

Gouvernance et cybersécurité – Le coût de la non-conformité

Me Julie-Martine Loranger

Novembre 2016



Le Défi :

- Remarque du Président Obama
Cybersecurity and Consumer Protection
Summit, Stanford University, February 13,
2015
- « Much of our critical infrastructure – our
financial systems, our power grid, health
systems – run on networks connected to
the Internet, which is hugely empowering
but also dangerous, and creates new
points of vulnerability that we didn't have
before. *Foreign governments and criminals
are probing these systems every single
day.* »



Le Défi :

- **L'attaque cyber :**
 - plus en plus fréquente
 - rapide
 - hautement dommageable
 - hautement médiatisée
 - affecte confiance
 - réputation
 - coûteuse et complexe

Cyber espionnage :

- **AMSC, firme américaine spécialisée dans logiciel pour turbine**
- **Allégation de vol du manufacturier en Chine Sinovel Wind Group Co.**
- **Ingénieur de AMSC, appropriation du code du Wisconsin, décrypté en Australie et courriel en Chine**
- **Investigation, FBI – copies contrefaites vendues aux USA**
- **Devant les tribunaux, tactiques dilatoires**
- **370 \$ à 5 \$**



Target : les chiffres

- **Courriel** : ouvert par un tiers - fournisseur de services :
 - employé d'une firme de réfrigération/ventilation engagé par Target (hameçonnage)
- **40 millions** : cartes de crédit à risque
- **70 millions** : clients dont les informations personnelles ont été mises à risque
- **700 000** : clients canadiens touchés



Target : les chiffres

- **Plus de 100** : poursuites judiciaires (USA)
 - consommateurs (recours collectifs)
 - actionnaires (actions dérivées)
 - banques (recours collectifs)
 - plusieurs recours collectifs au Canada, dont un au Québec
- **148 millions \$** : estimation - pertes probables et réclamations pour pertes potentielles et actuelles causées par vol de données
- **38 millions \$** : compensation par les assureurs

Industries – incidents entraînent recours collectifs

- **Services financiers** : JP Morgan – 2014 – 76 000 000 de clients touchés
- **Assurance** : Anthem inc. – 2015 – 80 000 000 de clients et d'employés touchés
- **Commerce de détail** : Target – 2013 – 70 000 000 de clients touchés
- **Technologie** : Adobe – 2014 – 36 000 000 de clients touchés
- **Web** : eBay – 2014 – 145 000 000 de clients touchés

Deloitte 2015 Cybersecurity Survey: Navigating a harsh cybersecurity landscape

Table 1: Share price declines of certain US and UK listed companies following cyber attacks

Company Name	Date of announcement of cyber security breach	Drop in share price following breach (%)	
		Three days	One month
Ebay	21 May 2014	1.48%	7.35%
AOL	28 April 2014	1.70%	23.56%
Target	19 December 2013	2.41%	5.79%
Adobe	3 October 2013	2.91%	4.04%
KT Corporation	29 July 2013	1.30%	5.82%
Ubisoft	2 July 2013	2.48%	2.48%
Betfair Group	30 September 2011	13.67%	13.67%
Heartland Payment Systems	20 January 2009	46.3%	49.54%
TK / TJ Maxx	17 January 2007	1.82%	6.49%

Cibles de choix

- Commerces de détail traditionnels et e-commerce
- Fournisseurs de services sur le web
- Institutions financières
- Courtiers en valeurs mobilières
- Compagnies d'assurance
- Entités gouvernementales
- Universités

Cibles de choix

- Nombre important de transactions par carte de débit et de crédit chaque jour
- Stratégies de fidélisation des clients (cartes-clients)
- Collection et rétention de renseignements personnels et financiers des clients et employés
- Plusieurs points d'entrée dans les systèmes informatiques et systèmes de points de vente
- Plusieurs intermédiaires ont accès aux différents systèmes informatiques (fournisseurs de services, employés)
- Renseignements personnels et financiers facilement vendus sur le web

Matérialisation d'un cyberrisque

Perturbation et cessation de certaines opérations

- Mise « hors ligne » de certains services aux clients
- Mise hors service de systèmes informatiques internes et externes
- Suspension des opérations qui relèvent des systèmes informatiques compromis

Impact sur la réputation de l'entreprise – impact sur la marque (« brand »)

- Impact sur la confiance des clients

Matérialisation d'un cyberrisque

- Monopolisation de ressources importantes à l'interne et à l'externe pour gérer la situation
- Poursuites judiciaires
 - recours collectifs – consommateurs, clients, employés
 - actions dérivées, recours des actionnaires
 - responsabilité des administrateurs
 - litige avec des partenaires d'affaires (banques, fournisseurs de services)
- Enquêtes réglementaires
- Coûts importants

Mythes

- La **cybersécurité** relève **uniquement** du service des technologies de l'information (« **TI** »)
- Les **administrateurs et la direction (management)** doivent être des experts en la matière
- L'**entreprise** a l'obligation de mettre en place des politiques et contrôles internes afin de prévenir **tous les cyberrisques**

Gestion des cyberrisques

- La gestion des cyber risques requiert la collaboration de plusieurs acteurs:
 - conseil d'administration et comité de gestion des risques
 - direction (management)
 - TI (spécialistes internes et externes)
 - conseillers juridiques internes et externes
 - employés
 - fournisseurs de services
 - experts
- **Gestion intégrée des risques**



Cadre législatif

- Régime général de la responsabilité civile 1457-1458 CCQ
 - Standards de pratique dans le domaine
 - Obligation de moyens
 - Faute, dommage et lien de causalité



Cadre législatif

- Certaines **obligations** existent :
 - lois relatives à la protection de la vie privée
 - Canada : *Loi sur la protection des renseignements personnels*, L.R.C. 1985, c. P-21 (divulgation volontaire)*
 - Renseignements personnels numériques (notification mandatoire – avis – tenue de registre)
 - Loi sur la protection des Canadiens contre le cybercriminalité
- Initiatives des autorités réglementaires (ACVM, OCRCVM, OSFI, AMF)
- Aux USA, le SEC/FINRA a émis des lignes directrices et surveille étroitement les émetteurs assujettis quant aux obligations d'information

* Loi fédérale qui s'applique aux organisations qui collectent, utilisent et divulguent des renseignements personnels dans le cadre de leurs activités commerciales à moins d'application de la législation provinciale.

Avis 11-326 du personnel des ACVM

Cybersécurité

17

- Évaluer / identifier les risques liés à la cybercriminalité
- Adopter des mesures de protection et de sécurité
- Sensibiliser et éduquer le personnel
- Suivre les meilleures pratiques des associations professionnelles et des organismes reconnus en sécurité informatique

Avis 11-326 du personnel des ACVM

Cybersécurité

- Les émetteurs doivent considérer ces risques, les incidents, les contrôles et doivent les communiquer au prospectus ou autre document d'information continue
- Les personnes inscrites : gérer les risques conformément aux critères de pratique dans le domaine (prudence)
- Procéder régulièrement à des tests et évaluations
- Revoir régulièrement les mesures de contrôle des risques et plan d'intervention

Avis 11-332 du personnel des ACVM

Cybersécurité

Le 27 septembre 2016

Certaines études portant sur l'incidence des atteintes à la cybersécurité, comme celles publiées par le Ponemon Institute¹ et PricewaterhouseCoopers², formulent les conclusions suivantes :

- en 2015, le nombre d'incidents détectés a augmenté de 38 % par rapport à 2014;
- le coût total moyen d'une atteinte à la protection des données s'établissait à 4 millions de dollars américains chez les sociétés ayant participé au sondage 2016 de Ponemon.

¹ *2016 Cost of data breach Study: Global Analysis*. Cette analyse comparative parrainée par IBM et menée de façon indépendante par le Ponemon Institute LLC porte sur 383 sociétés réparties dans 12 pays.

² *The Global State of Information Security Survey 2016* est une étude effectuée annuellement à l'échelle mondiale par PwC, CIO et CSO qui analyse les réponses de plus de 10 000 chefs de la direction, chefs des finances, chefs de l'information, chefs de la sécurité des systèmes d'information, chefs de la sécurité, vice-présidents et directeurs des technologies de l'information ainsi que les pratiques en matière de sécurité de 127 pays.

Avis 11-3332 ACVM

La gestion implique l'organisation des ressources, des politiques, du personnel, des pratiques et des technologies

- CA et comité du risque
- Direction
- IT spécialistes internes et externes
- employés
- fournisseurs
- experts

- « Despite ever-improving network defenses, the diverse possibilities available through remote hacking intrusion, supply chain operations to insert compromised hardware or software, actions by malicious insiders, and mistakes by system users will hold nearly all [information and communication technology] networks and systems at risk for years to come. **In short, the cyber threat cannot be eliminated; rather, cyber risk must be managed.** »
- James R. Clapper, US Director of National Intelligence Testimony to House Intelligence Committee, September 10, 2015

« Whatever sector you're in online security needs to form part of your business model. A habit as automatic as locking your front door. »

Former EU Commissioner Neelie Kroes

Conseil d'administration

- Rôle de surveillance (“oversight”) des risques, y compris des cyberrisques
- Ce rôle doit être actif – il doit y avoir un dialogue avec la haute direction
- Le CA doit être suffisamment informé pour apprécier les cyberrisques importants, le caractère suffisant et adéquat des procédures en place et du plan de réponse
- Les procès-verbaux des CA doivent attester de ce rôle (décision Wyndham)

- **Maintien du dialogue avec le CA**
- **Identification et évaluation** adéquate des cyberrisques
- Élaboration et mise en œuvre de **politiques et procédures de contrôle interne**
- **Surveillance** continue de ces risques
- **Délégation** de certaines responsabilités (équipe d'intervention)

Prévention et gestion des risques

- **Identification et évaluation des risques**
- Ressources internes vs expert externe
- Énumération, identification et ciblage des risques
 - énumérer et identifier les renseignements personnels et informations confidentielles à risque (clients et employés)
 - évaluer les politiques, procédures et contrôles actuels

Prévention et gestion des risques

→ **Élaboration de politiques et procédures**

- rédiger des politiques et procédures claires, concises
- dissémination dans l'entreprise
- formation des employés
- culture de vigilance
- mise à jour régulière des politiques et procédures

Réponse à un incident

- Mise en œuvre du plan de réponse
- Intervention de l'équipe identifiée dans le plan (juridique, conformité, TI, communications)
- Cohérence des communications – internes et externes
- Protection du privilège
- Effectuer les enquêtes internes requises afin d'identifier les origines de l'incident
- Circonscrire/atténuer l'impact de la brèche

Réponse à un incident

- Réviser les contrats pertinents concernant vos sous-traitants et fournisseurs de services, le cas échéant
- Réviser vos polices d'assurance et effectuer les avis nécessaires
- Besoin d'une firme de relations publiques?

Réponse à un incident

- Évaluer vos obligations de notification d'incidents
 - Lignes directrices sur les atteintes à la vie privée » (<http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26154§ion=HTML>)
- La notification des incidents au commissaire est **recommandée**, même lorsqu'elle n'est pas requise

Contacts

Julie-Martine Loranger

associée

514 397-4221

jmloranger@mccarthy.ca