LANGLOIS

AVOCATS - LAWYERS

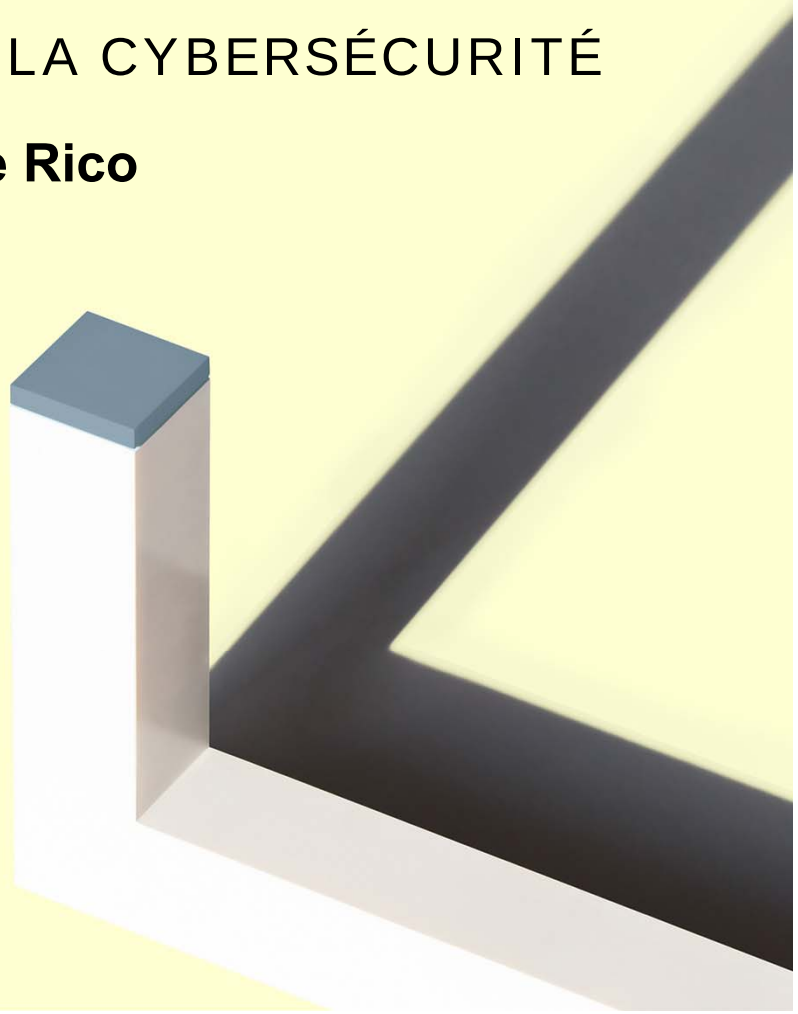
ENCADREMENT JURIDIQUE DE LA CYBERSÉCURITÉ

Jean-François De Rico

CSX™

CYBERSECURITY NEXUS

Journée CSX sur la cybersécurité
31 Mai 2016



PLAN

Les menaces et l'état de préparation

Les actifs et les risques organisationnel

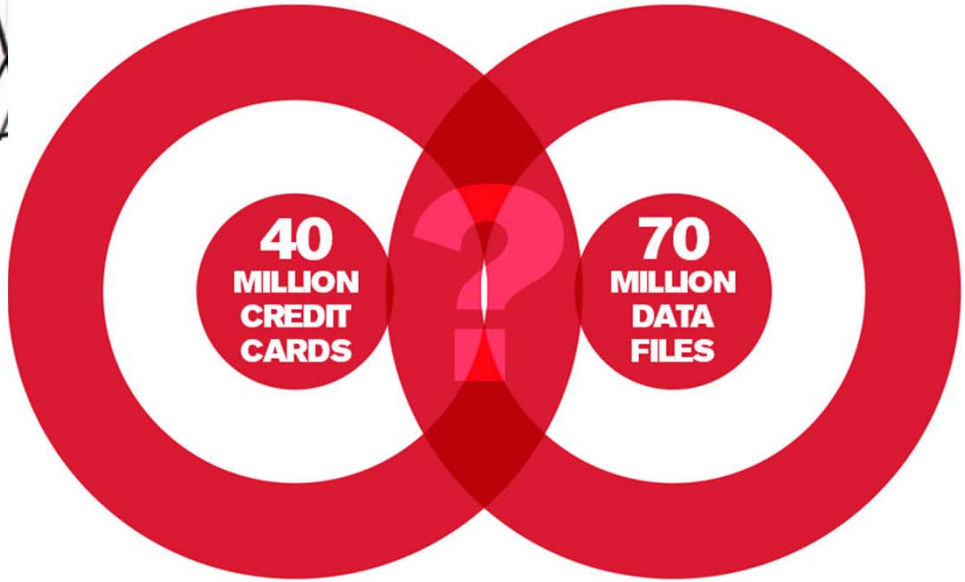
Les obligations

- Les sources
- Les catégories
- Les cas applications

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

HOME DEPOT HACKED

56 MILLION CUSTOMER CREDIT & DEBIT CARD DATA EXPOSED



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

This PSA is a joint product by the Federal Bureau of Investigation, the Department of Transportation and the National Highway Traffic Safety Administration.

March 17, 2016

Alert Number

MOTOR VEHICLES INCREASINGLY VULNERABLE TO REMOTE EXPLOITS

Cost of data breach at TJX soars to $256m

Suits, computer fix add to expenses

The Boston Globe

By Ross Kerber, Globe Staff | August 15, 2007

TJX Cos. said its costs from the largest computer data breach in corporate history, in which thieves stole more than 45 million customer credit and debit card numbers, have ballooned to $256 million.

PRC

Privacy Rights Clearinghouse

Empowering Consumers. Protecting Privacy.

télécommunications Xittel

Survivre aux DDoS

«UNE HISTOIRE VRAIE»

TÉLÉCOMMUNICATIONS XITTEL INC.

et

9116-6033 QUÉBEC INC., société légalement constituée faisant affaires sous le nom de **LES SYSTÈMES INFORMATIQUES CONCEPTA**

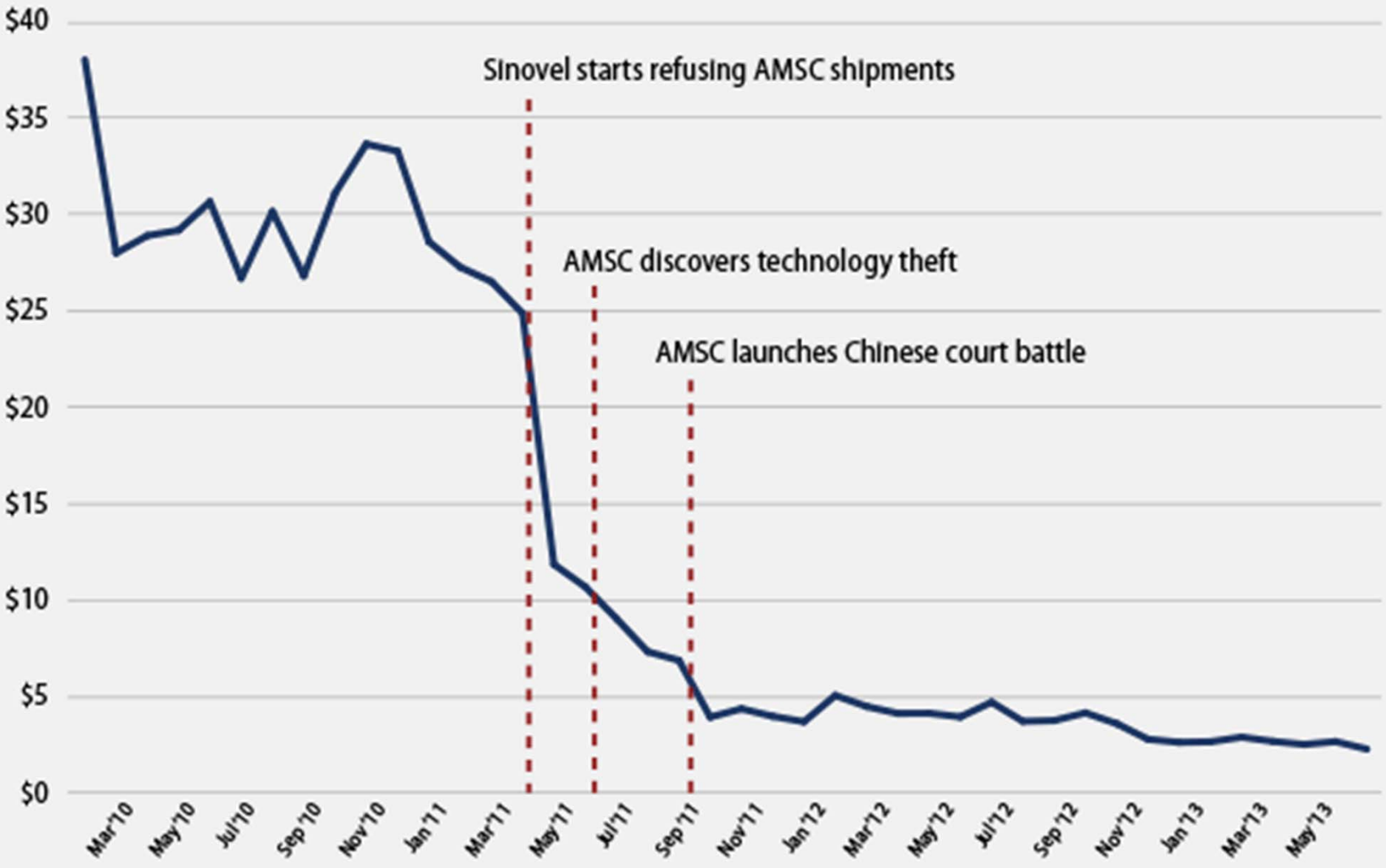
Demanderesses

c.

KEVIN COURTOIS

FIGURE 1

AMSC stock plunges after Sinovel theft



Source: Yahoo! Finance, "AMSC Historical Prices," available at http://finance.yahoo.com/q/hp?s=AMSC&a=00&b=1&c=2010&d=05&e=23&f=2013&g=m.

L'état de préparation en matière de cybersécurité des organisations canadiennes

RÉSULTATS DE L'ÉTUDE SUR LA SÉCURITÉ DE SCALAR 2016

ÉTAT DE LA SITUATION

RÉSULTATS DE L'ÉTUDE SUR LA SÉCURITÉ DE SCALAR 2016

654 professionnels de l'informatique et de la sécurité informatique situés au Canada

2/3 = organisations de 251 à 5000 employés au Canada

Secteurs activités diversifiés

Services financiers /Secteur public /Vente au détail /Services / Technologie et informatique / Services professionnels /Énergie et fournisseurs

scalar | Ponemon INSTITUTE

Moyenne de 40 cyber attaques	Hausse de 17 %
51 % ont connu un incident impliquant la perte ou la mise en danger d'informations sensibles	Hausse de 5 %
25 % des employés ont été la cible de tentatives d’hameçonnage	
70 % indiquent que des malwares ont échappé à leurs systèmes de détection d'intrusion	
moyenne d'un près d’un incident APT par mois	
38 % seulement des organisations ont en place des systèmes et des contrôles pour faire face aux menaces persistantes avancées (APT),	
moyenne de 5 attaques par déni de service (DoS),	
44 % ont subi une attaque de type DoS ayant provoqué une interruption d’affaires	coût des interruptions d'activité et des arrêts du système a atteint en moyenne 1,2 million de dollars.

MENACES

pays /nations – crime organisé – hacktivistes – insiders

ACTIFS INFORMATIONNELS

- renseignements personnels
- propriété intellectuelle
- Commerciales (clients-fournisseurs-partenaires – stratégie)
- données opérationnelles

VULNÉRABILITÉS

- personnes
- processus
- technologies

OBLIGATIONS

PRÉSERVER

- Confidentialité
- Intégrité
- Accessibilité/disponibilité

RISQUES

Perte/vol

Altération/ destruction

copie

accès

Divulgation

poursuites

Diffusion

Interruption des affaires

Perte de marché

Sanctions

Responsables – personnes impliqués

C.A. – Dirigeants – IT – Legal – RH – Fournisseurs

Le grand dictionnaire terminologique (GDT)

RISQUE INFORMATIQUE:

- Probabilité plus ou moins grande de voir une menace informatique se transformer en événement réel entraînant une perte.

MESURE DU RISQUE :

- probabilité d'occurrence d'une menace
- montant/importance de la perte consécutive à sa réalisation

Droit commun

Application générale

Protection des renseignements personnels

Responsabilité civile

Règlements et normes sectorielles

Criminel

Communication

Contrat

Loi concernant le cadre juridique des technologies de l'information

Loi sur la protection des renseignements personnels dans le secteur privé

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

Loi sur la protection des renseignements personnels et sur les documents électroniques (PIPEDA)

Loi anti-pourriel

Loi sur le droit d'auteur

Code criminel

Code civil du Québec

Code de procédure civile

Lois sur les Sociétés

Recours extraordinaires

Jurisprudence

Lois et règlements d'application spécifiques….

Lignes directrices - Normes

Contrats

LCCJTI // C-I-A

19. **Toute personne doit, pendant la période où elle est tenue de conserver un document, assurer le maintien de son intégrité et voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible et** de **l'utiliser aux fins auxquelles il est destiné.**

Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1

LCCJTI - Confidentialité

- 25. La personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les **mesures de sécurité propres à en assurer la confidentialité**, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.

Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1

LCCJTI – C-I-A

26. Quiconque confie un **document technologique** à un **prestataire de services** pour qu'il en assure la garde est, au préalable, tenu **d'informer** le prestataire quant à la protection que requiert le document en ce qui a trait à **la confidentialité** de l'information et quant aux **personnes qui sont habilitées** à en prendre connaissance.

Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que **les moyens technologiques** convenus soient mis en place pour en **assurer la sécurité, en préserver l'intégrité** **et, le cas** échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Il doit de même assurer le respect de toute autre obligation prévue par la loi relativement à la conservation du document.

Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1

LCCJTI - Confidentialité

- 34. Lorsque la loi déclare confidentiels des renseignements que comporte un document, leur **confidentialité doit être protégée par un moyen approprié au mode de transmission**, y compris sur des réseaux de communication.
- La documentation expliquant le mode de transmission convenu, incluant les moyens pris pour assurer la confidentialité du document transmis, doit être disponible pour production en preuve, le cas échéant

Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1

LPRPSP

- **10.** Toute personne qui exploite une entreprise doit **prendre les mesures de sécurité propres à assurer la protection des renseignements personnels** collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

LADOPPRP

- **63.1.** Un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels (…) et **qui sont raisonnables** compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

LADOPPRP

- **68.** Un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel:

  (…) à une personne ou à un organisme si (…) nécessaire dans le cadre de la prestation d'un service (…).

- Cette communication s'effectue dans le cadre d'une **entente écrite** qui indique:

  5° les **mesures de sécurité** propres à assurer la protection du renseignement personnel;

LADOPPRP

- **76.** Un organisme public **doit établir et maintenir à jour** un inventaire de ses fichiers de renseignements personnels.
- Cet inventaire doit contenir les indications suivantes:
- 1° la désignation de chaque fichier, les catégories de renseignements qu'il contient, les fins pour lesquelles les renseignements sont conservés et le mode de gestion de chaque fichier;

  4° les **catégories de personnes qui ont accès** à chaque fichier dans l'exercice de leurs fonctions;
- 5° les **mesures de sécurité** prises pour assurer la protection des renseignements personnels.
-

Rapport d'enquête sur la sécurité, la collecte et la conservation des renseignements personnels

TJX Companies Inc./Winners Merchant International L.P.

Le 25 septembre 2007

Intensité des obligations

L'organisation avait-elle un motif raisonnable pour conserver les renseignements personnels touchés par la brèche?

L'organisation conservait-elle les renseignements conformément à la *LPRPDÉ* et à la *PIPA*?

L'organisation avait-elle mis en place des mesures de sécurité raisonnables afin de protéger les renseignements personnels qu'elle conservait?

EXAMEN:

-Étendue et conformité de la conservation

-Mesures de protection de sécurité sans fil en place au moment de la brèche

-Mesures adoptées après l'incident

Cost of data breach at TJX soars to $256m

Suits, computer fix add to expenses

The Boston Globe

By Ross Kerber, Globe Staff | August 15, 2007

TJX Cos. said its costs from the largest computer data breach in corporate history, in which thieves stole more than 45 million customer credit and debit card numbers, have ballooned to $256 million.

Chrysler Finance (DaimlerChrysler / Services de financement auto TD inc.) - Perte d'Informations personnelles - Recours collectif national

Recours collectif

Belley c. TD Auto Finance Services Inc., 2015 QCCS 168

All persons, in all of Canada, whose personal information was stored or saved on a Data Tape, which was lost by Respondent while in transit on or about March 12, 2008, or any other group to be determined by the Court

Belley alleges that he was a **victim of an identity theft** and that a fraudster purchased four vehicles “immediately following the loss of his personal information”, *i.e*. between April 10 and May 13, 2008.

Fautes reprochées

negligent in allowing PI relating to its customers to be stored in the USA when it conducted its business in Canada and **knew that it would be making monthly credit reports to a credit agency** located in Rouyn Noranda, Province of Quebec;

negligent in sending the PI on a "physical" Data Tape, in a sealed envelope, through a regular delivery service by UPS the whole **without even keeping a back-up of the information**, so that the precise nature of the material lost cannot be ascertained;

chose not to encrypt of otherwise "password protect" the personal information contained on the Data Tape, making it available to any person who may gain access to it,

did not inform UPS of the content of the Data Tape, namely "sensitive personal information on approximately 240,000 of its customers" and declared a value of US $5 thereby attributing no value whatsoever (and no concern for) the sensitive PI

after the loss of the Data Tape, DaimlerChrysler was negligent in **failing to offer credit monitoring services to its customers** or to alert credit bureaus such as Equifax and TransUnion of the loss in order to have the appropriate "red flags" marked on the customers' credit files;

DaimlerChrysler was **negligent in delaying the notification to its customers** of the loss, which occurred on or about March 12, 2008;

Conclusion (sur autorisation)

In summary, the Petitioner contracted with the Respondent, entrusted it with her information and **the Respondent did not**, *prima facie*, **meet its obligations to store, keep and transfer the information safely**.

The facts alleged in the Motion provide an arguable case that TD Auto's negligence in the handling of the delivery, the loss and the consequences of the loss of the Data Tape might constitute an illicit and intentional violation of a right, the right to respect for one's private life, protected by the *Charter of Human Rights and Freedoms*

Condon c. Canada, 2014 CF 250 – Recours collectif

Requête en vue de faire autoriser une action comme recours collectif contre Sa Majesté la Reine (la défenderesse) / ministre responsable de l'administration et de la gestion du Programme canadien de prêts aux étudiants (le Programme)

En novembre 2012, le ministre a **perdu un disque dur externe** sur lequel étaient conservés les renseignements personnels des demandeurs et d'environ 583 000 personnes (le disque dur), dans ses bureaux de Gatineau (Québec) (la perte de données).

Ces renseignements personnels comportaient les noms, dates de naissance, adresses, soldes des prêts d'études, et numéros d'assurance sociale (le ou les NAS) de ces personnes (les renseignements personnels). Le disque dur n'a pas été retrouvé.

THE ALDO GROUP INC.
Plaintiff

v.

CHUBB INSURANCE COMPANY OF CANADA
Defendant

- [18] This claim was asserted against Aldo by Moneris/MasterCard. Moneris/MasterCard allege that Aldo's failure to comply with PCIDSS and with its duty to reasonably safeguard customer-entrusted account data resulted in this ADC Event.
- [19] On March 31, 2011[16], MasterCard claimed that BMO, the bank involved in processing Aldo's Payment Card transactions, was responsible for its merchant (Aldo)'s non-compliance with PCIDSS. MasterCard informed BMO and Moneris accordingly (**Mastercard/Moneris Claim**).
- [20] MasterCard threatened to impose an Assessment on Aldo for this breach of the PCIDSS. Based on the applicable Security Rules and Procedures (**Manual**), MasterCard assessed Aldo's overall financial liabilities at $US 4,884,128.13 in connection with this ADC Event. MasterCard indicated that Aldo's account could be debited by this amount.
- [21] Moneris forwarded this Mastercard letter to Aldo on April 1, 2011[17].
- [22] On April 4, 2011[18], Moneris wrote to Aldo. To avoid a USD$ 4.9 million assessment against Aldo's bank account, Moneris insisted that Aldo submit the relevant form[19] and evidence[20] confirming its full compliance with PCIDSS.
- [23] On April 18, 2011, MasterCard and Moneris debited Aldo's BMO accounts for USD$ 4.9 million (**Assessment**), allegedly pursuant to the terms of the Agreement.

4.7 Septième principe — Mesures de sécurité

MÉTHODE DE PROTECTION

physique

processus

technologique

sensibilisation / formation

LCCJTI - art 25

contrôle d'accès effectué au moyen

---procédé de visibilité réduite ou

---procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.

PIPEDA annexe 1 , 4.7.3

a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux;

b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif; et

c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.

Learning from Wyndham's Data Breach

However, the FTC pointed the finger at Wyndham's negligence in relation to security policies at the company's Phoenix data center—where the company stores and transfers data between its headquarters and its individual business units. As a result, Russian hackers managed to infiltrate its system and install phishing software on a myriad of Wyndham servers, gaining access to more than 500,000 customer accounts on three separate occasions between 2008 and 2010. Hackers then rang up more than $10.6 million in fraudulent credit card transactions, according to the suit filed in the U.S. District Court of Arizona.

But more troubling was that even after the company learned of the breach, it failed to take action to prevent it from happening again, according to the FTC's complaint, and as a result, the hackers were able to gain access on, not one, but two additional occasions. If Wyndham had added more complex user IDs and passwords, and made changes to software that was storing customer credit card data as unencrypted text, the company may have nipped the damage in the bud.

Obligation de notification

Lois du Canada
2015, c. 32

Projet de loi émanant du gouvernement (Sénat)

41e législature, 2e session
16 octobre 2013 - 2 août 2015

Parcourir les projets de loi

S-4 Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques et une autre loi en conséquence

Titre abrégé
Loi sur la protection des renseignements personnels numériques

Atteinte aux mesures de sécurité

Communication non autorisée ou perte de renseignements personnels, ou accès non autorisé à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation prévues à l'article 4.7 de l'annexe 1 ou du fait que ces mesures n'ont pas été mises en place.

ATTEINTES AUX MESURES DE SÉCURITÉ (art. 10.1 LPRPDE)

L'organisation doit **déclarer une atteinte** au commissaire et aviser l'intéressé « ***s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu*** ».

Préjudice grave vise notamment **la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles**.

L'**avis doit contenir** « **suffisamment d'information** » pour permettre à l'intéressé de comprendre l'importance, pour lui, de l'atteinte et de prendre, si cela est possible, des mesures pour réduire le risque de préjudice qui pourrait en résulter ou pour atténuer un tel préjudice.

L'avis doit être donné « **le plus tôt possible** » après qu'il y a eu atteinte.

Si une institution gouvernementale demande un délai à l'organisation pour mener une enquête en matière criminelle relative à l'atteinte aux mesures de sécurité, l'avis n'est donné qu'une fois que l'institution l'autorise à le faire (nouveau par. 10.1(6) de laLPRPDE).

ATTEINTES AUX MESURES DE SÉCURITÉ (art. 10.1 LPRPDE)

Avis relatif à une atteinte à toute autre organisation ou institution gouvernementale (art. 10.2)

Une organisation doit aussi aviser toute autre organisation ou institution gouvernementale capable de réduire le risque de préjudice pouvant résulter de l'atteinte ou d'atténuer ce préjudice

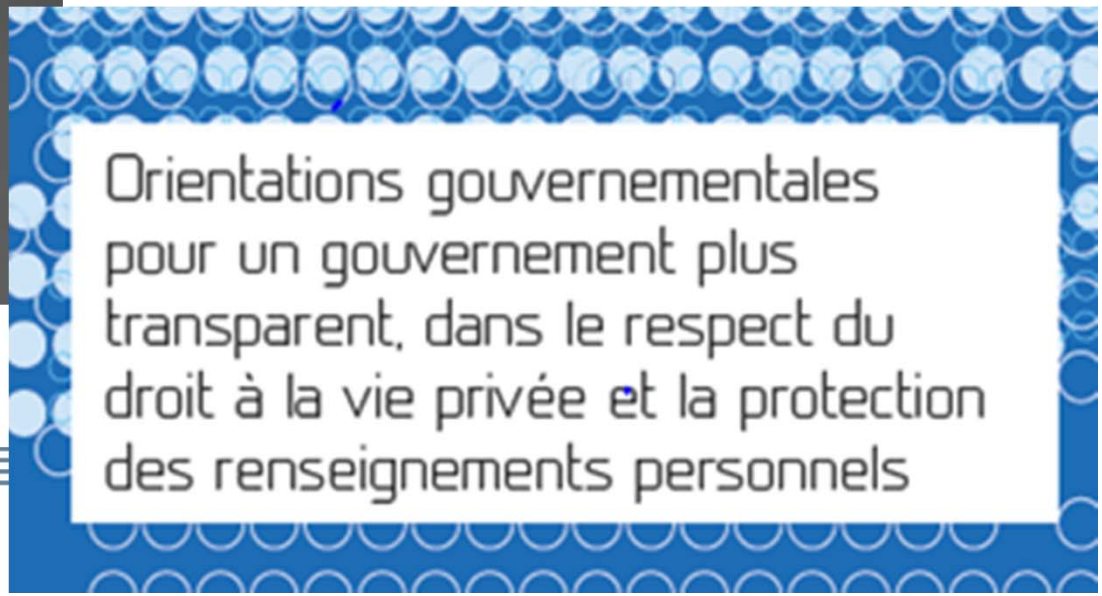
Registre des atteintes aux mesures de sécurité (art. 10.3)

Organisations doivent tenir et conserver un registre de toutes les atteintes aux mesures de sécurité qui ont trait à des renseignements personnels dont elles ont la gestion. Ces dossiers sont communiqués au commissaire sur demande.

Mars 2016

Règlement sur la notification et la déclaration des atteintes à la protection des données

1.3. LA DÉCLARATION DES FAILLES DE SÉCURITÉ



LANGLOIS

AVOCATS - LAWYERS

LOI SUR LE DROIT D'AUTEUR

Interopérabilité (30.61)
Recherche sur le chiffrement (30.62)
Sécurité (30.63)

Ne constitue pas une violation du droit d'auteur le fait de reproduire une oeuvre dans le seul **but d'évaluer la vulnérabilité d'un ordinateur, d'un système informatique ou d'un réseau d'ordinateurs ou de corriger tout défaut de sécurité**

-Doit donner au titulaire du droit d'auteur sur le programme un préavis suffisant faisant état de ceux-ci et de son intention de les rendre publics.

-Peut cependant les rendre publics sans préavis sil'intérêt du public d'être informé à cet égard l'emporte sur l'intérêt du titulaire de recevoir le préavis.

17.03: Duty to Protect and Standards for Protecting Personal Information

- (1) **Every person that owns or licenses personal information about a resident of the Commonwealth** shall develop, implement, and maintain **a comprehensive information security program** that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that **are appropriate to**
- (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;
- (b) the amount of resources available to such person;
- (c) the amount of stored data; and
- (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-002-3	Cyber Security - Critical Cyber Asset Identification
CIP-003-3	Cyber Security - Security Management Controls
CIP-004-3a	Cyber Security - Personnel & Training
CIP-005-3a	Cyber Security - Electronic Security Perimeter(s)
CIP-006-3c	Cyber Security - Physical Security of Critical Cyber Assets
CIP-007-3a	Cyber Security — Systems Security Management
CIP-008-3	Cyber Security - Incident Reporting and Response Planning
CIP-009-3	Cyber Security - Recovery Plans for Critical Cyber Assets
CIP-014-2	Physical Security

Energy—IT Security for Industrial Control Systems in Alberta's Electrical Industry

What we examined

We examined the Alberta Utilities Commission's role in:

- assessing risks and developing, implementing and communicating adequate IT security standards for ICS to mitigate those risks
- monitoring operators in the electrical industry for compliance with IT security standards for ICS and enforce compliance with the standards

principes directeurs pour les conseils d'administrations

1. **Understand and approach cybersecurity as an enterprise-wide** risk management issue, not just an IT issue.
2. Directors should **understand the legal implications** of cyber risks
3. Boards should have **adequate access to cybersecurity expertise**, and it should be on the agenda and discussed.
4. Directors should **set the expectation that management will establish an enterprise-wide risk management framework** with adequate staffing and budget.
5. Board-management discussion of cyber risk should include **identification of which risks to avoid, accept, mitigate, or transfer through insurance**, as well as specific plans associated with each approach.

Division of Corporation Finance
Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2

Cybersecurity

Disclosure by Public Companies Regarding Cybersecurity Risks and Cyber Incidents

Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A)

If one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions, the registrant should provide disclosure in the registrant's "Description of Business."

***Cybersecurity** is the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access.*
http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

CSA/ACVM Canadian Securities Administrators | Autorités canadiennes en valeurs mobilières

Avis 11-326 du personnel des ACVM
Cybersécurité

Les émetteurs, les personnes inscrites et les entités réglementées n'ayant pas encore évalué les risques liés à la cybercriminalité devraient tenter de trouver la meilleure façon de les gérer, notamment par les mesures suivantes :

- **sensibiliser le personnel à l'importance de la sécurité de l'information de la société et des clients et de la sécurité informatique, et au rôle qu'il a à jouer à cet égard;**

- **suivre les indications et les meilleures pratiques des associations professionnelles et des organismes reconnus en sécurité informatique;**

- **s'il y a lieu, procéder régulièrement à des tests et des évaluations de la vulnérabilité et de la sécurité chez les tiers.**

AUTORITÉ DES MARCHÉS FINANCIERS

CADRE DE SURVEILLANCE DES INSTITUTIONS FINANCIÈRES

Les risques inhérents évalués sont les suivants :
(…)
➢*Le risque des technologies de l'information*

LIGNE DIRECTRICE SUR LA GESTION DE LA CONTINUITÉ DES ACTIVITÉS

LANGLOIS KRONSTRÖM DESJARDINS avocats

Bureau du surintendant des institutions financières Canada | Office of the Superintendent of Financial Institutions Canada

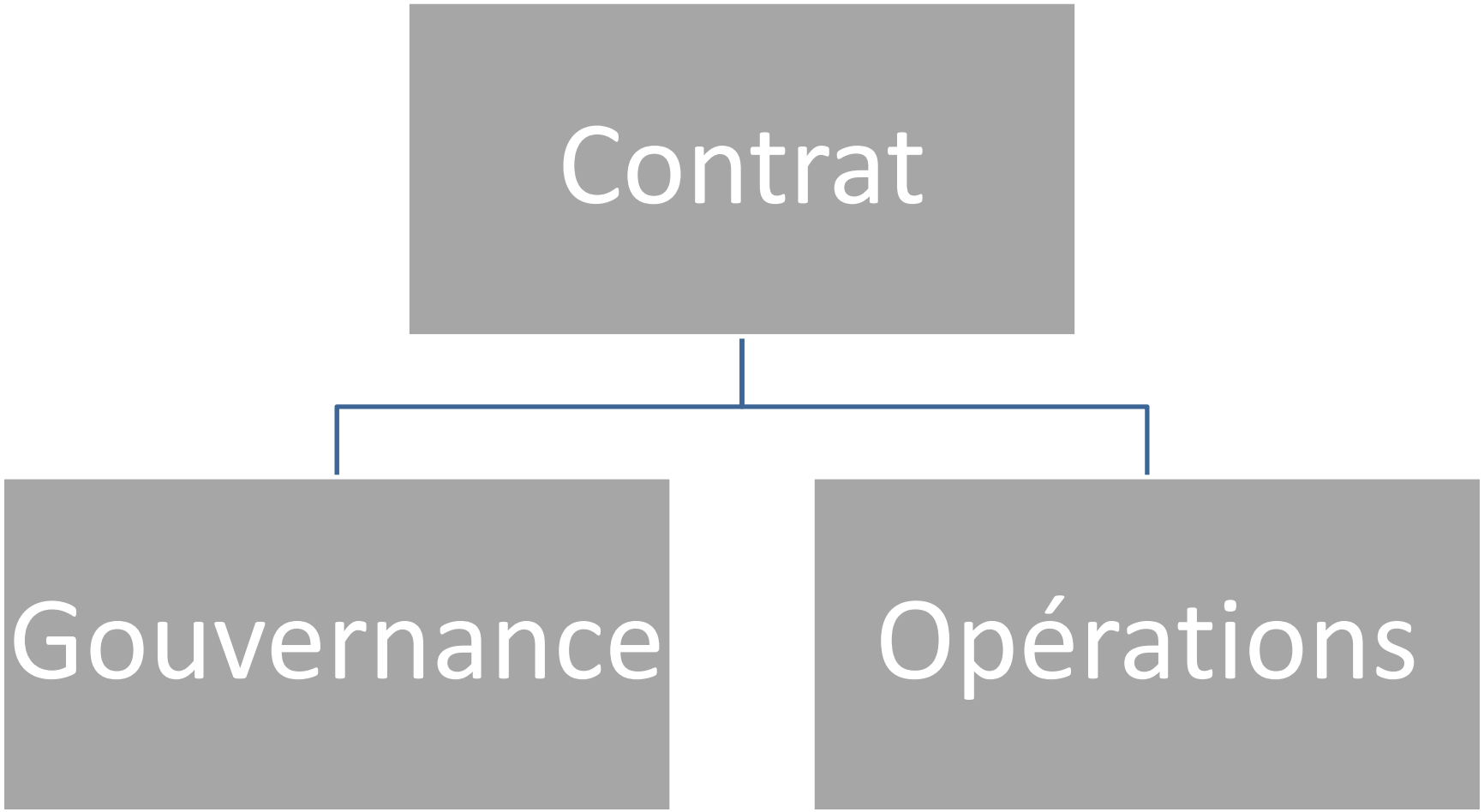
NOTE D'INFORMATION

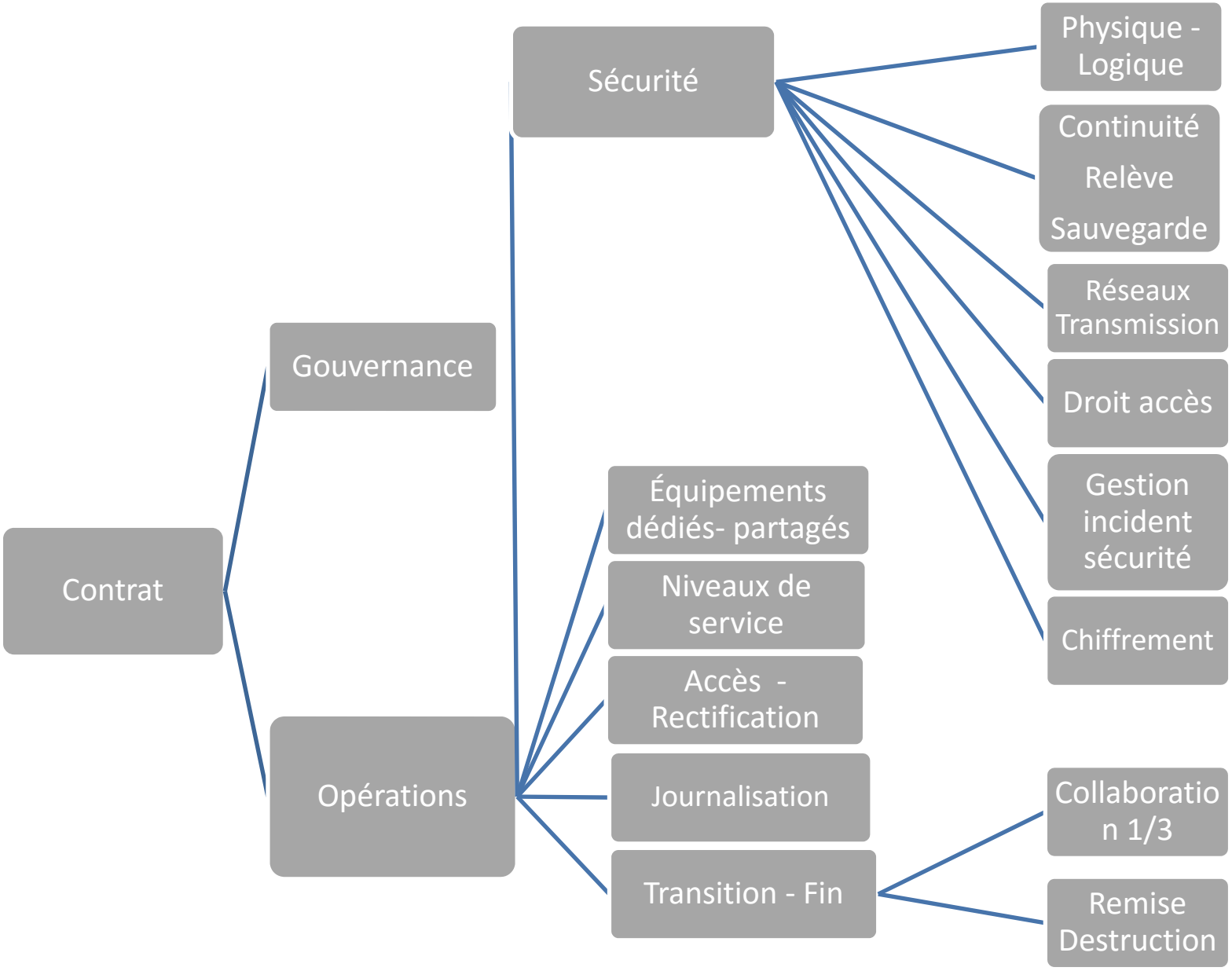
Date : Le 28 octobre 2013

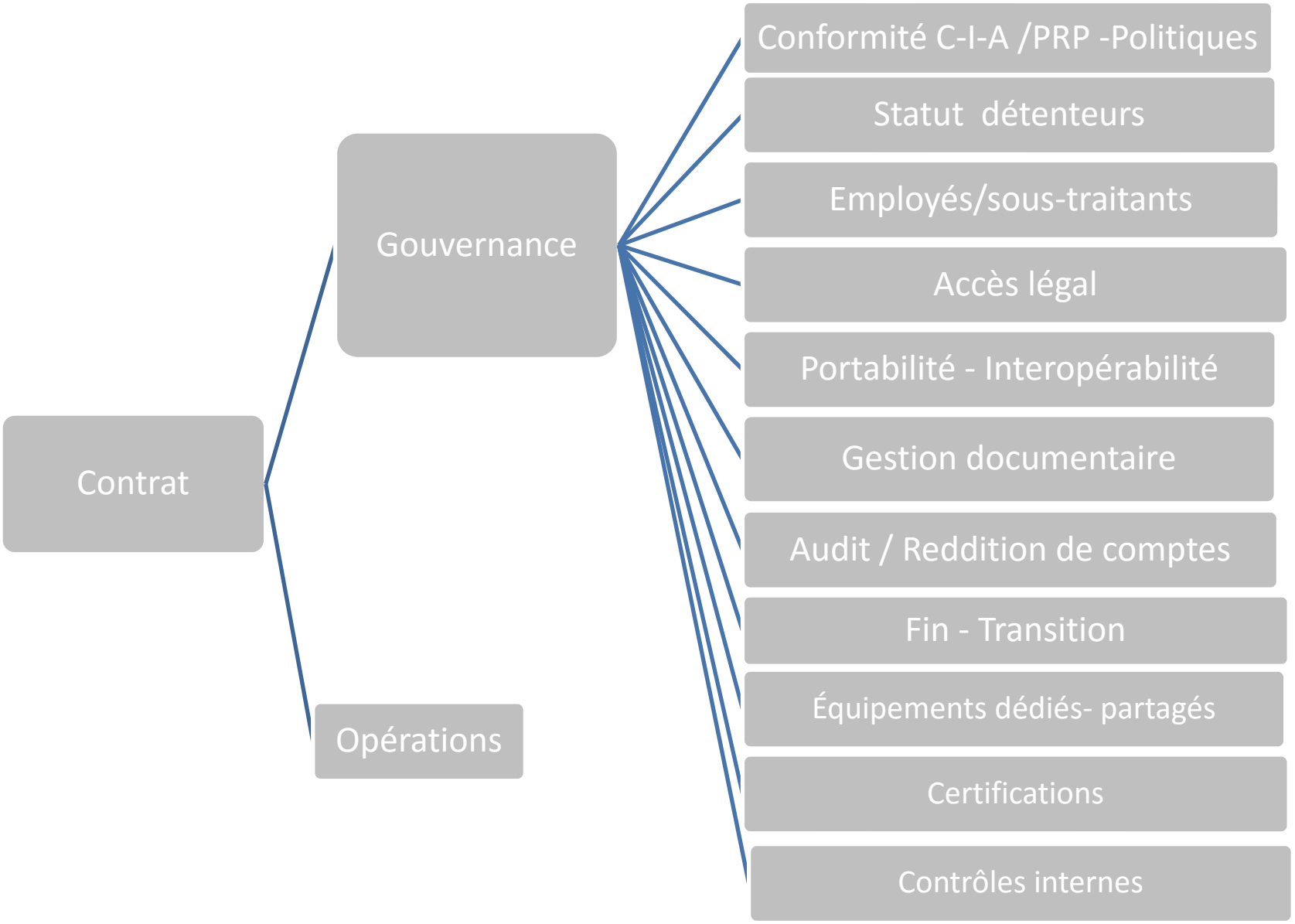
Destinataires : Institutions financières fédérales

Objet : Conseils sur l'autoévaluation en matière de cybersécurité

- Organisation et ressources
- Évaluation du cyberrisque et du contrôle
- Connaissance situationnelle
- Gestion du risque de menace et de vulnérabilité
- Gestion des incidents liés à la cybersécurité
- Gouvernance de la cybersécurité


Contrat
Gouvernance
Opérations


Contrat
Gouvernance
Opérations
Sécurité
Équipements dédiés- partagés
Niveaux de service
Accès - Rectification
Journalisation
Transition - Fin
Physique - Logique
Continuité
Relève
Sauvegarde
Réseaux Transmission
Droit accès
Gestion incident sécurité
Chiffrement
Collaboration 1/3
Remise Destruction


Contrat
Gouvernance
Opérations
Conformité C-I-A /PRP -Politiques
Statut détenteurs
Employés/sous-traitants
Accès légal
Portabilité - Interopérabilité
Gestion documentaire
Audit / Reddition de comptes
Fin - Transition
Équipements dédiés- partagés
Certifications
Contrôles internes

SHARED ASSESSMENTS

FedRAMP

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

ISO/IEC 27018

ISO International Organization for Standardization

PCI Security Standards Council™

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

COUVERTURES MULTIPLES

Les réclamations de tiers reliées à des intrusions, incluant les réclamations liées au défaut de protéger la confidentialité des données;

Les coûts reliés à la gestion de crise (forensics, recouvrement de données, relations publiques, suivi de crédit des clients affectés, etc…);

Coût associés à une demande de rançon par un pirate;

Pertes de revenus en raison de l'interruption d'accès aux systèmes informatiques;

Identification des auteurs

RECOURS EXTRAORDINAIRES

Norwich

Injonction

Anton Piller

To do list - En bref

Inventaire et classification des actifs informationnels

Analyse de risque et vulnérabilités

Gouvernance - responsabilité

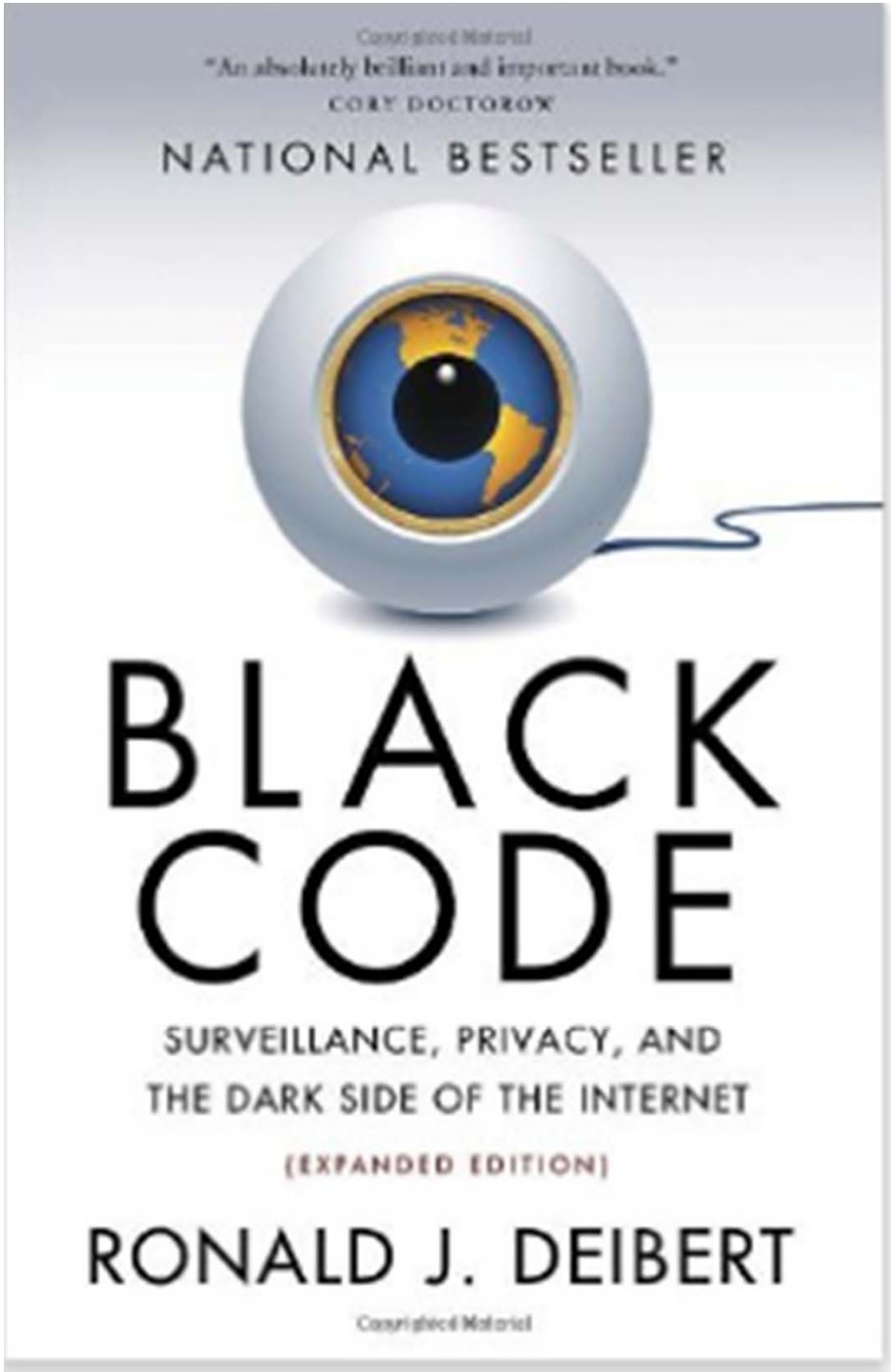
Procédures et mesures de sécurité

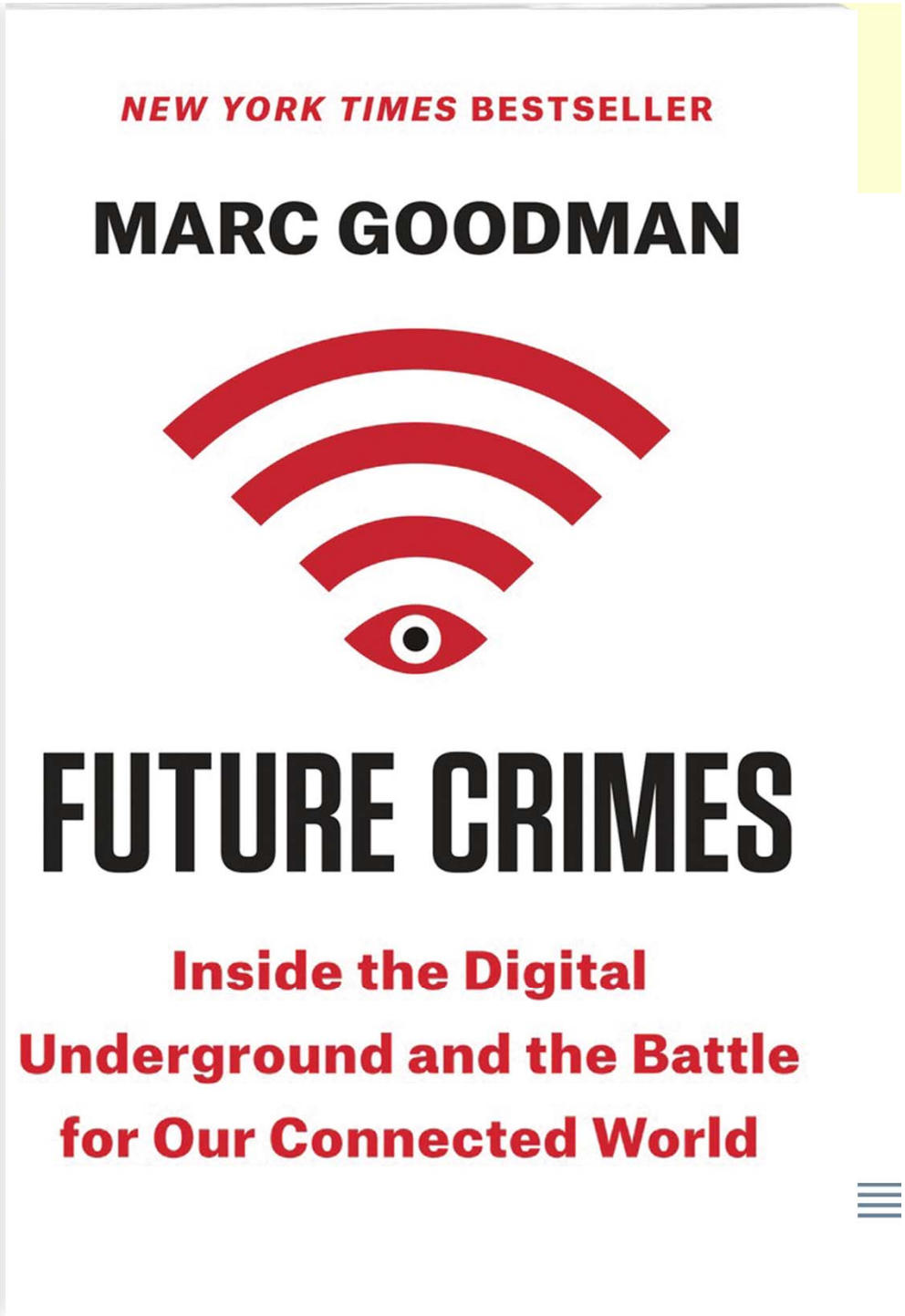
Encadrement de l'approvisionnement et des fournisseurs

Gestion des incidents

Assurance

Formation , sensibilisation


"An absolutely brilliant and important book."
CORY DOCTOROW
NATIONAL BESTSELLER
BLACK CODE
SURVEILLANCE, PRIVACY, AND THE DARK SIDE OF THE INTERNET
(EXPANDED EDITION)
RONALD J. DEIBERT


NEW YORK TIMES BESTSELLER
MARC GOODMAN
FUTURE CRIMES
Inside the Digital Underground and the Battle for Our Connected World


Preuve Préparation au litige
information
Co-Contractants
Fournisseur
Cyber-Assurance
Informations
Infonuagique
Vie privée
Hacking Social
Actionnaires
Employés
financière
Intrusion
Phishing
Relève
Régulateurs
Internet des objets
industriels
Cyber-Espionnage
privilégiées
Délits d'initiés
Sous-traitant
CCQ
LCCJTI
Dénonciation de risque
Mobilité
Destruction
Obligation de notification
Secrets
Fiabilité
Conformité
Renseignements personnels
Continuité des affaires
Divulgation de risques

LANGLOIS

AVOCATS - LAWYERS

Jean-François De Rico

jean-francois.derico@langlois.ca

514-842-9512 /418-650-7923

www.langlois.ca

www.linkedin.com/in/jfderico

twitter: @jfderico