et efficace des opérations devrait suivre le niveau d'importance des fonctions économiques critiques et non-critiques, dans le respect des objectifs établis par les autorités publiques concernées. Le maintien de la confiance dans le secteur financier s'améliore grandement lorsque les entités et les autorités publiques sont capables de s'entraider pour assurer la reprise et le rétablissement des fonctions, des activités et des processus essentiels. Par conséquent, avant qu'un incident ne se produise, le fait d'établir et de tester des plans d'urgence pour les activités essentielles et les processus clés, comme le financement, peut contribuer à rendre le rétablissement plus rapide et plus efficace.

Élément 7 : Échange de renseignements
Participer à l'échange, en temps opportun, avec les parties prenantes internes et externes (y compris les entités et les autorités publiques du secteur financier ou d'autres secteurs), de renseignements fiables et utiles relatifs à la cybersécurité portant sur les menaces, les vulnérabilités, les incidents et les interventions effectuées, afin de renforcer les défenses, de limiter les dommages, d'accroître la connaissance de la situation et d'élargir l'apprentissage.

L'échange de renseignements techniques, tels que les indicateurs de menace ou des détails concernant la façon dont les vulnérabilités ont été exploitées, permet aux entités de maintenir à jour leurs systèmes de défense et de prendre connaissance des nouvelles méthodes employées par les attaquants. Le fait d'échanger des connaissances élargies entre entités, entre les entités et les autorités publiques, et entre autorités publiques a pour effet d'approfondir la compréhension collective des moyens que les attaquants pourraient utiliser pour exploiter les vulnérabilités au sein du secteur tout entier et potentiellement perturber les fonctions économiques essentielles et compromettre la stabilité financière. Compte tenu de son importance, les entités et les autorités publiques devraient identifier et traiter les obstacles à l'échange de renseignements.

Élément 8 : Apprentissage continu
Passer en revue la stratégie et le cadre de cybersécurité sur une base régulière et chaque fois que les événements le justifient – y compris leurs composantes liées à la gouvernance, à l'évaluation des risques et des mesures de maîtrise associées, à la surveillance, à l'intervention, au rétablissement et à l'échange de renseignements – dans le but de répondre aux changements relatifs aux cyber risques, d'allouer des ressources, d'identifier et de combler les lacunes, ainsi que de tirer les enseignements.

Les cyber menaces et les vulnérabilités évoluent rapidement, tout comme les bonnes pratiques et les normes techniques destinées à y faire face. La composition du secteur financier évolue elle aussi au fil du temps avec l'apparition de nouveaux types d'entités, de produits et de services et le recours de plus en plus grand à des prestataires de service externes. Les stratégies et cadres de cybersécurité des entités, ainsi que ceux du secteur financier, doivent être examinés et mis à jour périodiquement pour s'adapter à l'évolution des menaces et des dispositifs de maîtrise, pour mieux sensibiliser les utilisateurs et pour déployer efficacement les ressources. D'autres secteurs, comme ceux de l'énergie et des télécommunications, présentent des dépendances externes [avec le secteur financier]; par conséquent, au cours de tout processus d'examen, les entités et les autorités publiques [du secteur financier] devraient tenir compte des changements qui interviennent dans ces secteurs.