

### *Quel est l'avenir de la sécurité avancée au Québec ?*

---

#### 1. LES FAITS

##### ► La cybercriminalité est un commerce en pleine expansion

Le volume des programmes malveillants a augmenté de 400% en 2008. Les analystes estiment qu'en 2009 les entreprises perdront près d'un trillion de dollars à la suite de perte ou de vols d'informations liés à la cybercriminalité.<sup>1</sup> Pourquoi une telle vague de délits ? L'origine se trouve dans la multiplication des accès à haute vitesse. Ajoutez à cela notre mode de vie mobile et la vague se transforme en tsunami.<sup>2</sup>

##### ► Le Canada est frappé

###### **LES CYBERCRIMINELS SE METTENT À LA DIVERSITÉ...**

L'anglais a cessé d'être la langue unique de la cybercriminalité. Depuis deux ans, le recours aux langues étrangères a été multiplié par six.

*2009 Threat Predictions,  
McAfee Avert Labs*

Aucun pays n'est à l'abri. En début d'année, la société Canadian Tire s'est vue obligée de rappeler 16 000 cartes de crédit pour cause d'une brèche de sécurité dans son système informatique. La crise économique actuelle accentue la tendance : toutes sortes de nouvelles fraudes mettent à profit l'incertitude financière alors même que les entreprises se voient forcées de couper dans leur budget.

Nul n'est à l'abri. Le Québec était en partie à l'abri des pirates informatiques en quasi-totalité anglophones. Il est maintenant ciblé grâce à des outils de localisation qui permettent aux pirates de « localiser » leur approche et d'aborder les victimes dans leur langue maternelle.<sup>3</sup>

##### ► La propriété physique est menacée

La fraude informatique n'est qu'une partie du problème. Les cybercriminels visent également les biens tangibles : les devises fortes, l'information critique et la destruction de biens physiques.

---

<sup>1</sup> Business risk \$1trillion losses from data theft : study, Reuters Newswire, January 29 2009.

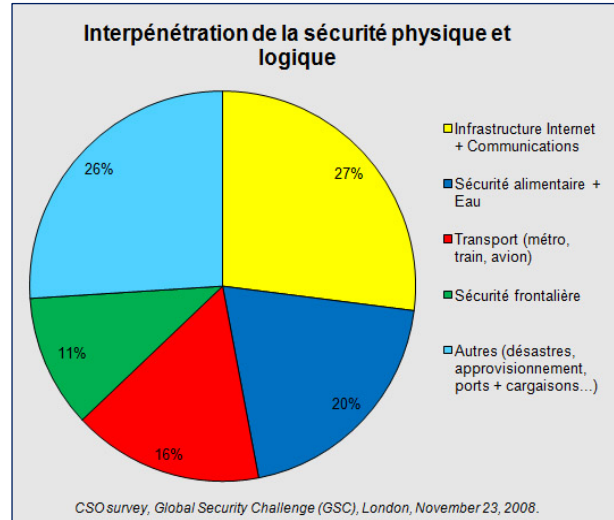
<sup>2</sup> Computer Viruses and Other Malicious Software : A Threat to the Internet Economy. OECD. 2009.

<sup>3</sup> 2009 Threat Predictions, McAfee Avert Labs.

---

Les spécialistes en sécurité estiment que l'infrastructure de télécommunications, la protection des réserves d'eau potable, la chaîne alimentaire, les réseaux de transport (métro, chemins de fer, aéroports) ainsi que les ports et les frontières terrestres figurent au premier rang de leurs préoccupations.

Dns un cas récent, un pirate informatique mécontent a tenté de détruire une plateforme pétrolière de forage. Les enjeux de sécurité physique et logique s'interpénètrent. Si une compagnie refuse l'accès à un intrus sur son site corporatif, il n'y a aucune raison de le laisser pénétrer dans ses locaux par la grande porte.



### ► L'administration Obama mise sur la sécurité

Le nouveau budget proposé par le président Barack Obama comprend 355 millions \$ afin d'accroître la sécurité des réseaux privés et publics américains. Ces fonds serviront à mettre au point une approche holistique et intégrée destinée à répondre aux menaces actuelles de cybersécurité, d'anticiper les menaces à venir et de poursuivre les partenariats innovateurs public-privé.

## 2. QUELLE EST LA SITUATION AU QUÉBEC ?

La première étude sur la sécurité avancée conduite par la CATA a permis d'identifier plus de 180 compagnies québécoises (à comparer avec environ 500 ailleurs au Canada) et de cerner trois enjeux principaux :

- *La technologie avancée en sécurité est de plus en plus accessible aux PME.* La demande pour des applications « clés en main » destinées aux PME avait déjà dépassé celle des solutions « sur mesure » offertes aux seules grandes entreprises.
- *Convergence de la sécurité physique et informatique.* De plus en plus d'applications informatiques (contrôle de l'accès aux réseaux, solutions d'imagerie à distance...) convergent avec la sécurité physique pour se fondre au sein d'une plateforme de sécurité intégrée. Toutefois les deux fonctions demeurent distinctes dans la plupart des entreprises. Elles relèvent de services différents ; elles sont



gérées par des experts avec des formations différentes. Comment unifier ce que nous appelons « sécurité avancée » ?

- *La défense du périmètre cède le pas à la protection des données.* La protection du réseau d'entreprise perd de son importance au fur et à mesure que la mobilité se répand (téléphones intelligents, ordinateurs portables), que les accès au réseau se multiplient (depuis le bureau, la maison ou les locaux du client) et que les menaces internes se généralisent (actes criminels, employés mécontents ou simplement négligents, logiciels défectueux). La conséquence est un recentrage de l'industrie de la sécurité sur la sécurité des données – sans négliger pour autant la défense du périmètre. Montée en force du concept de sécurité en couches.

### 3. POURQUOI LA « SÉCURITÉ AVANCÉE » ?

La CATA a décidé d'étudier la « sécurité avancée » et non pas seulement la « sécurité informatique ». En effet, la sécurité avancée est un nouveau champ de recherche qui comprend à la fois la protection logique et physique – plus spécifiquement le phénomène de convergence qui se produit quand les technologies hybrides (réseaux intégrés vidéo et données, cartes à puces, biométrie, senseurs, etc.) sont incorporées dans les systèmes de contrôle des accès physiques. Nous sommes convaincus que la sécurité au XXI<sup>e</sup> siècle exige une approche holistique.

### 4. L'ÉTUDE DE 2009

La sécurité est en pleine effervescence au Québec. Mais à quelle vitesse se développe-t-elle ? Où se situent ses forces et ses faiblesses ? Est-ce suffisant pour répondre aux nouveaux enjeux ? Comment se compare le Québec avec le reste du Canada ?

Ces enjeux, ainsi qu'une interrogation sur l'avenir de l'industrie de la sécurité avancée, justifient une nouvelle étude.

#### ► Objectifs

- Évaluer la **dynamique de l'industrie** de la sécurité avancée (sondage + analyse de fond).
- Informer le **marché québécois** en créant des liens entre fournisseurs et utilisateurs de sécurité avancée – y compris les utilisateurs canadiens hors Québec.
- Identifier les **prochains défis commerciaux** auxquels que devra relever l'industrie de la sécurité avancée au cours des trois prochaines années et au-delà (émergence de nouvelles technologies, concurrence internationale, crise économique, réglementation évolutive, problématique vie privée, etc.).

### ► Stratégies

- Sondage de l'industrie de la sécurité avancée (population of 700 compagnies)
- Entrevues qualitatives (20 + compagnies – niveau haute direction)
- Campagne médias + lancement de l'étude (simultanément dans deux villes Québec/Ontario)

### ► Thèmes

- Thème principal : Prévoir l'avenir en se fondant sur l'analyse des tendances structurantes d'hier et d'aujourd'hui.
- L'analyse de l'évolution entre 2003 et 2009 permettra de mesurer la capacité de l'industrie à s'adapter.
- Toutes les questions portant sur l'état actuel de l'industrie porteront sur sa capacité à faire face aux défis de demain.
- Environnement d'affaires :
  - **Omniprésence croissante de la sécurité avancée** dans la société québécoise.
  - Virtualisation de l'environnement informatique : quels sont les défis de sécurité soulevés par la **centralisation des données dans des serveurs lointains** et des applications « clients légers » hébergées dans le réseau d'entreprise ou même sur Internet ?
  - Quels sont les défis que posent à l'industrie de la sécurité avancée la **multiplication des terminaux mobiles** et la diversification des points d'accès au réseau d'entreprise ?
  - L'industrie s'achemine-t-elle vers la multiplication d'**entreprises de sécurité hyperspécialisées** ou, au contraire, vers la **consolidation en quelques grandes firmes intégrées** ?
  - Est-ce que les PME demeurent la principale source d'innovation et d'entrepreneuriat en matière de sécurité avancée ?
  - Comment l'industrie québécoise considère-t-elle les pays en émergence (Russie, Chine, Inde, Corée...) : comme des marchés potentiels ou comme des menaces ?
  - Examen des **barrières tarifaires** aux États-Unis, en Europe ainsi que dans les pays émergents.
  - Quel est l'impact au Québec des applications de sécurité sur plate-forme « open source » dont la NSA (National Security Agency) fait la promotion aux États-Unis ?
  - Impact des ministères canadiens de la Sécurité publique Canada et de la Défense nationale sur l'industrie québécoise.
  - Impact des politiques publiques d'approvisionnement en matière de sécurité avancée : y a-t-il une **politique gouvernementale d'achat** des produits de l'industrie domestique au niveau québécois ? Ou fédéral ?
  - Quelles sont les forces et faiblesses de l'industrie de la sécurité avancée au Québec ?
  - Tendances lourdes de l'industrie en Amérique du nord et dans le monde
  - Quels sont les segments de l'industrie québécoise qui réussissent le mieux sur le marché international ?

- Identification et caractérisation des liens entre les **universités** et les entreprises.
- Où se trouvent les **marchés actuels et ceux en croissance** ?
- Prospective
  - Identification des éventuelles **technologies de rupture** dans le domaine des technologies avancées.
  - Croissance du taux de pénétration des applications de sécurité avancée dans les organisations à travers tous les secteurs, tant privés que publics.
  - Évolution de l'usage d'Internet dans l'économie, y compris le commerce électronique et la gestion des affaires (intranet et extranet).
  - Examen des **impacts de la réglementation** (québécoise, canadienne et internationale) en matière de sécurité ainsi que des enjeux concernant la protection de la vie privée.
  - **Comment les utilisateurs de produits et services de sécurité se conforment-ils aux exigences de la réglementation ?**
  - Évaluation quantitative et qualitative de la **R-D au Québec** en matière de sécurité (liens entreprises-universités, accès au financement, commercialisation...).
  - Dans quelle mesure les **secteurs industriels connexes** (firmes conseils en TI, firmes de services professionnels, compagnies de télécommunications, éditeurs de logiciels, producteurs de sites web...) sont-ils disposés à intégrer des solutions de sécurité avancée dans leurs offres de produits et services ?
- Portrait de l'**avenir de l'industrie québécoise de la sécurité avancée** (horizon trois ans). Des scénarios prospectifs seront développés à partir de trois paramètres :
  - les séries temporelles 2003-2009 ;
  - l'examen des forces et faiblesses de l'industrie ;
  - l'identification d'une ou des tendances dominante (s).

#### ► Partenaires

- 1) Secteur public
  - gouvernement fédéral
  - gouvernement du Québec
  - forces de police
- 2) Secteur privé
  - sécurité
  - finance
  - autre usagers (services publics, transportation, télécommunications, etc.).

#### Associés

Les principaux intervenants du secteur de la sécurité avancée seront consultés au début du projet afin de valider les grandes hypothèses de travail, de tester le questionnaire ainsi que d'identifier des entreprises clés qui feront l'objet de recherches en profondeur (en vue de rédiger une série d'études de cas).

---

- Association canadienne de la sécurité (CANASA)	<a href="http://www.canasa.org/">http://www.canasa.org/</a>
- Association de la sécurité de l'information de la région de Québec (ASIRQ)	<a href="http://www.asiq.org/html/lasiq.html">http://www.asiq.org/html/lasiq.html</a>
- Association de Sécurité de l'Information du Montréal Métropolitain	<a href="http://www.asimm.org/pls/htmldb/f?p=105:34:3608550477591977">http://www.asimm.org/pls/htmldb/f?p=105:34:3608550477591977</a>
- Association fédérale des responsables de la sécurité (AFRS)	<a href="http://www.faso-afrs.ca/intro-f.html">http://www.faso-afrs.ca/intro-f.html</a>
- Canadian Information Processing Society (CIPS)	<a href="http://www.cips.ca">http://www.cips.ca</a>
- <i>Canadian Security Magazine</i>	<a href="http://www.canadiansecuritymag.com/">http://www.canadiansecuritymag.com/</a>
- Centre de la sécurité des télécommunications Canada (CSTC)	<a href="http://www.cse-cst.gc.ca/">http://www.cse-cst.gc.ca/</a>
- Disaster Recovery Information Exchange Canada (DRIE)	<a href="http://www.drie.org/">http://www.drie.org/</a>
- Industrie Canada : Industrie canadienne de la sécurité	<a href="http://www.ic.gc.ca/eic/site/ad-ad.nsf/fra/h_ad03910.html">http://www.ic.gc.ca/eic/site/ad-ad.nsf/fra/h_ad03910.html</a>
- Industrie Canada : Fournisseurs de solutions de sécurité	<a href="http://www.ic.gc.ca/eic/site/ict-tic.nsf/fra/h_it07470.html">http://www.ic.gc.ca/eic/site/ict-tic.nsf/fra/h_it07470.html</a>
- Institut de sécurité de l'information du Québec (ISIQ)	<a href="https://www.isiq.ca/accueil.html">https://www.isiq.ca/accueil.html</a>
Ministère du Développement économique, de l'Innovation et de l'Exportation ( <i>Direction des technologies de l'information et des communications</i> )	<a href="http://www.mdeie.gouv.qc.ca/index.php?id=5">http://www.mdeie.gouv.qc.ca/index.php?id=5</a>
- Portail Québécois de la Sécurité de l'information	<a href="http://www.cccure.net/">http://www.cccure.net/</a>
- RÉCO Québec (Réseau d'Échange en Continuité des Opérations du Québec)	<a href="http://www.reco-quebec.org/">http://www.reco-quebec.org/</a>
- Service canadien du renseignement de sécurité (SCRS)	<a href="http://www.csis-scrs.gc.ca/">http://www.csis-scrs.gc.ca/</a>
- Société canadienne de la sûreté industrielle inc. (SCSI)	<a href="http://www.csis-scsi.org/">http://www.csis-scsi.org/</a>
- <i>SP&amp;T News</i> (magazine published by Security Media, Inc.)	<a href="http://www.sptnews.ca/">http://www.sptnews.ca/</a>

---

## 5. FINANCEMENT DE L'ÉTUDE ET PARTENARIAT

Le financement de l'étude se fait sur une base de PPP – partenariat public-privé. Le coût pour le partenaire principal est fixé à 25 000\$ et à 10 000\$ pour le partenaire associé.

Avantages	Principal	Associé
Affichage du logo sur tous les produits de communications (dimension de l'affichage selon valeur de la participation) ainsi que dans les activités liées à l'initiative (ateliers, réunions, etc.)	*	*
Description en deux pages de l'entreprise publiée dans le rapport final (mission/vision/produits) Fr-Ang	*	
Citation dans le communiqué de presse principal Fr-Ang	*	
Citation dans les communiqués de presse thématiques (enjeux) Fr-Ang	*	*
Affichage du logo de l'entreprise sur le site web du rapport pendant un an et plus (dimension de l'affichage selon valeur de la participation)	*	*
Discours lors du lancement de l'étude – par exemple, Toronto et Montréal	*	
Invitation d'invités au lancement, incluant un kiosque commercial	*	*
Interview à la télévision web de l'AllianceCata	*	

#### ► Retour sur l'investissement

Pour un commanditaire, la commandite d'une étude scientifique et neutre est plus « rentable » pour la crédibilité de la marque de l'entreprise qu'une commandite traditionnelle de type publi-reportage. Les raisons sont multiples :

- Meilleure pénétration des messages du commanditaire dans les médias ;
- Crée des liens et une interaction entre l'entreprise commanditaire et les clientèles cibles (compagnies de sécurité, les utilisateurs corporatifs et les gouvernements) à un coût concurrentiel ;
- Accroît la sensibilisation des publics cibles aux enjeux de la sécurité dans la société et du rôle que joue le commanditaire ;
- Crée et renforce l'image de haut professionnalisme et de bon citoyen corporatif de l'entreprise commanditaire.

#### ► Paramètres mesurables

##### Médias traditionnels

- Sommaire de l'étude  
Le sommaire de l'étude, qui comprendra la liste et les logos des partenaires, sera distribué par les réseaux de la CATA ainsi que ceux des autres associations qui lui sont liées, le web, le marketing social (plus de 1 500 groupes spécialisés déjà identifiés). Dans le but de contribuer

au rayonnement de l'industrie, l'étude sera distribuée gratuitement dans le réseau des bureaux du Québec à l'étranger (Ministère des Affaires internationales) ainsi que dans le réseau canadien du ministère de Commerce international.

- **Couverture média**  
La couverture média générée tout au long de la période de commandite sera analysée pour identifier le nombre de mentions du nom du commanditaire. La couverture télévisuelle et web sera également notée, analysée et transmise au commanditaire.
- **Présence de l'industrie au lancement**  
Les fournisseurs et les utilisateurs de sécurité avancée seront invités à se joindre au lancement de l'étude. Ce sera une occasion unique pour le commanditaire de se faire mieux connaître et de réseauter avec des clients potentiels. Des représentants des provinces et du gouvernement fédéral seront également invités.
- **Presse d'affaires**  
La presse d'affaires spécialisées – Direction informatique et Les Affaires – sera mobilisée pour couvrir l'événement.

#### **Campagne intégrée virtuelle**

- **Courriels**  
CATA compte rejoindre 35 000 personnes/sociétés de TIC à travers le Canada. Des réseaux de distribution ont été mis en place grâce au jumelage de plusieurs bases de données d'associations en sécurité.
- **Présence web**  
La campagne de courriel dirigera l'utilisateur vers la page web sur la Sécurité Avancée. Un monitoring quotidien permettra de mesurer le nombre de visiteurs ainsi que d'impressions.
- **Le réseau social, blog et vidéo de la CATA**  
L'étude sera présentée sur la Web-TV de CATA et commentée par les commanditaires. Un blog spécialisé sera également créé et animé par les auteurs de l'étude.

#### **► Rapport de progrès**

L'Alliance CATA produira un rapport d'évaluation après le lancement à l'intention des partenaires. Il comprendra le détail de toutes les retombées médiatiques et promotionnelles avec une évaluation chiffrée.