AUTORITÉ DES MARCHÉS FINANCIERS

L'ENGRENAGE CYBERRISQUE, GOUVERNANCE ET CONTINUITÉ DES AFFAIRES

Serge Drolet, CISA CBCP PMP

26 avril 2018

AUTORITÉ DES MARCHÉS FINANCIERS

OBJECTIFS ET PLAN DE PRÉSENTATION

Objectifs :

- Partager une expérience concrète
- Améliorer la capacité à faire face au cyberrisque
- Impliquer la direction et les unités d'affaires

Plan

1. Contexte et tendances
2. Gouvernance et cyberrisque
3. Cybersécurité et continuité des affaires
4. Exercice de simulation d'une cyberattaque

AUTORITÉ DES MARCHÉS FINANCIERS

1. CONTEXTE DE L'AMF

Organisme gouvernemental
qui encadre le secteur financier québécois

Mission

- Protéger les consommateurs
- Favoriser le bon fonctionnement des marchés
  - Entrée en carrière (examens/permis), certificats et inscriptions
  - Encadrement et surveillance (inspections, enquêtes et poursuites)
  - Soutien aux consommateurs

Source : Rapport annuel AMF 2016-2017

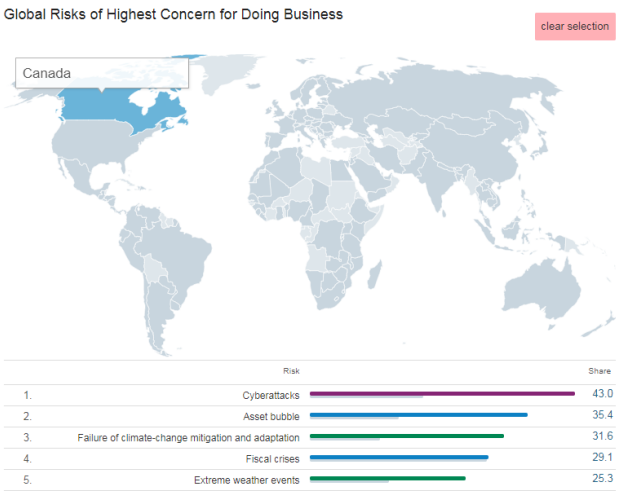
TENDANCES MONDIALES

Top 5 Global Risks in Terms of Likelihood

	2014	2015	2016	2017	2018
1st	Income disparity	Interstate conflict with regional consequences	Large-scale involuntary migration	Extreme weather events	Extreme weather events
2nd	Extreme weather events	Extreme weather events	Extreme weather events	Large-scale involuntary migration	Natural disasters
3rd	Unemployment and underemployment	Failure of national governance	Failure of climate-change mitigation and adaptation	Major natural disasters	Cyberattacks
4th	Climate change	State collapse or crisis	Interstate conflict with regional consequences	Large-scale terrorist attacks	Data fraud or theft
5th	Cyber attacks	High structural unemployment or underemployment	Major natural catastrophes	Massive incident of data fraud/theft	Failure of climate-change mitigation and adaptation

World Economic Forum : The Global Risks Report 2018, 13th edition
https://www.weforum.org/reports/the-global-risks-report-2018

TENDANCES CANADIENNES



World Economic Forum : The Global Risks Report 2018, 13th edition
https://www.weforum.org/reports/the-global-risks-report-2018

TOP RISQUES 2018

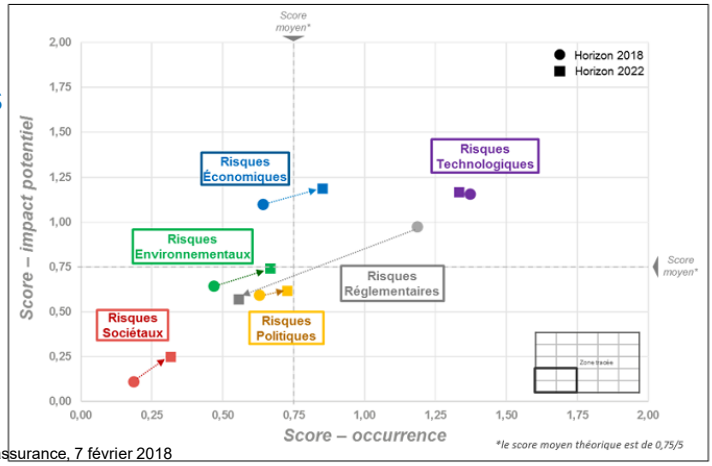
1. Cyber-risque
2. Effondrement financier
3. Changement climatique
4. Politique internationale
5. Avalanche réglementaire

TOP RISQUES 2022

1. Cyber-risque
2. Changement climatique
3. Disruption du secteur
4. Nouvelles technologies
5. Politique internationale

TENDANCES SECTORIELLES

« *Baromètre des risques émergents pour l'assurance* »*



* Fédération française de l'assurance, 7 février 2018
https://www.ffa-assurance.fr/content/premier-barometre-des-risques-emergents-pour-assurance

À RETENIR

- Le cyberrisque est un risque important
- Il est vraisemblablement là pour rester !
- Il devrait donc être sur votre tableau de bord de gestion des risques

Comment prendre en charge le cyberrisque ?

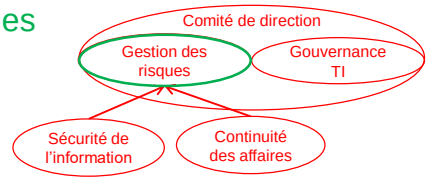
AUTORITÉ DES MARCHÉS FINANCIERS

7

2. GOUVERNANCE ET CYBERRISQUE

Exemples des domaines impliqués

- Gestion intégrée des risques
- Gouvernance des TI
- Continuité des affaires
- Sécurité de l'information



Chaque domaine a son focus, sa politique, son comité, ses priorités et ses intérêts

Comment vulgariser un risque de nature technique et opérationnel aux dirigeants ?

AUTORITÉ DES MARCHÉS FINANCIERS

8

LE CYBERRISQUE … CONCRÈTEMENT

Cyberrisque émergent = Cyberattaque

Fiche pour chaque risque

Exemples d'approche de sensibilisation

- Scénario optimiste
- Scénario réaliste
- Scénario pessimiste

AUTORITÉ DES MARCHÉS FINANCIERS

9

SCÉNARIO OPTIMISTE

Attaque limitée à un utilisateur ou un poste de travail

- Logiciel malveillant provenant d'un courriel ou de la navigation Web qui n'aurait pas été bloqué par les premiers niveaux de défense technologiques
- Les systèmes de surveillance et détection capteraient vraisemblablement l'attaque
- Le Centre de sécurité opérationnelle (CSO) déclenche la réponse aux incidents, isole et élimine la menace

AUTORITÉ DES MARCHÉS FINANCIERS

10

SCÉNARIO RÉALISTE

Attaque visant à perturber l'accessibilité à certains services

- Déni de service sur un service en ligne ou un site Web
- Nécessite des moyens limités et est à la portée d'un grand nombre d'attaquants potentiels
- Vise l'image de l'organisation ou d'un de ses partenaires et ne permet pas l'obtention d'informations confidentielles
- Repose sur une limitation technique, est relativement facile à détecter et à mitiger dans le temps

AUTORITÉ DES MARCHÉS FINANCIERS

11

SCÉNARIO PESSIMISTE

Attaque ciblée sophistiquée

… les fameuses *APT* *(menaces persistantes avancées)*

- Très difficile à détecter et se déroule généralement sur plusieurs semaines/mois
- L'attaquant cherche à exfiltrer/exploiter les données furtivement ou perturber les activités de sa cible
- Recherche un avantage monétaire/personnel/idéologique
- Nécessite des connaissances et capacités sophistiquées afin de contourner plusieurs niveaux de sécurité

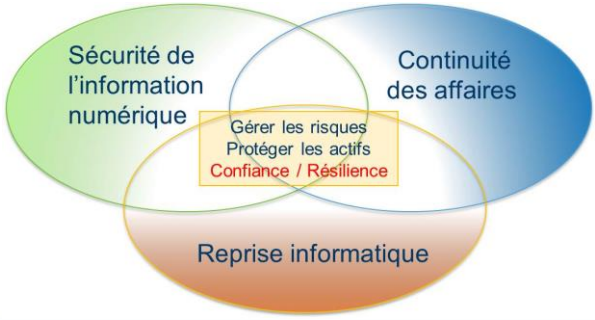
Comment se préparer à une cyberattaque ?

AUTORITÉ DES MARCHÉS FINANCIERS

12

3. CYBERSÉCURITÉ ET CONTINUITÉ DES AFFAIRES

- Journée de réflexion « cyber » en octobre 2015
- Vision Cybersécurité 2020
- Appui de la gouvernance TI lors d'une réorganisation
- Mise en place d'une équipe « cyber » en avril 2016



AUTORITÉ DES MARCHÉS FINANCIERS

PRATIQUES DU MARCHÉ

- Référentiels et outils utilisés:
  - ITIL : pour se positionner par rapport aux services TI
  - COBIT : pour se positionner par rapport à la gouvernance
  - NIST : pour structurer nos pratiques de cybersécurité/continuité
  - ISO : pour la sécurité de l'information / continuité / risques

… concrètement, principales sources utilisées pour la mise en œuvre :

  - NIST *Cybersecurity Framework / Contingency planning*
  - CSX (ISACA) et cours du SANS (*Managing Security Operations*)
  - DRI pour les pratiques de continuité

AUTORITÉ DES MARCHÉS FINANCIERS

CYBERSÉCURITÉ 2020
« COMMENT »

Alignée sur les pratiques reconnues (NIST) :

1. Identification : analyse de risques / reddition de compte
2. Protection : outils / tests d'intrusion / sensibilisation
3. Détection : surveillance / gestion des vulnérabilités
4. Réponse : gestion des incidents

CSO

5. Reprise : protection des données / plans de continuité des affaires et de reprise informatique

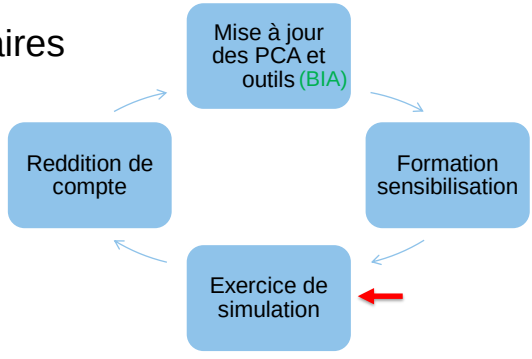
Mise en place d'un Centre de sécurité opérationnelle (CSO)

(Référence : présentation au CQSI du 13 avril 2018)

Comment s'assurer de l'efficacité des processus et plans lors d'un incident majeur ?

4. EXERCICE DE SIMULATION

Continuité des affaires



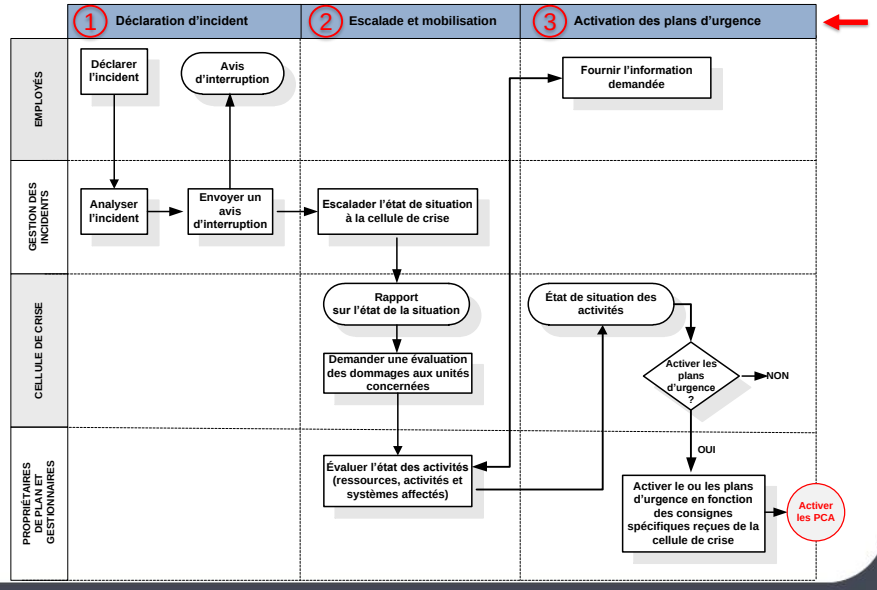
– Analyse de risques et bilan d'impacts d'affaires (BIA)

➢ Cyberattaque est le risque le plus redouté

EXERCICE DE SIMULATION

- Scénario : cyberattaque majeure
- Objectifs
  - S'approprier, mettre à l'épreuve et améliorer les procédures et outils d'urgence
- Intervenants : 10 gestionnaires
- Durée : 1h30
- Simulation en 3 étapes

ARRIMAGE DES PROCESSUS DE GESTION D'INCIDENT ET DE CRISE



DÉROULEMENT DE LA SIMULATION

Étape 1 : Gestion d'incident TI - Cyberattaque
- Mise en contexte (2 min)
- Réaction de la gestion d'incident TI (15 min)
- Mise en commun : rapport à la cellule de crise (3 min)

Étape 2 : Escalade et mobilisation - Cellule de crise
- Mise en contexte (2 min.)
- Réaction de la cellule de crise (15 min.)
- Mise en commun : décision des mesures à prendre (3 min.)

Étape 3 : Activation des plans d'urgence
- Mise en contexte (2 min.)
- Réaction des unités d'affaires (15 min.)
- Mise en commun (3 min.)

IMPORTANCE DE LA SIMULATION

- Impliquer / sensibiliser
  - Dirigeants (cellule de crise)
  - Responsables d'unités d'affaires
  - Responsables de la gestion d'incident
- Comprendre le déroulement d'une cyberattaque
- Améliorer les plans et processus d'urgence

Exercice de communication et de collaboration !

5. CONCLUSION

Partage d'expérience : une approche parmi d'autres, qui capitalise sur les mécanismes en place

- Gouvernance :
  - Gestion intégrée des risques (pourquoi)
    - Hauts dirigeants : suivi des risques, dont le cyberrisque
    - Scénarios optimiste / réaliste / pessimiste
  - Gouvernance des TI (comment)
    - Hauts dirigeants : encadrement/priorisation des investissements
    - Réorganisation des TI : équipe cybersécurité et continuité

AUTORITÉ DES MARCHÉS FINANCIERS

21

5. CONCLUSION (SUITE)

- Lien entre gouvernance et opération :
  - Sécurité de l'information (coordination)
    - Coordination entre domaines touchant la sécurité
    - Directives et formation / sensibilisation des employés
  - Continuité des affaires (s'exercer)
    - Hauts dirigeants et unités d'affaires
    - Exercice de simulation : cyberattaque majeure
- Opérationnel :
  - Équipe cybersécurité et continuité des affaires
  - Regroupement des capacités dans un CSO

AUTORITÉ DES MARCHÉS FINANCIERS

22

RÉFÉRENCES UTILES

Lignes directrices de l'AMF

- Gestion intégrée des risques
- Continuité des activités

Gouvernance des TI :

- Cadre normatif en ressources informationnelles (Gouv. Qc)
- Politiques publiées sur les sites Web de ministères et organismes gouvernementaux (Revenu Québec, Loto Québec, etc.)

Outils et référentiels

- ISACA : COBIT et CSX
- NIST : Cybersecurity framework et Contingency planning
- DRI pour la mise en œuvre de la continuité

AUTORITÉ DES MARCHÉS FINANCIERS

Questions?

MERCI!

Serge Drolet (LinkedIn)