Gérer les risques liés à la cybersécurité de la chaîne logistique avec le cadre de gestion ISO 27001:2013

Cristian Dragnef
IRCA ISMS LA, CRM
- Président, Seratos Inc -

SERATOS RATOS

Banque du Canada - Revue du système financier

- **Évaluation des vulnérabilités et risques — juin 2018**
  - > ***Vulnérabilité 1 : Niveau élevé d'endettement des ménages canadiens***
  - > ***Vulnérabilité 2 : Déséquilibres dans le marché canadien du logement***
  - > ***Vulnérabilité 3 : Menaces informatiques, risques opérationnels, et interconnexions des systèmes financiers***

SERATOS

Menaces informatiques — Éléments clés

- **Interconnectivité du système financier — manque de collaboration**
- **Sophistication des attaques — manque de compétences à l’interne**
- **Reconnaissance des intrusions — faible capacité de recouvrement et de confinement**

SERATOS

Pourquoi est-ce important ?

- **Moyenne mondiale — 141 $/enregistrement**
- **Canada**
  - ***Accès non autorisé — 201 $/enregistrement***
  - ***Interruption – 181 $/enregistrement***
  - ***Mauvaise gestion – 180 $/enregistrement***
- **É-U**
  - ***Accès non autorisé – 244 $/enregistrement***
  - ***Interruption – 209 $/enregistrement***
  - ***Mauvaise gestion – 200 $/enregistrement***

Source: IBM, 2017

SERATOS

Exposition aux risques opérationnels

Exposition		Menaces	Risques
Actifs organisationnels dans le champ	Confidentialité	Divulgation	Part de marché
	Integrité	Remaniement	Marge
	Disponibilité	Retards	Revenu
	Conformité	Tous	Non-conformité

SERATOS

Principes-clés en sécurité

Chaîne d'approvisionnement et cyberprotection

- **Attendez-vous à ce qu'il y ait des brèches de vos systèmes et concevez votre protection en conséquence**.
- **La cybersécurité n'est pas seulement un problème technologique, mais également un problème humain, de processus et de connaissances**.
- **La sécurité est la sécurité**

SERATOS

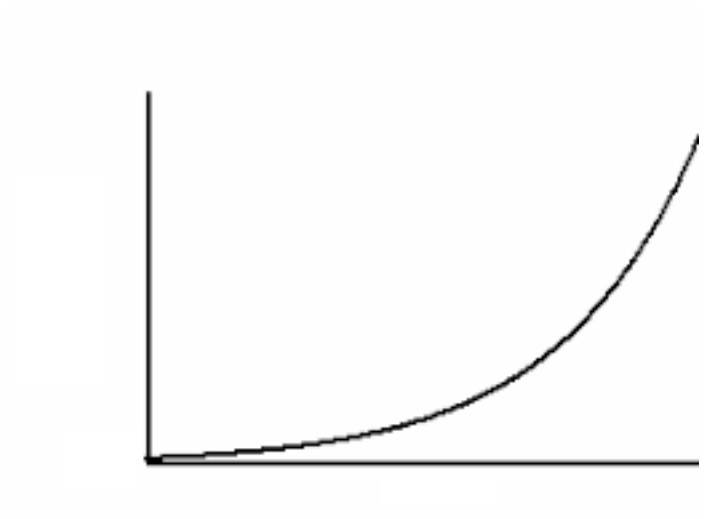
Approvisionnement et cyberprotection – les facteurs clés

- Les fournisseurs de produits ou services — de la conciergerie aux services de génie logiciel — ayant accès aux systèmes d'information, au code logiciel, ou aux adresses IP, sur les lieux ou à distance.
- Mauvaises pratiques de sécurité par les fournisseurs de paliers inférieurs.
- Logiciel ou matériel corrompu acheté chez les fournisseurs.
- Failles de sécurité dans les logiciels de gestion de la chaîne logistique ou dans les systèmes des fournisseurs.
- Matériel contrefait ou incorporant un programme malveillant.
- Stockage de données chez les tiers ou tiers agrégateurs de données.

SERATOS

Risques à la cybersécurité de la chaîne d'approvisionnement...

Peut-on les contrôler ? ...



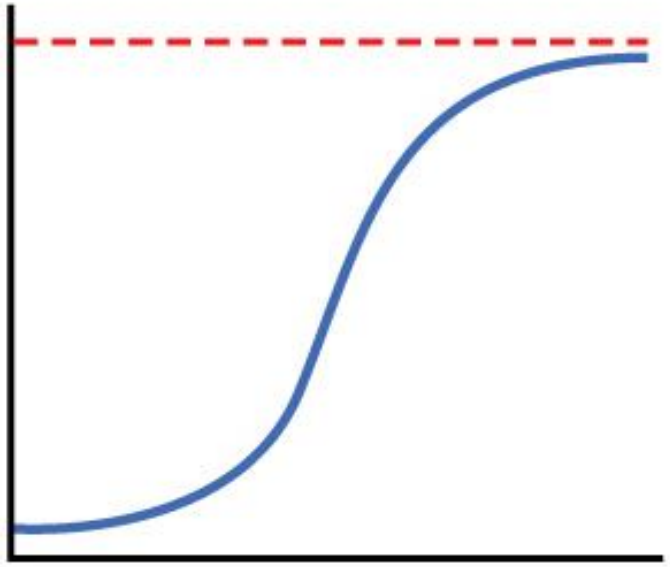
Conséquences de la non-conformité

- **Légales :** responsabilité civile, application des règles et pénalités causant des pertes financières directes ;
- **Affaires :** Perte de la part de marché, de la marge et de revenus.

SERATOS

ou….

…peut-on les optimiser ?



Stratégies de contrôle

- **Cadres de gestion des normes de cybersécurité**

  ISO 27001, NIST, CSA, PCI/DSS

- **Cadres de gestion de contrôles de la sécurité**
  - Traditionnel, intégré, adaptatif

Dépendances

- Profil de risque
- Couverture
- Efficacité opérationnelle

SERATOS

ISO/IEC 27001:2013

- Établit les normes pour la mise en place, la mise en œuvre, la maintenance et l'amélioration d'un SGSI dans le contexte de l'organisation.
- Comprend les normes d'évaluation et de gestion des risques.
- Les normes sont génériques et s'appliquent à toutes les organisations.
- Peut servir à des évaluations par les parties internes et externes.
- Aucune des normes des clauses de 4 à 10 ne peut être exclue pour être en conformité à ce standard.

SERATOS

Exigences du cadre de SGSI

- Le Système de gestion de la sécurité de l'information (SGSI) – *mise en œuvre et maintenance d'un SGSI documenté selon son profil de risque.*

ISO 27001:2013

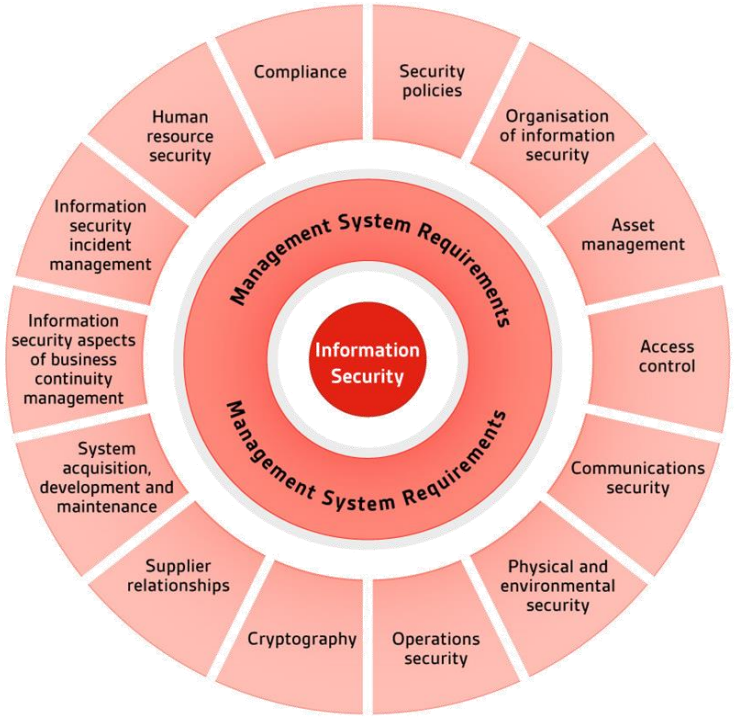
14 catégories de sécurité

Comprenant

35 sous-catégories de sécurité

Englobant

114 mesures de contrôle distinctes



Contrôles de la chaîne logistique d’approvisionnement (1)

Génériques

- Relations avec les fournisseurs (A.15)
- Gestion des incidents liés à la sécurité de l’information (A.16)
- Continuité de la sécurité de l’information (A.17.1)
- Conformité aux obligations légales et réglementaires (A.18.1)

SERATOS

Contrôles de la chaîne logistique d’approvisionnement (2)

Spécifiques

- La sécurité de l’information dans la gestion de projet (A.6.1.5)
- Appareils mobiles et télétravail (A.6.2)
- Sécurité physique et environnementale (A.11)
- Acquisition, développement et maintenance des systèmes d’information (A.14)

Quoi faire?

- Énoncez clairement et documentez vos besoins en sécurité
- Faites confiance, mais vérifiez
- Coûteux n’est pas toujours mieux.
- Restez vigilant. e. s

SERATOS

Merci !

SERATOS