IIACACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES

LETTRE DU PRÉSIDENT

N° 89

Donner l'exemple : l'ACCVM aide les sociétés membres à faire face aux cybermenaces mondiales

FAITS SAILLANTS :

Les six éléments clés d'un programme efficace de cybersécurité

La participation du conseil d'administration et du chef de la direction au programme de cybersécurité est essentielle

La première étape de l'évaluation du cyberrisque est de connaître quels sont les actifs que la société veut protéger et pourquoi

Un certain nombre de contrôles peuvent être utilisés pour protéger les systèmes de la société

L'ACCVM fournit une tribune pour discuter des problèmes et solutions ayant trait aux cybermenaces et elle offre des outils et modèles pour aider les sociétés

Le 9 novembre 2015, lors de la conférence pour les conseillers d'élite, j'ai donné un discours devant des conseillers inscrits auprès de l'OCRCVM et l'ACFM sur les menaces de cyberattaques contre les sociétés de courtage en valeurs mobilières et leurs clients. Le but de l'exposé était de décrire : la sophistication, l'envergure internationale et les graves conséquences des cyberattaques; les pertes financières et les données perdues par les sociétés et leurs clients; et l'impact négatif sur la réputation des sociétés et des conseillers à leur service. J'ai aussi expliqué les efforts déployés par l'Association canadienne du commerce des valeurs mobilières (ACCVM) pour sensibiliser les sociétés de courtage membres et les aider à faire face aux cybermenaces. Toutes les sociétés membres de l'ACCVM ont commencé à mettre en place des mesures adéquates pour se protéger des cyberattaques.

Les cyberattaques et leurs conséquences ont suscité un vif d'intérêt et soulevé beaucoup d'inquiétude parmi les sociétés membres de l'ACCVM. La publicité à l'échelle internationale générée par les cyberattaques (par exemple, le « gigantesque » piratage dont a été victime JPMorgan décrit dans le numéro du 10 novembre 2015 du Financial Times) en est une bonne illustration.

À quoi ressemble une cyberattaque?

J'ai commencé mon exposé en relatant ce qui est arrivé à deux entreprises. Dans le premier cas, tous les ordinateurs de l'entreprise ont été piratés et le réseau informatique de toute l'entreprise était complètement verrouillé. Les pirates ont ensuite informé l'entreprise qu'ils contrôlaient les ordinateurs et qu'à défaut de payer une certaine somme, le réseau informatique restera verrouillé et les données confidentielles seront supprimées ou rendues publiques. Le verrouillage du réseau et la demande de rançon qui a suivi sont désignés sous le terme « verrouillage cryptographique ». Dans le deuxième cas, un des responsables du service des technologies de l'information a avisé les hauts dirigeants que les systèmes informatiques de l'entreprise avaient été piratés au cours des six derniers mois. L'entreprise s'est retrouvée aux prises avec la tâche monumentale d'établir la nature de la défaillance de la sécurité informatique, et plus important encore, de cerner l'étendue des pertes financières et la quantité de données perdues.

Dans les deux cas, les entreprises ont dû mettre en place un plan d'action détaillé pour mettre fin rapidement au piratage, limiter les dommages causés aux clients et à l'entreprise, redémarrer l'entreprise et la faire fonctionner. Toutes les entreprises, qu'elles soient de petite ou grande taille, ont besoin d'un programme de remise en état à la suite d'un piratage informatique. L'expérience a montré que tant les entreprises de grande taille que celles de petite taille peuvent être l'objet d'une cyberattaque. Les entreprises de grande taille sont évidemment plus attrayantes et plus rentables, cependant les entreprises de petite taille sont perçues comme des cibles plus vulnérables par les pirates. Un programme de remise en état comprend plusieurs mesures et intervenants pour établir l'origine de la défaillance de la sécurité informatique : systèmes internes de la société ou systèmes d'un tiers fournisseur. Il doit comprendre : des consultations auprès d'informaticiens et d'enquêteurs spécialisés; une évaluation de l'importance des dommages (les personnes touchées et les informations piratées); un avis juridique pour minimiser les dommages civils et les coûts réglementaires; une stratégie de communication avec les clients, les forces de l'ordre et les compagnies d'assurance qui précise les informations à leur fournir ainsi que l'ordre chronologique dans lequel elles seront fournies; et des mesures appropriées et efficaces pour protéger l'entreprise.

Éléments d'un programme efficace de cybersécurité

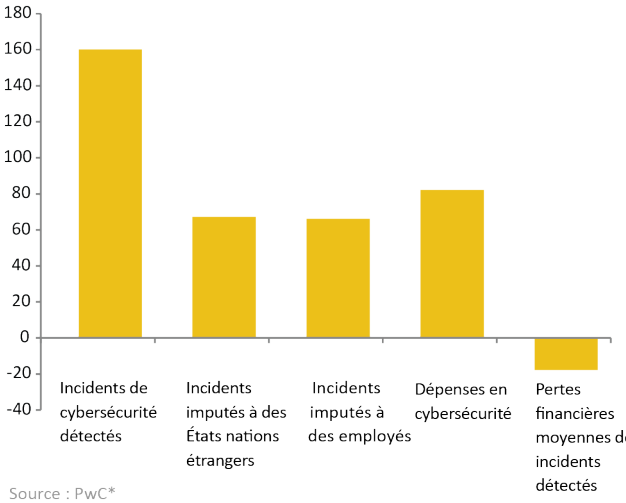
Le programme de cybersécurité d'une société membre de l'ACCVM devrait comprendre à peu près six éléments clés :

1. Gouvernance et gestion du risque

Le premier élément est de s'assurer d'une collaboration, d'un engagement et d'une participation sans réserve de la part du conseil d'administration et du chef de la direction de la société pour la mise en place d'un programme de cybersécurité. Un engagement ferme de la haute direction de l'entreprise envers la cybersécurité est important pour s'assurer que les responsables clés de tous les services de l'entreprise participeront au programme de cybersécurité. Les cyberattaques sont beaucoup trop sophistiquées et dangereuses pour en confier la prévention seulement au service des technologies de l'information de l'entreprise.

Graphique 1 : Incidents de cybersécurité au Canada

Changement 2015 vs 2014 (%)



Source : PwC*

2. Évaluation du risque

La société doit établir quels sont ses actifs essentiels qui peuvent être l'objet d'une cyberattaque. Un programme efficace peut être élaboré seulement si la société connaît quels sont ses « joyaux de la couronne » et en quoi ils sont vulnérables à une cyberattaque. La société doit établir la robustesse de ses moyens de défense et contrôles à l'interne, et évaluer les mécanismes de contrôle qu'elle exerce sur les tiers fournisseurs qui ont accès à son système informatique. La société doit donc faire preuve de diligence raisonnable à l'égard des tiers fournisseurs pour connaître tous leurs accès à son système informatique afin de minimiser le risque d'intrusion par des cybercriminels.

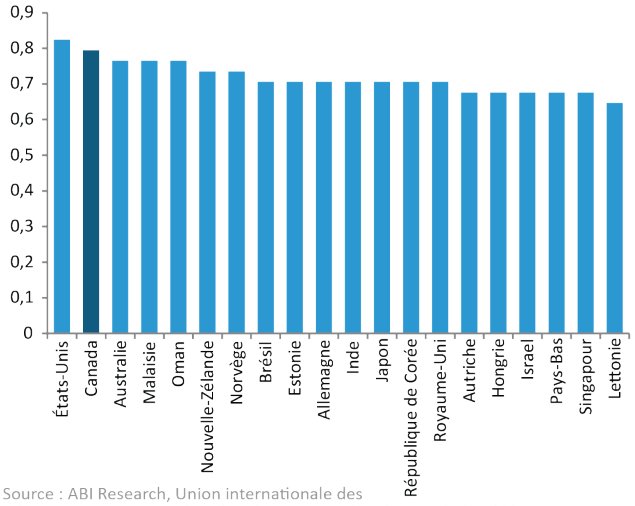
3. Contrôles techniques et procéduraux

La société peut se servir d'un certain nombre de contrôles pour protéger ses systèmes. Les contrôles appropriés dépendent surtout de la nature des activités commerciales de la société, des actifs à protéger, des interactions avec des systèmes à l'externe, et évidemment des moyens financiers de la société.

L'un des contrôles de sécurité les plus importants que toutes les sociétés devraient employer est le cryptage des renseignements confidentiels pour protéger les données tant sur les serveurs que sur chaque ordinateur. Une protection supplémentaire des données est la mise en place d'un « contrôle d'accès » efficace qui consiste à superposer des mesures de sécurité pour les personnes qui détiennent une autorisation d'accès aux renseignements confidentiels. Il faut aussi restreindre l'accès aux renseignements confidentiels uniquement à ce que l'utilisateur a besoin de savoir. Par exemple, un employé subalterne n'a pas besoin d'une autorisation d'accès aux informations les plus sensibles concernant les algorithmes de négociation et aux renseignements détaillés sur les clients, ainsi que le chef de la direction pour les mêmes raisons (qui d'ailleurs est souvent ciblé par les cybercriminels à cause de son poste et de l'autorisation d'accès qui y est associée).

Une facette importante des contrôles de sécurité est la gestion de l'usage de l'ordinateur par les employés de la société. Certes, les cyberattaques sont parfois le fait d'employés mécontents, Sony en est un exemple. Cependant, les cyberattaques ciblent généralement des employés qui ne se doutent de rien et qui deviennent victimes d'une attaque stratégique. Des courriels avec des pièces jointes contenant un programme malveillant capable de s'introduire sur les serveurs de la société sont transmis à des employés qui ne se doutent de rien, parfois au hasard ou parfois délibérément. Ces courriels s'appellent « tentatives d'hameçonnage ». En ouvrant les pièces jointes à un courriel, un programme malveillant peut s'introduire sur les serveurs de la société et ne pas être détecté pendant longtemps, ce qui permet au programme malveillant de connaître et recueillir les informations sensibles de l'entreprise, d'endommager les serveurs de la société, et de transmettre des renseignements confidentiels aux cybercriminels ou au plus offrant. On doit former les employés à être aux aguets pour détecter les courriels suspects et instruire les employés de ne pas les ouvrir s'il y en a dans leur boîte de réception.

Graphique 2 : Pays les mieux préparés contre les cyberattaques



Source : ABI Research, Union internationale des télécommunications, Indice de cybersécurité dans le monde (GCI)**

4. Plan d'intervention en cas d'incident

Malgré toutes les précautions prises par une entreprise, il est presque inévitable qu'elle sera victime à un moment donné d'une cyberattaque. Le programme détaillé des mesures à prendre en cas de la défaillance de la sécurité informatique s'appelle le « Plan d'intervention en cas d'incident (PII) ». Le PII assigne des tâches précises à certains membres du personnel et à des employés spécialement affectés auprès des fournisseurs, et il établit l'ordre chronologique des tâches à exécuter. Si le PII n'est pas suffisamment détaillé, beaucoup de temps sera perdu pour savoir qui fait quoi et à

quel moment. Le temps presse après une cyberattaque.

Le PII doit être mis à l'essai de temps à autre s'assurer de son efficacité et de sa facilité d'utilisation au sein de l'entreprise.

5. Partage d'information
Il est important de pouvoir consulter des sources d'information pour connaître : les techniques sur le renforcement de la protection contre les cyberattaques; et la nature des cybermenaces auxquelles est confronté le secteur des valeurs mobilières – dans le but d'aider les sociétés à concevoir et personnaliser un programme de cyberprotection qui leur convient. La meilleure façon d'obtenir de l'information est de consulter des sites Internet de partage d'information qui généralement se spécialisent par secteur. L'un des sites les plus populaires dans le secteur des valeurs mobilières est le *Financial Services Information Sharing and Analysis Center* (FS-ISAC) qui fournit : i) des renseignements détaillés en temps réel sur des cyberattaques récentes et les mesures adoptées par les entreprises attaquées; ii) des recommandations pour mettre en œuvre un programme efficace de protection contre les cyberattaques, et des pratiques exemplaires et protocoles pour surmonter une cyberattaque; et iii) un accès à une expertise technique à l'interne pour des conseils pratico-pratiques.

6. Cyberassurance
La cyberassurance dédommage la société en cas de cyberattaque. Souscrire ou non une assurance et établir quelle assurance serait appropriée pour la société sont des décisions complexes qui doivent tenir compte des coûts, des défaillances couvertes par l'assurance et du profil de risque de la société.

Le rôle de l'ACCVM:
L'ACCVM a agi de diverses façons pour aider les sociétés membres à faire face aux cybermenaces:

- Cela fait plus d'un an que l'ACCVM a pris des mesures pour sensibiliser davantage au risque des cyberattaques au moyen de divers comités et groupes de travail de l'ACCVM, et par le site Web de l'ACCVM.

- Tout au long de l'année écoulée, l'ACCVM a travaillé avec la *Securities Industry and Financial Markets Association* (SIFMA) des États-Unis sur un programme concernant les cybermenaces, notamment des façons de sensibiliser le secteur et des mesures précises pour aider les sociétés de courtage.

- En juin 2015, l'ACCVM a tenu une conférence sur la cybersécurité qui a attiré un grand nombre de personnes. Des conférenciers chevronnés ont parlé des menaces du piratage informatique et des moyens pour se protéger.

- L'ACCVM a créé un nouveau comité permanent, le Comité de l'ACCVM sur la cybersécurité, qui réunira en table ronde les sociétés de courtage membres pour : discuter d'un cyberprogramme; proposer des mesures applicables à tout le secteur afin d'aider les sociétés membres à mieux se protéger des cyberattaques; et créer des outils utiles comme les pratiques exemplaires d'une bonne protection contre les cyberattaques et des « listes de vérification » pour faire preuve de diligence raisonnable à l'égard des tiers fournisseurs de services informatiques aux sociétés membres. Le comité est aussi une tribune pour permettre au secteur de discuter avec les organismes de réglementation de l'adoption de directives appropriées sur les procédures et programme de cybersécurité.

- Pour aider les membres, le conseil d'administration de l'ACCVM a décidé que l'ACCVM paiera un abonnement d'un an au site de partage d'information FS-ISAC à ses membres de petite et moyenne taille. Les abonnés à FS-ISAC de par le monde reçoivent à temps des informations fiables conçues précisément pour protéger les systèmes et actifs essentiels des attaques physiques et cyberattaques.

- L'ACCVM négocie actuellement avec des fournisseurs de technologie pour qu'ils offrent au secteur des prix réduits sur des services de cybersécurité importants.

Conclusion
Les conséquences des cyberattaques pour les sociétés membres du secteur des valeurs mobilières peuvent être graves sur les plans : des pertes financières encourues par les sociétés et leurs clients; de la divulgation de renseignements confidentiels sur les sociétés et leurs clients; et de l'impact négatif sur la réputation des sociétés. Il est essentiel que les sociétés membres de l'ACCVM mettent au point un programme complet de cybersécurité qui les protège ainsi que les actifs et renseignements des clients. Pour qu'un programme soit efficace, il doit pouvoir compter sur la pleine collaboration de la haute direction et du conseil d'administration et sur un engagement sans réserve de la part de tous les professionnels au service de la société. Chaque société doit élaborer son propre programme de cybersécurité adapté au profil de risque de la société.

L'ACCVM se charge : de fournir le cadre et les ressources nécessaires pour établir une tribune permettant aux sociétés de discuter des problèmes et solutions ayant trait aux cyberattaques; d'élaborer une stratégie applicable au secteur; et de prendre des mesures ciblées, notamment une campagne de sensibilisation à l'intention du secteur, des outils et modèles pour aider les sociétés. De plus, l'ACCVM réunira les organismes de réglementation et les gouvernements pour mettre au point une réglementation et des moyens de défense appropriés pour faire face aux cybermenaces mondiales.

Veuillez agréer mes salutations distinguées.

Ian C. W. Russell, FCSI
Président et chef de la direction de l'ACCVM
Novembre 2015

*** Graphique 1 : Incidents de cybersécurité au Canada**
Source : Résultats clés du sondage 2016 sur l'état de la sécurité de l'information dans le monde (en anglais seulement)® – Comparaison avec les données canadiennes; 28 octobre 2015 : http://goo.gl/VhSX32

*** * Graphique 2 : Pays les mieux préparés contre les cyberattaques**
Source : ABI Research, Union internationale des télécommunications, Indice de cybersécurité dans le monde (GCI) : http://goo.gl/Ghbf84
Remarque : Le CGI vise à présenter l'engagement et l'état de préparation d'un pays en matière de cybersécurité et non le détail de ses capacités ou possibles lacunes.