PAR COURRIER ÉLECTRONIQUE : [redacted]

Montréal, le 30 mars 2016

[redacted]

Objet: Demandes d'accès – Informations diverses
N/D : GDC05-06-01-2341

[redacted]

Nous désirons donner suite à vos demandes d'accès reçues au Secrétariat général de l'Autorité des marchés financiers (l' « Autorité »), le 1er mars 2016.

Afin de faciliter le traitement de vos demandes et le repérage des informations que vous recherchez, nous avons regroupé vos quatre demandes.

Vous souhaitez obtenir les renseignements suivants :

1. *les rapports, bilans ou documents en lien avec des attaques informatiques ayant visé [notre] institution en 2013, 2014 et 2015* (1ère demande);

2. *les rapports, bilans ou documents en lien avec des virus ou autres logiciels malveillants ayant infecté le réseau informatique de [notre] institution en 2013, 2014 et 2015* (2e demande);

3. *les rapports, bilans ou documents en lien avec des données électroniques sous la responsabilité de [notre] institution qui ont été ou auraient été volées en 2013, 2014 et 2015* (3e demande);

4. *les dates, les noms des compagnies, les montants et la nature des services pour tous les contrats ayant été octroyés à des firmes externes pour trouver des failles de sécurité dans [notre] système et réseau informatique en 2013, 2014 et 2015* (4e demande).

En réponse à votre requête, vous trouverez ci-joint les renseignements et documents suivants.

Cyber-risque : une réalité incontournable

Les risques reliés à la cybersécurité s'avèrent une menace importante et grandissante pour l'intégrité et l'efficience des marchés et des institutions financières, pour la protection des investisseurs et des consommateurs ainsi que pour la confiance envers le système financier. De plus, ces risques interpellent, de façon croissante, les régulateurs et les organismes d'encadrement et de surveillance à l'échelle mondiale.

Les cyberattaques visent à acquérir, modifier, détruire ou perturber des données, réseaux ou systèmes informatiques cruciaux. Elles pourraient nuire gravement à l'Autorité et plus précisément aux marchés financiers ainsi qu'à la confiance des entreprises. Ces attaques sont lancées à travers le monde sans considération pour les frontières géographiques et les législations nationales.

L'Autorité n'est donc pas épargnée par les cyberattaques. Régulièrement, des attaques de nature et de gravité diverses sont détectées, contenues et analysées par notre équipe de sécurité. Que ce soit des tentatives d'intrusion dans nos réseaux, de destruction ou de perturbation de nos systèmes, la menace que représentent les cyberattaques est en constante évolution et symbolise un risque réel pour l'organisation.

L'approche de l'Autorité face à sa cybersécurité

La cybersécurité occupe une place de plus en plus grande à l'Autorité, dans un monde où les technologies de l'information sont en constante évolution.

L'information numérique est un des leviers d'importance qui permet à l'Autorité d'accomplir sa mission. Cette information est mise à contribution dans l'ensemble des opérations courantes. De plus, dans les dernières années, l'Autorité a grandement accru sa présence dans l'espace cybernétique si bien, qu'aujourd'hui, elle est en mesure d'offrir tant aux consommateurs qu'à l'industrie, plusieurs services en ligne dont certains de nature transactionnelle (demande de certificat, inscription à un examen, etc.).

Cette réalité impose à l'Autorité la responsabilité de prendre l'ensemble des mesures propres à maintenir la nécessaire confiance qui doit exister de la part de l'industrie financière et des citoyens, à l'égard de l'information numérique dont notre organisation est dépositaire.

Ainsi, les défis liés à la cybersécurité sont considérés avec sérieux par notre organisation et les ressources appropriées sont déployées afin d'y faire face. Au-delà des projets spécifiques et ponctuels en sécurité, des investissements significatifs sont effectués annuellement.

Afin d'assurer l'intégrité de son information numérique, l'Autorité a mis en place plusieurs mesures. Celles-ci couvrent un large spectre, allant de la gouvernance, au respect des normes et des bonnes pratiques de développement de systèmes jusqu'à des pratiques saines d'exploitation et l'établissement de directives sur les comportements adéquats, en passant par des outils technologiques de détection, d'interception et de contrôle des menaces cybernétiques reconnus par l'industrie.

L'ensemble de ces mesures vise à renforcer la confiance, agir de manière concertée, responsabiliser les utilisateurs et s'adapter aux menaces et aux risques. Elles se déclinent selon les axes suivants.

Au plan de la gouvernance

L'Autorité est dotée d'un cadre de gouvernance et de gestion en matière de sécurité de l'information. Elle voit à l'actualisation périodique de celui-ci. Ainsi, la structure dont elle s'est dotée lui permet de disposer d'une équipe dédiée à la sécurité de l'information qui implique directement plusieurs ressources ayant des rôles distincts et travaillant en étroite collaboration :

- dirigeant sectoriel de l'information;
- responsable de la sécurité de l'information;
- responsable de la sécurité de l'information numérique;
- responsable de la sécurité dans les projets;
- responsable de la sécurité opérationnelle;
- responsable de la continuité des affaires;
- responsable de la protection des données et du plan de relève T.I.

Toute cette équipe travaille et concerte son action dans des groupes de travail regroupant les acteurs concernés de l'organisation. Ces groupes permettent une action en adéquation avec le cadre de gouvernance en sécurité, qui intègre les aspects suivants :

- gestion intégrée des risques;
- protection et sécurité de l'information;
- sécurité de l'information numérique;
- gouvernance des technologies de l'information.

Sous l'impulsion de ces intervenants, les initiatives suivantes sont menées :

- La tenue et l'animation de séances du Comité de protection et de la sécurité de l'information (CPSI), afin d'assurer que les mesures de sécurité reconnues dans l'industrie soient mises en œuvre et que le risque résiduel soit connu et accepté par l'organisation;
- Concertation à l'égard des enjeux particuliers avec le Comité de gestion intégrée des risques (CGIR);
- La veille stratégique des cyber-risques pour assurer que l'équipe de sécurité comprend et peut surveiller efficacement les risques en matière de cybersécurité;
- La définition et le contrôle d'un ensemble de procédures afin de limiter les dommages dans l'éventualité d'une cyberattaque (processus de gestion des incidents).

Par ailleurs, l'Autorité administre un programme d'audit interne qui pose un regard critique sur les éléments d'importance de notre univers de risques dont celui de la cybersécurité.

Au plan technologique

L'équipe de sécurité numérique effectue une vigie afin de s'assurer que les cyberattaques n'atteignent pas nos réseaux et systèmes d'information, soit pour s'approprier de l'information confidentielle, soit pour altérer des systèmes d'information ou pour perturber les services offerts à la population. Celle-ci a également pour responsabilité de veiller à ce que l'organisation puisse intégrer, au moment approprié, les évolutions technologiques nécessaires à diminuer notre vulnérabilité et contrer les cyberattaques.

En collaboration avec le RSI, le RSIN met en œuvre, avec l'équipe des experts technologiques de la Direction principale des technologies de l'information (DPTI), des mesures de protection de son infrastructure promptes à répondre à d'éventuels incidents. Ces mesures technologiques impliquent, entre autres, et à titre d'exemple :

- La surveillance 24h/24 grâce à un service de télésurveillance de notre infrastructure numérique qui permet à l'équipe de sécurité de prendre en charge rapidement toute situation anormale, le cas échéant;
- L'application rigoureuse d'un processus d'installation des correctifs de sécurité informatique afin de limiter les vulnérabilités de ses systèmes, ce qui permet d'être à jour en tout temps et d'éviter des cyberattaques;
- L'établissement de plans de relève en cas d'incidents, dont les cyberattaques, afin de limiter les dommages sur ses opérations et le service au public.

Au plan de la sensibilisation et de la formation continue

L'humain demeure un facteur de risque central dans le cadre des cyberattaques. L'Autorité est investie dans un programme de sensibilisation auprès de ses employés et mise sur la formation continue de ses spécialistes, afin qu'ils conservent leurs compétences en matière de lutte aux cyberattaques.

Plus particulièrement, les initiatives prises sont les suivantes :

- Former continuellement les spécialistes en sécurité;
- Assurer le *membership* des experts en sécurité dans les associations spécialisées (ASIQ, ISACA, CAI, SCT (DSIG), etc.) afin qu'ils puissent partager et échanger les meilleures pratiques de l'industrie;
- Sensibiliser régulièrement le personnel à l'importance de la sécurité de l'information et au rôle que chaque employé joue à cet égard;
- Tester les réflexes de sécurité du personnel pour les sensibiliser aux comportements sécuritaires à adopter en matière de sécurité de l'information.

Au plan de la gestion des risques

La connaissance des cybermenaces par l'équipe de sécurité favorise l'efficacité des dispositifs de gestion des risques. Les mesures suivantes sont prises :

- Procéder régulièrement à des tests et à des évaluations de la vulnérabilité et de la sécurité;
- Assurer une veille de l'industrie, de l'actualité et des alertes diffusées par les diverses agences compétentes;
- Suivre les recommandations et les meilleures pratiques des associations professionnelles et des organismes reconnus en sécurité;
- Communiquer et surveiller le tableau de bord des risques pour la cybersécurité (CGIR).

Ainsi, l'Autorité s'est dotée de plusieurs mécanismes et contrôles, autant administratifs que techniques, pour être en mesure de prévenir et de réagir aux cyberattaques, et ce, dans un contexte où la seule constante dans le temps est le changement.

La performance de l'Autorité en matière de cybersécurité

L'Autorité a eu à gérer des incidents de sécurité numérique et il est prévisible que d'autres incidents se produiront. Jusqu'à présent, ces incidents cybernétiques n'ont pas donné lieu à des fuites ou vols d'informations et l'organisation continue de prendre les moyens appropriés pour prévenir ceux-ci. L'Autorité, pas plus qu'aucun autre organisme, ne pourra malheureusement jamais prétendre à l'inviolabilité.

L'Autorité dispose d'un processus de gestion des incidents de sécurité dans le cadre duquel ont été déclarés les incidents qui correspondent aux points #1 et #2 de votre demande. Ces incidents sont notamment identifiés en fonction d'une échelle de gravité à quatre niveaux (mineur, modéré, élevé et critique). Des statistiques globales, à cet égard, vous sont présentées ci-dessous.

Par ailleurs, notre organisation n'a connu aucune attaque informatique où des données électronique auraient été volées. Ainsi, aucun incident de cette nature n'a été déclaré en lien avec le point #3 de votre demande.

Failles de sécurité exploitées

Parmi les incidents de sécurité numérique que l'Autorité a eu à traiter au cours des années 2013 à 2015, 88 incidents sont reliés à l'introduction, jusqu'au poste de travail, de logiciels malveillants dont la contamination a pu être prévenue (66 cas) ou contrôlée (22 cas). Nous n'avons constaté aucun dommage qui en aurait découlé.

De ces incidents, 84 ont été jugés de gravité mineure, alors que 2 étaient de gravité modérée et que 2 autres étaient jugés de gravité élevée.

Les 2 incidents de gravité élevée sont liés à un virus qui a réussi à rendre indisponible des fichiers d'un lecteur réseau interne. Cet incident fût résolu grâce à notre infrastructure de sécurité résiliente, et ce, sans dommage pour l'organisation.

Actuellement, ce type de virus est identifié comme étant le principal facteur de risque, lié à l'introduction de code malveillant dans l'organisation et des moyens techniques sont en place et d'autres sont à venir afin de le réduire. Également, différentes initiatives de sensibilisation du personnel sont en place, incluant des communications régulières et des tests d'hameçonnage, et ce, afin d'augmenter le niveau de sensibilité.

Tentatives d'infiltration

Durant cette même période, 25 incidents sont reliés à des balayages et tentatives externes de toutes sortes qui ont été détectés par nos mécanismes de surveillance avant qu'ils ne puissent causer quelques dommages que ce soit.

De ces incidents, 23 ont été jugés de gravité mineure alors que 2 étaient de gravité modérée.

Afin de réduire les chances de succès de ce type d'attaque, des tests techniques d'intrusion sont effectués régulièrement et lorsque des failles sont identifiées, un plan d'action est élaboré pour corriger la situation le plus rapidement possible. De plus, un processus automatisé est en place pour l'application régulière des correctifs de sécurité sur les équipements.

La protection de son périmètre technologique et des renseignements confidentiels qu'il contient est une priorité pour l'Autorité. Notre organisation s'assure de demeurer agile dans sa gestion de la sécurité de l'information et ainsi pouvoir s'adapter rapidement à l'évolution des technologies et des normes du marché. Les moyens et pratiques internes sont au diapason de ces changements. En bref, l'Autorité est consciente que le risque nul n'existe pas, mais elle prend soin de se doter de moyens de protection reconnus sur le marché et pose les actions nécessaires au maintien de la confiance de l'industrie financière et du public.

Réponses spécifiques aux demandes d'accès

1ère et 2e demandes

En réponse à vos demandes énumérées aux points 1 et 2, nous vous informons que nous ne pouvons vous communiquer les documents que vous recherchez en application des articles 29 et 37 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1 (la « Loi sur l'accès »).

En effet, l'Autorité doit disposer de mesures adéquates afin d'assurer la protection de ses infostructures contre toute utilisation abusive et se prémunir contre toute menace et tout risque susceptible d'avoir un effet direct sur la disponibilité, l'intégrité et la confidentialité des informations qu'elle détient.

Or, les documents que vous recherchez sont des analyses détaillées et descriptives des incidents de sécurité numérique qui ont eu lieu au sein de notre organisation. Ils contiennent des recommandations quant aux améliorations à apporter et aux mesures de contrôle à instaurer. Ces informations révèlent les forces et les faiblesses de nos systèmes informatiques et leur divulgation pourrait réduire l'efficacité de nos programmes de sécurité.

3e demande

Aucun incident de cette nature ne s'étant produit, en réponse à votre demande énumérée au point 3, nous vous indiquons ne détenir aucun rapport, bilan ou document en lien avec des données électroniques de l'Autorité qui auraient été volées.

4e demande

Finalement, en réponse à votre demande énumérée au point 4, vous trouverez ci-joint un tableau qui présente le nom des prestataires de services, le numéro des contrats, le montant des contrats octroyés, les périodes couvertes ainsi qu'une description des mandats. Ainsi, pour la période visée par votre demande (2013, 2014 et 2015), nos travaux visant à identifier des failles de sécurité, en collaboration avec des consultants externes, se sont élevés à 360 046 $.

Vous noterez que les montants indiqués dans ce tableau n'ont pas nécessairement été déboursés en totalité par l'Autorité puisqu'il s'agit d'une estimation des coûts que celle-ci pourrait ou aurait pu encourir.

Nous vous informons que vous pouvez, en vertu de l'article 135 de la Loi sur l'accès, demander à la Commission d'accès à l'information de réviser la présente décision. Vous trouverez ci-jointe une note explicative concernant l'exercice de ce recours.

Veuillez agréer, [redacted], l'expression de nos sentiments les meilleurs.

Original signé

Me Benoit Longtin
Substitut à la responsable de l'accès
Secrétaire général adjoint
Autorité des marchés financiers

p.j.