SÉCAV 2010

L'industrie de la sécurité avancée au Québec - octobre 2010

Profil de l'industrie

CATAlliance
Alliance canadienne des technologies avancées

ISBN 978-2-9812174-0-0

Étude sur la sécurité avancée Québec 2010

© Alliance CATA et ScienceTech Communications, Montréal, QC, octobre 2010

Dépôt légal - Bibliothèque et Archives nationales du Québec, 2010
Dépôt légal - Bibliothèque et Archives Canada, 2010

© COPYRIGHT. TOUS DROITS RÉSERVÉS. TOUTE REPRODUCTION, MÊME PARTIELLE EST INTERDITE SANS AUTORISATION.

Table des matières

1. Préface : Réflexions sur la sécurité de l'information 1

2. Avant-propos 7

2.1 Évolution des tendances 7
2.2 Qu'est-ce que la « sécurité avancée » ? 10
2.3 Objet et organisation de l'étude 11
2.4 Méthodologie 13
2.5 La représentativité de l'échantillon d'entreprises 15
2.6 Équipe de réalisation et financement de l'étude 16
2.7 Financement de l'étude 16
2.8 Remerciements 16

3. Profil de l'industrie 19

3.1 Âge des entreprises 19
3.2 Taille et nature des entreprises de sécurité avancée 19
3.3 Une industrie très centralisée 23
3.4 Place des femmes dans l'industrie 25
3.5 Impact de la crise financière sur l'emploi 27
3.6 Impact de la crise financière sur les ventes 28
3.7 Niveau de l'emploi dans l'industrie québécoise de la sécurité avancée 29

4. État du marché 31

4.1 Taille des organisations clientes 31
4.2 Les grands secteurs du marché 32

5. Marché local, exportations et stratégie de croissance 35

5.1 Répartition entre marché domestique et exportations 35
5.2 Nature des exportations 37
5.3 Stratégie de croissance des exportations 39
5.4 Stratégie de diversification de l'offre 40

6. Recherche et développement (R-D) 43

6.1 Poids relatif de la R-D au Québec 43
6.2 Nature de la R-D au Québec 44
6.3 Les domaines d'applications de la R-D 44

7. Financement 47

8. Les obstacles au développement de l'industrie 49

9. Conclusion et pistes de recommandations 51

8.1 Des TIC à la gouvernance 51
8.2 Développement d'une offre adaptée aux PME 51
8.3 Manque de personnel qualifié 52
8.4 Pistes de recommandations 53

Annexe 1 : Étude cas 55

Auditia 56
Above Security 57
Carillon Information Security 59

Cedval Info inc. 60
Forensic 62
Gardien Virtuel inc. 64
IBM Canada 66
In Fidem 70
Institut national d'optique 73
Notarius inc. 75
Nurun Inc. 77
Optosecurity 78
PricewaterhouseCoopers (PwC) 80
RDDC Valcartier 82
SecureOps 85
S.I.C. Biometrics Inc. 86
Silanis 88
Waveroad Consult 91
Zerospam Sécurité 93

Annexe 2 : Questionnaire 95

Annexe 3 : Sigles et acronymes 101

Table des illustrations

Figure 1 - Google en Chine 7
Figure 2 - L'environnement d'affaires de la sécurité avancée 9
Figure 3 - Qu'entendons-nous par sécurité avancée ? 10
Figure 4 - Structure de l'industrie de la sécurité avancée 11
Figure 5 - Un taux de réponse élevé 14
Figure 6 - Les ¾ des firmes de sécurité sont des enfants d'Internet 19
Figure 7 - Taille de l'entreprise et taille de l'équipe 20
Figure 8 - Il y a plus d'entreprises spécialisées que d'entreprises hybrides 20
Figure 9 - Mais les emplois de sécurité se trouvent dans les entreprises hybrides 21
Figure 10 - Le reste du Canada a plus de grandes entreprises 21
Figure 11 - Nature des activités de l'entreprise 22
Figure 12 - La localisation des entreprises québécoises de sécurité avancée 24
Figure 13 - La place du Québec dans l'ensemble canadien 25
Figure 14 - Les pôles de sécurité dans l'ensemble canadien 25
Figure 15 – Faible représentation des femmes 26
Figure 16 - Fluctuation du nombre d'employés au Québec et dans le reste du Canada 27
Figure 17 - Fluctuation des ventes au Québec et dans le reste du Canada (2009) 28
Figure 18 - Un marché encore dominé par la grande entreprise 31
Figure 19 - Répartition du marché de la sécurité entre secteur privé et secteur public 32
Figure 20 - Le secteur financier est toujours le premier client de sécurité 33
Figure 21 - Une industrie tournée vers l'exportation 35
Figure 22 - Volume de ventes québécoises par destination 36
Figure 23 - Le commerce interprovincial sert de tremplin aux exportations internationales 36
Figure 24 - Marché domestique et exportation : comparaison Québec/Canada 37
Figure 25 - Volume de ventes canadiennes en fonction des destinations 37
Figure 26 - Forte présence des services 38
Figure 27 - La majorité des entreprises vise à accroître ses exportations 39
Figure 28 - Répartition des marchés géographiques (prévisions) 40
Figure 29 - Secteurs en expansion en 2010 40
Figure 30 - Faiblesse relative de la R-D québécoise 43
Figure 31 - Priorité à l'innovation 44
Figure 32 - Les grandes tendances de la R-D québécoise 45
Figure 33 - Le financement n'est pas un problème majeur 47
Figure 34 - Le recrutement de personnel est le principal obstacle 49
Figure 35 – Classement des commerces en fonction de la norme PCI-DSS 51
Figure 36 – Le commerce de détail au Québec 52

1. Préface : Réflexions sur la sécurité de l'information

* * *

Texte extrait d'une interview avec Marc Fournier, Associé délégué

Sécurité informatique et protection des renseignements personnels
PricewaterhouseCoopers (PwC)

* * *

Trop souvent encore les entreprises considèrent la sécurité comme une question de technologies de l'information et des communications (TIC), alors qu'elle est avant tout une question de gouvernance. La sécurité constitue un enjeu stratégique qui devrait être traité au niveau de la présidence de l'entreprise et de son conseil d'administration. Malheureusement, la plupart des dirigeants et des administrateurs se préoccupent uniquement des grandes lignes de la réglementation issue de la loi Sarbanes-Oxley (SOX) [1] et, pour le reste, ils délèguent la gestion de la sécurité au service des TIC.

La sécurité constitue un enjeu stratégique qui devrait être traité au niveau de la présidence de l'entreprise.

Le résultat est que les entreprises sont relativement bien informées sur la sécurité de leurs systèmes informatiques. Quand nous parlons avec nos interlocuteurs de la nécessité de protéger leurs systèmes, ils sont généralement réceptifs et nous avons réussi à mettre leurs infrastructures à l'abri.

Les secteurs mous de la sécurité se retrouvent tous du côté des renseignements personnels : données clients, cartes de crédits, vol d'identité, etc.

Tout le monde connait quelqu'un qui a été victime; ou encore, quelqu'un qui connaît quelqu'un qui a été victime... Peu à peu, la panique gagne. La victime du vol d'identité doit traverser une véritable épreuve pour rétablir son identité auprès des gouvernements, des institutions financières, sans oublier Equifax. Il y a cinq ans, une personne qui se faisait cloner sa carte de débit chez un dépanneur était marquée à vie, la banque ne la croyait pas, son crédit était miné, son nom circulait un peu partout. Certains ont dû prendre un avocat pour s'en sortir.

Aujourd'hui, les choses se sont quelque peu améliorées, parce que le fléau est mieux connu. Ainsi, les institutions financières offrent des assurances contre le vol d'identité.

Il n'en reste pas moins que le problème numéro un auquel nous avons à faire face en matière de sécurité est la protection des renseignements personnels. Si nous faisons exception des gros joueurs qui ont une approche anticipatoire de la sécurité, la majorité du marché continue à faire le minimum et se contente de respecter la réglementation, et encore, pas toujours.

Le problème numéro un auquel nous avons à faire face en matière de sécurité est la protection des renseignements personnels.

[1] Loi américaine de 2002 sur la réforme de la comptabilité des sociétés cotées et la protection des investisseurs, couramment appelé loi Sarbanes-Oxley, du nom de ses promoteurs, les sénateurs Paul Sarbanes et Mike Oxley.

La société de l'information aujourd'hui, en est encore au stade de l'industrie automobile des années 70 : souvenons-nous de la Ford Pinto qui prenait feu en raison de la mauvaise qualité de son réservoir. Au lieu de régler le défaut de fabrication, pendant des années la compagnie a préféré payer les amendes et les frais de poursuites.

La sécurité est encore un *no-man's land* juridique et réglementaire où il n'y a pas d'imputabilité. Dans la plupart des pays, les gouvernements demeurent passifs et les compagnies privées font ce qu'elles veulent avec l'information de leurs clients. Il est évident qu'une telle situation ne saurait être que transitoire. Deux solutions s'offrent à nous : l'autoréglementation et l'action de l'État.

La sécurité est encore un no-man's land juridique et réglementaire où il n'y a pas d'imputabilité.

La solution de l'autoréglementation

Le secteur du crédit a décidé de s'auto-réglementer en créant la norme PCI-DSS[2] et en ajoutant une puce électronique dans les cartes de crédit et de débit, pour diminuer la fraude entourant ces cartes, dont le vol des renseignements personnels fait partie intégrante.

Le secteur du crédit a décidé de s'auto-réglementer en créant la norme PCI-DSS.

En effet, les institutions financières perdaient plusieurs centaines de millions de dollars par année en raison de la fraude massive effectuée sur les cartes de paiement.[3] Les principales d'entre elles se sont réunies pour demander aux commerçants de mettre à jour leur équipement et d'adopter les meilleures pratiques du secteur de la sécurité. Le gouvernement n'a rien eu à voir dans l'ensemble de ces mesures. Il s'agit d'une initiative prise au niveau mondial par un organisme indépendant : le *Payment Card Data Security Standards Council* (PCI SSC)[4].

L'enjeu monétaire était immense, ce qui a facilité la concertation entre les maisons de crédit. Celles-ci ont agi de la sorte car elles voyaient dans l'autoréglementation une manière de diminuer leurs pertes sur les cartes de crédit, ainsi que d'éviter la réglementation gouvernementale. Elles savent toutefois que ce n'est pas la fin de la fraude informatique, ni du vol d'identité.

Elles savent toutefois que ce n'est pas la fin de la fraude informatique, ni du vol d'identité.

Pour venir à bout du phénomène, il faudra que la pression publique s'accentue, par le truchement d'articles dans les journaux, d'émissions à la radio et à la télévision, ainsi que de campagnes de la part des associations concernées. Une compagnie qui est accusée de négligence sur la place publique encourt des dommages considérables.

Pour venir à bout du phénomène, il faudra que la pression publique s'accentue.

Le rôle de l'État

Aux États-Unis, les pouvoirs publics ont adopté une approche originale : au lieu de réglementer le niveau de sécurité, ils s'efforcent de rendre obligatoire la divulgation des incidents de sécurité qui mettent en jeu des renseignements personnels. La Californie a joué un rôle précurseur à cet

[2] Payment Card Industry - Data Security Standard (PCI-DSS) est la norme pour le traitement sécurisé des paiements par carte de crédit qui est obligatoire à compter du 1er octobre 2010.
[3] La Gendarmerie royale du Canada (GRC) estime à 408 millions de dollars le montant des fraudes sur les cartes de crédit et de débit en 2008 - http://www.rcmp-grc.gc.ca/count-contre/cccf-ccp-fra.htm
[4] Le Payment Card Data Security Standards Council (PCI SSC) créé en 2006 par VISA, MasterCard, American Express, Discover Financial Services et JCB International - http://frca.pcisecuritystandards.org/

égard en légiférant dès 2003 sur l'obligation de divulguer les incidents et, depuis lors, plusieurs États ont fait de même.[5]

Aujourd'hui c'est au tour du gouvernement fédéral américain de se doter d'une législation sur la divulgation des incidents.[6] Cette approche par voie de législation est différente de ce que font depuis des années les organismes du type CERT qui privilégient la recherche, le développement d'outils et la formation, mais qui ne se penchent pas sur les cas types : il est arrivé telle chose à telle place et voici comment ça s'est passé…

Le gouvernement fédéral américain se dote d'une législation sur la divulgation obligatoire des incidents.

Avec la future loi sur la divulgation, quand une compagnie enregistrera une perte de données à caractère personnel (numéro d'assurance sociale ou de permis de conduire, date de naissance, noms et prénoms des parents, etc.), elle devra divulguer l'incident, donc envoyer des lettres à ses clients et le publiciser sur son site web. Il existe déjà aux États-Unis des bases de données compilant les brèches de données personnelles qu'il est possible de consulter en ligne. Il est possible d'y faire des recherches par entreprise, par industrie ou par région.

Le projet de loi américain oblige tout organisme public, privé ou associatif qui identifie une brèche de sécurité exposant des données personnelles à dévoiler l'incident, ce qui contraindra leurs dirigeants à se pencher sérieusement sur les questions de sécurité.

À mon avis, c'est un modèle très intéressant pour l'industrie américaine de la sécurité parce que le gouvernement s'adresse directement au secteur privé pour lui dire comment se comporter.

Le Canada ne fait rien de tel. D'ailleurs on entend très peu parler de sécurité au Canada. Il y a bien la *Loi sur la protection des renseignements personnels et les documents électroniques*, mais elle n'oblige pas les entreprises à divulguer les incidents dont elles sont victimes.[7] Le résultat est que la grande majorité des incidents demeurent cachés.

Le Canada ne fait rien de tel. D'ailleurs on entend très peu parler de sécurité au Canada.

Le résultat est que la grande majorité des incidents demeurent cachés.

Ainsi, le gouvernement fédéral est le premier à donner le mauvais exemple. Rappelons-nous l'incident du site web de Passeport Canada qui a dû être fermé parce les codes url s'étaient entrecroisés[8]. Au lieu d'informer les victimes et de partager l'enseignement qui s'en dégage avec l'industrie, le gouvernement a tout fait pour minimiser l'incident.

Sans réglementation qui oblige les entreprises – et les gouvernements – à la divulgation, il n'y aura pas de protection efficace des renseignements personnels.

---

[5] Dès juillet 2003, le *California Security Breach Notification Act* a rendu obligatoire la notification des atteintes à la sécurité des consommateurs résidant en Californie. Une loi comparable a été adoptée dans quatre autres États et est en préparation dans 18.

[6] Déposé au Sénat en août 2010, le projet *Data Security and Breach Notification Act* exige des entreprises et organismes qui gèrent et stockent de l'information sur les consommateurs, comme par exemple leurs numéros d'assurance sociale, d'adopter des mesures et politiques de sécurité raisonnable afin de protéger cette information et, dans l'éventualité d'une défaillance, de la divulguer à l'échelle nationale. C'est le plus récent de toute une série de projets déposés tant au Sénat qu'à la Chambre des représentants.

[7] La Loi sur la protection des renseignements personnels et les documents électroniques est entrée en vigueur par étapes entre janvier 2001 et janvier 2004. Elle porte surtout sur le consentement des consommateurs à la collecte, à l'utilisation et à la communication des renseignements personnels par les entreprises - http://lois.justice.gc.ca/fr/P-8.6/index.html

[8] En novembre 2007, un citoyen de Huntsville (Ontario) qui renouvelait son passeport en ligne s'est aperçu qu'en changeant une lettre sur l'url du formulaire électronique de Passeport Canada, il avait accès aux demandes non chiffrées d'autres personnes. Le citoyen en question a immédiatement prévenu Passeport Canada qui a dû fermer son site. « Security breach forced closure of online passport application service », CBC, 25 mai 2009 - http://www.cbc.ca/canada/story/2009/05/25/passport-online-applications052509.html#ixzz10HBKOqjn

La gouvernance entrepreneuriale est au cœur de la sécurité

Que ce soit à la suite d'une législation gouvernementale ou d'une mesure d'autoréglementation, il appartiendra en définitive à l'entreprise d'inventer sa propre stratégie de sécurité et de déployer des outils et processus qui soient efficaces. Or, dans la plupart des cas, la structure de gouvernance de l'organisation n'est pas adaptée à la sécurité car elle ne prévoit pas de mécanismes permettant de porter les incidents de sécurité à la connaissance de la haute direction.

La structure de gouvernance de l'organisation n'est pas adaptée à la sécurité.

En effet, trop souvent, le responsable de l'exploitation des systèmes informatiques et celui de la sécurité relèvent du vice-président des TIC. Quand survient un incident, les deux responsables se renvoient la balle et, dans le meilleur des cas, seul le vice-président sera prévenu. Il tranchera le litige au niveau du service des TIC. Une telle structure aboutit tout naturellement à prévenir la montée de l'information jusqu'à la haute direction.

Cette structure aboutit tout naturellement à prévenir la montée de l'information jusqu'à la haute direction.

Si, dans une entreprise, le président et son conseil d'administration ne savent pas ce qui se passe sur le terrain de la sécurité, l'information n'a aucune chance d'être portée à la connaissance de l'industrie de la sécurité ni aux victimes. C'est d'ailleurs un problème majeur dans tous les sondages sur la sécurité. Quand on demande « combien d'incidents avez-vous eus ? », on obtient rarement les vrais chiffres, parce que la personne qui remplit le questionnaire n'est bien souvent pas au courant des incidents qui ont eu lieu.

Dans le domaine de la sécurité, il est donc primordial de diviser les tâches entre la gouvernance et l'exploitation afin de s'assurer que les gens qui gèrent les systèmes informatiques et leur sécurité ne cachent pas les incidents. Il faut que la personne qui assume le rôle de gouvernance ou de surveillance de la sécurité soit systématiquement et de plein droit impliquée dans le processus de gestion des incidents de façon à ce qu'elle prenne les décisions nécessaires, comme aviser le service juridique ou la haute direction. Cette instance de référence ne doit pas appartenir au service des TIC.

Dans le domaine de la sécurité, il est primordial de diviser les tâches entre la gouvernance et l'exploitation.

Cette structure reflète que ce qui est en cause quand on parle de sécurité de l'entreprise est la sécurité de l'information, non la sécurité de l'informatique. Et ce n'est pas une simple question de sémantique. Les données n'appartiennent pas au service des TIC, elles appartiennent au service des finances ou au service de la mise en marché, bref, au service qui les génère. Ceci nous mène tout droit au principe d'imputabilité. Ceux qui génèrent les données doivent êtres imputables de leur intégrité, de leur disponibilité, de leur survivabilité afin de pouvoir continuer l'exploitation de l'entreprise en cas de bris majeur et, enfin, de leur confidentialité.

Ce qui est en cause quand on parle de sécurité de l'entreprise est la sécurité de l'information, non la sécurité de l'informatique.

Autrefois, les professionnels chargés des comptes à payer traitaient toutes leurs données manuellement. Ils contrôlaient toutes les données, qu'il s'agisse des autorisations à l'intention des fournisseurs ou de l'émission des chèques. Toutes les informations étaient physiquement situées dans les bureaux du service des finances ou de l'approvisionnement.

Maintenant, la comptabilité est informatisée et les professionnels des comptes à payer sont encore légalement responsables de leurs dossiers – comme avant. Pourtant, la liste des fournisseurs, les autorisations de

paiement, bref toutes les données, se trouvent situés ailleurs, à un autre étage, dans un autre bâtiment, parfois même dans une autre ville.

S'il y a un incident de sécurité, ces données tombent dans des mains non autorisées, peut-être hostiles. La moindre des choses est que le service des TIC avise alors le professionnel chargé du compte. Souvent ce n'est pas le cas : l'incident n'est pas rapporté au service chargé de piloter le dossier ou à la haute direction.

Voilà pourquoi il est essentiel de structurer le service de sécurité de l'entreprise en séparant certaines tâches qui sont incompatibles. Il doit y avoir l'encadrement d'un côté; et l'exploitation de l'autre. Notre rôle est de faire comprendre au client que ce n'est pas le service des TIC qui est responsable de ses données, c'est lui : le professionnel chargé du dossier. Peu importe la plateforme, papier ou informatique, il est responsable. Si quelqu'un dans l'entreprise décide d'ajouter son beau-frère sur la liste des fournisseurs et que des chèques sont émis, c'est lui, qui est responsable.

Ce n'est pas le service des TIC qui est responsable de ses données, c'est le professionnel chargé du dossier. Peu importe la plateforme : papier ou informatique.

À cet égard, l'administration publique québécoise a mis au point un cadre de gouvernance de la sécurité qui peut servir de modèle. Ainsi, dans chaque ministère ou organisme, le responsable de la sécurité de l'information (RSI) est imputable devant le sous-ministre; non devant le directeur des systèmes d'information (DSI). Pour être efficace, toute solution de sécurité doit passer par la division des fonctions de mise en œuvre et de surveillance des TIC. Le grand problème qui se pose aujourd'hui à la sécurité est organisationnel, pas technique.

Quand bien même une firme installerait 50 coupe-feux, si elle n'a pas séparé les tâches de gouvernance et d'exploitation des outils de sécurité, elle affichera toujours des rapports au beau fixe. Mais les dirigeants ne sauront jamais ce qui se passe en réalité. Il faudra qu'un incident majeur survienne et qu'une enquête externe soit commandée, pour que l'on apprenne que ce n'est pas le premier incident du genre, qu'il y en a eu des dizaines depuis des mois, mais qu'ils n'ont jamais été rapportés ni documentés. Même alors, bien souvent, personne ne veut rien dire. On a vu des cas extrêmes où le spécialiste de sécurité refusait de collaborer et où les dirigeants de l'entreprise concernée n'osaient pas le renvoyer de peur qu'il ne leur arrive la même chose qu'à la municipalité de San Francisco.

On a vu des cas extrêmes où le spécialiste de sécurité refusait de collaborer avec la haute direction.

Dans cette ville, quand l'administrateur du réseau interne a été renvoyé, il a refusé de donner le mot de passe du système qui gérait la paie des employés, les courriels et autres fonctions essentielles. Il a été jugé et envoyé en prison, mais il refusait encore de donner le mot de passe au responsable des TIC. En fin de compte, il a fallu que le maire de San Francisco en personne se rende à la prison où était incarcéré son administrateur de réseau, pour que celui-ci accepte de remettre le code. [9]

[9] Terry Childs est cet administrateur du réseau de fibre optique de la municipalité de San Francisco qui a refusé de livrer le code d'accès du système à ses supérieurs hiérarchiques sous prétexte qu'ils n'étaient pas compétents en matière de sécurité. Il a été arrêté en juillet 2008 et condamné à quatre ans de prison en août 2010. « Former San Francisco Network Admin Terry Childs Gets Prison Time' », *Digital Communities*, 10 août 2010.

Les grandes tendances de la sécurité

Pour les grandes organisations, le tournant a été la mise à jour de l'an 2000 qui a été accompagnée du déploiement des progiciels de gestion intégré, les fameux systèmes ERP. Depuis lors, on assiste à des cycles de cinq ans dans les mises à jour. Celle qui est en cours actuellement représente un grand pas en avant dans la facilitation du travail, mais cette facilité même crée de nouveaux enjeux de sécurité. À partir d'un seul terminal, parfois depuis un simple mobile, on a accès à toutes les données de l'entreprise. En réaction à ce risque accru, les grands développeurs de systèmes ERP – SAP, PeopleSoft, Oracle et autres – lancent à présent des logiciels d'appoint qui permettent de mieux sécuriser les transactions.

La facilitation du travail par les systèmes ERP crée de nouveaux enjeux de sécurité.

Par ailleurs, l'introduction rapide de la norme PCI-DSS amène de nouveaux joueurs à prendre conscience des enjeux de la sécurité des données. Grâce à cette norme, dans le domaine du commerce de détail, on voit des entreprises moyennes, de 500 à 1000 employés, se doter d'un cadre de gouvernance ainsi que de logiciels et de matériel de sécurité. Les plus petites entreprises n'ont pas assez de budget pour investir dans les services professionnels. Il leur faudrait du prêt-à-porter, mais l'industrie n'est pas arrivée à ce stade.

La norme PCI-DSS incite des entreprises de 500 à 1000 employés à investir en sécurité.

Les normes en matière de sécurité, comme par exemple ISO 27 000, sont encore faites pour le modèle de la grande entreprise. Il appartient aux spécialistes de sécurité de les adapter au contexte particulier de l'entreprise. En pratique, ce sont généralement les grandes sociétés de services professionnels qui remplissent cette fonction.

Il n'y a pas de solutions de prêt-à-porter parce que chaque client est différent. Les processus d'affaires et l'infrastructure physique varient d'une entreprise à l'autre, certaines reçoivent leurs clients dans leurs locaux, d'autres passent par des distributeurs et ont donc des locaux entièrement privés. Il y a trop de variables dans le secteur commercial pour pouvoir proposer des solutions prêt-à-porter.

Il n'y a pas de solutions de prêt-à-porter parce que chaque client est différent.

En même temps, la petite entreprise est souvent amenée à prendre plus de risques que la grande, car elle est en développement et que son niveau de notoriété est encore faible. Si une PME inconnue a un bris de sécurité, l'incident a de fortes chances d'impliquer peu de monde et d'avoir des répercussions moins importantes que si une grande banque se faisait attaquer.

En fin de compte, la sécurité est avant tout une affaire de gestion de risque qui doit être envisagée en termes de gouvernance de l'organisation et de stratégie d'affaires.

La sécurité est avant tout une affaire de gestion de risque.

2. Avant-propos

La sécurité de l'information est à l'ordre du jour. Le piratage brutal des serveurs de Google par des internautes basés en Chine, vraisemblablement liés au gouvernement de ce pays, a rappelé la fragilité de la sécurité informatique et le caractère hautement stratégique des enjeux.[10] Il y a des années que l'on annonce la fin des bidouilleurs amateurs (*hackers*) et la montée des pirates professionnels, malfaiteurs liés au crime organisé ou non, à l'espionnage économique et, dans le cas des attaques dénoncées par Google, à l'espionnage tout court des États.

FIGURE 1 - GOOGLE EN CHINE

Saisie d'écran le 24 septembre 2010 (version Hong Kong de Google Chine)

2.1 Évolution des tendances

En 2003, une première étude de l'Alliance CATA sur la sécurité avancée, avait identifié la convergence entre la sécurité physique et logique comme une tendance de développement. En effet, la sécurité informatique irrigue de plus en plus les outils traditionnels de la sécurité physique. Cette convergence a été confirmée sur le plan technologique, mais elle n'a pas été transposée sur le marché. Non pas, comme nous l'avons cru à l'époque, parce que des obstacles administratifs au sein des entreprises étaient en cause, mais plutôt parce que des impératifs culturels ont maintenu la différence.

Le champ de la sécurité physique est distinct de la sécurité de l'information. Tout ne peut pas se numériser. Un interrogatoire relève davantage des techniques policières qu'informatiques. Bell est une

[10] En janvier 2010, Google a annoncé que le mois précédent des pirates chinois avaient utilisé une faille au sein du format de document PDF pour infiltrer ses serveurs ainsi que ceux d'une dizaine d'entreprises américaines, dont Symantec, Juniper Networks et Northrop Grumman. Ce genre d'attaque dirigée contre les systèmes informatiques des grandes organisations est chose commune, mais ce qui l'est moins est qu'elle ait été rendue publique. L'incident a rapidement escaladé jusqu'au plus haut niveau gouvernemental avec échange de notes entre la Secrétaire d'État Hillary Clinton et son homologue chinois des affaires étrangères. David E. Sanger et David E. Sanger, « After Google's Stand on China, U.S. Treads Lightly », *The New York Times,* 14 janvier 2010.

des rares compagnies au Québec qui a ramené dans un même service les fonctions logique et physique de la sécurité. Après des années d'exercice et des succès en gestion, la distance entre les deux groupes demeure.

L'autre grande tendance identifiée en 2003 était l'arrivée sur le marché de produits et services de sécurité à destination du marché de la PME. Cette tendance a été confirmée grâce à l'action volontariste des grandes institutions de crédit : en imposant la norme PCI-DSS au commerce de détail, elles ont obligé les PME à prendre des mesures de sécurité homogènes à l'échelle de la planète – donc, au Québec.

Par contre, la nouvelle tendance lourde qui a fait irruption depuis 2003 est celle de la protection des données personnelles. Avant même l'arrivée d'Internet dans le grand public, la question des informations personnelles colligées dans des bases de données de plus en plus omniprésentes, avait alerté l'opinion publique. Or, voici que la vogue soudaine des sites sociaux appartenant à ce que l'on appelle le Web 2.0, a incité des centaines de millions d'internautes à publier des informations individuelles. On affiche sa vie privée, sa date de naissance, sa photo et celles de ses amis, le nom de son employeur et, pour faire bonne mesure, on annonce quand et où on part en vacances…

Pour un escroc informatique ou non, c'est une mine d'information qui ouvre la porte à toute une série de méfaits, depuis le cambriolage pur et simple du logement pendant un voyage annoncé jusqu'à toute une série de crimes informatiques comme le vol d'identité, le harcèlement, l'intimidation, etc. Un petit magazine français, *Le Tigre*, publie en novembre 2008 le portrait d'un jeune homme inconnu pris au hasard sur Internet à partir seulement des informations publiques trouvées dans le site de partage de photos Flickr et quelques autres sites sociaux, principalement Facebook. Toute y passe, la vie intime et professionnelle de l'inconnu surnommé Marc L***, ses petites amies et ses collègues de bureau (voir encadré). En quelques jours, les grands médias s'emparent de la nouvelle qui devient une affaire nationale, tandis que le principal intéressé s'efforce d'effacer les traces qu'il avait maladroitement laissées dans le cyberespace – en vain, bien sûr.

Portrait d'un inconnu

« Bon anniversaire, Marc (prénom d'emprunt). Le 5 décembre 2008, tu fêteras tes vingt-neuf ans. Tu permets qu'on se tutoie, Marc ? Tu ne me connais pas, c'est vrai. Mais moi, je te connais très bien. C'est sur toi qu'est tombée la (mal)chance d'être le premier portrait Google du *Tigre*. Une rubrique toute simple : on prend un anonyme et on raconte sa vie grâce à toutes les traces qu'il a laissées, volontairement ou non sur Internet. Comment ça, un message se cache derrière l'idée de cette rubrique ? Évidemment : l'idée qu'on ne fait pas vraiment attention aux informations privées disponibles sur Internet, et que, une fois synthétisées, elles prennent soudain un relief inquiétant…

Alors, Marc. Belle gueule, les cheveux mi-longs, le visage fin et de grands yeux curieux. Je parle de la photo prise au Starbuck's Café de Montréal, lors de ton voyage au Canada, avec Helena et Jose, le 5 août 2008. La soirée avait l'air sympa, comme d'ailleurs tout le week-end que vous avez passé à Vancouver. J'aime particulièrement cette série, parce que Jose a fait des photos, et ça me permet de te voir plus souvent. Vous avez loué un scooter, vous êtes allés au bord de la mer, mais vous ne vous êtes pas baignés, juste traîné sur la plage. En tout, tu as passé un mois au Canada. Au début tu étais seul, à l'hôtel Central, à Montréal (série de photos « autour de mon hôtel »). Tu étais là-bas pour le travail…

Donc à Montréal, tu étais dans un bureau avec Steven, Philipp, Peter, en train de travailler sur des plans d'architectes, devant deux ordinateurs, un fixe et un portable. En agrandissant la photo, on peut même voir que tu avais un portable Packard-Bell et que tu utilisais des pages de brouillon comme tapis de souris. Je n'ai pas dit que c'était passionnant, j'ai dit qu'on pouvait le voir. Le 21 août, c'est Steven qui t'a accompagné à l'aéroport. Retour en France, où t'attendait un mariage (Juliette et Dominique), puis, la semaine suivante, le baptême de ta nièce, Lola, la petite sœur de Luc (qui fait des têtes rigolotes avec ses grosses lunettes), à Libourne… »

Le portrait continue ainsi pendant deux pleines pages du magazine et on découvre la vie de Marc L*** et de sa petite amie Claudia R***, qui travaille au Centre culturel franco-autrichien de Bordeaux. Celle-ci, aux dires du journaliste, « est charmante, petits seins, cheveux courts, jolies jambes » – tout y est, même le numéro de téléphone mobile du principal intéressé.

Raphael Meltz, *Le Tigre*, numéro 28, novembre 2008 - http://le-tigre.net/Marc-L.html

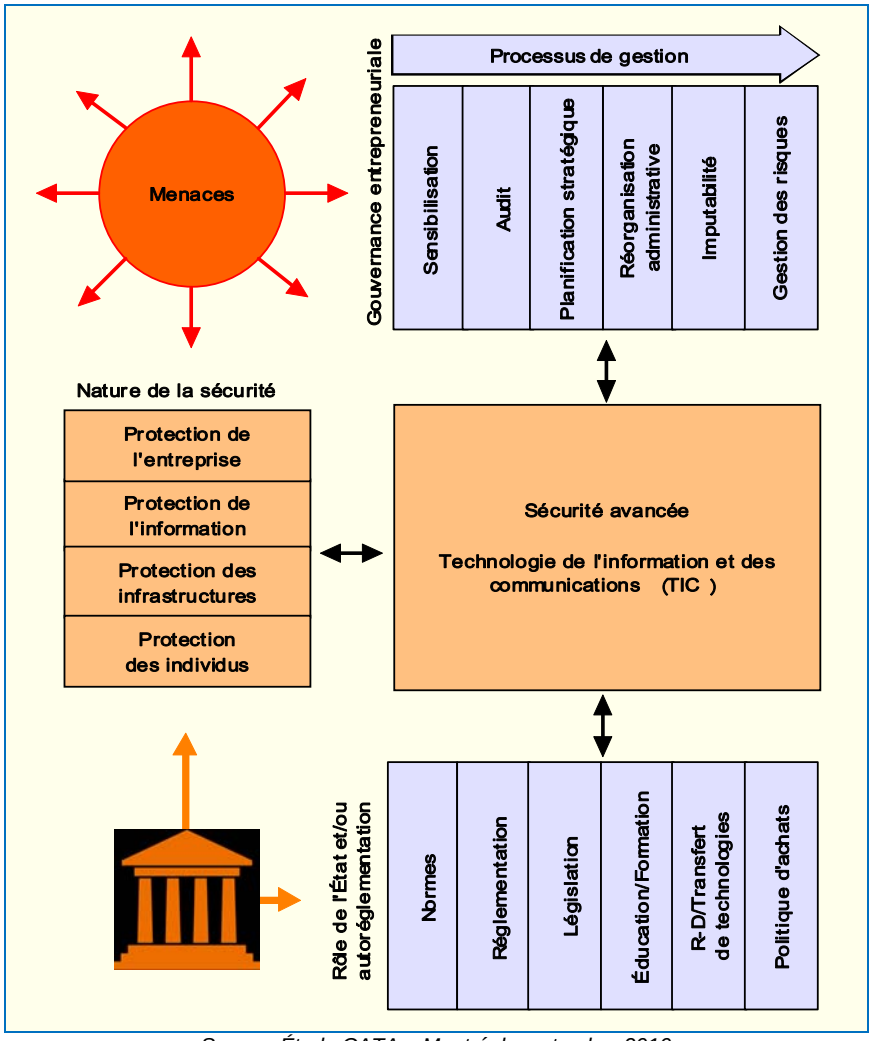
Au Canada seulement, plus de 11 000 personnes ont été victimes de vol d'identité en 2009, occasionnant près de 11 millions de dollars de pertes. Si le nombre de victimes demeure plus ou moins le même année

après année, le montant des pertes augmente sans cesse, passant de 6,5 millions de dollars en 2007 à 10,9 millions en 2009.[11]

Autre tendance lourde : le glissement progressif de la sécurité hors du champ de la seule technologie. La sécurité est avant tout une affaire de gestion de l'entreprise, et cela au plus haut niveau – de stratégie de gouvernance. En fait, dans sa préface à l'étude de 2003 de l'*Alliance* CATA, le regretté Robert Garigue[12] avait clairement annoncé le métamorphose de la sécurité :

> *La sécurité concerne la gestion globale de l'organisation. Elle demande à être traitée comme un enjeu d'affaires et non comme une simple question de technologie. Si nous acceptons ce postulat, il faut être prêt à affronter une série de conséquences qui modifient du tout au tout notre façon de travailler, et même de vivre.*

FIGURE 2 - L'ENVIRONNEMENT D'AFFAIRES DE LA SÉCURITÉ AVANCÉE



Source: Étude CATA – Montréal, septembre 2010

[11] Les sommes d'argent perdues signalées par les victimes de vol d'identité au Canada sont passées de très exactement 6 467 387,75 $ en 2007 à 10 882 279,04 $ en 2009, selon le Groupe de l'analyse des renseignements criminels du Centre antifraude du Canada (CAFC), aussi appelé *PhoneBusters*. « Activités de fraude en marketing de masse et de vol d'identité », Rapport statistique annuel 2009, 27 pages. Cf. p. 6.

[12] Robert Garigue (1952-2007) a commencé sa carrière dans les forces armées canadiennes où il est devenu un des théoriciens à l'origine du concept de cyberguerre. Sous-ministre adjoint au bureau des TIC du gouvernement du Manitoba, puis vice-président et chef de la sécurité successivement à la Banque de Montréal et à Bell Canada, il a soutenu en 2005 une thèse de doctorat à l'Université Carleton sur l'interopérabilité des données. Il est mort à Montréal à l'âge de 55 ans.

[13] Robert Garigue, « Perspective du la sécurité avancée », La sécurité avancée : Québec 2003, Alliance CATA, p. v.

Tous les indicateurs montrent que la sécurité déborde du cadre de l'exploitation des TIC pour être redéfinie comme une fonction de gestion. Ce faisant, la place qu'occupe la sécurité dans les entreprises change, se veut plus stratégique et se rapproche de la haute-direction et du conseil d'administration. Parallèlement, la place de l'État en matière de sécurité continue de croître ou plutôt devrait continuer de croître, car le Canada semble paradoxalement frappé d'indécision : après des années d'attente, le gouvernement fédéral a enfin déposé en octobre 2010 une Stratégie de cybersécurité, mais celle-ci demeure timide.[14]

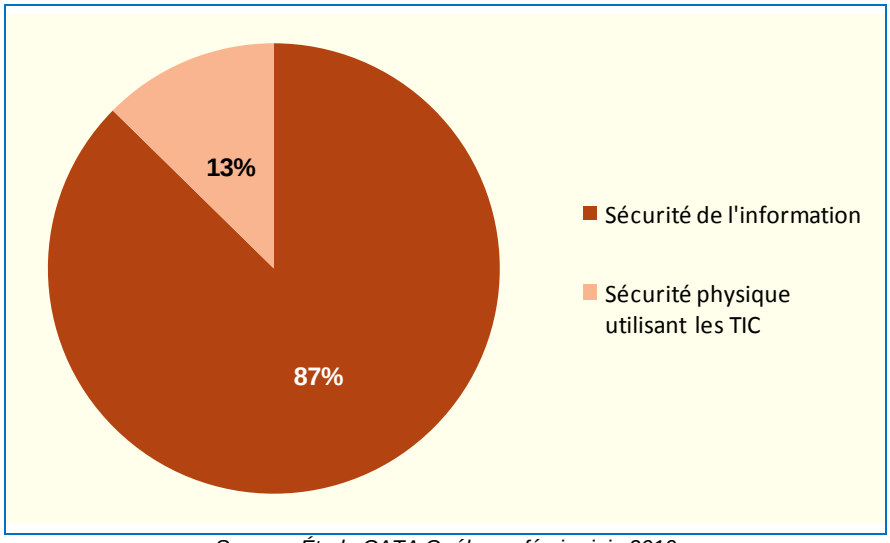
> Tous les gouvernements des pays du G8 participent activement aux associations de sécurité du domaine aéronautique. Seul le Canada ne le fait pas. C'est dommage parce que non seulement sa présence contribuerait à renforcer la sécurité au Canada, mais cela permettrait aussi de mettre en évidence les compagnies canadiennes qui travaillent dans le secteur.
> Patrick Patterson, Carillon Information Security

2.2 Qu'est-ce que la « sécurité avancée » ?

L'expression « sécurité avancée » englobe les firmes œuvrant dans la sécurité de l'information ainsi que celles qui utilisent les technologies de l'information et de la communication (TIC) en sécurité. Cela exclut, d'une part, la défense et, d'autre part, les détectives privés, les agents de sécurité, les entreprises de blindage et de coffres-forts, le convoyage de fonds, etc.

Ainsi, 87% des répondants sont des entreprises issues du domaine de la sécurité de l'information, tandis que 13% utilisent des solutions de TIC dans des dispositifs physiques.

FIGURE 3 - QU'ENTENDONS-NOUS PAR SÉCURITÉ AVANCÉE ?



Source : Étude CATA Québec – février-juin 2010

Un exemple typique de ces dernières est fourni par Genetec qui a été un pionnier des systèmes de sécurité intégrés sur réseau IP. Aujourd'hui, Genetec offre des solutions de vidéosurveillance sur IP, de contrôle d'accès et enfin de reconnaissance automatique de plaques d'immatriculation. Comme on le voit, la solution intègre la sécurité physique et les TIC et son support est Internet.

Toute définition est arbitraire. C'est ainsi qu'il y a des zones de chevauchement entre les solutions de défense et celles de sécurité avancée. Le domaine de la sécurité publique (qui recouvre le domaine des infrastructures publiques et des intervenants de première ligne) est au point de rencontre entre l'industrie de la défense et celui de la sécurité.

[14] La nouvelle politique gouvernementale précise le rôle des principaux intervenants gouvernementaux, affirme la nécessité de partenariats publics-privés et annonce une législation visant à responsabiliser le rôle des fournisseurs d'accès Internet (FAI). Stratégie de cybersécurité du Canada, 5 octobre 2010 - http://www.securitepublique.gc.ca/prg/em/cbr/ccss-scc-fra.aspx

D'une façon générale, il n'y a pas un domaine réservé à la sécurité physique et un autre à la sécurité de l'information ; on ne peut plus opposer les systèmes gouvernementaux aux systèmes commerciaux; non plus qu'on peut tracer une ligne nette entre ce qui relève de la défense et des applications civiles. Internet fait converger dans le cyberespace des industries auparavant distinctes. L'univers de la sécurité est entré en effervescence et il se redéfinit avec des frontières changeantes et parfois encore floues. Ce renouveau, toutefois, est uni par un solide fil conducteur : la numérisation de l'information.

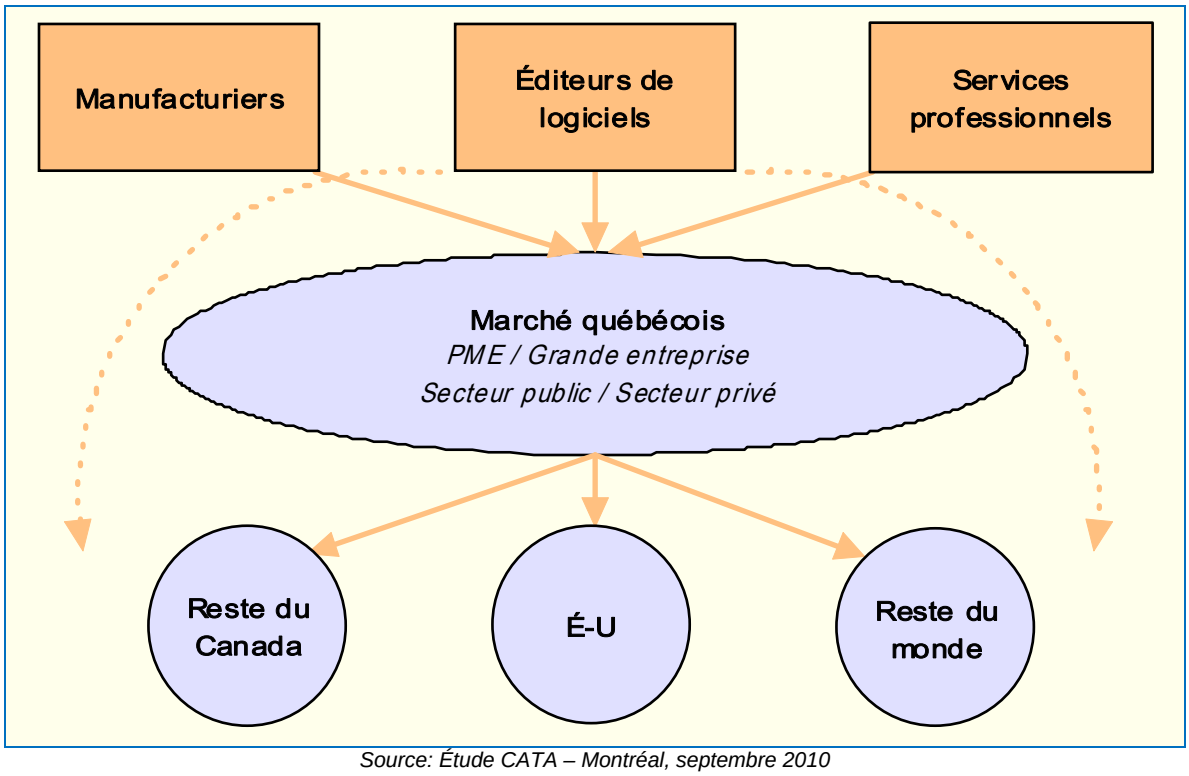
2.3 Objet et organisation de l'étude

L'étude de CATA Québec porte sur les fabricants de matériel, les éditeurs de logiciels aussi bien que sur les fournisseurs de services professionnels. Dans la pratique, les fabricants de matériel de sécurité sont toujours ou presque, aussi des éditeurs de logiciels, et tous deux fournissent généralement des services professionnels.

Par contre, les fournisseurs de services professionnels ont un comportement commercial distinct. Plusieurs d'entre eux se font une gloire de ne rien produire en matière de produits ou de logiciels : leur force est d'être technologiquement neutre. Ils peuvent ainsi accompagner en toute objectivité leurs clients dans leurs choix de plateformes technologiques.

Les sociétés de services professionnels ont généralement un grand degré d'intimité avec leurs clients, ce qui limite leur « exportabilité ». Le savoir-faire de leurs employés est leur « matière première » : elles vendent du temps-personne. Pour exporter, elles doivent donc essaimer hors Québec et dans la grande majorité des cas embaucher du personnel local. Quand CGI crée un groupe de sécurité à Ottawa ou à Toronto, elle embauche du personnel ontarien. Mais alors, peut-on encore parler d'exportation hors Québec ?

FIGURE 4 - STRUCTURE DE L'INDUSTRIE DE LA SÉCURITÉ AVANCÉE



Source: Étude CATA – Montréal, septembre 2010

À l'inverse, les grandes sociétés de services professionnels comme Deloitte, KPMG ou PricewaterhouseCoopers (PwC) ouvrent un bureau au Québec, elles embauchent du personnel québécois qui vend un savoir-faire québécois. Sont-elles encore des sociétés étrangères ?

Une attention spéciale a été portée aux marchés desservis par les entreprises de sécurité avancée : en fonction de la taille des clients (grande entreprise ou PME), des secteurs verticaux (gouvernement, finance, transport, commerce, etc.), ainsi bien sûr que du lieu d'expédition (Québec, reste du Canada, États-Unis, reste du monde).

Le sondage effectué par l'équipe ScienceTech entre février et juin 2010 est la source principale (mais pas exclusive) des chapitres 4 et 5 de cette étude. Dans la mesure du possible, nous avons établi une démarcation visible entre l'exposition des résultats et leur analyse.

Chapitre 3 : Profil de l'industrie
Ce chapitre trace le portrait des entreprises de sécurité avancée. Où sont-elles situées géographiquement ? Quels sont leur taille, leur âge, leurs structures ? Sont-elles des entreprises spécialisées qui ne font que de la sécurité (des *pure players*) ou ont-elles des activités multiples ? Une attention spéciale a été accordée à l'impact de la crise financière sur les entreprises.
Chapitre 4 : État du marché
Qui sont les clients des entreprises de sécurité avancée : grandes ou petites entreprises ? Dans quels domaines sont-ils situés : finance, transport aérien ou routier, commerce de détail, forces de police et autres intervenants de première ligne, etc ? Comment évoluent les marchés ?
Chapitre 5 : Exportations et stratégie de croissance
Où les entreprises québécoises vendent-elles leurs biens et services ? Les marchés canadiens aussi bien qu'internationaux sont examinés. On ne cherche pas seulement à savoir où vont les expéditions hors Québec, mais aussi quels sont les atouts de nos entreprises et les obstacles qu'elles rencontrent.
Chapitre 6 : Recherche et développement (R-D)
La R-D définit en grande partie la sécurité avancée. Ce chapitre a pour but d'évaluer l'intensité de la R-D dans chaque segment de l'industrie, la nature de cette R-D et ses objectifs : fait-on de la R-D pour créer des nouveaux produits, pour améliorer des produits existants ? Pour ouvrir de nouveaux marchés ?
Chapitre 7 : Financement
Le financement est au cœur du développement de toute entreprise. Ce chapitre examine les besoins des entreprises et les sources de financement.
Chapitre 8 : Les obstacles au développement de l'industrie
Chapitre subjectif par excellence, les entreprises identifient ici ce qui fait obstacle à leur développement : recrutement de personnel qualifié, protectionnisme américain, programmes gouvernementaux : tout y passe. Les enseignements de ce chapitre sont à la fois surprenants et révélateurs.
Chapitre 9 : Conclusion et pistes de réflexion
Un chapitre de conclusion porte sur les grands enjeux auxquels est confrontée l'industrie. Il se fonde à la fois sur les résultats du sondage et sur les interviews qualitatives effectuées par l'équipe de CATA Québec auprès des dirigeants de l'industrie.

Trois annexes complètent l'étude :
Annexe 1 : Les études de cas
Vingt études de cas mettent en évidence des modèles d'affaires très différents les uns des autres. Le choix des entreprises étudiées ne relève pas d'un classement ou d'un palmarès. Il s'agit d'instantanés sur des entreprises qui illustrent les pratiques et processus identifiés dans les chapitres précédents.
Annexe 2 : Version française du questionnaire utilisé pendant le sondage (une version anglaise a été utilisée pour les entreprises qui le demandaient ainsi que pour les entreprises hors Québec).
Annexe 3 : Sigles et acronymes utilisé dans l'étude.

2.4 Méthodologie

Le projet de sécurité avancée de CATA Québec comporte deux volets indissociables : identification et enquête sur le terrain.

Dans un premier temps, il a fallu recenser les entreprises de sécurité avancée. À partir du répertoire de 181 entreprises identifiées lors de l'étude de 2003, une mise à jour a été effectuée au moyen d'un rappel téléphonique systématique. Ce travail a été complété par le dépouillement des listes de participants aux principales expositions consacrées à la sécurité, ainsi que la consultation des annonceurs du magazine Sécus. Un premier groupe d'une centaine d'entreprises québécoises a alors été identifié.

L'Alliance CATA a également noué des alliances ponctuelles avec des associations spécialisées dans la sécurité :

- ✓ Canadian Information Processing Society (CIPS)
- ✓ Information Systems Audit and Control Association (ISACA)
- ✓ Association de Sécurité de l'information du Montréal Métropolitain (ASIMM)
- ✓ Société canadienne de la sûreté industrielle (SCRS)
- ✓ Institut pour la sécurité de l'information (ISIQ)[15]
- ✓ TechnoCompétences
- ✓ Association canadienne de la sécurité (CANASA)

Entre février et juin 2010, 167 entreprises québécoises faisant de la sécurité avancée ont été identifiées. Au même moment, une série d'interviews personnalisées a été menée, ce qui a donné lieu à 20 études de cas.

La population de base est passée de 181 en 2003 à 167 en 2010, soit une baisse de 8%. Que signifie cette évolution ? Quatre firmes sur les 10 qui avaient fait l'objet d'études de cas dans l'étude de 2003, ont disparu. Nous pensons à Dephy Technologies qui était à la fine pointe des instruments de détection des intrusions pour les douanes et les aéroports. Leur équipe était constituée presque uniquement de docteurs en informatique et en mathématiques de haute volée. Sign@metric avait mis au point un logiciel destiné à mesurer la commande cérébrale et la réponse neuromusculaire qui entrent en jeu lorsqu'une personne signe un document. Une technologie imparable pour dépister les fraudeurs. Disparue elle aussi.

Il s'agissait dans les deux cas d'entreprises qui avaient réussi une percée technologique et mis au point un produit remarquable. Dans les deux cas, l'autopsie du décès est facile à faire : la commercialisation n'a pas suivi l'avancée technologique. Toutefois, la disparition de quelques *start-ups* prometteuses par voie de faillite n'explique pas l'ensemble du phénomène de diminution du nombre d'entreprises. Il faut compter avec un mouvement vigoureux de fusions-acquisitions.

Malheureusement, dans la majorité des cas, les firmes québécoises sont achetées par des firmes américaines (le phénomène n'est pas propre au Québec, on le retrouve partout au Canada). Même quand les emplois restent au Québec, le pouvoir de décision s'en va. Il y a des exceptions: quand la québécoise Radialpoint achète ZeroKnowledge; ou encore, quand Dessau Soprin achète Elytra à Ottawa avec une bonne équipe de spécialistes en cryptographie.

Nous nous retrouvons donc en 2010 avec moins d'entreprises en sécurité avancée. L'industrie est plus concentrée.

* * *

L'étude sur la sécurité avancée au Québec est le fruit d'un effort collectif. Elle a été financée en partie par trois organismes, tant du secteur public – Agence de développement économique du Canada pour les régions du Québec (DEC) et le ministère du Développement Économique, de l'Innovation et de

[15] L'ISIQ a fermé ses portes le 1er juin 2010.

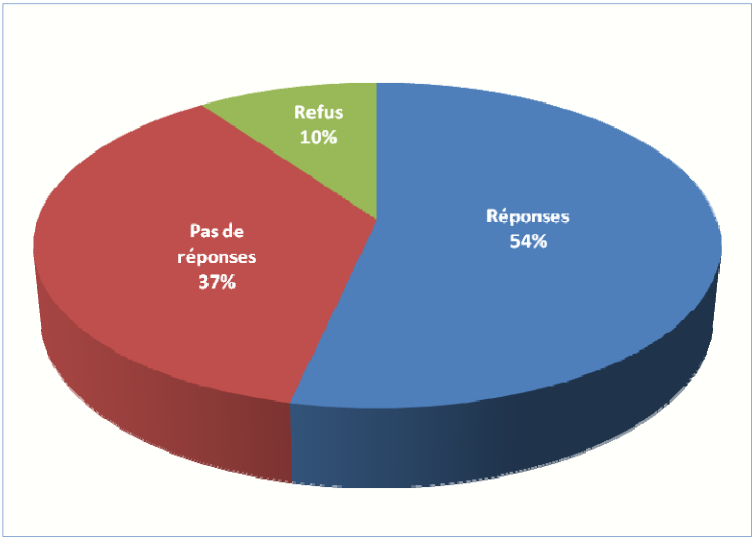
l'Exportation (MDEIE) - que du secteur associatif – Alliance canadienne des technologies avancées (*Alliance* CATA).

Lors de l'envoi des questionnaires, l'*Alliance* CATA a fait parvenir par courriel un questionnaire bilingue à toutes les entreprises identifiées et les associations ont fait de même avec leurs membres. Un suivi téléphonique a été systématiquement effectué (jusqu'à un maximum de trois rappels aux termes desquels l'entreprise était inscrite comme non répondante). Il en est résulté 90 réponses provenant aussi bien de la base de données actualisée de l'*Alliance* CATA que des associations.

Ces réponses ont été traitées de la façon suivante. Les réponses aux dix premières questions qui concernaient les coordonnées et les données générales des entreprises ont donné naissance à une base de données publique, qui sera affichée sur le site de CATA-Québec : http://www.cata.ca/Cata_Quebec/

Un sondage a également été mené auprès d'entreprises canadiennes de sécurité, ce qui a permis d'établir des comparaisons fort utiles pour le développement de l'industrie au Québec. Sur les 524 entreprises identifiées et contactées, 80 ont répondu. Aucun suivi téléphonique n'a été effectué.

FIGURE 5 - UN TAUX DE RÉPONSE ÉLEVÉ



Sondage	2003	2010
Réponses	50,3 %	53,9 %
Pas de réponse	45,3 %	36,5 %
Refus de répondre	4,4 %	9,6 %
Total	100 %	100 %

Source : Étude CATA Québec – février-juin 2010

2.5 La représentativité de l'échantillon d'entreprises

La vérification de la représentativité de l'échantillon d'entreprises ayant participé à l'étude (90 répondants) est faite par rapport à la base de données (167 entreprises) de CATA Québec décrite précédemment.

Nous avons comparé le pourcentage d'entreprises québécoises ayant participé à l'étude et celui que l'on retrouve dans la population canadienne. Pour cela, un test d'inférence (le test du Chi carré univarié : Xo) est effectué. Il permet alors de valider la représentativité de l'échantillon québécois en comparant celui-ci à la population totale. Ce test statistique permet de calculer une probabilité d'erreur d'échantillonnage, et le seuil d'erreur toléré est de 5 %.

	Pourcentages obtenus au Québec	
Québec (répondants)	90	53, 89 %*
Québec (non répondants)	77	46,11 %**
Total	167	

** Pourcentage des entreprises situées au Québec dans la base de données de CATA Québec qui ont répondus (90/167)*
*** Pourcentage des entreprises situées au Québec dans la base de données de CATA Québec qui n'ont pas répondus (77/167)*

Ho : Le pourcentage des entreprises situées dans l'échantillon est proche de celui de la population totale.

H1 : Le pourcentage des entreprises situées dans l'échantillon est très différent de celui de la population totale.

Calculer la statistique $Xo = [((90-77)-0,5)^2/77]^{½} = 1,424$
Fixer le seuil d'erreur à 5% c.-à-d. $Xo_{.05} = \mathbf{3,84}$
Rejeter Ho si Xo > 3,84

Dans ce cas, Xo = 1,424 < 3,84 => on accepte alors Ho. **Le pourcentage des entreprises situées au Québec dans l'échantillon des entreprises ayant participé à l'étude est proche de celui de la population totale québécoise.**

2.6 Équipe de réalisation et financement de l'étude

L'étude 2010 sur l'industrie de la sécurité avancée au Québec a été dirigée par Jean-Guy Rens, vice-président de l'Alliance canadienne pour les technologies avancées (CATA) et associé principal de ScienceTech Communications Inc., en collaboration avec Huguette Guilhaumon, associée principale de ScienceTech Communications Inc. L'équipe d'analystes était composée de Pierre Bess, d'E&B Tech Logique, ainsi que d'Ali El Azzouzi, de DataProtect (Casablanca, Maroc).

John Reid, président de l'*Alliance* CATA a supervisé le financement et l'administration de l'étude en collaboration avec Cathi Malette, directrice à la gestion.

2.7 Financement de l'étude

La constitution de la base de données et la réalisation de l'étude ont été financées dans la majeure partie par l'*Alliance* CATA, l'Agence de développement économique du Canada pour les régions du Québec (DEC) et le ministère du Développement Économique, de l'Innovation et de l'Exportation (MDEIE).

2.8 Remerciements

L'équipe de CATA Québec et de ScienceTech Communications tient à remercier tout particulièrement les personnes suivantes de leur collaboration, sans laquelle cette étude n'aurait pas vu le jour.

Bergeron, Éric	Président et chef de la direction, Optosecurity
Bois, Jules	Directeur exécutif secteur public Québec, IBM
Bolduc, Jocelyne	Conseillère en développement économique, Direction des technologies de l'information et des communications, ministère du Développement Économique, de l'Innovation et de l'Exportation (MEIE)
Chouinard, Mathieu	Président d'In Fidem
Dicaire, Benoit	Président, Infrax inc.
Dion, Marcel	Président et chef de la direction, Above Security
Doyon, Patrick	Directeur du marketing, Forensic
Estrela, Marco	Vice-président ventes et marketing, Gardien Virtuel
Fournier, Marc	Partenaire associé, PriceWaterhouseCoopers
Galarneau, Pierre	Institut national d'optique (INO)
Langlois, Guillaume	Directeur exécutif associé, Nurun
Meehan, François	Président, Cedval
Olivier, Véronique	Présidente, Waveroad Consult
Patterson, Patrick	Président, Carillon Information Security
Petrogiannis, Tommy	Président Silanis
Piché, Mario	Conseiller, Direction Développement d'affaires et du nord, Développement économique Canada (DEC)
Poellhuber, David	Directeur et chef de la direction, Zérospam
Reverd, Christophe	Président d'Auditia
Talbot, Éric	Président et co-propriétaire, S.I.C. Biometrique
Tremblay, Charles	Directeur commercial, Notarius
Vézina, Guy	Directeur général, RDDC Valcartier

Nous sommes particulièrement redevables aux personnes œuvrant dans le mouvement associatif. L'industrie de la sécurité est représentée par plusieurs associations qui n'ont pas hésité à nous donner

accès à leurs membres pour distribuer le questionnaire du sondage et à faire la promotion de l'étude. Depuis la confection du questionnaire jusqu'à l'analyse des réponses, leur apport a été précieux.

Gagnon, Sylvie	Présidente, TechnoCompétences
Pepin, François	Président, Information Systems Audit and Control Association (ISACA)
Boutin, Michel	Président, Association de la sécurité de l'information du Montréal métropolitain (ASIMM)
Marrette, Bob	Directeur exécutif, Canadian Society for Industrial Security (CSIS Inc)
Lane, Greg	Président, Canadian Information Processing Society (CIPS)
Edmond, Mona	Directrice du marketing, Canadian Security Association, CANASA
Christian, Martin	Institut québécois de la sécurité de l'information (a aujourd'hui cessé ses activités)

Avertissement :

L'Alliance CATA et l'équipe de ScienceTech assument la responsabilité de toute erreur qui se serait glissée dans l'étude sur l'industrie de la sécurité avancée au Québec. Les nombreuses personnes qui ont généreusement collaboré à ce projet, non plus que les partenaires et les clients qui nous ont fait confiance, ne sauraient en aucun cas être tenus responsables du contenu de l'étude.

3. Profil de l'industrie

3.1 Âge des entreprises

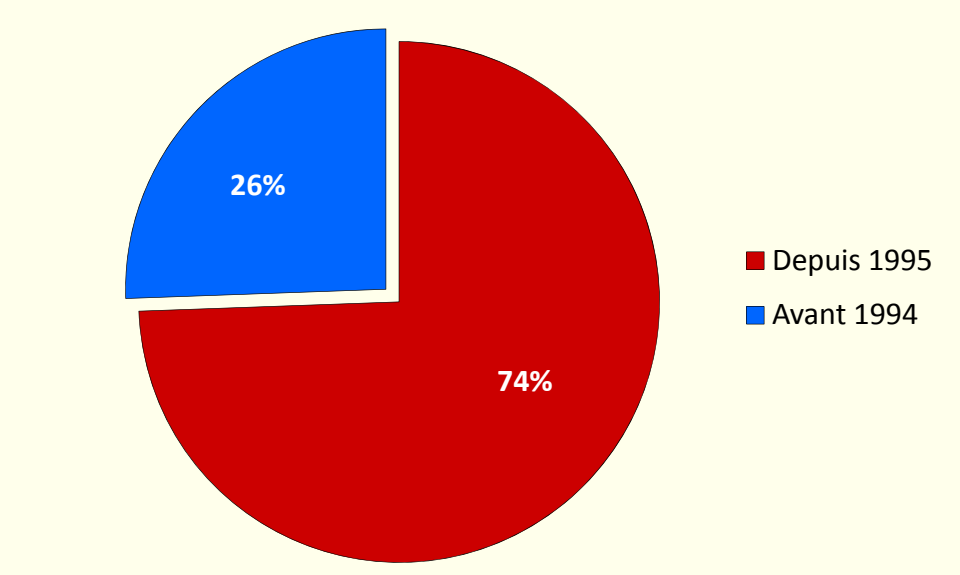
L'analyse de la structure de l'industrie fait ressortir que les entreprises de sécurité avancée sont jeunes. La majorité d'entre elles ont été créées après 1995, première année où Internet fait sentir son impact sur l'économie.

Internet a affecté la sécurité informatique, comme il était prévisible, mais aussi, la sécurité physique (on relie les caméras de vidéosurveillance à une centrale de contrôle).

Il faut aussi considérer le double impact d'Internet :
- d'une part, le réseau sert à la gestion de la sécurité (vidéosurveillance);
- d'autre part, il génère une vulnérabilité nouvelle (crime informatique).

FIGURE 6 - LES ¾ DES FIRMES DE SÉCURITÉ SONT DES ENFANTS D'INTERNET

En quelle année votre entreprise a-t-elle été créée ?



Source : Étude CATA Québec – février-juin 2010

3.2 Taille et nature des entreprises de sécurité avancée

A - L'entreprise et l'équipe

Tout d'abord, il convient de distinguer deux notions différentes : la taille des entreprises qui font de la sécurité avancée et la taille des équipes de spécialistes en sécurité. En effet, un spécialiste de sécurité d'IBM au Québec peut bien fonctionner dans une petite équipe d'une dizaine de personnes, son environnement de travail ne saurait se comparer avec celui d'une entreprise comme idMouse à Longueuil, par exemple, qui compte aussi une dizaine de personnes.

En effet, l'équipe québécoise de sécurité d'IBM s'intègre dans une entreprise qui compte 5 500 employés au Québec, 22 000 au Canada, 398 000 dans le monde… Il peut compter sur un réseau de 4 500 professionnels en sécurité répartis dans le monde. Les dix employés d'idMouse ne peuvent compter que sur leurs propres ressources pour innover, trouver de nouveaux clients, vendre et… boucler les fins de mois. Nous sommes en présence de deux mondes.

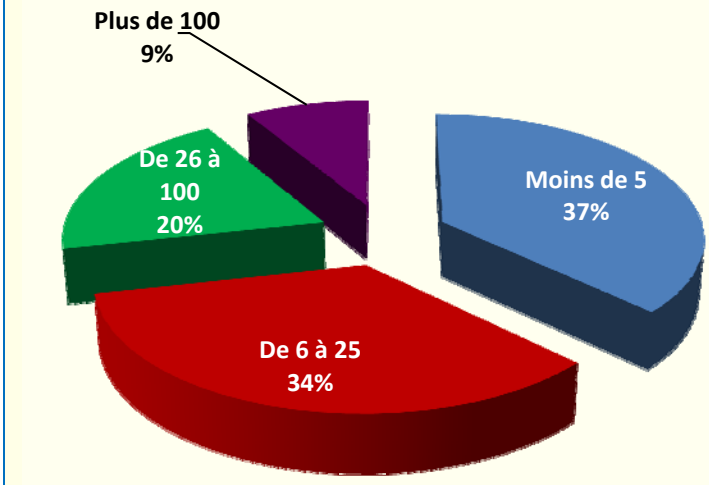
Le fait majeur qui se dégage de l'industrie de la sécurité est la petite taille des entreprises et des équipes. La très grande majorité des entreprises (71%) compte moins de 25 employés (figure 7 a). Si l'on tient compte des seuls employés affectés à la sécurité, cette proportion grimpe à 78% (figure 7 b). La sécurité est donc affaire de très petites équipes qui travaillent dans de très petites entreprises.

Il y a beaucoup plus de consultants et de microfirmes au Québec qu'au Canada. Cela s'explique par les mise-à-pied nombreuses dans les TI au cours des dernières années. Spécialistes et ingénieurs ont opté pour la consultation.
Marc Fournier, Price Waterhouse Coopers

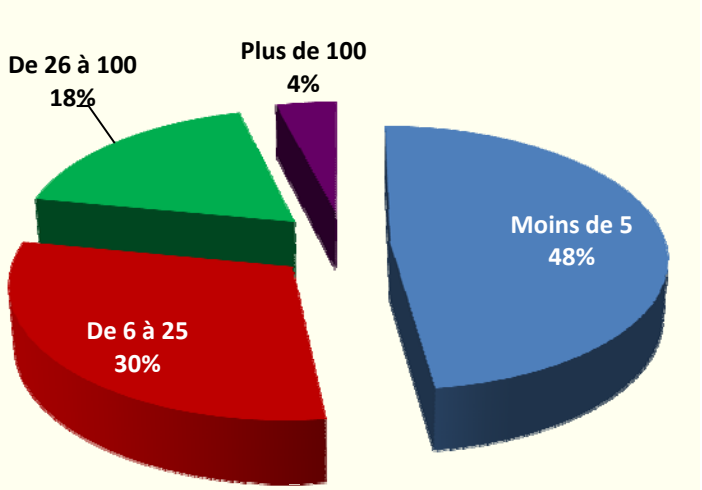
FIGURE 7 - TAILLE DE L'ENTREPRISE ET TAILLE DE L'ÉQUIPE

Combien d'employés travaillent actuellement à temps plein dans votre entreprise ?

7 a – Taille de l'entreprise en général



7b – Taille de l'équipe de sécurité

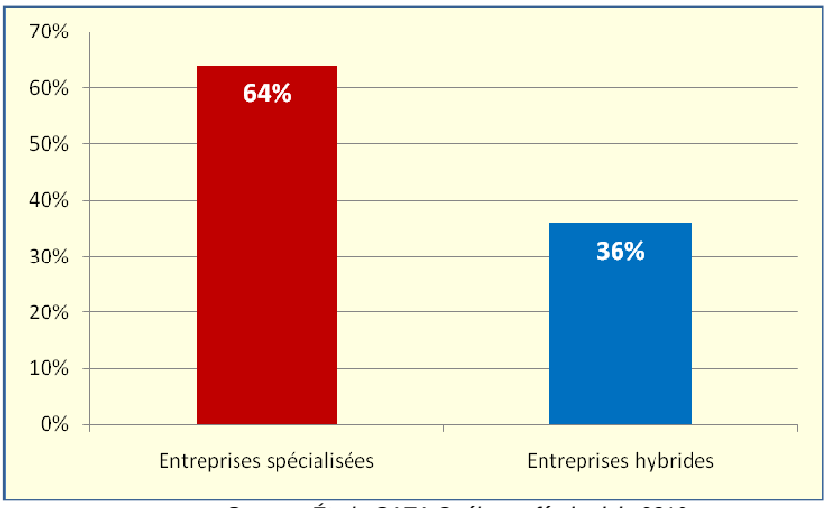


Source : Étude CATA Québec – février-juin 2010

B - Entreprise hybride et entreprise spécialisée

Parmi les entreprises de sécurité, il y a bien plus d'entreprises spécialisées que d'entreprises qui ont des activités diversifiées en TIC (64% de spécialistes pour 36% d'hybrides). Mais cette façon de compter ne rend pas compte de la réalité sur le terrain. Les grosses équipes de sécurité appartiennent toutes à des compagnies hybrides qui tirent moins de 1% de leur chiffre d'affaires du domaine de la sécurité (Bell, CGI, PwC). À l'inverse, les entreprises homogènes sont toutes des PME, aucune n'atteint 100 employés et la plus grande d'entre elles a 70 employés (Silanis Technology).

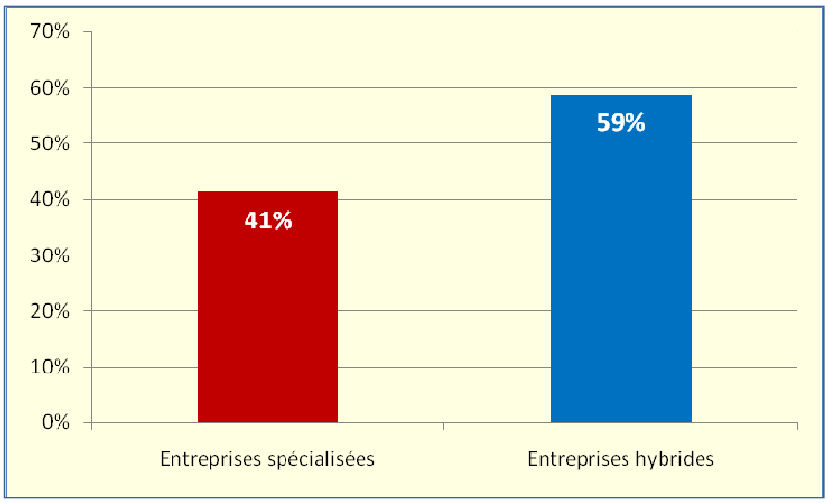
FIGURE 8 - IL Y A PLUS D'ENTREPRISES SPÉCIALISÉES QUE D'ENTREPRISES HYBRIDES…



Source : Étude CATA Québec – février-juin 2010

Plus des deux-tiers des experts en sécurité se retrouvent donc dans des entreprises hybrides. Cela signifie que les entreprises spécialisées sont avant tout des PME et des micro-entreprises, tandis que les entreprises hybrides sont des grandes entreprises. Celles-ci sont de deux types : celles qui déploient des grands services de sécurité (Bell, CGI et PwC) ; ou encore, celles qui déploient des petites équipes de sécurité adossées sur une expertise multidisciplinaire et internationale (IBM Canada, DMR-Fujitsu, Nurun).

FIGURE 9 - … MAIS LES EMPLOIS DE SÉCURITÉ SE TROUVENT DANS LES ENTREPRISES HYBRIDES



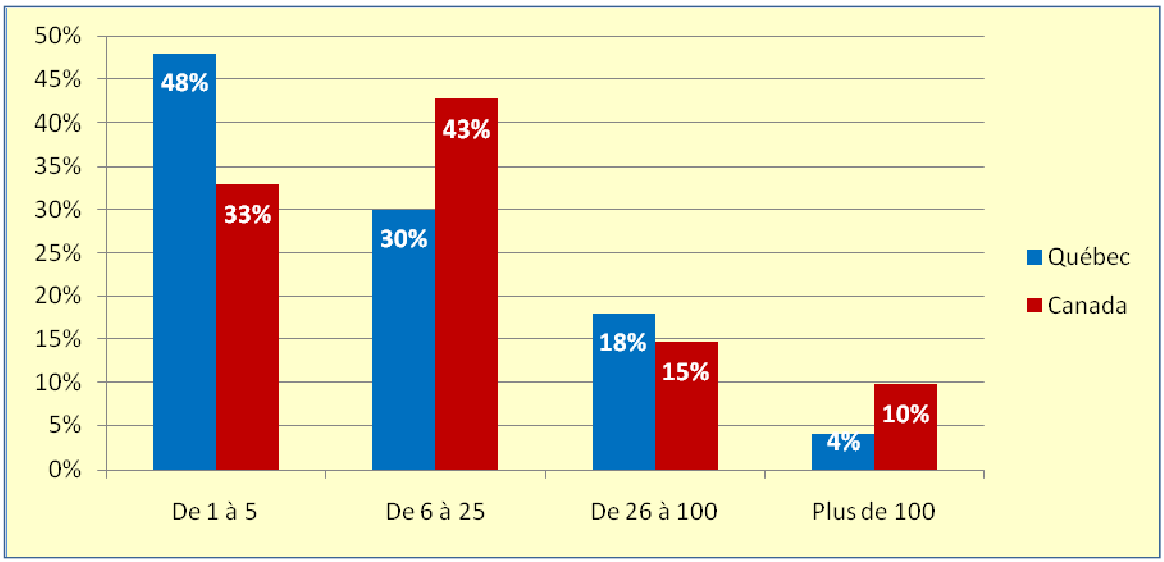
Source : Étude CATA Québec – février-juin 2010

Analyse comparative

Ce qui distingue le Québec du reste du Canada est le grand nombre de micro-entreprises (il y a 9 % de plus de micro-entreprises de un à cinq employés au Québec qu'au Canada) et l'absence de grande entreprise de sécurité au Québec – il y a bien l'exception de Silanis, mais ce n'est pas encore une grande entreprise, même si elle a vocation de le devenir et en a plusieurs des caractéristiques.

Hors Québec, il y a des grandes entreprises en sécurité, comme Entrust, Certicom ou Marsh Networks qui sont spécialisées en sécurité et ont atteint la taille critique – sans compter les grandes entreprises hybrides qui sont aussi présentes au Québec (Deloitte, CGI, IBM Canada…).

FIGURE 10 - LE RESTE DU CANADA A PLUS DE GRANDES ENTREPRISES



Source : Étude CATA Québec – février-juin 2010

La seule façon d'augmenter le nombre de nos employés serait de percer hors-Québec. Pour cela, il faut des revenus et nos ventes au Québec ne nous permettent pas d'accumuler de surplus.

David Poellhuber, Zerospam

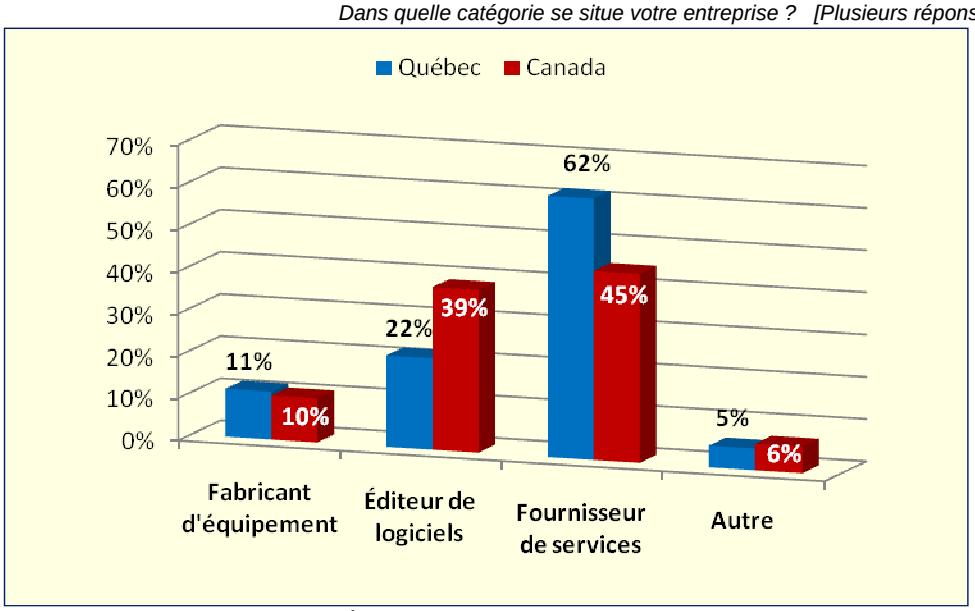
C – Grandes catégories d'activités

L'industrie québécoise de la sécurité avancée est dominée par les fournisseurs de services : près des deux-tiers des répondants. Cette hypertrophie du secteur des services professionnels est un signe d'autant plus significatif que les éditeurs de logiciels sont réduits à la portion congrue : 21% des répondants.

Par rapport à 2003, au Québec, le nombre de fournisseurs de services a augmenté passant de 51% à 61%. Le nombre d'éditeurs de logiciels a légèrement diminué passant de 25% à 21% et le nombre de fabricants d'équipements a chuté de 50%, passant de 24% à 12%.

FIGURE 11 - NATURE DES ACTIVITÉS DE L'ENTREPRISE

Dans quelle catégorie se situe votre entreprise ? [Plusieurs réponses possibles.]



Source : Étude CATA Québec – février-juin 2010

Analyse comparative

Le reste du Canada, à savoir principalement l'Ontario, possède un solide noyau d'éditeurs de logiciels : presque deux fois plus qu'au Québec. Outre les firmes bien connues comme Entrust et Certicom, il faut aussi penser à l'écosystème de PME innovantes créé par Research in Motion (RIM) pour assurer la sécurité du Blackberry et de ses serveurs. Il y a là un moteur qui alimente la demande pour toujours plus d'innovation, toujours plus de valeur.

Analyse

C'est la partie créatrice de l'industrie québécoise de la sécurité avancée qui semble en panne. Non pas que les services professionnels ne créent pas de valeur. Améliorer les processus, réduire le gaspillage et les frais d'exploitation en adoptant des pratiques plus efficaces, stimuler les profits en augmentant la capacité de production ou en exploitant de nouveaux marchés : tout cela crée de la valeur.

Mais le mode de fonctionnement d'une firme de services professionnels est contractuel. La société vend son expertise en fonction du temps de travail de ses ressources humaines. Au contraire, un éditeur de logiciel ou un fabricant d'équipement procède en deux temps : il investit d'abord (infrastructures et R-D) et il commercialise ensuite ses produits.

Ce processus en deux temps permet aux éditeurs de logiciel et aux manufacturiers de dissocier les profits du temps de travail. Si la R-D demeure encore largement tributaire du temps de travail, les activités de marketing et de vente ne le sont pas ou peu. Dès lors, que l'innovation corresponde à un besoin du marché et que le marketing soit efficace, l'éditeur de logiciel ou le manufacturier entre alors dans une phase de création de valeur pure.

À titre de référence, on peut dire qu'au Québec l'industrie voisine du multimédia est entrée dans ce cercle vertueux de la création de valeur pure. L'industrie de la sécurité avancée non.

D – Détail des activités

De nombreuses entreprises ont répondu au sondage en indiquant qu'elles couvraient toute la gamme des activités de sécurité. Il s'agit principalement des fournisseurs de services professionnels dont la raison d'être est d'offrir une gamme aussi élargie que possible de services de sécurité. Certaines firmes affichent toutefois une spécialité en cryptographie, en biométrie, en systèmes de relève ou en surveillance IP, mais elles constituent l'exception. Les fournisseurs de services sont des conseillers en gestion ou des conseillers en TIC et ils offrent de plus en plus des services d'impartition, sans doute en raison de la difficulté qu'éprouvent les organisations clientes à gérer cette activité.

Toute autre est la situation des éditeurs de logiciels et les fabricants d'équipement qui d'ailleurs sont souvent les mêmes entreprises : à la fois éditeurs et fabricants. Comme en 2003, l'authentification est l'activité de choix de l'industrie québécoise. Il convient toutefois de noter que cette activité recouvre toute une gamme de technologies, comme la biométrie, la cryptographie ou les cartes à puce.

La surveillance IP est également populaire et une nouvelle activité fait son entrée : la sécurité mobile. Il est à noter que certaines entreprises sont principalement orientées vers les logiciels et produits reliés à la défense. Toutefois, elles diversifient leur offre en direction de la sécurité civile par le truchement des applications destinées aux intervenants de première ligne, dont les besoins sont voisins de ceux de la défense. Nous pensons particulièrement aux logiciels de détection optique.

Il convient de souligner la fréquence des activités de formation, tant parmi les fournisseurs de service que parmi les éditeurs de logiciels et fabricants d'équipement. Est-ce un signe du désarroi éprouvé par le marché devant le phénomène de la sécurité? Pour vendre des services de sécurité, il faut non seulement sensibiliser les clients, il faut les former.

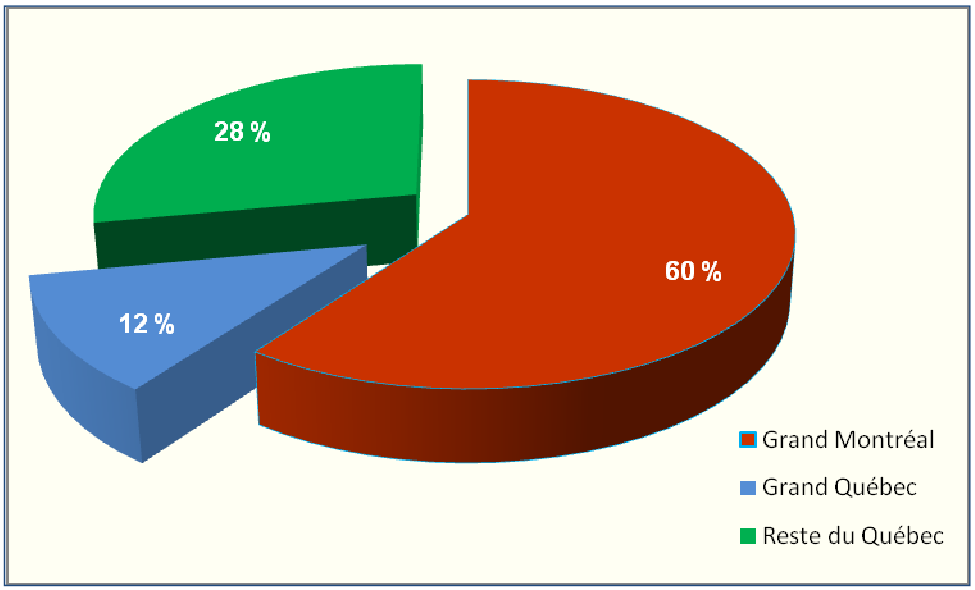
En outre, les questions de sécurité informatique renvoient de plus en plus à des processus complexes de gestion et de gouvernance. La législation et la réglementation sur la protection des renseignements personnels sont en évolution constante. Il en résulte que sécurité et formation vont de pair.

3.3 Une industrie très centralisée

Au Québec l'industrie de la sécurité avancée compte un pôle stratégique à Montréal (100 sociétés) et un pôle secondaire à Québec (20 sociétés).

- Ensemble, les deux pôles réunissent plus de 80% des entreprises québécoises de sécurité avancée.

FIGURE 12 - LA LOCALISATION DES ENTREPRISES QUÉBÉCOISES DE SÉCURITÉ AVANCÉE [16]



Source : Étude CATA Québec – février-juin 2010

Analyse

Comme en 2003, l'industrie de la sécurité est urbaine et située dans le sillage des grandes entreprises et des gouvernements. Les rares joueurs situés hors Montréal et hors Québec sont des travailleurs indépendants ou des micro-entreprises.

Les pôles stratégiques ont une importance nationale et internationale, c'est là où on trouve les grands joueurs.

Analyse comparative

Le cœur de l'industrie canadienne de la sécurité est l'Ontario qui compte 298 entreprises, soit près de 49% de l'ensemble de l'industrie – contre 167 au Québec –, soit 27% de l'industrie (voir figure 13). D'une façon générale, on peut dire que la situation est comparable à celle qui prévalait en 2003.

Le mouvement de rationalisation et de concentration de l'industrie semble se retrouver dans toutes les régions du pays (le nombre d'entreprises canadiennes a diminué de 12,5% entre 2003 et 2010).

La force de l'Ontario dans le domaine de la sécurité s'explique par la présence de deux pôles stratégiques sur son territoire : Toronto et Ottawa (voir figure 14).

La sécurité électronique

Le Forum économique mondial situe le Canada au troisième rang mondial pour le nombre de serveurs Internet sécurisés par habitant. Le marché du logiciel de sécurité est celui qui connaît la croissance la plus rapide au Canada. Sa valeur était estimée à plus de 300 millions de dollars en 2006, et sa croissance annuelle était de 12,1 %. On prévoyait alors que les dépenses reliées à la sécurité connaîtraient une croissance annuelle composée de 10,75 % au cours des cinq années suivantes pour atteindre une valeur de 440 millions de dollars en 2010.

Vincent Butaye, Agence wallonne à l'exportation et aux investissements étrangers, mai 2010.

[16] Par Grand Montréal, nous comprenons les 48 municipalités membres de la Communauté métropolitaine de Montréal; le Grand Québec renvoie aux 28 municipalités membres de la Communauté métropolitaine de Québec (CMQ).

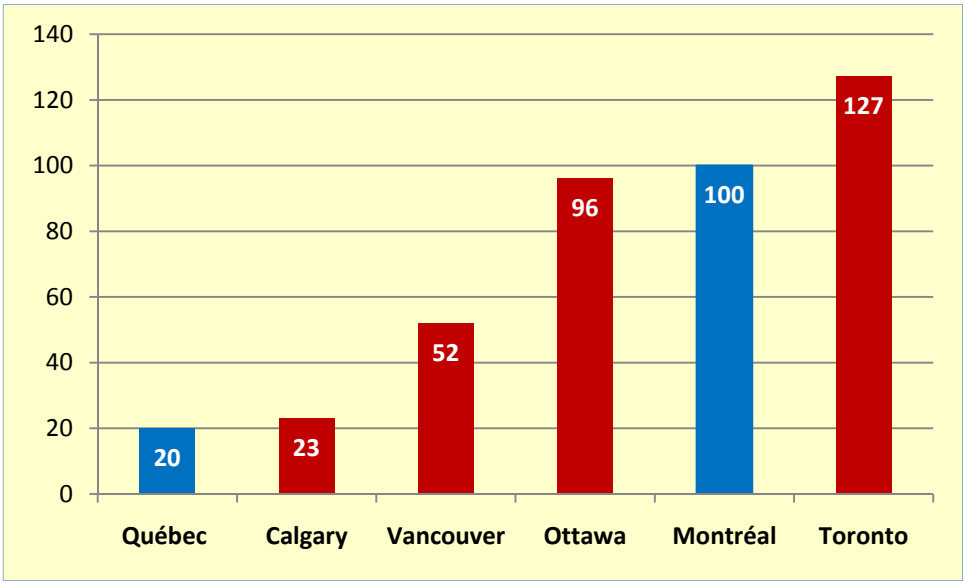
FIGURE 13 - LA PLACE DU QUÉBEC DANS L'ENSEMBLE CANADIEN

Régions	2003		2010	
	Sociétés	%	Sociétés	%
Ontario	342	49,0	298	48,8
Québec	181	25,9	167	27,3
Colombie britannique	72	10,3	61	10,0
Prairie	66	9,5	52	8,5
Atlantique	37	5,3	30	4,9
Canada (y compris le Québec)	698	100	611	100

Source : Étude CATA Québec – février-juin 2010

Montréal est en concurrence avec Toronto et Ottawa. Ces trois villes ont atteint une masse critique qui leur assure un avenir dans cette industrie. Par ailleurs, Montréal doit aussi affronter la concurrence de Québec qui confirme sa situation de pôle secondaire.

FIGURE 14 - LES PÔLES DE SÉCURITÉ DANS L'ENSEMBLE CANADIEN [17]



Source : Étude CATA Québec – février-juin 2010

3.4 Place des femmes dans l'industrie

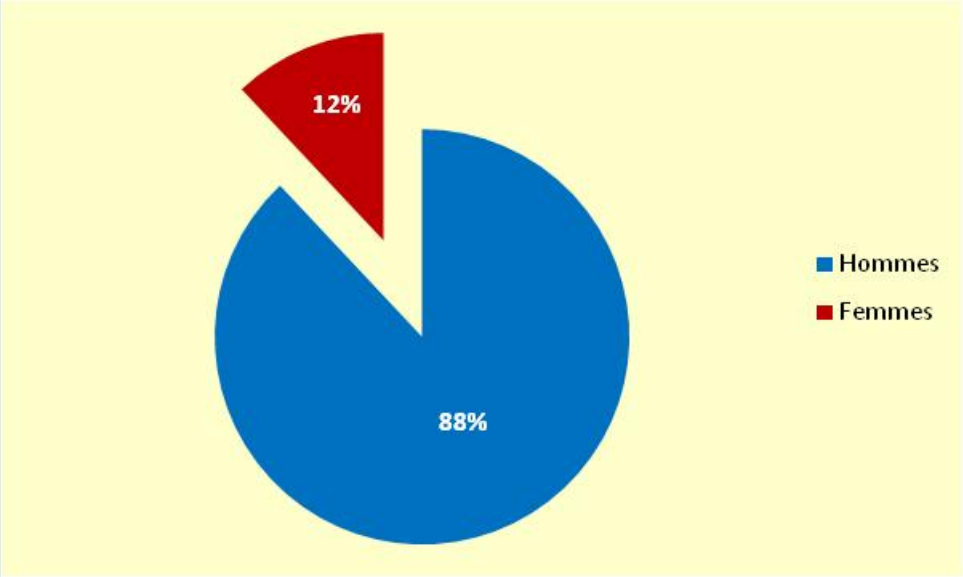
Avec 12% des emplois, les femmes sont presque absentes de l'industrie québécoise de la sécurité avancée. La situation est comparable dans le reste du Canada où l'étude permet d'identifier 10% de femmes dans le secteur des TIC.

Cependant, le sous-secteur de la sécurité avancée n'est pas homogène. Plus de la moitié des expertes en sécurité se retrouvent dans les entreprises de 100 employés ou plus. À l'autre extrémité de l'échelle, nous n'avons identifié presque aucune femme parmi les consultants ou travailleurs autonomes.

[17] Tous les chiffres réfèrent à la communauté urbaine de ces villes. Ainsi Toronto comprend les 25 municipalités membres du *Greater Toronto Area*; Montréal les 48 municipalités membres de la Communauté métropolitaine de Montréal; Ottawa les 11 municipalités qui ont été fusionnées en 2001, Vancouver les 21 municipalités de Vancouver Metro et Québec les 28 municipalités membres de la Communauté métropolitaine de Québec (CMQ). Seule Calgary a été considérée comme un tout indépendant.

FIGURE 15 - FAIBLE REPRÉSENTATION DES FEMMES

Combien de femmes y a-t-il parmi les employés spécialisés en sécurité ?



Source : Étude CATA Québec – février-juin 2010

Analyse

Il est connu que les femmes sont sous-représentées dans les TIC en général. En témoigne, le CEFRIO qui estime que la représentation des femmes est de 30% dans le domaine des TIC et moins encore s'il s'agit d'un poste de direction.[18] Mais que dire alors de la sécurité avancée qui n'attire que 10 à 12% de femmes dans ses rangs?

Toutes les analyses effectuées au sujet des femmes dans un environnement de TIC sont certainement valables pour la sécurité. Mais comment expliquer le rejet franc et massif que trahissent les données relevées dans cette étude? Il semble qu'il soit plus facile d'intéresser les femmes à devenir policières qu'à travailler dans la sécurité informatique. Les États-Unis comptent 100 000 femmes chargées du maintien de l'ordre, soit 12% de l'ensemble des services. Leur proportion s'élève à 25% dans les agences fédérales et dans les corps policiers des principaux centres urbains.[19]

Or, comme on l'a observé ci-dessus (3.3 – Une industrie très centralisée), les firmes de sécurité avancée sont pour la plupart situées dans les centres urbains. Le taux d'emploi féminin de l'industrie de la sécurité avancée (10 à 12%) doit donc se comparer avec celle des forces de polices des grands centres (25%).

Cette comparaison indique que l'aspect « répressif » n'est pas à l'origine de la désaffection des femmes vis-à-vis la sécurité avancée. Il faut sans doute rechercher les causes dans la structure même de l'emploi comme, par exemple, le manque de sécurité, les horaires contraignants, ou encore dans la culture de l'industrie des TIC. Est-ce que cette situation changera au fur et à mesure que la sécurité échappe aux TIC et se rapproche des services professionnels?

[18] *«La contribution des femmes aux TIC»*, Présentation faite dans le cadre de la 100e activité des MSG, CEFRIO, 14 avril 2008
[19] Lynn Langton, Statistician, "Women in Law Enforcement, 1987–2008", Bureau of Justice Statistics, U.S. Department of Justice, Washington, June 2010.

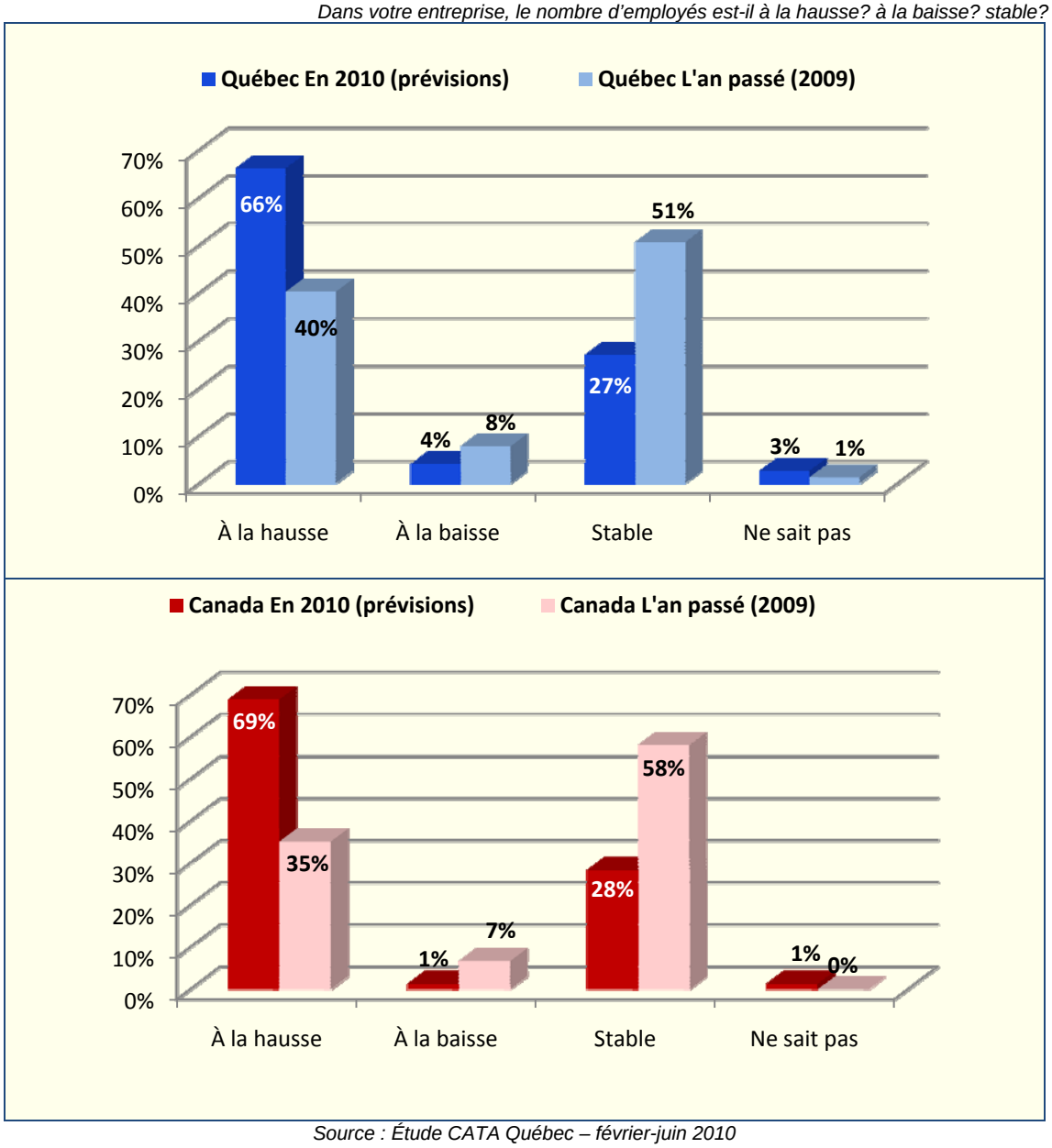
3.5 Impact de la crise financière sur l'emploi

La crise financière de 2009 a eu un impact limité sur le secteur de la sécurité avancée. Seulement 8% des entreprises québécoises déclarent avoir enregistré une diminution du nombre d'employés en 2009 (7% dans le reste du Canada), tandis que 40% affirment avoir enregistré une augmentation (35% dans le reste du Canada).

En 2010, tant les Québécois que les Canadiens sont confiants dans leur carnet de commandes et 66% des entreprises québécoises comptent embaucher (69% pour les entreprises du reste du Canada).

FIGURE 16 - FLUCTUATION DU NOMBRE D'EMPLOYÉS AU QUÉBEC ET DANS LE RESTE DU CANADA

Dans votre entreprise, le nombre d'employés est-il à la hausse? à la baisse? stable? NSP.



Source : Étude CATA Québec – février-juin 2010

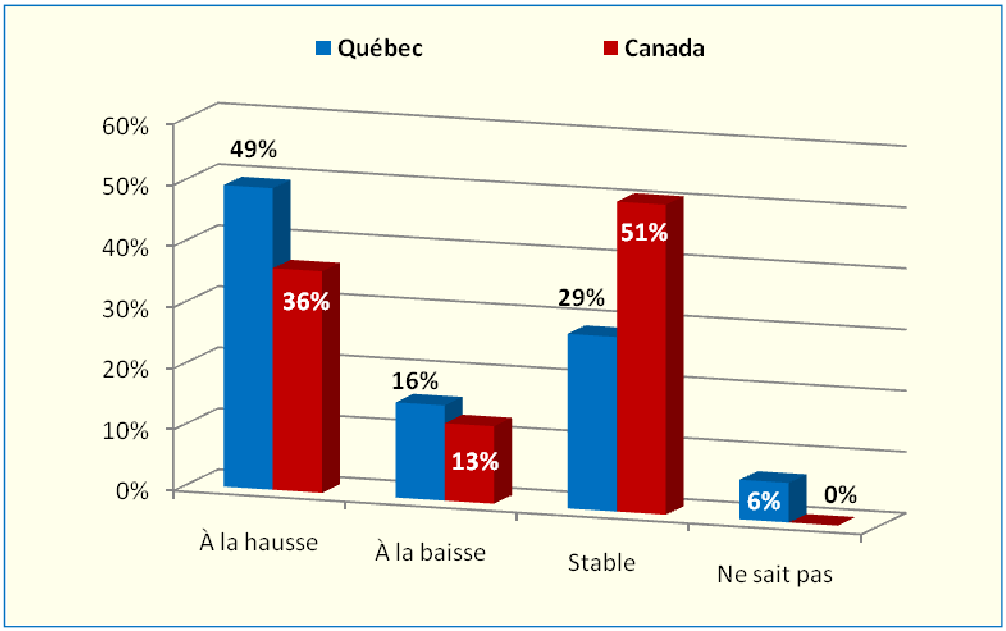
Nos ventes en Europe nous ont mis à l'abri de la récession mais le bilan est plutôt stable que croissant.
Éric Bergeron, Optosecurity

3.6 Impact de la crise financière sur les ventes

De même, si l'on aborde la crise financière en fonction des ventes, on se rend compte que la moitié environ des entreprises québécoises ont accru leur chiffre d'affaires en 2009 (36% dans le reste du Canada). Ces résultats confirment ceux de l'emploi : la crise a été faible dans le secteur québécois de la sécurité et relativement moindre que dans le reste du Canada.

FIGURE 17 - FLUCTUATION DES VENTES AU QUÉBEC ET DANS LE RESTE DU CANADA (2009)

Comment définiriez-vous vos ventes de l'an passé (2009) ? [sécurité seulement]



Source : Étude CATA Québec – février-juin 2010

Comment expliquer cette bonne performance relative de l'industrie de la sécurité au Québec? Un élément de réponse pourrait être fourni par la pratique des grandes entreprises de conseil de recourir de façon systématique à des consultants extérieurs : la non-reconduction de contrats de consultants n'apparaît pas dans les chiffres de l'emploi. [20]

Il y a des pigistes ailleurs au Canada mais bien moins qu'au Québec. Les grandes firmes sont dépendantes des contrats qui entrent ou qui sortent. Quand elles perdent un compte majeur, il y a plein de gens qui se font remercier et se mettent à leur compte.
Marc Fournier, PricewaterhouseCoopers

Un autre élément de réponse pourrait être la présence au Québec d'un secteur public fort et l'efficacité des mesures de relance adoptées par le gouvernement pourrait aussi expliquer que la crise ait été moins forte au Québec que dans le reste du Canada, c'est-à-dire essentiellement en Ontario.

Enfin, quand on se reporte aux résultats de 2003, on s'aperçoit que 89% des répondants affirmaient alors que leurs ventes étaient à la hausse – contre 49% en 2010. Cette mise en perspective nous permet

[20] La question sur le niveau de l'emploi temporaire avait été posée dans le sondage de CATA-Québec (Dans votre société, combien de consultants travaillent à temps partiel en sécurité?), mais elle n'a pas produit de résultats significatifs. Les personnes interviewées ont de la difficulté à évaluer le nombre de pigistes à l'intérieur de leur entreprise.

d'estimer que la crise financière a causé un ralentissement de la croissance de l'industrie québécoise de la sécurité avancée, mais pas un véritable recul.

3.7 Niveau de l'emploi dans l'industrie québécoise de la sécurité avancée

L'échantillon sondé compte 1 641 travailleurs spécialisés dans le domaine de la sécurité.

Analyse

Il est difficile de chiffrer avec précision le nombre total de personnes employées dans l'industrie québécoise de la sécurité avancée. Une extrapolation simple donne une population d'environ 3 800 personnes (43 % des entreprises ont répondu à cette question).

En 2003, par le même procédé d'extrapolation, nous avions obtenu 3 900 employés. Comme il s'agit dans les deux cas d'une approximation assez générale, il nous est impossible de conclure à une baisse significative du niveau de l'emploi. Tout au plus, pouvons-nous affirmer que la population de l'industrie de la sécurité est restée stagnante au cours des dernières années.

Une cause de cette apparente stagnation pourrait être la crise financière de 2008/2009 qui, même si elle eu des effets minimes sur le niveau de l'emploi, a freiné son expansion.

L'autre cause, plus structurante, est le nombre important de conseillers indépendants ou pigistes qui sont, par définition, difficiles à identifier et répondent rarement aux sondages. Les 3 800 personnes identifiées ne constitueraient donc que le noyau dur de l'industrie.

Le phénomène est commun à l'ensemble des TIC où les grandes firmes vendent du « temps-personne » et sont tributaires des contrats qui entrent et qui sortent. Quand un contrat est perdu, les employés sont licenciés. Or, ces employés très qualifiés ne disparaissent pas du marché du travail du jour au lendemain : ils se mettent à leur compte et deviennent conseillers indépendants.

Il n'est que penser à ce qui s'est passé quand CGI a perdu le contrat d'impartition des TIC du Mouvement Desjardins au profit d'IBM : on parle d'un contrat de 120 millions de dollars par an. Il y avait 500 employés chez CGI affectés au contrat de Desjardins.[21] Même si tous n'ont pas été licenciés, cela libère une grande quantité de spécialistes qui sont réembauchés ailleurs ou se mettent à leur compte.

[21] Denis Lalonde, « Desjardins opte pour IBM Canada », Direction informatique, 5 mai 2010.

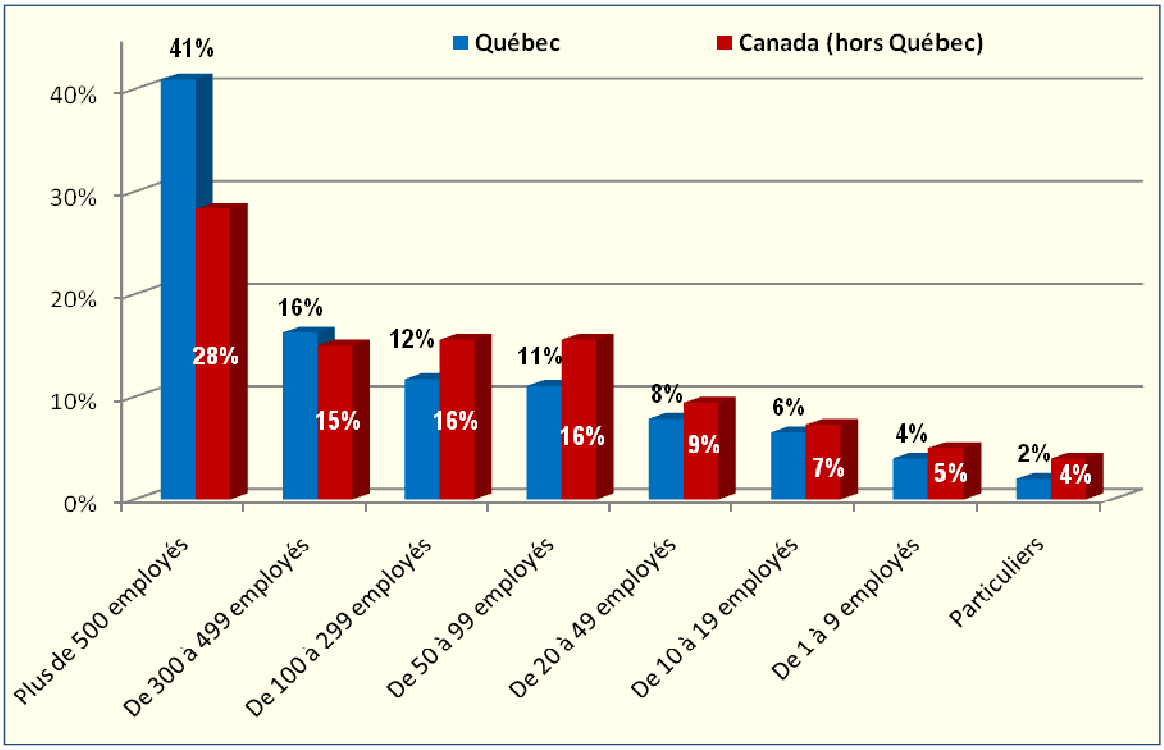
4. État du marché

4.1 Taille des organisations clientes

Les clients des entreprises québécoises de sécurité avancée sont en grande majorité des grandes et moyennes entreprises : 41% des clients comptent plus de 500 employés.

Dans le reste du Canada, la domination du marché de la grande entreprise est relativement moins importante. En effet, la PME de 50 à 500 employés constitue 47% du marché – contre seulement 39% au Québec.

FIGURE 18 - UN MARCHÉ ENCORE DOMINÉ PAR LA GRANDE ENTREPRISE



Source : Étude CATA Québec – février-juin 2010

Analyse

Un marché dominé par quelques grands clients est un signe manifeste de jeunesse. En effet, on sait que ce sont les grandes, voire les très grandes entreprises, qui sont les acheteurs précoces (*early adopters*) des services de sécurité. Elles ont créé des équipes dédiées à la sécurité dès l'époque des ordinateurs centraux, quand l'apparition des systèmes d'accès partagés a imposé des règles de sécurité internes. L'arrivée d'Internet a changé les processus du tout au tout en ouvrant les systèmes sur l'extérieur. Le défi de la grande entreprise a été alors de s'adapter.

Au contraire, la PME a généralement vécu en dehors de toute problématique sécuritaire jusqu'à l'arrivée d'Internet pour une bonne raison : elle n'était pas informatisée. Quant à la minorité qui avait acquis des ordinateurs de bureau avant 1995, elle les utilisait en mode autonome; quand elle les reliait en réseaux privés, il s'agissait de systèmes rudimentaires le plus souvent destinés à partager une imprimante dans un espace commun où tout le monde se connaissait, ce qui ne requerrait pas de mesures particulières de sécurité.

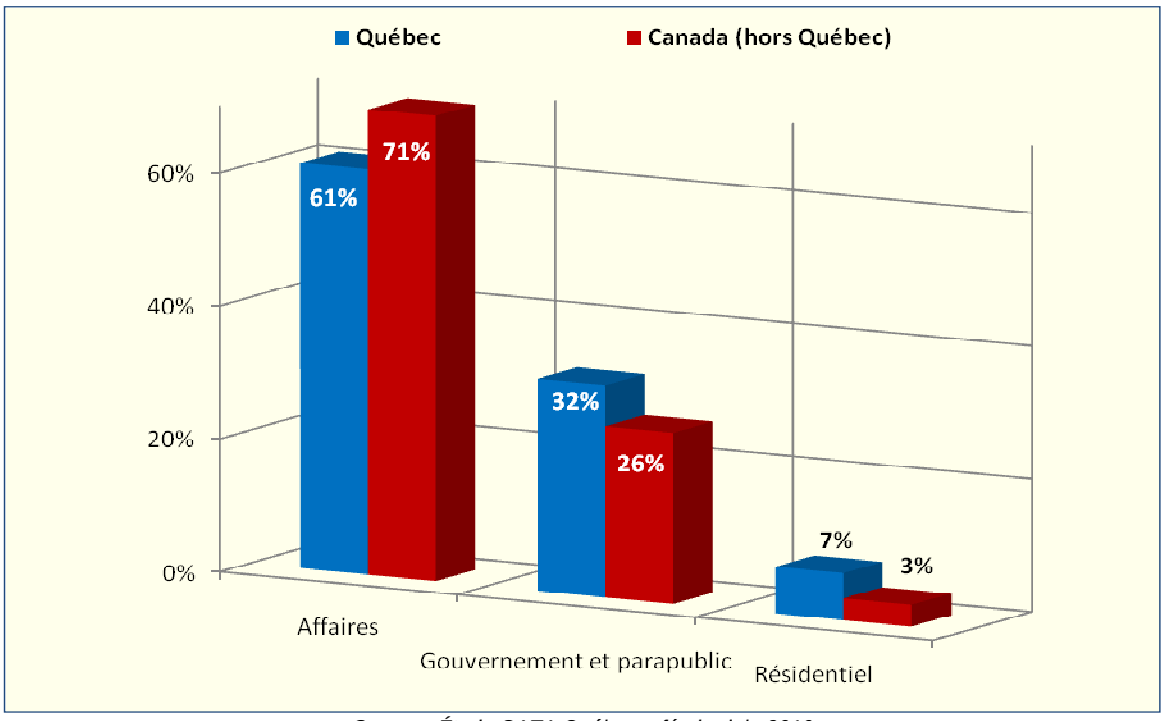
Le grand défi des entreprises de sécurité avancée au Québec est donc de pénétrer le marché de la PME. Pour cela, il ne suffit pas de faire de la publicité, ni même d'éduquer les clients. Il faut d'abord que les entreprises de sécurité adaptent leur offre à ce nouveau marché. Il faut passer d'une offre de produits haut de gamme entièrement personnalisée à une offre axée sur des produits semi-standardisés, abordables et facile d'entretien.

> Cela nous permet, entre autres, d'offrir des services à la carte et de n'intervenir, par exemple, que sur la détection d'intrusions ou la gestion des vulnérabilités. Nous offrons également des forfaits économiques pour des bouquets de services. Cette flexibilité tarifaire est la solution qui convient parfaitement aux besoins des PME.
>
> Marco Estrela, Gardien Virtuel

4.2 Les grands secteurs du marché

L'industrie de la sécurité avancée vend avant tout au secteur privé : les deux-tiers environ de ses clients sont des entreprises privées, contre un tiers des organismes publics ou parapublics. Dans le privé, c'est toujours le secteur financier (banques, assurances, institutions de courtage) qui domine le marché. La part du public est relativement moindre dans le reste du Canada, mais il s'agit d'une différence de degré, non d'une différence radicale qui indiquerait des comportements opposés.

FIGURE 19 - RÉPARTITION DU MARCHÉ DE LA SÉCURITÉ ENTRE SECTEUR PRIVÉ ET SECTEUR PUBLIC [22]



Source : Étude CATA Québec – février-juin 2010

Cette présence significative du secteur public dans le marché de la sécurité avancée est logique. La sécurité fait partie des fonctions traditionnelles de l'État. Bien au-delà du simple maintien de l'ordre,

[22] Les proportions ne renvoient pas aux nombres d'entreprises de sécurité déclarant desservir tels ou tels marchés, mais bien aux volumes réels d'activités. Ainsi une entreprise déclarant desservir le marché Affaires à 75% et le marché du Gouvernement et du parapublic à 25% sera inscrite en fonction des proportions déclarées.

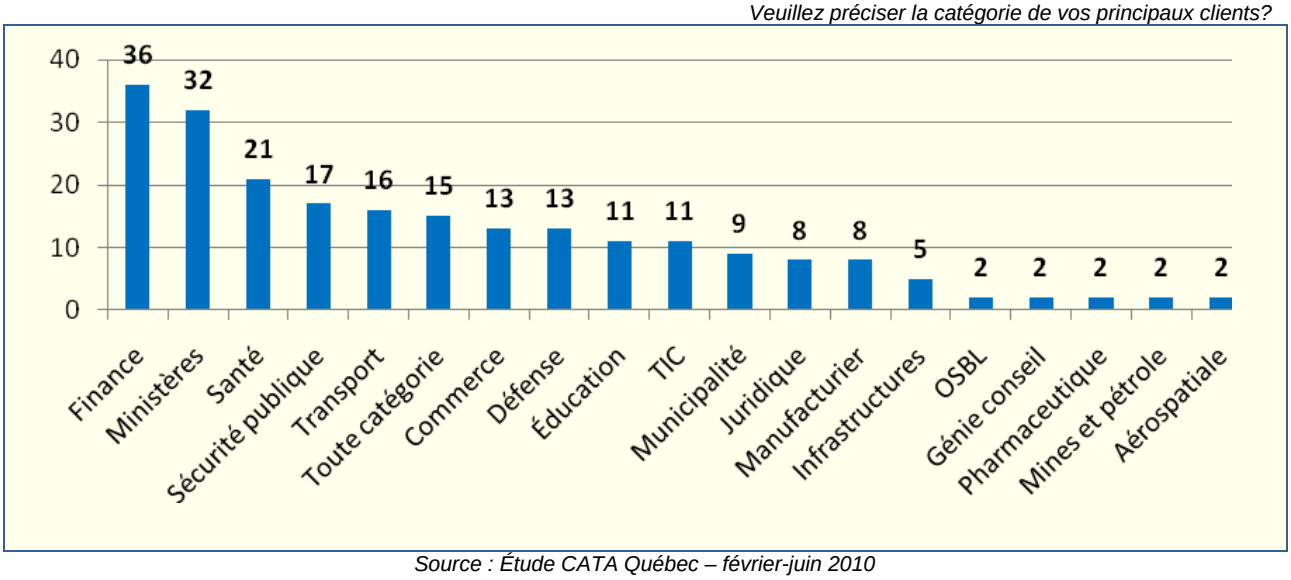
l'impératif sécuritaire guide l'action de l'État en matière de santé et d'éducation, de défense et de sécurité publique (corps de police et premiers intervenants), de transport (ports et aéroports), de pouvoirs locaux (municipalités, MRC), etc. Dans tous ses rapports avec les citoyens et les entreprises, l'État et ses agences doivent veiller à la sécurité des transactions et au respect de la vie privée. Cela se retrouve dans le marché des biens et services de sécurité.

Notons la présence d'un secteur juridique (avocats et notaires) très dynamique qui s'affiche non seulement comme marché pour la sécurité avancée, mais aussi comme producteur de biens et services. La montée en puissance de Notarius comme autorité de certification est sans doute la partie émergée d'un iceberg juridique appelé à jouer un rôle croissant dans l'industrie de la sécurité et de son double qui est la protection de la vie privée.

La sécurité des infrastructures, qui comprend l'énergie, peut sembler sous-représentée (cinq entreprises), mais si on la considère avec le transport (16 entreprises), on se rend compte qu'il s'agit d'un secteur d'activités clé de la sécurité avancée. Notons toutefois qu'il ne s'agit pas d'un marché intégré, mais plutôt d'une collection de plusieurs marchés disparates.

FIGURE 20 - LE SECTEUR FINANCIER EST TOUJOURS LE PREMIER CLIENT DE SÉCURITÉ

Veuillez préciser la catégorie de vos principaux clients?



Source : Étude CATA Québec – février-juin 2010

> La sécurité est l'enfant pauvre de la PME. Or, ce sont elles qui sont visées en priorité par les pirates informatiques qui s'entraînent sur ce type d'entreprises avant de s'attaquer aux grandes institutions comme les gouvernements et les banques.
> Véronique Olivier, Waveroad Consult

5. Marché local, exportations et stratégie de croissance

5.1 Répartition entre marché domestique et exportations

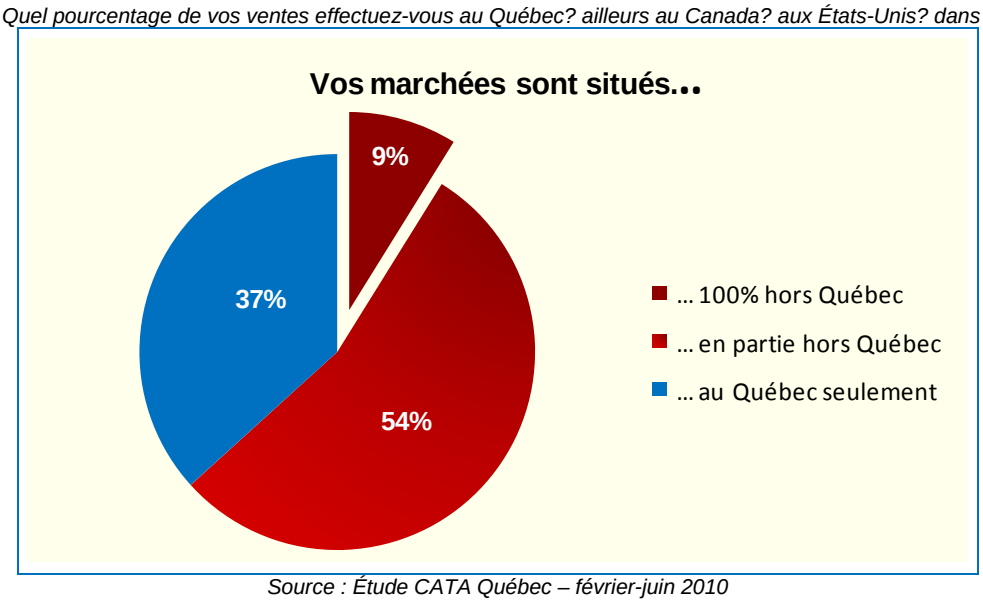
Au total, 50 entreprises sur 79 répondants (c'est-à-dire un taux de 63%) exportent hors du Québec. Nous incluons ici les expéditions vers les autres provinces canadiennes et les pays étrangers. L'industrie de la sécurité avancée au Québec est donc une industrie largement exportatrice.

Le fait saillant n'est pas que près des deux-tiers des entreprises québécoises desservent des marchés hors Québec, mais plutôt qu'une minorité y vende 100% de sa production. C'est le cas de la principale entreprise québécoise de sécurité, Silanis Technology. Or, elle n'est pas seule : en tout sept entreprises ont déclaré ne rien vendre au Québec.

À l'inverse, 29 entreprises sur 79 ont déclaré desservir uniquement le Québec (c'est-à-dire 37% des répondants).

FIGURE 21 - UNE INDUSTRIE TOURNÉE VERS L'EXPORTATION

Quel pourcentage de vos ventes effectuez-vous au Québec? ailleurs au Canada? aux États-Unis? dans d'autres pays?



Source : Étude CATA Québec – février-juin 2010

Si nous considérons l'intensité des expéditions, il convient de pondérer quelque peu ces résultats puisque le gros des ventes est dirigé vers le marché domestique : outre les 29 entreprises qui vendent uniquement au Québec, 23 autres y réalisent plus de 50% de leur chiffre d 'affaires. Qui plus est, ce sont les grandes sociétés de services professionnels (Deloitte, PwC, KPMG…) et les grandes firmes de conseil TIC (CGI, IBM, Bell…), qui desservent avant tout le marché local.

« Le Canada est perçu à l'étranger comme étant digne de confiance et offrant des services de qualité. Cette réputation facilite beaucoup les affaires à l'international.»
Marcel Dion. P-d.g Above Security

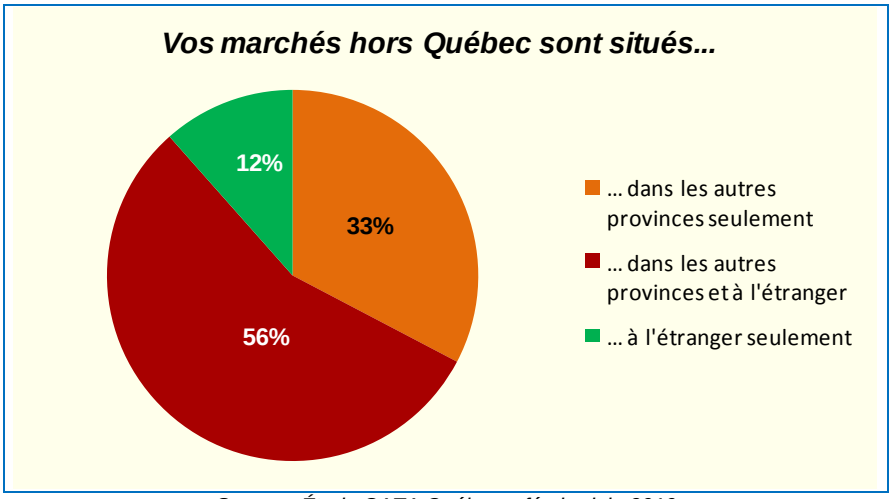
FIGURE 22 - VOLUME DE VENTES QUÉBÉCOISES PAR DESTINATION

Quel pourcentage de vos ventes effectuez-vous…	*… au Québec*	*… ailleurs au Canada*	*… aux États-Unis*	*… dans d'autres pays*
0%	7	32	53	46
1-25%	13	23	14	16
26-50%	7	16	9	11
51-99%	23	7	2	6
100%	29	1	1	0
Total (nb d'entreprises)	79	79	79	79

Source : Étude CATA Québec – février-juin 2010

Si on considère les seules entreprises qui vendent hors Québec, on s'aperçoit que près de 90% vendent dans les autres provinces canadiennes : 33% vendent seulement dans les autres provinces canadiennes et 56% à la fois dans les provinces canadiennes et à l'étranger (figure 23). Vendre dans les autres provinces canadiennes semble bien être un premier pas à franchir avant d'affronter les marchés internationaux.

FIGURE 23 - LE COMMERCE INTERPROVINCIAL SERT DE TREMPLIN AUX EXPORTATIONS INTERNATIONALES



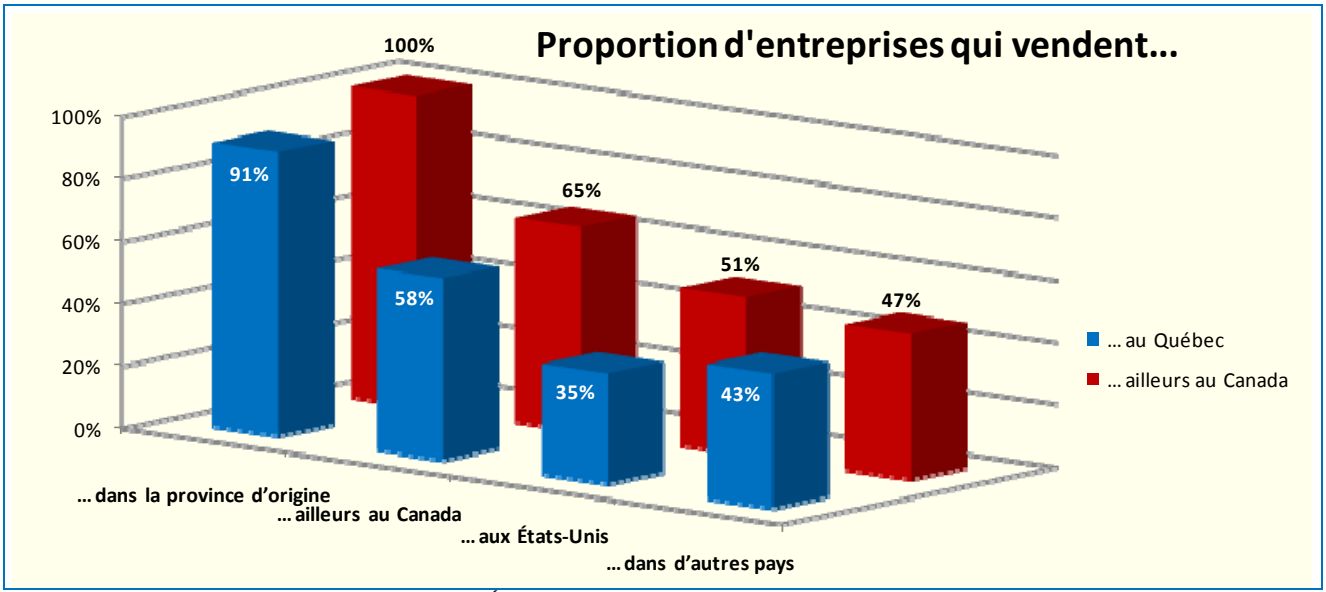
Source : Étude CATA Québec – février-juin 2010

Analyse comparative

Si nous considérons l'ensemble des marchés géographiques, les ventes des entreprises des autres provinces du Canada sont assez comparables avec celles des entreprises québécoises. La seule différence marquée est la plus forte proportion d'entreprises canadiennes qui exportent aux États-Unis (51% pour les entreprises hors Québec, contre 35% seulement pour les entreprises québécoises). À l'inverse, le phénomène des entreprises « tout-à-l'exportation » semble inconnu ailleurs au Canada.

En Europe – 50% des ventes de l'entreprise – notre stratégie de vente repose sur un réseau de revendeurs ainsi que des partenariats avec des sociétés de sécurité physique tels qu'ADT, Prosegur et Accenture.» Eric Talbot, S.I.C. Biometrics

FIGURE 24 - MARCHÉ DOMESTIQUE ET EXPORTATION : COMPARAISON QUÉBEC/CANADA



Source : Étude CATA Québec – février-juin 2010

FIGURE 25 - VOLUME DE VENTES CANADIENNES EN FONCTION DES DESTINATIONS

Quel pourcentage de vos ventes effectuez-vous…	… dans votre province	… ailleurs au Canada	… aux États-Unis	… dans d'autres pays
0%	0	26	37	40
1-25%	11	18	15	16
26-50%	14	23	18	16
51-99%	25	8	5	3
100%	25	0	0	0
Total (entreprises)	75	75	75	75

Source : Étude CATA Québec – février-juin 2010

Nous ne vendons qu'à l'extérieur du Canada. La seule raison qui explique notre présence à Montréal, ce sont les crédits d'impôt à la recherche et la présence d'universités de grande valeur.
Tommy Petrogiannis, pdg Silanis

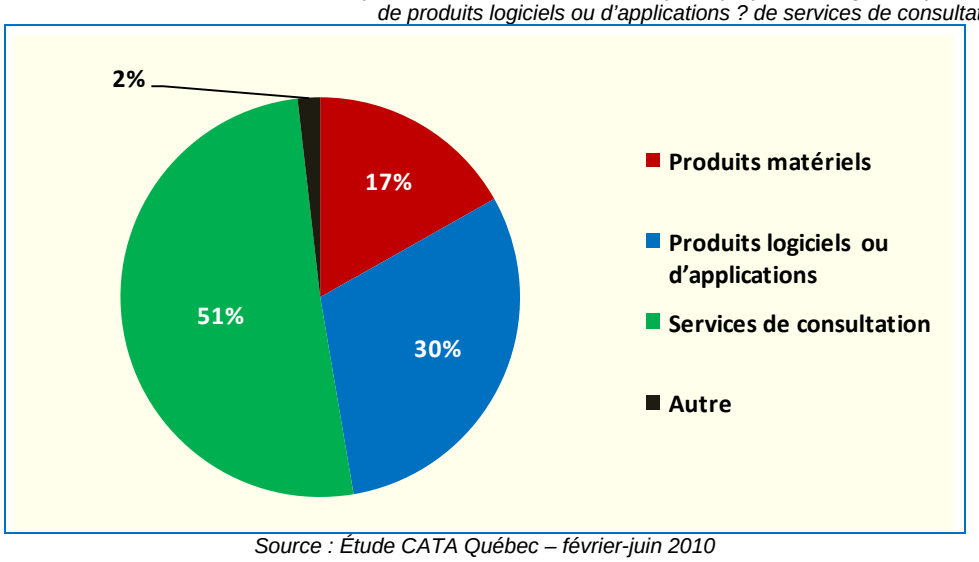
5.2 Nature des exportations

Plus de la moitié des exportations interrégionales et internationales est constituée de services, ce qui renvoie à la domination des fournisseurs de services sur la sécurité avancée au Québec : 62% des entreprises du secteur œuvrent dans le domaine des services professionnels (voir figure 11 : Nature des activités de l'entreprise). La part des logiciels (30%) est presque le double de celle des équipements (17%), ce qui renvoie également aux poids relatifs des éditeurs de logiciels et des manufacturiers dans le secteur.

Nous travaillons aux États-Unis et au Moyen-Orient grâce à l'établissement d'alliances avec des firmes complémentaires à nos services. Cela nous permet, notamment, d'enrichir notre veille technologique et nos connaissances parce que les cultures en sécurité sont différentes d'un pays à un autre.
Mathieu Chouinard, In Fidem

FIGURE 26 - FORTE PRÉSENCE DES SERVICES

Pour ceux qui vendent hors Québec, dans quelle proportion s'agit-il de produits matériels ? de produits logiciels ou d'applications ? de services de consultation ? autres ?



Source : Étude CATA Québec – février-juin 2010

Analyse

Le fait que plus de la moitié des exportations internationales est constituée de services, illustre bien la caducité de la théorie économique traditionnelle qui veut que les services se prêtent mal au commerce internationale en raison de l'impossibilité de les stocker et de leur caractère intangible. La numérisation massive de l'information et d'un grand nombre de processus a transformé la nature des services, ainsi que l'explique fort bien Statistique Canada :

> *« Cependant, ces caractéristiques ont été quelque peu influencées par les bouleversements technologiques. Producteurs et consommateurs peuvent maintenant échanger plus facilement des services à grande distance par les réseaux de télécommunications. De plus, certains services (télésanté, télé-éducation et services bancaires en ligne), traditionnellement considérés comme non échangeables, peuvent désormais s'échanger par des moyens électroniques. »* [23]

Encore faut-il distinguer le conseil sur mesure non quantifiable, non stockable et non reproductible, de l'ensemble des services commerciaux. À titre d'exemple, l'élaboration d'un audit de sécurité ou d'un plan directeur, nécessite une interaction de proximité entre le fournisseur et le client. Il s'agit de services qui ne s'exportent pas aisément – contrairement aux services commerciaux comme les services financiers, de télécommunications, de télémaintenance ou encore d'accès à de l'information médiatisée.

Le modèle même de service commercial est le système e-SignLive mis au point par Silanis Technology afin de permettre à des personnes situées en divers points du globe de certifier un document électronique basé sur la plateforme LotusLive d'IBM et accessible par abonnement. Le système guide l'utilisateur pas à pas à travers le document à remplir et à signer (contrat légal, bon de commande, accord de confidentialité, police d'assurance, demande crédit, etc.). Une première version de ce service a été lancée au mois d'avril 2010 qui est pour le moment géré par une division autonome de Silanis. Une fois la période d'incubation terminée, la division pourra, le cas échéant, être externalisée et constituée en société. [24]

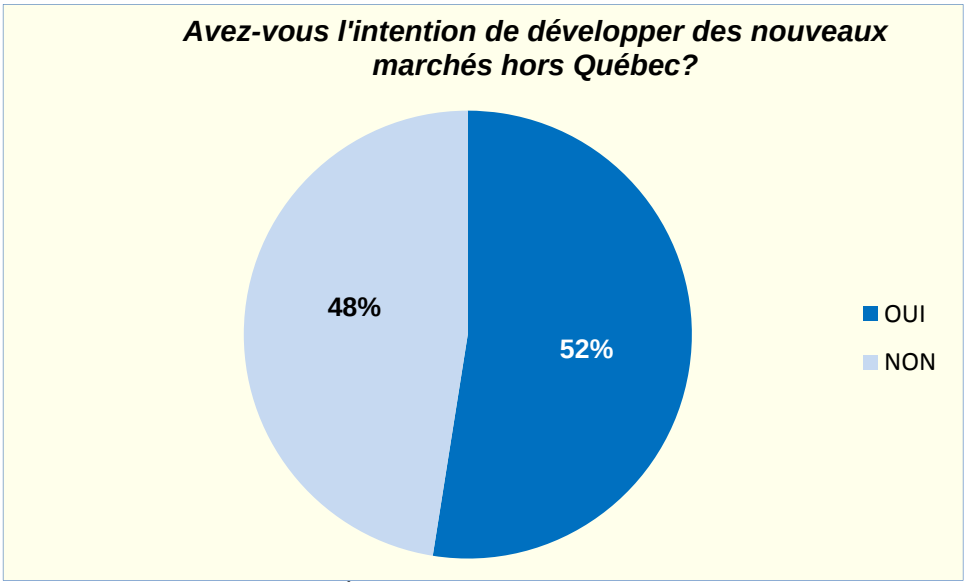
[23] Chrstine Roy, Les industries de service et le commerce des services, Division des industries de service, Statistique Canada, août 2001.
[24] Voir site d'e-SignLive - http://www.e-signlive.com/

De cette façon, le logiciel de signature électronique qui est le produit de base de Silanis est transformé en service commercial et conserve toutes ses caractéristiques d'exportabilité.

5.3 Stratégie de croissance des exportations

Une légère majorité d'entreprises déclare vouloir développer des nouveaux marchés d'exportation en 2010 ou d'ici deux ans. Il s'agit aussi bien d'entreprises ayant déjà une expérience d'exportation que d'entreprises uniquement locales.

FIGURE 27 - LA MAJORITÉ DES ENTREPRISES VISE À ACCROÎTRE SES EXPORTATIONS

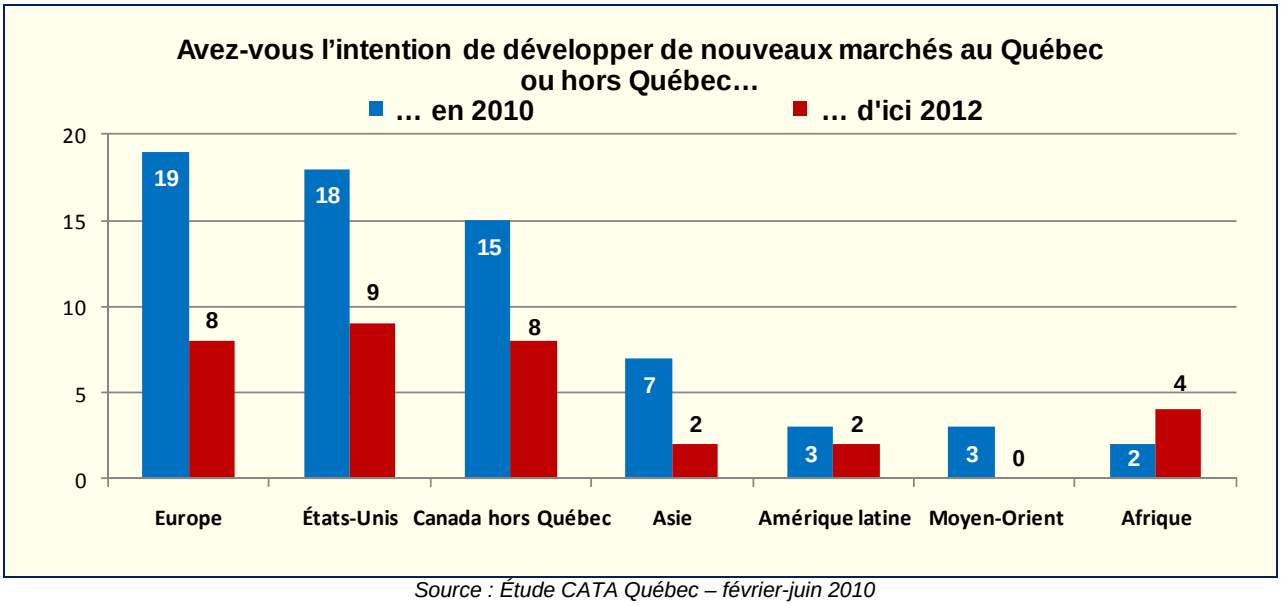


Source : Étude CATA Québec – février-juin 2010

L'Europe, les États-Unis et les autres provinces canadiennes demeurent les destinations de choix dans les stratégies d'expansion des exportations. Parmi les entreprises qui déclarent vouloir attaquer le marché canadien, la majorité (huit sur 15) nomment l'Ontario. Parmi celles qui citent l'Europe, rares sont celles qui mentionnent un pays particulier (Grande-Bretagne : 2; France : 1; Russie : 1). L'Asie est relativement peu présente dans les plans d'avenir de l'industrie québécoise de la sécurité.

> Les États-Unis demeurent le marché de choix mais nous sommes de plus en plus nombreux à nous intéresser à l'Afrique.
> *Éric Talbot, S.I.C. Biometrics*

FIGURE 28 - RÉPARTITION DES MARCHÉS GÉOGRAPHIQUES (PRÉVISIONS) [25]



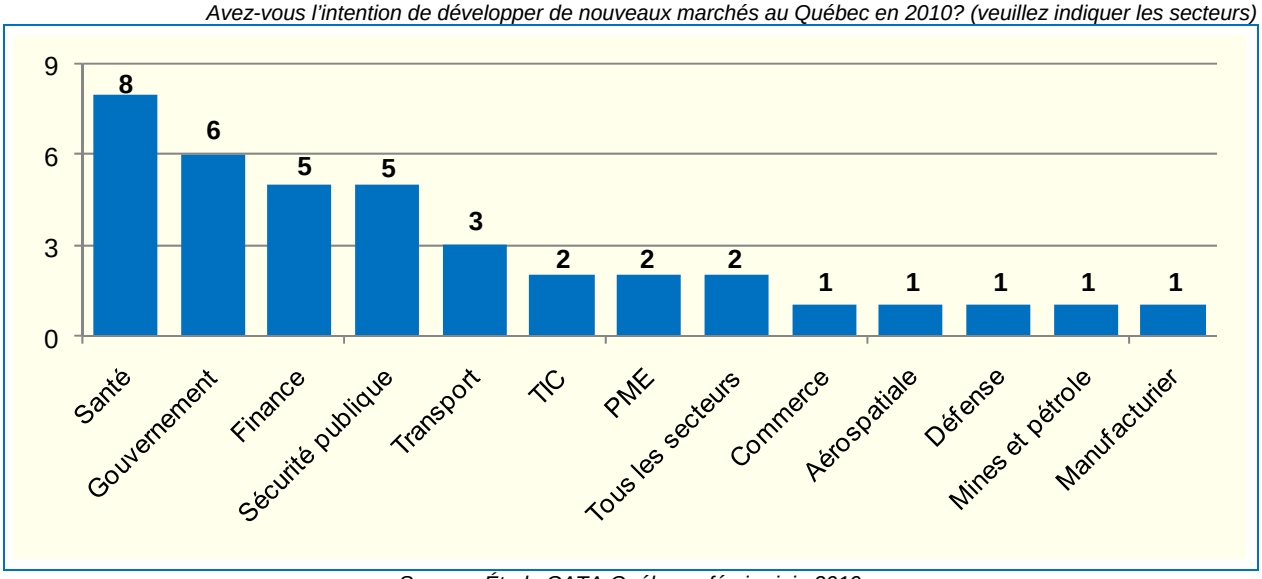
Source : Étude CATA Québec – février-juin 2010

5.4 Stratégie de diversification de l'offre

Peu d'entreprises ont répondu à la question sur la diversification de l'offre, ce qui rend hasardeux l'identification d'une tendance forte. [26] Notons quand même que la diversification de l'offre ressemble beaucoup à l'offre actuelle, avec une prédilection pour la santé.

FIGURE 29 - SECTEURS EN EXPANSION EN 2010

Avez-vous l'intention de développer de nouveaux marchés au Québec en 2010? (veuillez indiquer les secteurs)



Source : Étude CATA-Québec – février-juin 2010

[25] Cinquante deux compagnies ont répondu, mais seules 43 d'entre elles ont été retenues; les réponses trop vagues ont été écartées (monde, pays en développement, francophonie…).

[26] La question portait sur des prévisions pour 2010 et 2012. Les réponses pour 2012 n'ont pas été représentées dans le tableau car elles étaient généralement les mêmes que pour 2010.

Deux répondants ont désigné la PME comme un marché à part entière, ce qui est significatif car ils indiquent ainsi que cette catégorie d'entreprises a un comportement homogène à travers tous les secteurs de l'économie. Un des répondants va jusqu'à préciser la nature de son expansion prévue en direction des PME, soit la création de modèles logiciels (*templates*) de gestion des incidents.

> Une stratégie de rechange consiste à attaquer systématiquement le marché ontarien. Sur ce marché, nous poursuivons une stratégie différente du Québec. Nous visons avant tout la PME par une nouvelle offre de package de services conseil offerte à un prix fixe. Pour cela, il faudra mettre en place un réseau de distributeurs locaux.
> Benoit H. Dicaire, Infrax

6. Recherche et développement (R-D)

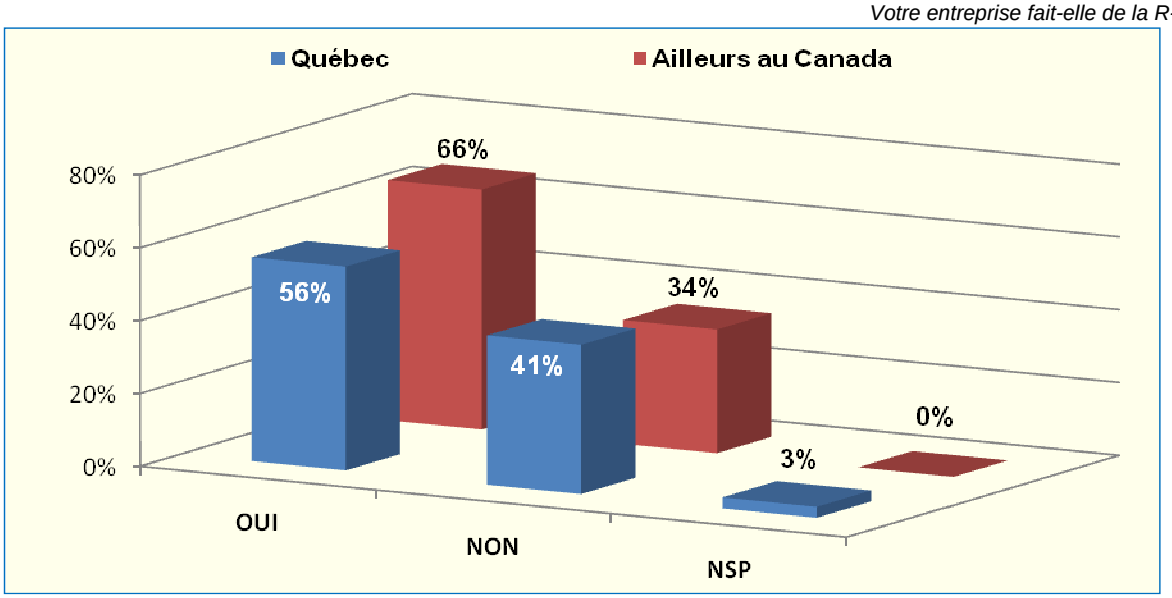
6.1 Poids relatif de la R-D au Québec

Plus de la moitié des firmes de sécurité avancée au Québec font de la R-D (56%). Par contre, cette bonne performance demeure nettement inférieure au reste du Canada (66%).

Si le nombre d'entreprises québécoises qui font de la R-D est moindre qu'ailleurs au Canada, cela s'explique par le grand nombre de fournisseurs de services au Québec. En effet, 57% des fournisseurs de services ne font pas de la R-D. À l'inverse, la quasi-totalité des éditeurs de logiciels et des manufacturiers font de la R-D (un éditeur de logiciel et un fabricant disent ne pas faire de R-D et encore faut-il préciser que tous deux se présentent aussi comme fournisseurs de services).

FIGURE 30 - FAIBLESSE RELATIVE DE LA R-D QUÉBÉCOISE

Votre entreprise fait-elle de la R-D ?



Source : Étude CATA-Québec – février-juin 2010

Analyse comparative

En 2003, au Québec, neuf entreprises de sécurité avancée sur 10 affirmaient faire de la R-D. Ce nombre a diminué à moins de six entreprises sur 10. Ceci est conséquent avec la baisse du nombre de firmes en édition de logiciels et en fabrication d'équipement.

Analyse

Il convient de souligner que nombre d'entreprises jouent plusieurs rôles simultanément. Ainsi, les manufacturiers de produits de sécurité sont souvent aussi des éditeurs de logiciels (cinq sur neuf répondants). Tous deux, les éditeurs de logiciels et les manufacturiers peuvent également offrir des services professionnels (huit éditeurs sur 18 et un manufacturier sur neuf). Nous avons vu comment Silanis Technology était en train de créer un nouveau service de documents électroniques certifiés avec vocation d'essaimage (*spin-off*).

Cette effervescence fonctionnelle atteste de la vitalité de l'industrie de la sécurité avancée. Plutôt que de l'immaturité, il faut y voir la caractéristique première d'une industrie qui doit coller à une réalité mouvante. La sécurité avancée ne sera jamais une industrie stable.

> Cinq ans de recherche et 60 brevets déposés : nous entamons notre première année d'exploitation et nous savons que notre solution est la meilleure.
> *Éric Bergeron, Optosecurity*

6.2 Nature de la R-D au Québec

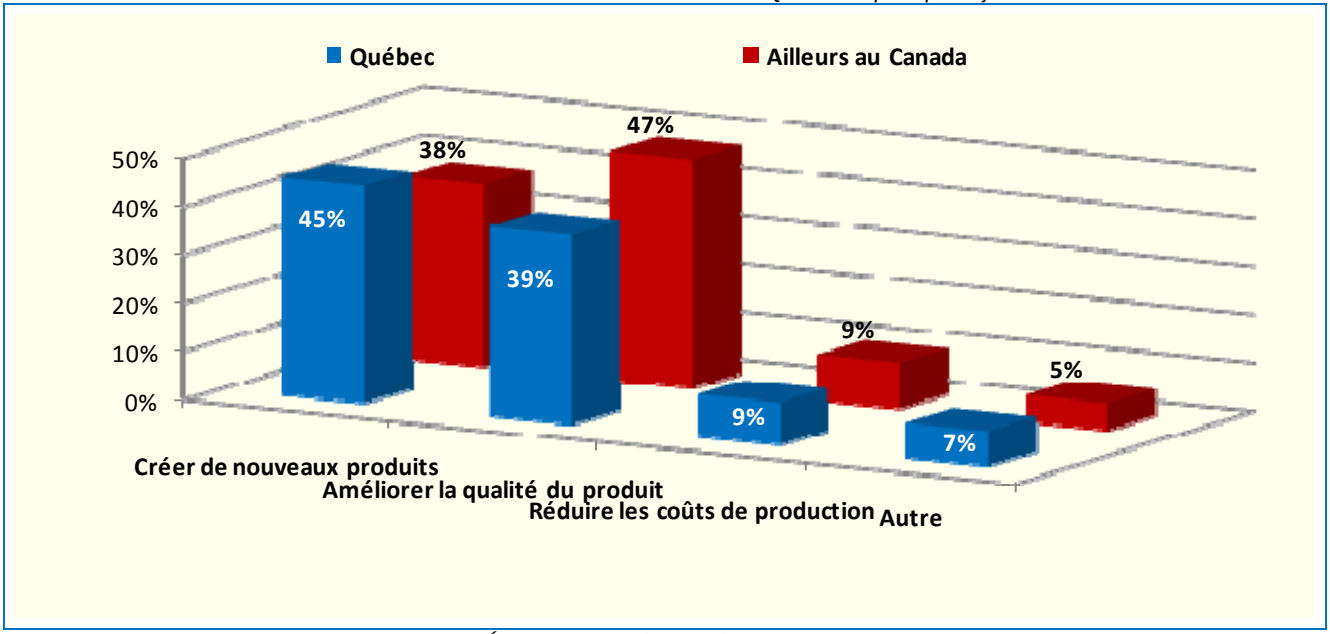
Au Québec, la création de nouveaux produits l'emporte sur l'amélioration de la qualité du produit. La créativité est au rendez-vous, mais pense-t-on suffisamment à la commercialisation et aux besoins des clients?

Ailleurs au Canada, le phénomène est inverse : on privilégie l'amélioration de la qualité du produit.

Par contre, la réduction des coûts de production n'est pas un facteur significatif, tant au Québec qu'ailleurs au Canada.

FIGURE 31 - PRIORITÉ À L'INNOVATION

Quel est le principal objectif de votre effort de R-D ?



Source : Étude CATA-Québec – février-juin 2010

6.3 Les domaines d'applications de la R-D

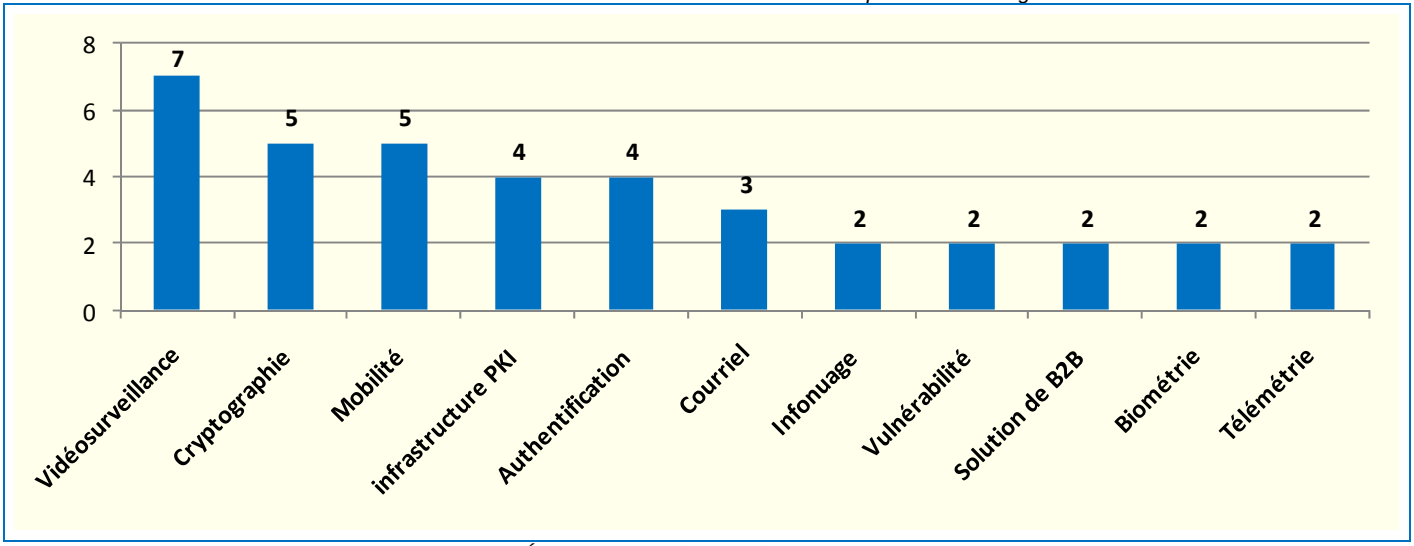
La vidéosurveillance IP, la cryptographie et la mobilité sont les technologies montantes de l'industrie québécoise de la sécurité, en termes de compagnies effectuant de la R-D. L'authentification, la cryptographie et l'infrastructure PKI, étant des technologies sœurs, on peut les réunir dans la même catégorie, ce qui souligne encore plus le caractère concentré de la recherche québécoise.

Toutefois, cet indicateur dénote une communauté d'intérêt, mais ne peut pas rendre compte du poids réel des activités de recherche dans chaque domaine spécifique.

Ainsi, à titre d'exemple, Silanis consacre 18% de ses revenus à la R-D, soit plus d'un million de dollars par an et la firme détient 12 brevets (12 autres sont en attente d'approbation). Cette entreprise consacre le gros de son effort de recherche à la preuve électronique (*Electronic Evidence*), c'est-à-dire aux technologies d'authentification/cryptographie qui pèsent donc d'un poids nettement plus lourd que sa place dans le tableau ci-dessous ne pourrait le laisser croire.

FIGURE 32 - LES GRANDES TENDANCES DE LA R-D QUÉBÉCOISE

Veuillez indiquer le domaine général de vos activités de R-D ?



Source : Étude CATA-Québec – février-juin 2010

Zerospam consacre un tiers de ses ressources à la R-D notamment pour se tenir à jour sur les manœuvres des pirates et autres spammeurs sur Internet.
David Poellhuber, Zerospam

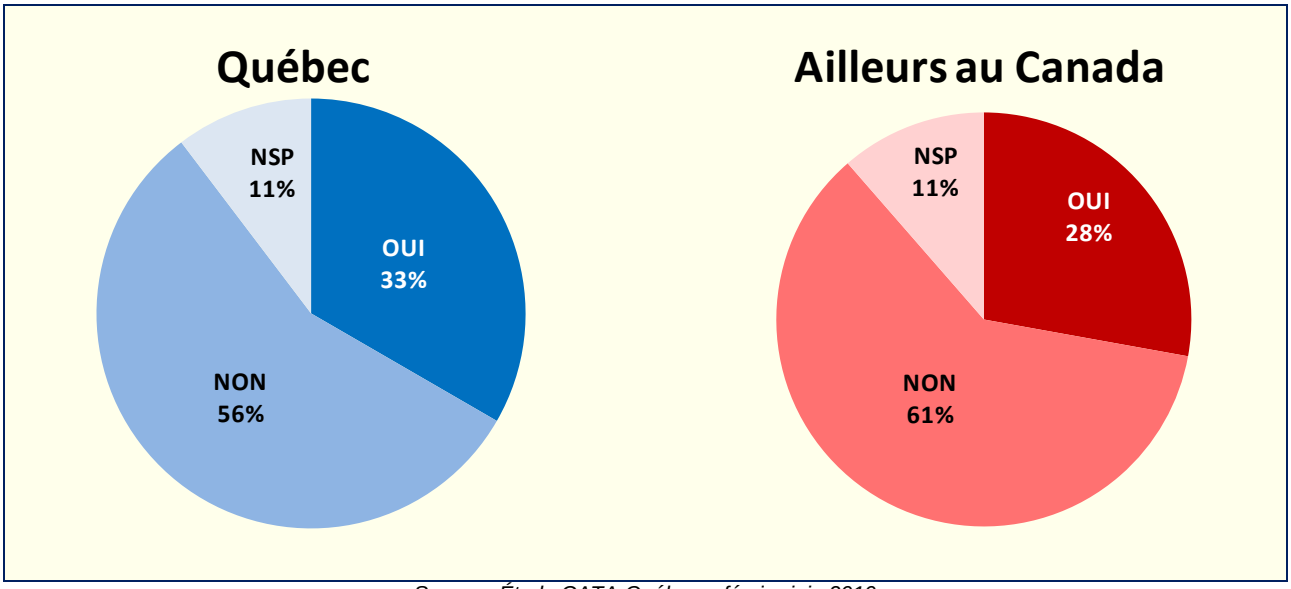
7. Financement

Seul le tiers des répondants québécois se dit à la recherche de financement, ce qui est bien inférieur à la situation de 2003 où 48% d'entre eux se disaient à la recherche de financement. Même si on considérait les 11% qui prétendent être indécis comme les entrepreneurs qui ont abandonné leurs projets de recherche de financement faute de capital de risque, on arriverait encore à un tassement de la recherche de financement.

Cette tendance est compatible avec les résultats dans les autres provinces canadiennes où seulement 28% des répondants sont à la recherche de financement, contre 44% en 2003.

FIGURE 33 - LE FINANCEMENT N'EST PAS UN PROBLÈME MAJEUR

Êtes-vous à la recherche de financement ?



Source : Étude CATA-Québec – février-juin 2010

Malgré le peu de réponses enregistrées sur les buts de la recherche de financement, deux thèmes se dégagent nettement : le développement de nouveaux marchés (huit réponses sur 12) et la R-D (cinq réponses sur 12). La plupart des entreprises à la recherche de nouveaux marchés visent surtout des segments verticaux du marché domestique – seules deux compagnies mentionnent les marchés d'exportation.

Parmi les autres raisons mentionnées, citons en vrac la formation, l'assurance qualité, l'achat de comptes recevables et des mesures d'employabilité dans le cadre d'un programme d'Emploi Québec.

RDDC Valcartier dispose des ressources scientifiques et financières nécessaires pour encourager les entreprises en défense et sécurité à s'engager dans les activités de R-D. Un des objectifs vises par RDDC Valcartier est de favoriser la synergie public-privé en matière de sécurité.
Richard Delagrave, RDDC Valcartier

8. Les obstacles au développement de l'industrie

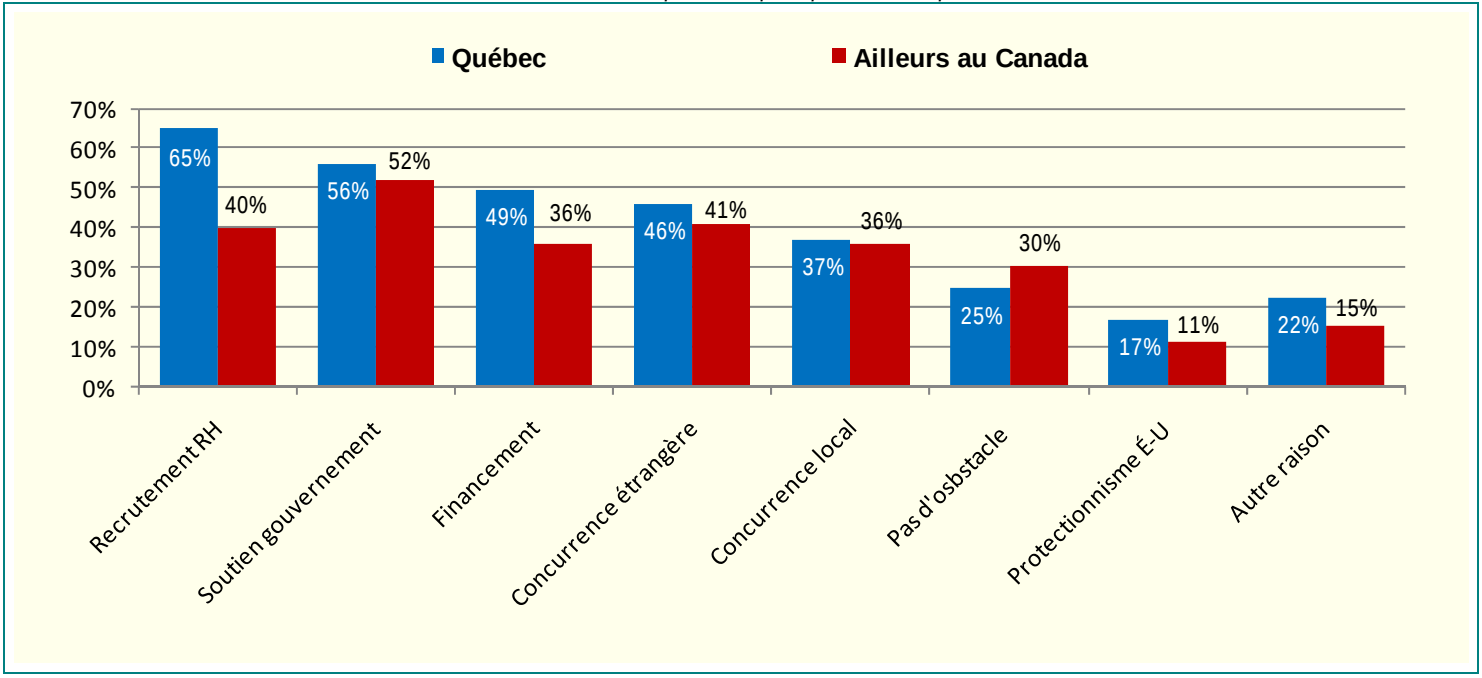
Le grand obstacle de l'industrie québécoise de la sécurité avancée est de loin le recrutement de personnel qualifié (65% des répondants). Ce résultat est d'autant plus remarquable qu'il tranche nettement avec les résultats des autres provinces canadiennes qui le mentionnent dans 40% seulement des cas.

L'autre grande « découverte » de cette enquête est la quasi-absence de problème posé par le protectionnisme américain (17% seulement des répondants l'ont identifié comme un obstacle au Québec, 11% ailleurs au Canada). Même si on ne tient compte que des exportateurs de biens et services, la proportion de ceux qui considèrent le protectionnisme américain comme un obstacle ne s'élève qu'à 22%. C'est un signal fort que nous envoie l'industrie sur l'ouverture du marché américain, dans le secteur économique le plus sensible entre tous – à savoir, la sécurité avancée.

Par contre, la force du dollar canadien sur le marché des changes a été citée comme un obstacle à l'exportation sur le marché américain.

FIGURE 34 - LE RECRUTEMENT DE PERSONNEL EST LE PRINCIPAL OBSTACLE

Selon vous, quel est le principal obstacle que doit affronter l'industrie de la sécurité?



Source : Étude CATA-Québec – février-juin 2010

Analyse

A - Formation

La situation sur le plan du recrutement a empiré depuis 2003 où le problème apparaissait relativement secondaire (seuls 29% des répondants identifiaient alors le manque de personnel qualifié comme un obstacle). Que s'est-il passé depuis?

Manifestement, la sécurité avancée est devenue une préoccupation plus générale que par le passé, mais la formation n'a pas suivi. Encore faut-il savoir de quelle formation il s'agit? Dans bien des cas, la

formation en TIC n'est pas suffisante. La majorité des cyberattaques proviennent de l'intérieur des organismes visés, ce qui renvoie l'impératif sécuritaire à un mélange d'expertise TIC, de gestion administrative ainsi que de techniques d'enquête et interrogation.

En outre, l'importance croissante des services professionnels au sein du secteur de la sécurité pose un défi : le service conseil exige du personnel expérimenté. On ne vend pas le service d'un jeune diplômé à une entreprise ou une administration publique déjà dotée d'un service interne hautement spécialisé. Il existe donc une demande pour des experts déjà expérimentés, qui demeure insatisfaite.

B – Rôle de l'État

L'État a un double rôle d'utilisateur et de législateur en matière de sécurité et de respect de la vie privée. Certains répondants ont souligné le manque de législation québécoise sur le vol d'information confidentielle, comparativement à la situation prévalant aux États-Unis ou dans les pays européens. Selon eux, faute d'un tel cadre législatif et réglementaire, bien des entreprises ne font pas les efforts nécessaires pour maintenir un environnement sécuritaire dans leurs infrastructures TIC.

Par ailleurs, plusieurs petites entreprises de sécurité avancée se plaignent des difficultés qu'il y a de faire affaire avec le gouvernement aussi bien au niveau québécois que fédéral. Cette critique est très comparable à ce que nous notions en 2003 : l'administration publique tend à privilégier les grandes entreprises et à rédiger les appels d'offre en fonction de celles-ci. Il est plus facile pour une administration publique qui est par définition grande, de traiter avec une grande entreprise qu'avec une PME. La grande entreprise a des structures comparables : un vice-président parle à un sous-ministre, un directeur de service à un directeur général et ainsi de suite.

Pourtant, certaines grandes entreprises sont passées maîtres dans l'art de traiter avec des PME. Une compagnie comme IBM a créé un écosystème de partenaires où elle puise une grande partie de son innovation et qui lui permet de s'adapter à des marchés pointus où elle serait absente sans cela. Ericsson Canada à Montréal et Research in Motion (RIM) à Waterloo ont créé des écosystèmes puissants (dans lesquels la sécurité est présente) où se joue en grande partie l'avenir de leurs téléphones intelligents.

Les administrations publiques du XXIe siècle ne peuvent plus se permettre de négliger les PME comme source d'approvisionnement, surtout dans le secteur de la sécurité qui fait partie de leur activité centrale (*core business*). L'industrie de la sécurité n'a pas besoin de subventions, aucun répondant n'a soulevé cette possibilité, mais elle a besoin de contrats et de partenariats avec un gouvernement qui s'adapte aux structures de la PME.

Or, l'administration publique est souvent contrainte de traiter avec des grandes entreprises pour des raisons d'universalité et de couverture géographique. Dans tous les cas où le gouvernement et ses agences sont contraints de se tourner vers la grande entreprise, il conviendrait de prévoir, dans les appels de proposition, une série de clauses pour les PME chargées de la sous-traitance.

Dans les faits, la grande entreprise recourt déjà à l'expertise des PME pour répondre aux besoins globaux du gouvernement. Il s'agit principalement pour les dirigeants gouvernementaux d'améliorer ce qui existe déjà, non d'inventer ex nihilo. En quoi pourraient consister ces améliorations?

À titre d'exemple, il est possible de conférer dans les appels de proposition une place officielle et visible aux PME aux côtés des soumissionnaires principaux, et ce, tout au long de l'exécution du mandat. Il est aussi possible de créer des campagnes d'information à l'intention de la PME pour favoriser les partenariats avec les grands donneurs d'ordre. Bref, il faut concevoir une action plurielle, continue, avec des résultats qui visent le moyen terme.

9. Conclusion et pistes de recommandations

Le développement du secteur de la sécurité avancée au Québec est tributaire de trois variables clés :

- ✓ Le développement d'une offre de sécurité avancée fortement imbriquée dans la gouvernance des organisations en lieu et place d'une approche strictement technologique;
- ✓ le développement d'une offre adaptée aux PME;
- ✓ le manque de personnel qualifié.

8.1 Des TIC à la gouvernance

La sécurité est en train de s'affranchir de son image de TIC pour devenir une question de gouvernance. Cette transition est accélérée par la décision du *Payment Card Data Security Standards Council* d'imposer la norme PCI-DSS dans le secteur du commerce.

Conséquence

La sécurité cesse d'être un sous-secteur des TIC pour devenir une partie intégrante de la gouvernance, de la gestion et de la stratégie de l'organisation, bref, pour se comporter comme les autres activités de services professionnels (vérification financière, conseil fiscal, gestion d'entreprise…).

8.2 Développement d'une offre adaptée aux PME

La même décision du *Payment Card Data Security Standards Council* commence enfin à faire naître une offre de sécurité destinée à la PME. Nous annoncions cette évolution dans l'étude de 2003 sur la sécurité avancée, mais la transition a été plus longue que prévue, en raison de l'absence d'incitatifs. Il appartient au secteur du crédit d'avoir pris l'initiative de sensibiliser à la sécurité toutes les entreprises utilisatrices de terminaux point de vente et de commerce électronique.

Conséquence

Le secteur du commerce de détail a soudain pris conscience de l'importance de protéger les renseignements personnels de ses clients. C'est un grand pas dans le sens d'une plus grande responsabilisation des pratiques commerciales. Toutefois, la norme PCI-DSS s'applique différemment selon les niveaux d'intensité des transactions effectuées par les commerçants.

FIGURE 35 – CLASSEMENT DES COMMERCES EN FONCTION DE LA NORME PCI-DSS

Niveau	Intensité des transactions
Niveau 1	Tout commerce effectuant plus de six millions de transactions annuelles de carte de paiement, y compris l'e-commerce, ou dont les données ont déjà été compromises.
Niveau 2	Tout commerce effectuant entre 1 et 6 millions de transactions annuelles de cartes de paiement.
Niveau 3	Tout commerce effectuant entre 20 000 et 1 million de cartes de paiement.
Niveau 4	Tous les autres commerces à faible volume de transactions.

Source : http://frca.pcisecuritystandards.org/

Seuls les commerçants de niveau 1 sont astreints à des audits annuels par un vérificateur externe et à un scan trimestriel de vulnérabilités sur les points d'accès externes (site Web, messagerie…). Cette approche graduelle est réaliste. Selon les participants au sondage, elle fait pénétrer la sécurité dans des entreprises commerçantes de 500 employés ou plus (certains disent 1 000 employés ou plus). Quoiqu'il en soit, c'est le « M » de PME qui est visé par cette expansion de la sécurité.

La petite entreprise échappe aux aspects les plus contraignants de la norme PCI-DSS dans le sens où l'audit externe est remplacé par un questionnaire d'auto-évaluation.

Résumé de la norme PCI-DSS

La norme PCI-DSS comporte 12 exigences qui peuvent être regroupées en six thèmes :

- ✓ Création et maintien d'un réseau sécurisé
- ✓ Protection des données des titulaires de cartes de crédit
- ✓ Élaboration d'un programme de gestion des vulnérabilités
- ✓ Mise en œuvre d'un système de contrôle d'accès
- ✓ Surveillance et tests réguliers des réseaux
- ✓ Adoption d'une politique de sécurité de l'information

Il en résulte que la norme PCI-DSS vise en premier lieu les entreprises de plus de 500 employés. On a vu que ce marché constitue à lui seul 41% du marché québécois de l'industrie de la sécurité. Or, dans le secteur du commerce de détail, ces grands établissements représentent moins d'un pour cent du marché. Le potentiel de croissance de la sécurité dans le secteur du commerce de détail est immense, mais il n'est pas ou peu soutenu par l'imposition de la norme PCI-DSS.

FIGURE 36 – LE COMMERCE DE DÉTAIL AU QUÉBEC

Catégorie d'effectif	Nombre d'employés	Nombre d'établissements	Proportion par catégorie
Micro	1 - 4	12 523	38,74%
Petit	5 - 49	18 042	55,82%
Moyen	50 - 99	1 728	5,35%
Grand	500 +	30	0,09%
Total	---	32 323	100,00 %

Source : Statistique Canada, Structure des industries canadiennes, décembre 2008.

8.3 Manque de personnel qualifié

Le manque de personnel qualifié est sans aucun doute un frein à la croissance des entreprises de sécurité avancée : 65% des entreprises déclarent avoir des problèmes de recrutement de personnel qualifié (proportion qui s'élève à 97% des répondants qui disent vouloir embaucher en 2010).

Conséquence

L'avenir de l'industrie de la sécurité avancée au Québec repose sur l'existence de personnel qualifié de calibre international.

Pour illustrer l'importance décisive de ce facteur, nous citerons l'exemple de Silanis Technology : cette entreprise ne vend rien au Québec, ni même au Canada d'ailleurs. Ses vendeurs sont tous localisés aux États-Unis, sa vice-présidente marketing vit à Vancouver et pourtant l'entreprise est basée à Montréal. Quand on pose la question du choix de Montréal, le président de Silanis cite l'avantage comparatif prodigué par les crédits d'impôts à la R-D et la présence de quatre universités où se trouvent « des talents fantastiques ».[27]

[27] Tommy Petrogiannis, interview du 9 mars 2010.

L'effort accompli par les universités en matière de formation de sécurité de l'information est donc fondamental. Mais il n'est pas suffisant, ainsi que l'atteste la réponse au sondage de l'Alliance CATA. En outre, l'université ne constitue qu'un des volets de la formation en sécurité, l'autre étant entre les mains des entreprises et associations spécialisées du secteur privé : mentionnons le rôle de l'ISACA dans la certification CISM, CISP et CobiT; ou encore celui de CIPS dans la certification ISP/ITPC; sans compter les instituts privés du type TECHNOCompétences.

Ces quelques exemples entre tant d'autres montrent que l'infrastructure de formation existe. Par contre, la volonté politique de mobiliser le réseau de la formation ainsi que l'industrie, fait défaut. À preuve les deux signaux négatifs qui ont été envoyés à la formation en sécurité avancée par les pouvoirs publics. Le premier vient du Canada avec la fermeture en 2009 du programme Sécurité et protection des renseignements personnels de l'Institut de technologie de l'information du CNRC (ITI-CNRC). Bien que situé à Fredericton (Nouveau-Brunswick), ce programme travaillait depuis 1995 avec les universités de tout le pays.

Le deuxième vient du Québec même avec la fermeture en juin 2010 de l'Institut de sécurité de l'information du Québec (ISIQ). Sa mission était « de contribuer à créer une culture de la sécurité, d'assurer une sorte de veille... Aussi, la filière PME regroupait une vingtaine de petites entreprises en sécurité, pour les amener à devenir plus compétents et plus forts. »[28]

La fermeture de ces deux centres de recherche et de formation en sécurité de l'information atteste d'une certaine léthargie en matière de sécurité tant du côté des intervenants gouvernementaux que du secteur privé.

8.4 Pistes de recommandations

Pour contribuer au développement de l'industrie québécoise de la sécurité avancée, les gouvernements devraient tenir compte de certains facteurs :

- ✓ L'industrie de la sécurité avancée est un secteur distinct des TIC et son évolution accentuera encore cette spécificité.

- ✓ La Loi canadienne *sur la protection des renseignements personnels et les documents électroniques* est insuffisante pour protéger le public et pour inciter les acteurs économiques à se doter de politiques de sécurité, elle doit être complétée par une législation contraignante basée sur la transparence et la divulgation des incidents.

- ✓ La formation en sécurité doit être encouragée dans les universités québécoises par tous les moyens à la portée du gouvernement (bourses d'études, fonds de recherche, contrats gouvernementaux, etc.), y compris une politique de sensibilisation à l'égard des femmes qui sont sous-représentées dans ce secteur et qui constituent un réservoir de main d'œuvre inexploité.

[28] Jean-François Ferland, « La fin de l'ISIQ due à une impasse », *Direction informatique*, 7 juin 2010.

Annexe 1 : Étude cas

Les entreprises qui font l'objet d'une présentation détaillée ont été choisies en fonction de leur appartenance aux différents segments de cette industrie de façon à donner un aperçu aussi complet que possible de la variété des activités de l'industrie de la sécurité avancée au Québec. Il ne s'agit donc pas d'un palmarès des meilleures entreprises choisies en fonction d'un quelconque critère comparatif (innovation technologique ou marketing, chiffre d'affaires, meilleures pratiques, etc.).

La longueur des études de cas varie beaucoup d'une entreprise à l'autre et il ne faut pas y voir un jugement de valeur : ce n'est pas parce qu'une étude de cas est détaillée que l'entreprise est forcément plus innovante, active ou digne d'intérêt. Il faut plutôt y voir un reflet de la politique des dirigeants en matière de partage de l'information : certains d'entre eux ont été très généreux de leur temps, d'autres ont éprouvé des réserves devant certaines questions qu'ils considéraient comme confidentielles.

Liste des études de cas

- ✓ Auditia
- ✓ Above Security
- ✓ Carillon
- ✓ Cedval
- ✓ Forensic
- ✓ Gardien virtuel
- ✓ IBM Canada
- ✓ In Fidem
- ✓ Infrax
- ✓ Institut national de l'oprique (INO)
- ✓ Notarius
- ✓ Nurun
- ✓ Optosecurity
- ✓ PriceWaterhouse Coopers (PwC)
- ✓ RDDC Valcartier
- ✓ SecureOps
- ✓ S.I.C. Biometrics
- ✓ Silanis Technology
- ✓ Waveroad
- ✓ Zéropsam

Auditia

2484, rue Bennett
Montréal, Qc
H1V 3S4
(514) 660-8281
creverd@auditia.ca

Entrevue	Christophe Reverd, consultant
Contact	Christophe Reverd
Données de base	Constitution de la compagnie 2007 Nombre d'employés 1 Nombre d'employés au Québec 1 Marché Québec
Stratégie	Offrir le plus vaste éventail de services possible
Avantages et enjeux	Les petites compagnies ont difficilement accès aux grands clients. Ils doivent nécessairement passer par les grandes firmes de sécurité qui jouent le rôle d'intermédiaire.

Co-fondateur du premier fournisseur Internet en France en 1995, Christophe Reverd s'est installé au Québec en 2007. Il offre des services dans les 12 domaines de la sécurité de l'information prévus dans la norme PCI-DSS, ainsi que dans la continuité des affaires, la gouvernance et le légal jusqu'aux appels d'offres (clauses de sécurité) et la sécurité dans les télécommunications.

« Le Québec connaît une pénurie de ressources en TI et c'est également vrai en sécurité. Paradoxalement, il y a également une forte concurrence avec les grandes firmes de sécurité pour la clientèle des grands donneurs d'ordre. Mais, c'est toujours les firmes entreprises de sécurité qui remportent le contrat. Les micro-entreprises, comme la mienne, nous sous-traitons, » explique Christophe Reverd.

Above Security

1919, boul. Lionel Bertrand, suite 203
Boisbriand, Qc
J7H 1N8
450) 434-8060
marisol.litalien@abovesecurity.com
www.abovesecurity.com

Entrevue	Marcel Dion, CGA, Président et chef de la direction
Contact	Marisol Litalien, Directrice des communications et du marketing
Données de base	Constitution de la société: 1999 Siège social: Boisbriand Nombre d'employés en sécurité: 35 R-D: 10 Produits: Télésurveillance des réseaux Centre de Gestion de la Sécurité Clients: 80% - entreprises de 500 employés 20% - entreprises de 50 à 500 employés
Mission	Impartiteur en sécurité de l'information, Above Security ne vend pas de logiciels mais des services
Stratégie	Croissance internationale par le développement de partenariats
Moyens	Son programme bien structuré de recrutement et de formation de partenaires-revendeurs accélérera sa pénétration des marchés étrangers
Marchés	Canada, Amérique latine, Caraïbes et Europe
Avantages et enjeux	Above Security fait partie des fournisseurs de solutions en sécurité à l'échelle internationale qui sont membres du FIRST (*Forum of Incident Response and Security Teams*).

Above Security a été créée en 1999 par Marcel Dion et son fils Martin Dion, respectivement comptable et informaticien, chacun complétant l'expertise de l'autre. Ensemble, ils ont mis au point une solution de surveillance de la sécurité des réseaux qui protègent les organisations contre les attaques informatiques externes et les fraudes internes.

Above Security se présente comme le partenaire stratégique en matière de gestion des risques informationnels. Son principal service est la télésurveillance des réseaux informatiques. À partir d'un Centre de Gestion de la Sécurité (*Security Operation Center*), des analystes sont à pied d'œuvre 24/7 pour détecter toute intrusion et assurer la confidentialité des données échangées dans les réseaux de ses clients.

Des sondes sont installées stratégiquement dans les systèmes d'information qui recueillent et analysent le trafic et les messages circulant sur les réseaux, serveurs, systèmes d'exploitation et applications. Dès qu'une intrusion survient ou tout autre type d'anomalie, une alarme est transmise au centre de surveillance d'Above Security qui priorise l'incident et évalue l'impact sur les opérations de l'entreprise cliente.
Les systèmes de détection d'Above Security analysent également les données émises par les systèmes d'information des entreprises, ce qui permet de faire la détection d'usage non conforme d'Internet part les utilisateurs internes; accès à des sites pornographiques, le clavardage intempestif, l'usage de logiciel P2P, etc.

Plus d'une dizaine d'informaticiens certifiés travaillent en R-D pour intégrer les systèmes de protection contre les menaces informatiques. Quand une nouvelle menace est détectée, les experts d'Above Security sont proactifs et intègrent des mesures préventives selon le cas.

L'entreprise, qui compte 45 employés en 2010, offre également des services-conseils professionnels soit des audits opérationnels, audits techniques, politiques de sécurité, formation, plan de continuité des affaires, plan de recouvrement TI et conformité à des normes et standards tels que PCI-DSS, WLA:SCS, Bâle II et ISO 27001. [29]

L'entreprise dessert plus de 250 clients de grande taille dans 22 pays : 30% proviennent du Canada, 50% des Caraïbes et 20% d'ailleurs dans le monde. La clientèle provient du domaine des finances, de la pharmacie, des télécommunications, des manufacturiers et des gouvernements.

Sa stratégie d'affaires est basée sur les ventes directes pour les deux-tiers et le dernier tiers par un réseau de partenaires revendeurs. L'entreprise compte cibler davantage les revendeurs dans sa stratégie d'affaires au cours des années subséquentes et démarcher, en priorité, les marchés de l'Amérique latine, du reste du Canada et d'Europe.

Le chiffre d'affaires d'Above Security a augmenté à chaque année, y compris en 2009 lors de la crise financière. Le président estime que « le Canada est perçu à l'étranger comme étant digne de confiance et offrant des services de qualité. Cette réputation facilite grandement les affaires à l'international. »

L'entreprise n'a aucun problème de financement. Elle a pu compter les premières années sur l'aide d'Investissement Québec et de Développement Économique du Canada.

Above Security fait partie du nombre restreint et sélect de fournisseurs de solutions en sécurité à l'échelle internationale à être membre de FIRST (*Forum of Incident Response and Security Teams*). Cette participation permet à l'entreprise d'être informée, de façon instantanée, sur les plus récentes menaces informatiques et la façon d'y remédier. Above Security a été parrainée par la Défense Nationale du Canada pour faire partie de FIRST.

[29] ISO 27000 : norme internationale de système de gestion de la sécurité de l'information ;
PCI-DSS (Payment Card Industry) – mesure de contrôle dans l'industrie financière et de crédit ;
WLA :SCS – Contrôle et mesures propres au monde des loteries ;
Bâle II : dispositif prudentiel destiné à appréhender les risques bancaires et de crédit.

Carillon Information Security

356, rue Joseph-Carrier
Vaudreuil-Dorion, Qc
J7V 5V5
ppaterson@carillon.ca
514-485-0789

Entrevue	Patrick Patterson, president	
Contact	Patrick Patterson	
Données de base	Incorporation de la société	2001
	Siège social	Vaudreuil-Dorion
	Nombre d'employés en sécurité	7
	Employés au Québec	7
Mission	Offrir des services de gestion de l'identité à l'industrie aéronautique	
Stratégie	Se concentrer sur une seule clientèle en offrant un service ciblé	
Avantages et enjeux	L'engagement du gouvernement du Canada au sein de l'industrie aéronautique n'inclut pas le renforcement de sa sécurité; le fait de négliger cet important aspect constitue un enjeu majeur.	

Carillon Information Security a été fondée en 2001 par un groupe de quatre professionnels qui œuvraient en sécurité informatique dans le domaine de l'aéronautique. Le groupe était convaincu que le marché et le secteur étaient porteurs. « Au début, nos services portaient sur les infrastructures à clés publiques; puis, au fil des ans, nous avons recentré notre offre sur la gestion de l'identité », explique Patrick Patterson.

En 2001, la clientèle de Carillon se trouvait exclusivement hors-Canada, principalement en Europe. Aujourd'hui, ce ratio est plus équilibré avec 50% des clients au Canada et 50% dans le reste du monde.

Les contrats en gestion de l'identité sont généralement d'une durée de trois à quatre ans. Un plan de gestion de l'identité permet de réduire le nombre d'authentifications nécessaires pour accéder aux applications corporatives, ainsi que le nombre d'appels reçus par les services de soutien aux utilisateurs (par exemple, le recouvrement de mots de passe). Carillon participe activement au développement du programme mondial Transglobal Secure Collaboration Program (TSCP) sur le contrôle de l'identité dans l'industrie aéronautique. L'initiative TSCP à laquelle les grands joueurs de l'industrie participent, vise à diminuer le temps d'attente à l'information, à contrôler l'accès à leur propriété intellectuelle et à faciliter la conformité aux lois régissant l'exportation d'équipements et de technologies contrôlés.

L'avantage concurrentiel de Carillon est son expertise du milieu aéronautique. « Nous connaissons en profondeur les lois et réglementations de l'industrie et nous agissons à titre de conseillers techniques. Nous sommes partie prenante des associations du secteur, dont l'Association de transport aérien (ATA) et représentons des clients auprès d'associations comme le TSCP et CertiPath, qui regroupent les grandes sociétés du domaine aéronautique, ainsi que le gouvernement américain. »

« Tous les gouvernements des pays du G8, comme la France, le Royaume-Uni et les États-Unis participent activement aux associations de sécurité du domaine aéronautique. Seul le Canada ne le fait pas. C'est dommage parce que non seulement sa présence contribuerait à renforcer la sécurité domestique, mais aussi parce que cela permettrait de mettre en évidence les compagnies canadiennes qui travaillent dans le secteur. Il faut le dire et le redire : l'industrie aéronautique est un domaine stratégique pour le Canada et le gouvernement doit prendre une part active dans la promotion de la sécurité de cette industrie, » conclut Patrick Patterson.

Cedval Info inc.

1019 boul. Perrot
Notre-Dame-de-l'Ile-Perrot, Qc
J7V 3H7
514-816-5869
fmeehan@cedvalinfo.com
www.cedvalinfo.com

Entrevue	François Meehan, président	
Contact	François Meehan	
Données de base	Constitution de la société	2003
	Siège social	Notre-Dame-de-l'Ile-Perrot
	Nombre d'employés en sécurité	2
	Employés aux États-Unis	1
	R-D	2
	Produits	Test de pénétration de réseaux informatiques Audits de sécurité Solution de monitoring Aide à la conformité (SOX bill C-198 ISO 27001)
	Clients	Industries pharmaceutiques, manufacturières et autres.
Stratégie	Développement vers le Canada et les États-Unis	
Moyens	Développement de la R-D : Solutions logicielles d'aide à la conformité informatique pour les réglementations SOX,[30] Bill 198[31], ISO 27001[32]	
Avantages et enjeux	Cedval observe un regain de popularité notable pour la sécurité des TI par les entreprises et note les efforts de celles-ci en matière de gouvernance pour se conformer à leurs obligations de conformité.	

Cedval Info a commencé ses opérations en 2003. « C'est une entreprise pharmaceutique qui m'a permis de me lancer. Je travaillais trois jours semaine pour ce client et je développais une clientèle les deux autres jours, » explique François Meehan. Aujourd'hui, Cedval compte deux associés et un carnet de commandes parmi les entreprises de 500 employés et plus. Le secteur public ne représente que 10% du chiffre d'affaires.

Bien des grandes firmes de consultation livrent des services de qualité inégale. Cedval y a vu une occasion de fournir des services experts en sécurité, surveillance réseau et conformité.

« On a fait aussi un peu de « télé-réalité ». Il s'agissait de Loft Story et notre mandat consistait à mettre en place un système surveillance des équipements informatiques et évaluer la sécurité du réseau, » rappelle François Meehan.

30 Loi Sorbanes-Oxley, souvent appelé SOX. La loi créée en 2002 a pour but de réformer la comptabilité des sociétés cotées en bourse pour mieux protéger les investisseurs.
31 Bill 198, législation ontarienne promulguée en avril 2003, aussi connue sous le nom de C-SOX pour sa parenté avec la loi américaine dans les pratiques comptables et la sécurité des investisseurs.
32 L'ISO/CEI 27001 est une norme internationale de système de gestion de la sécurité de l'information, publiée en octobre 2005 par l'ISO.

Aujourd'hui, Cedval a développé une solution qui a été présentée avec succès au CRIM en 2010 et qui contribue à une meilleure gestion des incidents. Il s'agit d'un registre des incidents avec des fonctionnalités d'alertes et de journal de bord.

« Beaucoup d'entreprises veulent obtenir la certification ISO 27001. Pour ce faire, elles doivent avoir en place un système de gestions des incidents. Notre solution comporte de nombreux avantages pour elles. »

« La solution est simple : lorsqu'une alerte est émise par le système de monitoring, notre passerelle va générer un ticket dans le système *Help Desk*. Notre passerelle est bidirectionnelle, lorsqu'un professionnel en sécurité traite le ticket d'alarme et se charge du traitement de l'événement, le système de monitoring inscrit l'alerte dans le journal de bord mensuel et comptabilise le traitement de l'alerte conformément aux exigences d'ISO. Notre solution est disponible en tant que logiciel libre (Open source) et nous offrons un service d'aide pour les entreprises qui ont besoin de notre expertise, » explique le président.

« Comme notre solution logicielle est basée sur la philosophie des logiciels libres, elle permettra à un plus grand nombre d'entreprises d'entamer un processus en ce sens. Nous comptons accroître notre marché pour nos services d'audits de sécurité des services en TIC par le biais de conférences de sensibilisation de la sécurité de l'information, » conclut François Meehan.

Forensic

5757, boul. Cavendish
Côte-Saint-Luc, Qc
H4W 2W8
514-448-2751
patrick.doyon@forensic.com
www.forensic.com

Entrevue	Patrick Doyon, directeur du marketing	
Contact	Patrick Doyon	
Données de base	Siège social	Montréal
	Nombre d'employés en sécurité	200
	Employés au Québec	150
	R-D	25
	Clients	Gouvernements
Stratégie	L'entreprise utilise une stratégie B2G mixte de ventes directes et d'associations avec des revendeurs.	
Moyens	Forensic compte quatre bureaux à l'étranger : États-Unis (Floride), Afrique du sud, Irlande et Thailande.	
Marchés	Forensic vend partout dans le monde et s'attaque présentement à l'Afrique, l'Amérique latine et l'Asie.	
Avantages et enjeux	La reconnaissance balistique est un domaine de peu de joueurs. Forensic est dominant et doit toujours améliorer ses produits et services pour se maintenir à niveau. L'enjeu actuel est de convaincre les instituts des différents pays de partager avec d'autres leur base de données, le but étant de créer une base de données mondiale.	

Forensic Technology analyse les crimes, les armes et les suspects avec les technologies les plus évoluées au monde. La firme est, sans conteste, le joueur dominant dans le domaine de la balistique sur la scène internationale.

L'ensemble du système d'identification et d'analyse des douilles s'appelle IBIS Technology. Le système comporte plusieurs solutions dont la principale est la station d'imagerie pour balles, BulletTRAX-3D, utilisée dans le cadre d'enquêtes criminelles. Utilisant la toute dernière technologie sensorielle en trois dimensions, cette récente addition à la ligne de solutions IBIS donne aux opérateurs la possibilité de saisir des images numériques 2D et de créer des modèles topographiques de la surface d'une balle en trois dimensions. Le système BulletTRAX-3D est à la fois facile d'utilisation et hautement automatisé. Il permet aux opérateurs, pour la première fois, de prendre des mesures quantitatives de la surface d'une balle. Aucun autre système d'imagerie balistique ne combine la plus récente technologie 3D, la qualité de l'image ultra précise et la capacité éprouvée de fonctionner en réseau.

Une deuxième solution qu'offre Forensic Technology est le serveur de corrélation qui reçoit, gère et compare les signatures numériques uniques provenant des images de preuves balistiques. Ces signatures numériques sont ensuite mathématiquement comparées et classées en fonction de leurs similarités. Cette puissance de comparaison permet aux opérateurs d'effectuer des recherches rapides parmi des centaines ou des milliers de pièces, se concentrant seulement sur les candidats les plus probables.

Forensic Technology a également mis au point la station d'analyse de preuves balistiques la plus avancée au monde pour la résolution de crimes commis avec armes à feu – MatchPoint+. Avec de nouveaux outils

de visualisation qui permettent d'arriver à des conclusions éclairées, MatchPoint+ offre la plus récente technologie pour comparer et analyser à distance des preuves de douilles et de balles en deux et trois dimensions. MatchPoint+ donne aussi la possibilité de comparer des images numériques en mode côte à côte ou afficheur multiple. Aucune autre unité de comparaison ne combine la toute dernière technologie IBIS avec la visualisation d'images de haute résolution et la capacité éprouvée de fonctionner en réseau.

Stratégie d'affaires

La reconnaissance balistique est un marché niche au sein de la médecine légale. La stratégie de Forensic Technology est d'amener ses clients provenant de 35 pays et appartenant à 33 centres de médecine légale à partager leurs bases de données respectives. Hébergée chez Forensic Technology, cette base serait alors la plus grande base au monde de reconnaissance balistique. « Nous avons un marché captif, c'est vrai mais c'est un marché exigeant. Nos clients appartiennent au secteur gouvernemental et la plupart sont des scientifiques. Ils s'attendent à un perfectionnement constant de nos logiciels et de notre base de données. C'est un grand défi, » explique Patrick Doyon, vice-président marketing.

Gardien Virtuel inc.

1556, boul. de l'Avenir, bureau 110
Laval, Qc
H7S 2N5
514-236-0056
info@gardienvirtuel.ca
www.gardienvirtuel.ca

Entrevue	Marco Estrela, Vice-président aux ventes et marketing	
Contact	Marco Estrela	
Données de base	Constitution de la société	2003
	Siège social	Laval
	Nombre d'employés en sécurité	20
	Employés au Québec	20
	R-D	8
Mission	L'entreprise, certifiée ISO 27001, est spécialisée en vérification et audit de systèmes d'information, en tests de sécurité interne et externe, en applications internet et en audits de certifications basés sur les politiques des entreprises clientes ou selon les meilleurs pratiques de l'industrie, tel que ISO 17 799, ISO 27 001, CobiT, OCTAVE, OSSTMM.[33] La mission de l'entreprise est d'augmenter l'intégrité, la disponibilité et la confidentialité des réseaux et données de ses clients.	
Stratégie	Gardien Virtuel mise son développement sur la création d'une centrale de télésurveillance, inaugurée en avril 2010.	
Avantages et enjeux	Gardien Virtuel a misé sur le R-D ainsi que sur des partenariats université-secteur privé.	

Dès sa création en 2003, Gardien Virtuel visait une clientèle dans le secteur financier incluant les assurances et le secteur public. Aujourd'hui, la clientèle du gouvernement représente 20% des activités de la firme et le vaste marché des PME est dans la ligne de mire. Gardien Virtuel offre l'ensemble des services professionnels d'une société de sécurité, depuis les tests de pénétration interne et externe, jusqu'aux audits, tests de sécurité d'applications web, plan de continuité et accompagnement. Trois services distinguent la firme de ses concurrents : un service d'enquête juridico-informatique (*forensic*) mené par un expert reconnu, un programme d'audit pour l'obtention de la certification ISO 27 001 et une centrale de télésurveillance. Gardien Virtuel est la première firme canadienne spécialisée en sécurité de l'information à être certifiée ISO 27 001.

« Nous venons à peine d'inaugurer notre centrale de télésurveillance en avril 2010. Ce projet représente trois années de recherche et développement conduites par deux PhD à l'interne, en collaboration avec l'Université du Québec à Montréal, Polytechnique, l'Institut tunisien INSAT et l'université française SUPINFO. « Nous avons fait appel à l'expertise la plus pointue sur le marché international, explique Marco Estrela. Le résultat : le centre de surveillance est doté de programmes extrêmement flexibles qui

[33] Le CobiT (Control Objectives for Information and related Technology) : Objectifs de contrôle de l'Information et des Technologies Associées) est un outil fédérateur qui permet d'instaurer un langage commun pour parler de la Gouvernance des systèmes d'information tout en tentant d'intégrer d'autres référentiels tels que ISO 9000. Octave (Operationally Critical Threat, Asset, and VulnerabilityEvaluation) : Ensemble de techniques et de méthodes d'évaluation et de planifications de la sécurité. OSSTMM (Open Source Security Testing Methodology Manual) : Méthodologie Open Source pour les audits de sécurité.

s’adaptent aux besoins de la clientèle. Cela nous permet, entre autres, d’offrir des services à la carte et de n’intervenir, par exemple, que sur la détection d’intrusions ou la gestion des vulnérabilités. Nous offrons également des forfaits économiques pour des bouquets de services. Cette flexibilité tarifaire est la solution qui convient parfaitement aux besoins des PME. »

IBM Canada

140, Grande Allée Est, 5e étage
Québec, Qc
G1R 5N6
Tél. : (418) 521-8230
www.ibm.ca

Contact	Jules Bois, Directeur exécutif secteur public - Québec	
Interview	John Kokonis, Directeur exécutif unité d'affaires – Services de sécurité IBM	
Données de base	Constitution en société	1917 (au Canada)
	Siège social (Groupe SPT) Succursales	Markham, Ontario Ottawa, Montréal, Vancouver, Calgary
	Secteurs d'activité	Fournisseur de services, éditeur, intégrateur et impartiteur
	Technologies	Gestion des identités et des accès, Sécurité des applications, Conformité de la sécurité, Sécurité des infrastructures et Sécurité des informations.
	Employés	± 4 500 professionnels en sécurité dans le monde, 110 pour le Canada, dont 10 au Québec (base) + experts en impartition dans divers services.
	Revenus	n.d.
	Segments du marché	Institutions financières, Services publics (électricité), Commerce, y compris PME, Gouvernement.
	Situation géographique des clients	Canada
Mission	Offrir ce qu'il y a de mieux dans tous les domaines de la sécurité. Cette approche de bout en bout englobe la protection des personnes et de leur identité, les données, les applications, la conformité aux règlements et les meilleures pratiques. Mais si IBM offre toute la gamme des solutions de sécurité, elle permet à ses clients de choisir à la carte ce dont ils ont besoin sans imposer de forfaits contraignants.	
Stratégie	L'offre de sécurité d'IBM est basée sur les acquisitions. Depuis 2006, IBM a acheté onze entreprises de sécurité. L'entreprise complète cette stratégie d'intégration verticale par une série d'alliances avec des firmes spécialisées, comme PGP (chiffrement pour la protection des données d'entreprise).	
Moyens	Ces achats sont guidés par les besoins exprimés par les groupes de sécurité d'IBM dont les professionnels travaillent en étroite collaboration avec ceux chargés des acquisitions.	
Avantages et enjeux	- Chaque professionnel en sécurité au Québec a accès à l'expertise des 4 500 professionnels du groupe ; - le phénomène de « cloud computing » accroît les vulnérabilités.	

Historique de l'entreprise

Dans le domaine particulier de la sécurité, IBM Canada a une longue tradition. Ainsi, les procédures de sécurité et de protection de la confidentialité d'IBM Canada ont été mises en place en 1998 par trois experts basés à Toronto. Un important facteur de croissance a été l'acquisition en avril 2000 du Groupe LGS, comprenant le laboratoire Domus de sécurité de l'information basé à Ottawa (Domus avait été acheté par LGS en 1998). Le laboratoire Domus se spécialise dans l'évaluation des normes des produits de sécurité et des produits cryptographiques.

Plateforme technologique

IBM affirme être « technologiquement neutre » en matière de sécurité. Même si l'entreprise offre toute la gamme ou presque des systèmes et solutions de sécurité existants, elle n'hésite pas à fournir des produits tiers pour préserver le capital investi de ses clients ou leurs préférences.

Sa plate-forme technologique est sans cesse mise à jour au moyen d'un investissement massif en R-D, veille technologique et suivi des menaces. Le travail de contre-ingérence et de formation en matière de sécurité d'IBM est effectué par la division X-Force qui est issue en grande partie de l'entreprise Internet Security Systems (ISS) acquise en 2006. Or, ce sont les chercheurs de X-Force qui ont identifié le plus de menaces et de vulnérabilités au niveau mondial (plus de 51%). Grâce à ce travail de veille, X-Force dispose aujourd'hui d'une base de données détaillée de 48 000 cas d'incidents documentés dans tous les domaines de la sécurité. Au total, IBM détient 3 000 brevets dans le domaine de la sécurité.

L'offre d'IBM en sécurité est fondée sur son expertise professionnelle (gamme de services Tivoli), les solutions de chiffrement des données stockées, les applications et processus, les services réseaux et systèmes d'extrémité et, enfin, une nouvelle offre de services impartis.

Cette offre s'appuie sur une infrastructure globale de neuf centres virtuels d'opérations de sécurité (SOC), répartis entre l'Amérique du Nord (4), l'Europe (2), l'Asie/Pacifique (2) et un tout nouveau à Bengalore (Inde), ce qui permet à IBM d'assurer la supervision des besoins de ses clients 24/7: missions critiques, monitoring des systèmes d'électricité, traitement des données et gestion des liens de communication, ainsi que l'impartition de certains services (comme la prévention des intrusions, par exemple). Un des quatre SOC nord-américains est situé à Toronto.

Par ailleurs, il existe quatre centres IBM de continuité des opérations et de relève au Canada même (Montréal, Toronto, Calgary et Winnipeg), qui font partie d'un réseau mondial comprenant 120 centres similaires. Alimenté par une génératrice, le Centre de Montréal est doté d'une infrastructure informatique reliée par lignes directes aux systèmes hôtes situés à Markham (Ontario), Boulder (Colorado), Gaithersburg (Maryland) et Sterling Forest (New York). Dans cet environnement parallèle sous haute protection, une centaine d'espaces de travail peuvent accueillir en tout temps les employés des clients sinistrés. [34]

Stratégie de l'entreprise

Sur le plan mondial, IBM est en train de prendre le leadership de l'expertise grâce à sa politique d'acquisitions de compagnies, dont on peut dire qu'elle en a fait une science. Ainsi, pour décider d'une acquisition, il est bien sûr nécessaire qu'il y ait une bonne affinité entre l'acheteur et l'acheté. Le vice-président Marketing et stratégie pour IBM Rational Software, Scott Hebner, explique:
« IBM Software n'achète pas une compagnie à moins qu'elle n'ait déjà déterminé que ses clients ont un besoin; qu'un logiciel produit par une compagnie extérieure donnée remplit ce besoin; et qu'il est plus

[34] Centre IBM de continuité des opérations et de relève de Montréal : http://www-03.ibm.com/services/continuity/resilience.nsf/pages/montreal/$file/montreal_center-information-brochure_french.pdf

raisonnable d'acheter cette compagnie que d'essayer de mettre au point un système équivalent en partant de zéro, ou de concocter quelque chose à partir des produits existants d'IBM. » [35]

Tout aussi important aux yeux de la direction est l'existence de suffisamment de chevauchement avec ses propres produits de sorte que les « gadgets logiciels » ou « *widgets* » de la nouvelle compagnie puissent facilement s'insérer dans les activités globales de vente d'IBM. Ainsi, la compagnie achetée pourra croître à l'intérieur d'IBM plus rapidement que si elle était restée indépendante. Quand la compagnie achetée a une image de marque forte, qui commande la fidélité d'une clientèle établie, elle pourra même conserver son nom qui deviendra une marque IBM.

La plupart des autres produits sont intégrés dans la division de gestion et de sécurité Tivoli qui est elle-même issue d'une acquisition. Tivoli était à l'origine une petite entreprise texane spécialisée dans la gestion des serveurs; aujourd'hui, c'est une des divisions les plus dynamiques et les plus rentables d'IBM.

Le résultat est une feuille de route atypique dans l'industrie des TIC où les statistiques démontrent que 30% seulement des opérations de fusion-acquisition sont couronnées de succès. Au contraire, IBM réussit toutes ses acquisitions, comme en témoigne la liste des achats sans le secteur de la sécurité :

- juillet 2010 : **BigFix**, pour 400 millions de dollars (estimation), développeur de solutions logicielles pour automatiser la gestion de la conformité et la sécurité (Californie);
- février 2010: **Initiate Systems**, développeur de logiciels de gestion des données de base de l'entreprise (Illinois);
- janvier 2010 : **National Interest Security Company (NISC)** pour 1,3 milliard de dollars (estimation), développeur de systèmes de sécurité et d'exploration de données pour la défense et le contre-espionnage, la santé et l'énergie (Washington DC);
- septembre 2009 : **Guardium** pour 225 millions de dollars, développeur d'outils de sécurité pour les bases de données (Massachusetts);
- juillet 2009 : **Ounce Systems**, développeur d'outils de sécurité et de détection de vulnérabilités (Massachusetts);
- mars 2008 : **Encentuate**, développeur de logiciels d'identité et de gestion d'accès (Californie);
- septembre 2007: **Softech**, développeur d'outils de sécurité et de gestion pour les bases de données (New Jersey);
- juillet 2007: **Watchfire**, pour 100 millions de dollars (estimation), développeur d'outils de tests de sécurité (Canada); [36]
- janvier 2007: **Consul**, développeur d'outils pour les audits et la conformité (Pays-Bas);
- octobre 2006: **Internet Security Systems (ISS)** pour 1,3 milliard de dollars, développeur d'outils de sécurité sur Internet qui a aussi donné naissance à X-Force en 1998 (Georgie).

Cette stratégie a été couronnée en février 2010 par *SC Magazine* (http://www.scmagazine.com/) qui a choisi IBM comme la meilleure compagnie de sécurité à la conférence RSA de San Francisco.

Nature du marché

Le marché de la menace s'est déplacé vers les systèmes d'extrémité. En conséquence, la priorité qui était traditionnellement accordée au trafic entrant porte maintenant sur le trafic de sortie. Les clients veulent s'assurer que leurs bases de données soient accessibles seulement aux bonnes personnes. Ils estiment que leurs activités centrales sont désormais bien protégées et veulent accroître la protection du périmètre.

Chaque année, X-Force publie un bilan mondial sur les tendances et risques en termes de cybercriminalité. Au sein de ce panorama global, le marché canadien apparaît toujours en retrait par rapport à la moyenne des pays industrialisés. Même le secteur bancaire apparaît relativement peu

[35] Wasde Roush, IBM and the Art of Acquisitions, *Xconomy*, Boston, 14 avril 2008.
[36] Entreprise basée à Ottawa-Kanata et fondée en 1996, Watchfire avait fait œuvre de pionnier en matière d'outils de test pour sites web. L'entreprise avait créé le premier système de vérification des liens (Linkbot). Par la suite, elle avait mis au point des outils englobant l'ensemble de la gestion des sites web : Watchfire Enterprise Solution (WES) en octobre 2000, puis WebXM en février 2002. L'entreprise comptait environ 85 employés au moment de l'acquisition.

développé. Une raison du manque de dynamisme de ce marché pourrait être la légèreté de la réglementation canadienne qui est peu contraignante et peu incitative.

IBM Canada dessert essentiellement le marché canadien. Ses exportations consistent principalement à fournir des services aux entreprises canadiennes qui ont des activités à l'étranger.

Enjeux

IBM est des chefs de file mondiaux sur le marché de la sécurité. La force d'IBM vient en grande partie de ses outils de collaboration qui lui permettent de mobiliser très rapidement les meilleures spécialistes dans un domaine particulier afin de traiter en ligne un incident même inusité, d'en extraire les principales caractéristiques et de mettre au point une solution.

Pour demeurer à la pointe de l'industrie de la sécurité, IBM est en train de réorienter son offre en fonction des nouvelles vulnérabilités que contient l'informatique de type « infonuage » (*cloud computing*). Grâce à la nature « réseautée » de l'entreprise à l'interne et à l'externe (coopération avec les gouvernements et les éditeurs de logiciels), IBM entend maintenir son avantage concurrentiel.

In Fidem

300, avenue Saint-Sacrement, bureau 412
Montréal, Qc
H2Y 1X4
514-847-3664
matthieu.chouinard@infidem.biz

Entrevue	Mathieu Chouinard	
Contact	Mathieu Chouinard	
Données de base	Siège social Nombre d'employés en sécurité Employés au Québec R-D Clients	Montréal 15 15 3 Affaires – 70% Gouvernements – 30%
Mission	In Fidem s'assure de doter les organisations des meilleurs moyens qui permettent de gérer et de contrôler leur sécurité en se basant sur une approche de gestion des risques ainsi que sur un transfert de compétences par la formation de ses clients.	
Stratégie	In Fidem veut être un rassembleur dans le secteur d'activité afin d'offrir à ses clients une palette complète de services en sécurité, que ce soit par embauche ou par partenariat. Outre les contacts directs avec la clientèle, In Fidem assure sa commercialisation en participant à des conférences et des séminaires.	
Marchés	Québec - plus de 90% Canada et États-Unis – 5% Reste du monde – 5%	
Avantages et enjeux	In Fidem est bien positionnée au Québec avec 15 experts-conseils dans le domaine de la sécurité. Cette équipe est composée d'experts seniors qui comptent une grande expertise en gouvernance et organisation de la sécurité.	

Mathieu Chouinard œuvre en sécurité depuis 1997. Il a créé In Fidem, en 2005, avec pour mission d'aider les organisations à prendre le contrôle de leur sécurité de bout en bout. L'entreprise planifie et réalise des plans directeurs, met en place des programmes de conformité, réalise des audits et veille à la sensibilisation ainsi qu'à la formation de sa clientèle.

« Le mot clé chez In Fidem est l'accompagnement. Nous faisons le point avec nos clients sur leur situation et leurs besoins, puis nous proposons des programmes pour qu'ils puissent atteindre leurs objectifs d'affaires, » explique Mathieu Chouinard.

In Fidem travaille aux États-Unis et au Moyen-Orient : « Nous avons cette chance grâce à l'établissement d'alliances avec des firmes complémentaires à nos services. Cela nous permet, notamment, d'enrichir notre veille technologique et nos connaissances parce que les cultures en sécurité sont différentes d'un pays à un autre. Les Américains, par exemple, ont vécu des situations qui les rendent moins tolérants aux risques que les Canadiens, » indique Mathieu Chouinard.

Le président d'In Fidem croit qu'une réglementation accrue en sécurité au Canada aurait un impact mitigé : « Il faut sensibiliser et éduquer les gens pour créer un impact durable. La sécurité, c'est une culture et cela s'apprend. La réaction envers l'exigence de conformité est souvent de mettre en place des contrôles sans se soucier de leur importance, sans gérer la réaction humaine envers le changement créé par l'intégration d'une nouvelle mesure de sécurité. Si on veut avoir du succès à long terme, il faut réussir à modifier les comportements et la culture envers l'adoption de nouvelles approches. »

INFRAX inc.
2, Place du Commerce, bureau 160
Montréal (Ile-des-sœurs), Qc
H3E 1A1
(877) 767-1070
http://www.infrax.com/

Interview	Benoit H. Dicaire, stratège en sécurité informationnelle	
Contact	Benoit H. Dicaire, idem	
Données de base	Constitution de la société	1995
	Siège social	Montréal
	Nombre d'employés en sécurité	1
	Employés au Québec	1
	R-D	s.o.
	Revenus	n.d.
	Clients	
Stratégie	Développement d'une expertise mesurable par certification systématique.	
Moyens	Sous-traitance pour les grandes firmes de conseil informatique.	
Avantages et enjeux	Développement d'un modèle (*template*) de déclaration d'incidents et de triage à destination du marché ontarien.	

Historique de l'entreprise

Infrax a été créée en 1995 pour répondre aux besoins engendrés par la popularisation d'Internet. Ses premiers grands contrats ont été la mise en place des accès Internet pour les employés de Québec-Téléphone à Rimouski (passerelles, politiques de sécurité…) et la création d'un extranet pour Avnor Pâtes et papier (aujourd'hui Abitibi Bowater) afin de gérer les commandes du *New York Times*. C'est ainsi qu'Infrax est devenu un spécialiste d'architecture de réseaux IP sécurisés.

Infrax a rapidement augmenté jusqu'à huit employés en 2005. À ce moment, Infrax a cédé ses employés au Groupe Informatique TechSolCom. Le principe était pour le président d'Infrax de se concentrer sur l'exécution du volet sécurité des mandats, tandis que TechSolCom assurerait la gestion des mandats. L'entente a bien fonctionné pendant quelques années jusqu'à ce qu'Infrax reprenne son autonomie.

Aujourd'hui, Infrax est une micro-entreprise qui travaille principalement pour Telus dans le cadre du RITM. Son président participe en tant que consultant à l'élaboration du cadre de gestion technologique et de sécurité de l'information.

Offre

- Politiques et normes de sécurité
- Classification des données
- Gestion de risques
- Diagnostic de l'architecture
- Évaluation du profil de sécurité

Pour le marché de la PME, Infrax a créé un package de services conseil destiné à gérer les incidents de sécurité : modèles (*templates*) de déclaration d'incidents et de triage pour diriger les demandes vers la cellule de crise de l'organisation.

Stratégie d'affaires

- Développement d'une expertise mesurable grâce à des certifications aussi complètes que possible en sécurité de l'information, en technologies de l'information, en gestion de projets : Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Project Management Professional (PMP) et tout récemment Certified in the Governance of Enterprise IL (CGEIT).
- Participation à des associations telles COMPTIA, ISSEA et la Worldwide Association of Business Coaches.
- Conférences spécialisés : Colloque québécois de la sécurité de l'information (CQAI), Rendez-vous de la sécurité de l'information (RSI), Passeport Formation des auditeurs de Montréal, etc.

Nature du marché

Infrax travaille pour les grandes entreprises (Telus, Desjardins, les manufacturiers…) et un peu pour le gouvernement du Québec. En tant que micro-entreprise, Infrax agit souvent comme sous-traitant d'une grande société de services.

Infrax avait une partie de sa clientèle aux États-Unis jusqu'en 2007, mais la hausse du dollar canadien a rendu ses services non concurrentiels sur le marché américain. En outre, la crise financière de 2008 a ralenti les affaires aux États-Unis.

La stratégie de rechange d'Infrax consiste à attaquer systématiquement le marché ontarien. Sur ce marché, Infrax poursuit une stratégie différente du Québec. La firme vise avant tout la PME par sa nouvelle offre de package de services conseil offerte à un prix fixe. Un réseau de distributeurs locaux sera donc mis en place.

Concurrence

La concurrence sur le marché québécois de la sécurité est intense, car il n'existe pas de leader incontestable en matière de sécurité. CGI aurait pu jouer ce rôle de leader, mais son équipe de sécurité est trop fragmentée entre ses verticales, il lui manque un grand centre de sécurité. Deloitte semble être le plus gros joueur, mais son siège social pour le Canada est à Toronto.

Parallèlement aux grands joueurs de services professionnels, il y a une pléthore de petites entreprises et de micro-entreprises.

Enjeux

Les entreprises ne respectent souvent pas les lois canadiennes et québécoises sur la sécurité des renseignements personnels, parfois par ignorance ou encore parce que ce n'est pas obligatoire, mais le plus souvent en raison de l'inadéquation des structures organisationnelles en place.

La responsabilité de la protection de la vie privée (*Chief Privacy Officer*) est souvent confiée à un avocat du service du contentieux. Or, le service des TIC n'invite pas le CPO aux réunions techniques. Celui-ci n'est donc pas au courant des derniers changements techniques apportés aux systèmes informatiques et les responsables des TIC ne sont pas au courant des nouvelles lois et règlements ou encore de la nature précise des derniers contrats conclus par l'entreprise.Le résultat de ce flou administratif est que les processus et systèmes de l'entreprise ne sont pas conformes au cadre législatif en vigueur et se retrouvent à risque.

Chaque firme de sécurité doit avoir dans sa boîte à outils un cadre de gestion de la sécurité (*security framework*) de l'information (qui couvre donc aussi bien la sécurité informatique que la sécurité physique) afin de s'assurer que le client puisse prendre des décisions homogènes, conforme aux lois et règlements et basées sur de l'information de qualité.

Institut national d'optique

2740, rue Einstein
Québec, Qc
G1P 4S4
418-657-7006
pierre.galarneau@ino.ca
www.ino.ca

Entrevue	Pierre Galarneau, vice-président	
Données de base	Constitution de la société	1985
	Siège social	Québec
	Nombre d'employés en sécurité	35
	Employés au Québec	225
	R-D	En continu
	Produits	Télésurveillance des réseaux Centre de Gestion de la Sécurité
	Clients	50% - centres de recherche 37% - universités 13% - entreprises privées
Mission	Centre d'expertise de calibre mondial en optique et photonique	
Stratégie	Croissance internationale par vente directe, distributeur et développement de partenariats	
Moyens	Les programmes de R-D assurent la dominance d'INO sur plusieurs marchés ainsi que les liens avec le ministère de la Défense.	

L'Institut national d'optique, créé en 1985, est situé dans le Parc technologique du Québec métropolitain. L'INO est un centre d'expertise de calibre mondial en optique et photonique qui aide les entreprises en vue d'améliorer leur compétitivité et de contribuer à leur développement. Il assure sa croissance en créant de la propriété intellectuelle qu'il met en valeur par des contrats de recherche et développement, par la production de prototypes, par le transfert de technologies et en mettant de l'avant des projets novateurs et créateurs d'emploi.

Au cours des dernières années, l'INO a eu à de multiples reprises l'occasion de réaliser des projets liés au domaine de la sécurité, que ce soit pour le compte ou en collaboration avec le ministère de la Défense nationale par le biais d'un de ses centres de recherche (RDDC-Valcartier, RDDC-Toronto), le gouvernement américain (USAF, US-ARMY) ainsi que les industries œuvrant dans le domaine.

Plateforme technologique

Avec 225 employés, dont 80% possèdent une éducation supérieure en science et technologie, l'INO poursuit 14 axes de développement. Dans le domaine de la sécurité et de la défense, l'INO produit des capteurs infrarouges à non refroidissement et vend la technologie à des grandes firmes de défense. « Il y a des grandes entreprises qui font ce produit comme Raydon et DSF, mais notre offre s'arrime à la leur, » explique Pierre Galarneau.

L'INO était dans une position privilégiée pour développer cette technologie parce que l'entreprise avait créé une variété de fibres optiques spécialement adaptées aux besoins spécifiques de ces capteurs.

Les capteurs à fibre se démarquent avantageusement des capteurs électroniques par leur insensibilité aux interférences électromagnétiques, à la corrosion, aux radiations et aux températures élevées

(environnements hostiles); par leur petite dimension (typiquement < 1 mm) et leur grande portée (1 à 10 000 m) ainsi que par l'absence de conductivité électrique et leur faible conductivité thermique.

Modèle d'affaires

L'INO n'a pas de concurrents parce que l'entreprise procède par transferts technologiques. Le modèle d'affaires est comparable aux FRANHOFER d'Allemagne[37].

Deux personnes à temps plein sont responsables de la commercialisation directement avec la clientèle et, également, par l'entremise de distributeurs. Pierre Galarneau explique : « La récession n'a pas ralenti nos opérations. Nous avons obtenu beaucoup de contrats en lien avec l'Afghanistan et la montée du terrorisme. Nos revenus ont augmenté de 36% en 2009 et de 20% en 2008. Nous prévoyons croître en 2010. »

Sur la R-D et les relations internationales

L'INO maintient et développe des collaborations à l'échelle nationale et internationale. Plus d'une vingtaine de programmes dont plusieurs en sécurité sont en cours. Ces activités touchent 10 pays (États-Unis, Brésil, Allemagne, France, Belgique, Suisse, Finlande, Pologne, Égypte et Japon). La moitié des partenaires de l'INO sont des centres de R-D, 37 % sont des universités, et les autres sont des entreprises privées. Ces collaborations portent sur les échanges de personnel ou des études conjointes dans certains domaines. Ces activités sont importantes, car elles permettent à l'INO de compléter sa veille technologique, de valider l'information obtenue lors de différentes conférences scientifiques sur l'état de la technologie, et de se maintenir à la fine pointe des avancées dans ses divers champs d'activités.

[37] Le Fraunhofer-Gesellchaft est un organisme allemand dédié à la recherche en sciences appliquées.

Notarius inc.

1080, Côte du Beaver Hall, bureau 700
Montréal, Qc
H2Z 1S8
(514) 281-1577
http://www.notarius.com/

Entrevue	Charles Tremblay, Directeur commercial service aux membres	
Données de base	Constitution de la société	1996
	Siège social	Montréal
	Nombre d'employés total	50
	Nombre d'employé en sécurité	3
	R-D	En continu
	Produits	Autorité de certification (signature numérique); Gestion de la sécurité de l'information
	Clients	Secteur financier, commerce de détail, ordres professionnels, ministère, défense nationale, premiers répondants, etc
Mission	Autorité de certification québécoise	
Stratégie	Démontrer que la signature électronique est non seulement sécuritaire mais économique	
Moyens	Miser sur la R-D dans le domaine de l'infrastructure à clés publiques et le développement de logiciels relié à la certification de documents électroniques PDF Adobe	

Notarius, filiale technologique de la Chambre des notaires du Québec, est un organisme à but non lucratif créé en juin 1996. Notarius a mis en place une infrastructure à clés publiques assurant la délivrance d'une signature numérique de confiance adaptée aux normes de pratiques professionnelles de différents secteurs économiques. En effet, la création, la transmission et l'archivage de l'information par voie électronique ont changé la donne. Aujourd'hui, tout professionnel qui se sert de ce support d'information doit assurer la sécurité et l'intégrité de ses documents électroniques.

La signature numérique est basée sur une infrastructure à clés publiques et fonctionne à partir d'un procédé technologique, reconnu mondialement, appelé cryptographie à clés asymétriques. Les certificats de Notarius sont émis par une autorité de certification, enregistrée sous le nom de Centre de certification du Québec (CCQ), à la suite d'une vérification de l'identité et d'une validation du statut professionnel du futur détenteur. La signature numérique est une marque personnelle, une clé privée de signature, apposée sur un document électronique et qui confirme de manière irréfutable l'auteur du document électronique et en protège l'intégrité contre toute tentative de modification.

Notarius est l'organisme de certification d'un très grand nombre de corporations professionnelles. Il compte parmi ses membres au Canada des associations d'ingénieurs et d'architectes. Au Québec, la solution offerte par Notarius est, non seulement, adoptée par des ordres et des associations, mais également par des entreprises appartenant à diverses sphères d'activité qui veulent conférer à leurs documents électroniques une authenticité fiable et en protéger l'intégrité tout au long du cycle de vie du document.

Les ordres et associations adoptent d'emblée la solution parce que celle-ci sous-tend directement leur mission de protection du public. Ce dernier a ainsi l'assurance qu'un document électronique est bel et bien l'œuvre d'un membre en règle de l'Ordre ou de l'association professionnelle, ayant toutes les compétences pour exercer sa profession. Pour le professionnel, elle protège l'intégrité de son œuvre sur support électronique contre toute tentative de modification ou de manipulation de ses documents par des clients ou partenaires mal intentionnés.

« Nous avons toujours considéré le papier comme étant notre concurrent, explique Charles Tremblay. Dans le cas des grandes entreprises, il a fallu démontrer que la solution pouvait aisément s'inscrire dans les processus d'affaires et entraîner des économies par rapport au papier. N'oublions pas que grâce à la signature, on saute l'étape de l'impression papier, de la reliure, de l'archivage des originaux et de la numérisation, et enfin de l'envoi, par messager… ce qui réduit grandement l'empreinte environnementale. »

Nurun Inc.

330, rue Saint-Vallier Est, bureau 120
Québec, Qc
G1K 9C5
418 627-2001

Entrevue	Guillaume Langlois, directeur exécutif associé
Contact	Guillaume Langlois
Données de base	Constitution de la société 1985 Siège social Montréal Succursale Québec Nombre d'employés en sécurité 35 Employés au Québec 450
Mission	L'unité d'affaires services conseils Nurun s'engage à accompagner ses clientèles dans l'élaboration de leurs stratégies d'affaires et à contribuer à l'atteinte de leurs objectifs organisationnels et communicationnels en faisant appel aux technologies de l'information.
Stratégie	Attirer, mobiliser et retenir les talents permet à Nurun d'être le leader de l'intégration de solutions d'affaires Web conviviales, sécuritaires et optimales par la conception et la mise en œuvre de modèles d'affaires et de services d'entreprises innovants et adaptés.
Avantages et enjeux	Nurun mise sur une approche multidisciplinaire, pragmatique et axée sur la satisfaction de sa clientèle afin de proposer une vision intégrée des aspects organisationnel, juridique, humain et technologique de la sécurité de l'information. Pour réaliser leur mission de façon efficace, les organisations doivent désormais tirer profit des nouveautés du Web 2.0, réagir rapidement aux changements technologiques et disposer de moyens de communication modernes pour échanger avec leur clientèle et leurs partenaires. Le défi que Nurun relève consiste à mettre en œuvre l'ensemble de ces services tout en assurant la sécurité de l'information.

Depuis 1985, Nurun s'est fait connaître pour son expertise en matière de sites de gouvernement enligne acquise principalement auprès du gouvernement du Québec. Depuis quelques années, Nurun services-conseils se diversifie et est de plus en plus présente en sécurité dans le marché de l'industrie privée, la santé et le commerce enligne.

« En plus d'être reconnu en matière d'implantation de solutions technologiques de sécurité, Nurun possède une offre de service complète en sécurité de l'information. Nous offrons notamment des services de gouvernance, de conformité, de sensibilisation, d'analyses de risques, de sécurité dans les développements, de gestion de l'identité et des accès. Notre clientèle est essentiellement québécoise, mais nous réalisons également des mandats ailleurs au Canada, aux États-Unis, en France et en Chine, » explique Guillaume Langlois.

Optosecurity

505, boul. du Parc-Technologique
Québec QC
G1P 4S9
418 653 7665
lfrancoeur@optsecurity.com
www.optosecurity.com

Entrevue	Éric Bergeron, Président et chef de la direction	
Contact	Lucie Francoeur Constitution de la société Siège social Nombre d'employés en sécurité	Directrice du marketing et des communications 2004 Québec 40
Mission	Optosecurity s'engage à accroître la sécurité dans le monde	
Stratégie	Établir la norme d'excellence en matière de technologie de détection des menaces.	
Moyens	Agit comme chef de file dans l'industrie de la sécurité grâce à une technologie novatrice et des produits et solutions uniques dans le but d'établir de nouvelles normes en matière de détection des menaces.	
Avantages et enjeux	Les politiques de R-D des gouvernements du Canada et du Québec ont joué un rôle majeur dans le développement d'Optosecurity.	

Éric Bergeron est ingénieur physicien de formation mais se définit avant tout comme un entrepreneur. Il possède 20 ans d'expérience en gestion au sein d'entreprises en démarrage dans le secteur technologique : les « *start-up* ». C'est en 2003 qu'Éric Bergeron s'intéresse à une technologie qu'a développé l'Institut national de l'optique (INO), à Québec, pour une application militaire. « L'INO n'avait pas d'entrepreneur à l'interne pour développer cette technologie. J'ai donc créé un *spin-off* et pendant près de deux ans, j'ai développé une compagnie avec mes seules ressources. En 2005, j'ai réussi à lever 5M$ d'investissements en capital de risque, ce qui m'a permis d'embaucher une équipe de chercheurs et de commencer à développer le produit avec un premier client » explique Éric Bergeron.

Cinq ans plus tard, la technologie d'imagerie en rayons-X n'a plus rien à voir avec l'application initiale à l'origine de la création de l'entreprise. Principalement parce qu'elle est devenue une application commerciale destinée à des fins civiles aussi bien que militaires. Optosecurity a développé le tout premier système de détection automatique de menaces aux points de contrôle de sécurité de bagages à main. La solution de détection des armes conçues par Optosecurity repose grandement sur l'extraction des caractéristiques et la reconnaissance des formes, bien qu'elle se serve également de l'analyse de base du matériel et de nombreux algorithmes complexes relatifs au traitement des signaux. L'OptoScreener peut être utilisé dans tous les lieux qui exigent une sécurité maximale, comme les centrales nucléaires et les postes de contrôle d'infrastructures critiques.

« Nous pouvons détecter une bouteille de nitroglycérine dans les bagages, alors qu'à l'œil nu, le récipient semble être rempli d'eau, précise le président qui ajoute : l'OptoScreener est un système d'aide à la décision qui accroît les capacités des systèmes de détection à rayons-X conventionnels et qui permet aux

agents de sécurité de mieux identifier les menaces potentielles, comme les armes et les liquides dangereux. »

Optosecurity a déposé 60 brevets dans différents pays. L'entreprise est la première à offrir un tel service de protection des passagers et des infrastructures critiques. Au cours des prochaines années, la firme étendra ses services à la détection de menaces, notamment des cargaisons aériennes et portuaires.

Aujourd'hui, alors que la compagnie entre officiellement dans sa première année d'exploitation commerciale, Optosecurity fait affaire principalement aux États-Unis avec des clients reliés au domaine de la défense mais aussi avec des centrales nucléaires et d'autres installations à haute sécurité.

PricewaterhouseCoopers (PwC)

1250 boul. René-Lévesque Ouest, 28e étage
Montréal, Qc
H3B 2G4
(514) 205-5001
http://www.pwc.com/ca/

Interview	Marc Fournier, Associé délégué, et Maxime Rousseau, Premier conseiller	
Contact	Marc Fournier	
Données de base	Constitution de la société	1849
	Siège social	New York
	Nombre d'employés	Monde : 163 000 Canada : 5 200 Sécurité monde : 2 300
	Employés au Québec	n.d.
	R-D	s.o.
	Revenus	n.d.
	Clients	Banques, grandes entreprises
Stratégie	Veille technologique et mise au point de processus éprouvés en matière de gouvernance de la sécurité.	
Moyens	Services professionnels de haut niveau.	
Avantages et enjeux	Adapter la gouvernance de l'entreprise aux exigences de la sécurité.	

Historique de l'entreprise

L'origine de la sécurité informatique à PricewaterhouseCoopers (PwC) est ancienne. Le contrôle des accès et de la sécurité des systèmes informatiques a commencé avec la popularisation des logiciels comptables dans les années 70, la mise au point d'une prestation de sécurité est devenue indissociable de la gestion d'entreprise. C'est donc très tôt que PwC – tout comme ce qu'on appelle les « Big Four » [38] – se sont assuré que les données comptables dans les entreprises où elles agissent comme vérificateurs demeurent protégées contre la modification. La sécurité informatique est née dans les sociétés de services professionnels.

Il s'agissait d'abord de pouvoir certifier les états financiers des clients. Par la suite, avec l'expansion des systèmes informatiques dans toutes les sphères de l'activité humaine, nous avons cherché à aider nos clients à se protéger, à protéger leurs systèmes et aussi à mettre en place des outils de sécurité qui leur permettent d'être plus efficaces en termes de gestion des accès, de conformité à la réglementation ainsi que de protection des renseignements personnels.

Le besoin de protection a évolué et il existe aujourd'hui de nombreuses firmes qui sont spécialisées en sécurité. Toutefois, même si une firme comme PwC consacre une part minime de ses ressources à la sécurité, en termes d'effectifs, cela fait quand même, à l'échelle mondiale, quelque 2 300 conseillers qui sont spécialisés dans ce domaine. C'est probablement beaucoup plus important que bien des firmes qui font uniquement de la sécurité.

[38] L'expression « Big Four » designe les quatre grandes sociétés de services professionnels : Deloitte Touche Tohmatsu, Ernst & Young, KPMG et PricewaterhouseCoopers.

Plateforme technologique

« PwC est un fournisseur de services, déclare Marc Fournier. Nous ne fabriquons et ne vendons aucun outil de sécurité. Notre rôle est d'aider un client à choisir le bon outil, à l'installer, à le configurer et à mettre les processus en place pour permettre de gérer l'outil ainsi que la valeur qu'il engendre. »

Stratégie d'affaires

Selon Marc Fournier : « La force des services de PwC repose sur deux caractéristiques :
- nous sommes présents dans 151 pays sur les projets les plus variés qui soient, ce qui fait qu'il y a toujours quelqu'un dans le monde qui est capable d'exécuter le mandat;
- la force de ce réseau est multipliée par la longueur de l'expérience en sécurité, donc par la maturité des solutions mises au point. »

« Nous avons ainsi pu monter un système de vigie qui s'exerce sur la scène internationale et à travers les années. La stratégie de PwC est d'aider ses clients technologiquement avancés à prévoir le futur. »

Nature du marché

« Le marché de la sécurité au Québec est encore dans une phase de transition. Il n'y a pas si longtemps encore, quand nous présentions à un client l'état des risques encourus en faisant des comparaisons avec les États-Unis, l'Europe ou l'Australie, il protestait que les choses étaient différentes ici. Il ne voyait pas le risque. Il a fallu attendre que ce même client lise dans le journal que son concurrent éprouvait des difficultés ou encore que lui-même affronte un incident, pour qu'il commence à réagir. »

Enjeux

« PwC est entièrement orientée vers la stratégie et les processus tactiques. Notre rôle est de placer les questions de sécurité sur le niveau de la gouvernance et de la stratégie de l'information. »

RDDC Valcartier

Recherche et Développement pour la défense Canada (RDDC)
2459, boulevard Pie-XI Nord
Québec, Qc
G3J 1X5
Tél : (418) 844-4000
www.valcartier.drdc-rddc.gc.ca/

Interview	Guy Vézina, Directeur général Richard Delagrave, Directeur général adjoint	
Contact	Richard Delagrave, Directeur general adjoint	
Données de base	*Constitution de la société*	1945
	Siège social	Québec, Qc
	Nombre d'employés en sécurité	100
	Employés au Québec	400
	R-D	Conception, développement et évaluation de : Systèmes de protection du personnel; Systèmes de protection des plateformes; Systèmes d'arme; Systèmes de commandement et contrôle; Systèmes complexes (renseignement, surveillance et reconnaissance).
	Revenus	70 M $
	Clients	Forces canadiennes, Canada, États-Unis, OTAN, pays alliés
Stratégie	RDDC Valcartier axe sa stratégie d'opération sur les activités et les besoins du ministère de la Défense nationale. RDDC Valcartier utilise aussi les retombées de son programme de R-D de calibre international afin d'offrir des possibilités commerciales au secteur privé pour les applications militaires ou civiles. Les entreprises qui collaborent avec le Centre bénéficient aussi de son réseau national et international de contacts.	
Moyens	RDDC Valcartier demeure à l'affût de partenaires novateurs sur le plan technologique et avant-gardistes qui peuvent aider à continuer à faire face à ces défis. Les partenariats de R-D pour la défense Canada incluent des collaborations avec d'autres organisations nationales et la communauté internationale. Ces collaborations sont facilitées par les programmes de partenariat de R-D pour la défense Canada.	
Avantages et enjeux	RDDC Valcartier dispose des ressources scientifiques et financières nécessaires pour encourager les entreprises en défense et sécurité à s'engager dans les activités de R-D. Un des objectifs vises par RDDC Valcartier est de favoriser la synergie public-privé en matière de sécurité.	

Historique de l'entreprise

Recherche et développement pour la défense Canada — Valcartier a vu le jour en 1945. Son but était de renforcer le parc technologique de l'armement canadien en encourageant la R-D. Depuis, des découvertes technologiques majeures en matière de défense et de sécurité nationale se sont succédées.

À l'origine, la plupart des technologies qui faisaient l'objet de recherches s'inscrivaient dans une perspective exclusivement militaire: d'abord les missiles (1945-1945) et la défense active contre les missiles balistiques intercontinentaux (1955-1975), puis la consolidation des systèmes d'armes, de l'électro-optique et des systèmes d'information appliqués au commandement et au contrôle (1970-1995).

Aujourd'hui, les programmes de recherche mis de l'avant par RDDC Valcartier ont des applications qui sont à la dois liées à la défense et à la sécurité (militaire ou civile). Il s'agit d'un changement de cap important, que RDDC Valcartier a effectué dès les débuts de l'application de l'informatique et des technologies de l'information aux besoins des Forces canadiennes, phénomène qui prend une ampleur considérable depuis le début des années 90.

Plateforme technologique

RDDC Valcartier a trois principaux champs d'expertise

- ✓ Les systèmes d'information
- ✓ Les systèmes optroniques
- ✓ Les systèmes de combat

Les applications en défense et sécurité se retrouvent surtout dans les recherches qui portent sur les systèmes d'information et, accessoirement seulement, du côté des systèmes optroniques et des systèmes de combat.

En matière de systèmes d'information, RDDC Valcartier met au point et fournit des techniques et des architectures informatiques; des dispositifs et des systèmes de gestion de l'information, des outils visant à améliorer l'efficacité du cycle décisionnel, et des moyens de simulation. En particulier, il étudie et améliore les techniques, les architectures et les outils de soutien aux processus de création et de partage de la connaissance et de l'information dans le but d'améliorer la capacité des Forces canadiennes à maîtriser le champ de bataille sur le plan cognitif.

Stratégie d'affaires

RDDC Valcartier vise à faire bénéficier les entreprises privées et les organismes publics intéressés à faire des affaires dans le domaine de la défense et de la sécurité. Il offre de nombreuses possibilités d'alliances bilatérales et multilatérales afin d'enrichir le bassin de connaissances accessibles au secteur privé.

RDDC Valcartier invite les entreprises privées à collaborer activement dans le domaine de la défense et de la sécurité en participant à la recherche scientifique. En particulier, le RDDC Valcartier offre :

- ✓ des services spécialisés de R-D pour des applications militaires et civiles;
- ✓ des possibilités de transfert technologique;
- ✓ la disponibilité de laboratoires uniques dans les domaines des systèmes optroniques, des systèmes d'information et des systèmes de combat;
- ✓ des occasions de partenariats en R-D;
- ✓ la possibilité de répondre aux appels d'offre publics.

Des services spécialisés d'ingénierie, d'essais et d'évaluation sous forme de solutions clés en main :
ingénierie Défense Valcartier (IDV);
le Centre d'essai et d'expérimentation en munitions (CEEM).

Enjeux

Le contexte de défense et de sécurité dans lequel se trouve le Canada aujourd'hui est influencé par quatre facteurs étroitement liés :

1 - Émergence de la menace asymétrique
Les menaces à la sécurité nationale du Canada changent de nature avec l'émergence du terrorisme international et la radicalisation de certains éléments dans les sociétés des nations développées. La menace posée aujourd'hui par le terrorisme est asymétrique et changeante. Les adversaires potentiels possèdent l'agilité, l'accès facile à la technologie et l'aptitude de détecter rapidement les vulnérabilités sociales, militaires et technologiques et de les exploiter.

2 - Mondialisation des sciences et de la technologie
Le rythme accéléré des progrès scientifiques et technologiques fournit une possibilité d'amélioration rapide et rentable de la capacité des Forces canadiennes. Toutefois, parallèlement, ces mêmes progrès scientifiques et technologiques procurent à nos adversaires les moyens de défier sur un mode asymétrique nos capacités militaires et de viser les intérêts vitaux du Canada. Il importe de bien comprendre les enjeux de ces progrès scientifiques et technologiques et d'y faire face de façon structurée et efficace.

3 - Complexité croissante de l'éventail des conflits
Les Forces canadiennes doivent agir dans des conflits dont l'éventail est de plus en plus complexe. Le rôle prioritaire de maintien de la paix a été, dans une grande mesure, remplacé par un rôle beaucoup plus complexe de rétablissement de la paix.

Le théâtre d'opérations des Forces canadiennes n'est plus exclusivement tourné vers l'extérieur de l'Amérique du Nord, car le contexte de la sécurité nationale est en train de changer de façon radicale. Les nouvelles menaces portent sur l'infrastructure critique de la nation, mais aussi sur la santé, les changements climatiques, le bio et le cyber terrorisme. C'est dire qu'elles visent dorénavant toute la population. En fait, la participation des Forces canadiennes à la sécurité du pays et de l'Amérique du Nord est désormais la première des priorités.

4 - Le programme canadien de défense et de sécurité
Les enjeux nationaux de sécurité sont désormais indissociables de ceux liés à la sécurité publique. Le gouvernement du Canada, le ministère de la Défense nationale et les Forces canadiennes prennent les mesures qui s'imposent pour déterminer ensemble les capacités nécessaires à la défense et à la sécurité publique du pays.

La défense cybernétique

Les infrastructures critiques du Canada, de même que la sécurité générale des Canadiens, représentent un défi constant pour les organisations de sécurité publique au pays. Ces infrastructures touchent aussi bien les installations administrées par les différents paliers de gouvernement, que par les grandes entreprises privées et les sociétés d'État. Ces infrastructures sont gérées par un ensemble complexe de réseaux et de systèmes d'information pour lesquels la sécurité doit être assurée de manière continue.

Les systèmes d'information constituent ainsi la pierre angulaire pour la planification et le contrôle des activités de défense. Les réseaux et les systèmes informatiques sont omniprésents au sein du ministère de la Défense nationale : en effet, ils sont utilisés à tous les niveaux des systèmes de gestion administrative, de commandement et de contrôle, ainsi que des systèmes d'opération des systèmes tactiques de défense. De ce fait, les capacités informatiques ont besoin d'être protégées afin de faire face à la menace cybernétique, qu'elle provienne de groupes terroristes, de criminels ou de pays étrangers.

RDDC Valcartier s'applique à mettre au point de nouvelles approches et outils permettant d'identifier de manière efficace les vulnérabilités des systèmes informatiques, ainsi que les menaces technologiques potentielles. Ses travaux permettent d'améliorer l'ingénierie de ces systèmes, tant dans les phases de conception, d'architecture, de développement que de maintenance, ainsi que pour les besoins de surveillance du fonctionnement des systèmes en place. L'équipe scientifique effectue ses activités en tenant compte à la fois des besoins militaires et de la sécurité publique, en étroite collaboration avec les autres laboratoires de recherche, les partenaires gouvernementaux et industriels.

SecureOps

740, rue Notre-Dame Ouest, bur. 1500
Montréal, Qc
H3C 3X6
Tél : 514-982-0678
www.secureops.com

Interview	Loren Goldig, président et chef de la direction	
Contact	Loren Goldig loren.goldig@secureops.com	
Données de base	*Constitution de la société* *Siège social* *Secteur d'activité* *Nombre d'employés en sécurité* *Revenus* *Marchés* *Clients*	1999 Montréal Fournisseur de service et gestion de la sécurité 40 Entre 5 et 10M$ Québec, Canada, États-Unis Finance, industriel, télécommunications et détail
Stratégie	Développement d'une force nord-américaine et desserte des grandes compagnies	
Moyens	Présence aux États-Unis (Chicago et New York)	

SecureOps se décrit comme une firme spécialisée qui rend des services d'impartition à ses clients tout en leur garantissant un service 24/7 de veille et d'assistance. La firme offre un service clé-en-main et une gamme complète de services de sécurité, y compris dans le domaine des applications mobiles.

SecureOps se spécialise dans la conception de plan directeurs de sécurité ainsi que leur actualisation. Par ailleurs, la firme offre un service unique d'encryptage pour les ordinateurs portables aussi sur une base de 24/7.

Le Centre opérationnel de surveillance de SecureOps est situé rue Notre-Dame à Montréal et garantit un support continu ainsi qu'un monitorage des réseaux de ses clients. Il est conçu de telle sorte qu'il peut traiter des centaines de milliers de systèmes dans le monde.

La question que SecureOps pose à ses clients potentiels est : souhaitez-vous vraiment confier la sécurité de vos équipements et de vos données à un spécialiste en TIC ?

S.I.C. Biometrics Inc.

43, boul. des Vignes
Ile Perrot, Qc
J7V 7S1
450-424-2772
www.sic.ca

Entrevue	Éric Talbot, président et co-propriétaire	
Contact	Éric Talbot	
Données de base	*Constitution de la société*	1999
	Siège social	Montréal
	Succursales	Paris, Qatar
	Nombre d'employés en sécurité	15
	Employés au Québec	3
	R-D	4
Mission	S.I.C. Biometrics Inc. est une entreprise privée qui conçoit, fabrique et commercialise des produits et des solutions biométriques utilisés pour protéger les gens, les institutions, les entreprises, les bâtiments et les équipements contre le vol, la fraude et le terrorisme.	
Stratégie	S.I.C. Biometrics travaille sur l'Europe, les États-Unis et le Moyen-Orient et utilise des techniques de vente distinctes sur chacun de ces marchés.	
Moyens	S.I.C. Biometrics noue, dans le cadre de projets d'envergure tels que la sécurisation des aéroports, les gouvernements, des ports, etc, des alliances avec des partenaires stratégiques.	
Avantages et enjeux	S.I.C. Biometrics est la seule à offrir une plate-forme évolutive biométrique sur le marché qui donne un maximum de compatibilité aux différents systèmes déjà existants et un meilleur retour sur l'investissement. Clientèle institutionnelle et privée variée : BBDO, Transcontinental, Académie nationale de Police de France, CSSS Jeanne-Mance, etc.	

C'est à la faveur de la vente de sa compagnie d'informatique en 1999 qu'Éric Talbot a choisi de se réorienter vers la sécurité et la biométrie en particulier. «J'ai fait une étude de marché et j'ai conclu que la biométrie sera un domaine en forte croissance au cours des prochaines années,» explique Éric Talbot.

S.I.C. propose une série de produits et de logiciels liés au contrôle des accès et de la sécurité informatique. Le produit vedette est une carte à puce avec capteurs biométriques intégrés. La carte qui se fonde sur la reconnaissance des empreintes digitales permet de nombreuses applications de contrôle, tels que l'accès au réseau, l'accès physique aux bureaux, l'accès à des équipements spécialisés ou comme carte de poinçon.

Les clients de S.I.C. comprennent que cette technologie contribue à la productivité de l'entreprise. Ainsi, par exemple, pour une entreprise de 3 200 employés, la carte permet d'économiser plus d'un million de minutes de travail (perte de mot de passe, temps du centre de soutien technique). Le système se paie en 11 mois, incluant la formation et permet d'économiser plus de 0,5 M $ dans les années subséquentes.

Pour vendre ses produits et services aux États-Unis (25% des ventes de l'entreprise), S.I.C. s'allie à des partenaires stratégiques tel Accenture, Orange Business Services, Agilex, BAE et CACI, ce qui lui permet d'accéder au gouvernement américain.

En Europe (50% des ventes de l'entreprise), la stratégie de vente repose sur un réseau de revendeurs ainsi que des partenariats avec des sociétés de sécurité physique tels qu'ADT, Prosegur et Accenture.

Dans les années à venir, S.I.C. entend développer le continent africain et y ouvrir un bureau.

« Le Canada, explique Éric Talbot, est un marché sous-développé en matière de sécurité comparativement à l'Europe et aux États-Unis. La vision à court terme en matière de risque est dominante avec pour conséquence que le niveau de fraude tant dans le secteur privé que public est très élevé. »

Silanis

8200, boul. Décarie, bureau 300
Montréal, Qc
H4P 2P5
http://www.silanis.com/

Entrevue	Tommy Petrogiannis, président Silanis	
Contact	Tommy Petrogiannis	
Données de base	*Constitution de la société* *Siège social* *Secteur d'activité* *Nombre d'employés en sécurité* *Nombre d'employés au Québec* *R-D* *Revenus* *Marchés* *Clients*	1992 Montréal Signature électronique 75 70 25 6,2 millions (2009) Entreprises : 75%, Gouvernement É-U : 25% Gouvernement, assurances
Mission	Silanis fournit des solutions visant à automatiser les approbations (BPA) et, depuis 2010, vend des licences de sites transactionnels fondés sur les BPA.	
Stratégie	Silanis compte près de vingt ans d'expérience dans le développement et le déploiement de logiciels de gestion d'approbations. Silanis s'est spécialisé dans le domaine des assurances, des banques et de la gestion immobilière. Forte d'un partenariat avec IBM, les clients de Silanis proviennent tous des États-Unis. Dans les années 90, Silanis travaillait essentiellement par vente directe. Puis la compagnie a changé son modèle et aujourd'hui, elle ne travaille qu'en concert avec des partenaires, principalement IBM.	
Moyens	12 brevets déposés, 12 brevets en attente	
Marchés	Assurance et Service financiers – 75% Gouvernements – 25%	
Avantages et enjeux	Silanis incarne le « bureau sans papier ». La compagnie a informatisé l'ensemble des approbations nécessaires, par exemple, à l'achat d'une maison, depuis l'offre d'achat jusqu'aux copies finales à présenter au notaire. Ainsi, la conclusion chez le notaire de l'achat d'une propriété, qui pouvait durer jusqu'à trois heures, est maintenant réduite à 15 minutes – parce que tous les documents ont été préalablement lus, approuvés et signés par les parties. Silanis a eu gain de cause contre une contestation juridique du processus, ce qui confirme la solidité de la signature électronique et des processus de BPA sur le plan légal.	

Historique de l'entreprise

Selon le président de Silanis, Tommy Petrogiannis, le cœur des processus d'affaires est l'approbation de documents écrits : « Dans un bureau, tous les documents sont aujourd'hui générés électroniquement et imprimés pour lecture ou pour signature, ce qui cause un goulot d'étranglement. La gestion organisationnelle consiste surtout à approuver les processus que matérialisent ces documents. »

Il y a quelques années, les tablettes graphiques et les systèmes à stylet semblaient une solution à ce problème. Mais cette technologie n'a jamais dépassé le marché niche, du moins jusqu'au lancement de l'iPad par Apple. En 1992, Tommy Petrogiannis et ses deux associés, Joseph Sylvester et Michael Laurie, ont décidé de se concentrer plutôt sur le processus de validation des documents. Ils ont alors créé Silanis, et ils ont élaboré un logiciel qui facilite la création, la gestion et la distribution de documents informatisés grâce à un système de signatures électroniques.

Le deuxième client de Silanis, après Ontario Hydro, a été Walt Disney Imaging. Depuis lors, Silanis a surtout œuvré aux États-Unis. L'année 1997 est un autre jalon important pour Silanis : les chefs d'état-major américains (Joint Chiefs of Staff), basés au Pentagone, ont décidé d'adopter la méthode de signature électronique ApproveIt® Desktop de Silanis, afin d'accélérer la circulation des documents entre les 1 500 employés de leurs services.

Le deuxième jalon a été posé en 2000, lorsque le commandement du service médical des forces terrestres des États-Unis (MEDCOM) a doté ses 40 000 employés des solutions informatiques de Silanis, dans ce qui demeure le plus grand déploiement de logiciels de signature électronique à ce jour.

Décrite comme une « entreprise à surveiller » par le magazine *CIO*, Silanis est reconnue par le groupe de recherches Gartner comme chef de file en développement de logiciels de signature électronique. Silanis a une clientèle de plus de 1 000 organismes et de près d'un demi-million d'utilisateurs. Ses clients œuvrent dans les milieux financiers et gouvernementaux, l'industrie manufacturière, le secteur de la santé et les secteurs réglementés par la *Federal Drug Administration* (FDA) aux États-Unis.

Le troisième jalon est en devenir. Silanis a créé en 2010 une nouvelle division Esignlife actuellement en incubation, dont la mission sera d'offrir aux PME, sous forme de service, le processus de signature électronique hébergé sur la nouvelle plateforme d'affaires d'IBM, LotusLive.

Plateforme technologique

Le produit principal de Silanis est la famille des produits ApproveIt. Le but était que la signature électronique devienne aussi simple et acquière la même valeur juridique qu'une signature classique sur papier. Les produits sont adaptés aux opérations des entreprises; ils n'exigent pas que les processus d'affaires soient reconfigurés.

Les produits ApproveIt sont divisés en deux suites, l'une axée sur l'approbation électronique et l'autre sur les transactions en ligne.

Plate-forme courriel : la suite eApproval (approbation en ligne) offre une gamme complète de produits de signature électronique et de gestion d'approbations. Ces produits peuvent être déployés dans un service spécifique, pour une ligne de produits, ou peuvent être combinés pour mettre en ligne tout le processus d'approbation des signatures qui se faisait auparavant sur support papier.

Plate-forme Web : la suite eTransaction (transaction en ligne) offre un système sûr et extensible de registre en ligne paramétrable pour les transactions financières qui comprennent des documents négociables. Les produits opèrent ensemble pour générer, identifier et suivre les propriétaires de copies et les transferts pendant la vie active de tous ces documents.

Stratégie d'affaires

Silanis vend un système d'automatisation des processus d'affaires, de leur simplification avec des gains de productivité et d'efficacité. Comme le dit Tommy Petrogiannis : « La bureautique est toujours en équilibre entre la facilité d'utilisation et les besoins de sécurité. » Il faut donc que la technologie soit transparente pour l'utilisateur, qui ne veut surtout pas être forcé de télécharger constamment des

certificats ou des clés publiques. Silanis surveille les processus à partir d'un serveur centralisé qui est invisible pour les utilisateurs.

Silanis considère que la sécurité n'est pas seulement fondée sur l'application de la technologie, mais résulte d'un processus. Cette expertise est partagée avec les clients de l'entreprise pour mieux réorganiser et planifier des processus qui sont légalement exécutoires, tout en respectant les besoins des clients sur le plan commercial, légal et technologique. Par sa force de ventes directes, Silanis peut collaborer avec ses clients afin de déterminer les meilleures solutions pour une entreprise et son environnement. Les marchés cibles touchent particulièrement les champs d'activité qui sont sujets à des réglementations strictes et à des directives difficiles à suivre à l'aide d'opérations papier, tels que le gouvernement, les services financiers, l'industrie manufacturière et les marchés réglementés par la FDA.

Nature du marché

Au cours des dernières années, Silanis a décidé de se spécialiser en finances, notamment dans le domaine des assurances, des prêts hypothécaires et de la gestion immobilière. Il s'agit de marchés réglementés, complexes où le processus d'approbation est une des fondations de la prise de décision de l'organisation. « Il a fallu plusieurs années, explique Tommy Petrogiannis, aux industries pour comprendre comment intégrer la signature électronique dans leurs processus d'affaires. Les entreprises intéressées à adopter l'automatisation des approbations y sont maintenant poussées par les économies générées ou pour fidéliser leurs propres clientèles. C'est ce qui explique la force de Silanis dans les marchés réglementés et dans les pays qui ont une législation qui régit l'acceptation de signatures numériques. De plus, l'efficacité des processus PDA est maintenant reconnue. »

Les autres joueurs dans ce marché comprennent les sociétés qui développent des logiciels de signature numériques et les firmes de consultants qui élaborent des produits sur mesure pour leurs clients.

Un grand nombre d'industries sont résolument engagées dans le processus PDA et font partie de la « *early majority* ». D'autres, comme le secteur de la santé sont des « early adopters ».

Enjeux

Le futur marché est sujet aux lois et règlements des divers gouvernements ou des divers organismes qui régissent l'industrie, ainsi que des associations qui définissent les normes émergentes. Plusieurs marchés ont déjà publié leurs standards qui soutiennent la technologie de Silanis, et les ouvertures de marché ne dépendent de l'adoption de lois ou règlements additionnels.

Silanis a été plus durement frappée par la crise financière que bien d'autres entreprises québécoises, car son marché est aux États-Unis. Ses revenus sont passés de 7,5 millions en 2008 à 6,2 millions en 2009, soit une baisse de 18%.[39] Toutefois, l'entreprise n'a pas de dettes et ses réserves financières lui permettent d'envisager l'avenir sans crainte.

« 2009 a été une très mauvaise année pour nos clients aux États-Unis, mais maintenant les affaires ont repris et nous estimons que 2010 en sera une de reprise. Avec les nouvelles règles que le gouvernement Obama va adopter pour les secteurs de la finance et de la gestion immobilière, cela nous permettra d'accroître notre part de marché. »

[39] Bloomberg-BusinessWeek, September 16, 2010 3:37 PM ET : http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=104549

Waveroad Consult

4710, rue Saint-Ambroise, suite 264
Montréal, Qc
H4C 2C7
Tél. : 514.935.2020
http://waveroad.ca/

Interview	Véronique Olivier, présidente	
Contact	Idem	
Données de base	Constitution de la société	2001
	Siège social	Montréal
	Nombre d'employés en sécurité	8
	Employés au Québec	8
	Revenus	n.d.
	Clients	Finance, énergie, télécom
Stratégie	Introduction de nouveaux produits et attaque de nouveaux marchés	
Moyens	Diversification des activités	
Avantages et enjeux	Crédibilité de l'entreprise basée sur expertise et bas prix	

Historique de l'entreprise

Fondée en 2001, l'entreprise a vu le jour sous le nom de Waveroad Partenaires en Télécommunications et œuvrait principalement dans le domaine des télécommunications. « Avec les changements des marchés économiques au niveau des besoins d'affaires et de communications ainsi qu'avec l'évolution des technologies, nous avons voulu offrir une expertise de services plus vaste, explique Véronique Olivier. La convergence des technologies et l'évolution des processus d'affaires nous amenèrent donc à créer au cours des ans une seconde pratique, celle de la sécurité procédurale et technique, et à œuvrer particulièrement sur la planification stratégique de projets. Waveroad ConsulT prend alors son essor. »

« En 2007, fort de notre expertise acquise des processus, de la sécurité et des technologies IP, nous avons développé une solution de prévention de la fraude effectuée sur les transactions IP. Ces efforts ont donné naissance au produit IntegriT, présenté sous la bannière Waveroad SecuriT. »

Nature de l'offre

- Services professionnels en sécurité des TIC, y compris accompagnement à la certification ISO 27 001, PCI-DSS, CISA, CISSP, etc. En matière de sécurité, Waveroad Consult se spécialise dans la gouvernance de la sécurité et les solutions de sécurisation.
- Formation dans les domaines de la sécurité, des télécommunications, des certifications et de la gestion.
- Validation technologique des produits / applications : le processus de validation représente, en quelque sorte, les fondations d'un produit, il permet de tracer une ligne directrice pour les phases de développement à venir.

Stratégie d'affaires

- Neutralité technologique et accompagnement des clients dans les choix de solutions.

- Accompagnement des clients sur des projets, de façon à répondre aux besoins d'affaires et selon les meilleurs pratiques.

Nature du marché

- Le marché de base de Waveroad Consult est constitué par les secteurs de la finance, du commerce détail, de l'ingénierie. Ses marchés secondaires sont les télécommunications et le parapublic (municipalité, ressources naturelles…).
- Actuellement concentrée au Québec, Waveroad Consult prévoit attaquer les marchés des États-Unis et de France également d'ici 2012.

Enjeux

La sécurité est l'enfant pauvre de la PME. Or, ce sont elles qui sont visées en priorité par les pirates informatiques qui s'entraînent sur ce type d'entreprises avant de s'attaquer aux grandes institutions comme les gouvernements et les banques. Le rôle de Waveroad Consult est d'aider la PME à relever ce défi, pour lequel les grandes sociétés de services professionnels ne sont pas équipées.

Zerospam Sécurité

2520, rue Beaubien Est, bureau 200
Montréal, Qc
H1Y 1G2
514-527-3232
www.zerospam.ca

Entrevue	David Poellhuber, président et chef de la direction	
Contact	David Poellhuber	
Données de base	Constitution de la société	2003
	Siège social	Montréal
	Nombre d'employés en sécurité	10
	Employés au Québec	10
	R-D	4
	Produits	Filtre anti-pourriel et services périphériques (continuité, archivage, services DNS)
	Clients	50% - entreprises de 1 à 50 employés 30% - entreprises de 50 à 500 employés 20% - grandes entreprises
Mission	Impartiteur de sécurité. Zerospam ne vend pas de logiciels mais des services.	
Stratégie	Pénétration au Canada. Croissance par acquisition aux États-Unis dès que le financement sera réuni	
Moyens	Obtenir une masse critique au Québec ; R-D.	
Marchés	Pénétration horizontale B2B en misant sur tous types d'entreprises, petite, moyenne et grande.	
Avantages et enjeux	Les sociétés canadiennes ont avantage à héberger leurs courriels au Canada plutôt qu'aux États-Unis, ce qui les met à l'abri d'une saisie au nom du Patriot Act.[40]	

Dans la situation économique actuelle, les entreprises et les organismes cherchent des moyens de réduire leurs coûts et d'être plus efficaces. Les solutions de filtrage offertes en mode logiciel-service ont des avantages : « Nous offrons une alternative aux PME : au lieu de devoir s'équiper de logiciels et de gérer les licences, nous prenons en charge la gestion de leurs courriels dans un infonuage composé de serveurs interconnectés au moyen d'une bande passante. Les frais de collocation dans l'infonuage sont minimes et l'entreprise n'a pas d'immobilisation, » explique David Poellhuber.

Les solutions anti-pourriel offertes en mode logiciel-service dégagent les équipes TI du carcan des mises à jour et des tâches liées à l'installation, à la configuration, à l'optimisation et aux problèmes de comptabilité. Elles protègent les infrastructures des clients en éliminant chaque jour des milliers de pourriels en amont du serveur et elles réduisent considérablement le gaspillage de la bande passante.

Le courriel est universel. Zerospam dessert toutes les entreprises, quelque soit leur taille ou la nature de leurs activités. Le plus petit client de Zerospam est un courtier en valeurs mobilières et le plus gros une Commission scolaire avec 25 000 comptes de courriels. Zerospam dessert la clientèle de la SAQ, Via

40 Le USA Patroit Act : Loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme. Cette loi anti-terroriste a été votée par le Congrès des États-Unis et signée par George W. Bush le 26 octobre 2001, quelques semaines après les événements du 11 septembre.

Rail, Oxfam et le CRIM. 93% des entreprises desservies utilisent une infrastructure basée sur Microsoft Exchange, mais le service demeure parfaitement transparent quelque soit la plate-forme utilisée.

Le service de sécurité imparti n'est pas encore répandu au Québec. Le cycle de vente est long, particulièrement dans les bureaux du gouvernement et dans les grandes entreprises. « Cela s'explique. Les grands services de TIC ont l'habitude de tout régler par l'achat d'équipement, de logiciel et l'embauche. L'habitude d'extérioriser certaines tâches n'est pas acquise. Pourtant, c'est tellement plus économique et efficace, » poursuit David Poellhuber.

Pour croître, Zerospam prévoit créer des réseaux de vente hors-Québec et investir dans de la publicité ciblée. « Nous visons le Canada, mais aussi les États-Unis et la France. Nous correspondons avec plusieurs entreprises mais ce que nous recherchons tout particulièrement est un joueur d'importance en TIC qui possède une grande clientèle et qui prendrait notre offre dans son bouquet de services, » dit David Poellhuber

Zerospam consacre un tiers de ses ressources à la R-D notamment pour se tenir à jour sur les manœuvres des pirates et autres spammeurs sur Internet. « En 2008, 85% des courriels étaient des pourriels. Aujourd'hui, ce taux est de 95% et va en augmentant. C'est un vrai gaspillage de bande passante mais plus encore, cela fragilise les entreprises, » précise David Poellhuber. Aussi, la firme de recherche IDC, prévoit une croissance annuelle de 27% des services de sécurité en nuage d'ici 2013.

Annexe 2 : Questionnaire

ALLIANCE CANADIENNE POUR LES TECHNOLOGIES AVANCÉES (*ALLIANCE* CATA)

L'industrie de la sécurité avancée au Québec

Le projet d'étude de l'*Alliance* CATA traite exclusivement de la sécurité avancée – sécurité informatique + sécurité physique faisant appel aux technologies de l'information et des communications (TIC). Son but est de mesurer la performance de l'industrie de sécurité avancée au Québec ainsi que dans le reste du Canada, d'évaluer sa capacité à répondre aux demandes du marché et, enfin, d'en faire la promotion à l'étranger.

Veuillez prendre note que ce questionnaire s'adresse uniquement aux entreprises qui œuvrent dans le secteur de la sécurité.

Québec

Développement économique Canada pour les régions du Québec

Canada Economic Development for Quebec Regions

Avec la coopération du ministère du développement économique, de l'innovation et de l'exportation (MDEIE) et de l'Agence de développement économique du Canada (DEC)

Par courriel service@cata.ca
ou par télécopie (514) 313-5751

Contact
Huguette Guilhaumon, directrice à l'Innovation
36, place Trafalgar, Montréal, QC, H3H 1T3
Tél. 514.656.3254

COORDONNÉES DE L'ENTREPRISE – INFORMATION GÉNÉRALE	
Q.01	**Nom** ……. **Prénom** …… **Courriel** …… **Téléphone** …… **Titre** ……. **Nom de la société** …… **Site Web** …… **N° civique** …… **Rue/Place/Boul./Av.** …… **Ville** ……. **Province** ……
Q.02	**Votre entreprise fournit-elle ou utilise-t-elle des produits et services de sécurité avancée?** ☐ **Fournisseur** ☐ **Utilisateur**

Q.03	**En quelle année votre entreprise a-t-elle été créée ?** *[Veuillez marquer l'année de l'incorporation au Canada.]* **……..**
Q.04	**Combien d'employés travaillent actuellement à temps plein dans votre entreprise ?** *[Chiffres pour le Canada entier]* **Employés en général ……..** **Employés en sécurité ……..**

Q.05	**Où sont situés les employés spécialisés en sécurité :** *[Personnes à temps plein]* **☐ Au Québec** **☐ Aux États-U** **☐ Ailleurs au Canada** **☐ Ailleurs dans le mo**
Q.06	**Combien de femmes y a-t-il parmi les employés spécialisés en sécurité ?** *[Si vous n'avez pas le nombre exact, inscrivez une approximation en pourcentage.]* **Au Québec ☐** **Ailleurs au Canada ☐**
Q.07	**Dans votre société, combien de consultants travaillent à temps partiel en sécurité (Québec seulement) ?** *[EN ÉQUIVALENT PERSONNES - Veuillez tenir compte de la longueur moyenne de l'embauche des pigistes. Par exemple, si l'entreprise a actuellement 3 pigistes engagés pour trois mois chacun, soit au total neuf mois, veuillez marquer: 9/12 ou encore 0,75. - Si vous n'êtes pas sûr, faites une approximation.]* **Au Québec ……..** **Ailleurs au Canada ……..**
Q.08	*[Ne tenir compte que des employés reliés au secteur de la sécurité au Québec]* **Dans votre entreprise, le nombre d'employés est-il :** / **L'an passé** *(2009)* / **En 2010** *(prévisions)* **À la hausse ……** ☐ ☐ **À la baisse ……..** ☐ ☐ **Stable ……..** ☐ ☐ **NSP ……..** ☐ ☐

ACTIVITÉS DE L'ENTREPRISE

Q.09	**Dans quelle catégorie se situe votre entreprise :** *[Plusieurs réponses possibles.]* **☐ Fabrication d'équipement ☐ Fournisseur de services** **☐ Éditeur de logiciels ☐ Autre (veuillez préciser SVP)** **……..** **……..**

Q.10	**Quels sont les principaux produits ou services offerts par votre entreprise ?** [Produits ou services de sécurité seulement. Prière d'indiquer au moins un produit ou service.] **1°) .....** **2°) .....** **3°) .....** **Produits additionnels, s'il y a lieu : .....**

Les réponses aux questions suivantes seront traitées de façon **confidentielle**. Elles n'apparaîtront pas dans la base de données et seront utilisées sous forme agrégée à des fins uniquement statistiques. Ni la CATA, ni ses partenaires n'utiliseront les réponses aux questions suivantes. Elles ne sont ni rétrocédées à des tiers ni utilisées à d'autres fins que celle requises à l'analyse des résultats de cette enquête.

DESCRIPTION DU MARCHÉ DE VOTRE ENTREPRISE

Q.11	**Qui sont actuellement vos principaux clients?** *[Plusieurs réponses possibles]* **Entreprises de plus de 500 employés** **Entreprises de 300 à 499 employés** **Entreprises de 100 à 299 employés** **Entreprises de 50 à 99 employés** **Entreprises de 20 à 49 employés** **Entreprises de 10 à 19 employés** **Entreprises de 1 à 9 employés** **Particuliers**
Q.12	**Dans quels grands secteurs économiques se répartissent vos clients ?** *[EN POURCENTAGE - La somme des trois nombres doit être égale à 100.]* **- Secteur affaires: __ %** **- Secteur public et parapublic: __ %** **- Secteur résidentiel: __ %**
Q.13	**À l'intérieur de ces secteurs, veuillez préciser la catégorie de vos principaux clients?** *[Ne citez pas les noms des compagnies, mais seulement les catégories]* **Affaires** (banque, assurance, transport routier, commerce de détail, stations d'essence, notaires, etc.) **……** **Public et parapublic** (ministère, défense nationale, premiers répondants, école/université, santé, etc.) **……** **Consommateurs** (directement aux propriétaires ou via les compagnies d'alarmes) **……**
Q.14	**Quel pourcentage de vos ventes effectuez-vous…** **…. % …au Québec ? …. % …ailleurs au Canada ?** **…. % …aux États-Unis ? …. % …dans d'autres pays ?**

Q.15	**Pour ceux qui vendent hors Québec, dans quelle proportion s'agit-il ?** *[EN POURCENTAGE - La somme des quatre nombres doit être égale à 100.]* **… de produits matériels? __ %** **… de produits logiciels ou d'applications? __ %** **… de services de consultation? __ %** **… autres? __ %** **Si vous avez répondu « Autres », veuillez préciser : ……**
Q.16	**Comment définiriez-vous vos ventes de l'an passé (2009) ?** *[sécurité seulement]* **☐ En croissance ☐ Stable ☐ En décroissance ☐ NSP**
Q.17	**Avez-vous l'intention de développer de nouveaux marchés au Québec ou hors Québec ?** **☐ OUI, au cours de l'année (2010)** **☐ OUI, d'ici deux ans (vers 2012)** **☐ NON** **☐ NSP / Pas sûr**
Q.18	**Si vous avez répondu « OUI », veuillez préciser :** **- Hors Québec en 2010** (veuillez indiquer vers quelles provinces ou pays) : **……** **- Hors Québec d'ici 2012** (idem) : **……** **- À l'intérieur du Québec en 2010** (veuillez indiquer les secteurs : transport, santé, police, milieu juridique, etc.) : **……** **- À l'intérieur du Québec d'ici 2012** (idem) : **……**

STRATÉGIE D'ENTREPRISE

Q.19	**Votre entreprise fait-elle de la R-D ?** **OUI ☐ Non ☐ NSP ☐** **Si OUI, combien d'employés sont affectés à la R-D ?** *[équivalents chercheurs / années]* : **……**
Q.20	**Veuillez indiquer le domaine général de vos activités de R-D ?** *[par exemple : authentification, infrastructure à clés publiques (ICP), carte à puce, vidéo surveillance, télédétection, etc.]* **……** **……**
Q.21	**Quel est le principal objectif de votre effort de R-D ?** *[Veuillez choisir au maximum 2 réponses. Merci!]* **Améliorer la qualité du produit ☐** **Réduire les coûts de production ☐** **Créer de nouveaux produits ☐** **Autre ☐** **Si vous avez répondu "Autre",**

	veuillez spécifier, SVP _____
Q.22	**Êtes-vous à la recherche de financement ?** **Oui ☐ Non ☐ NSP ☐** **Si OUI, dans quel but?** **[** Veuillez préciser si c'est pour financer la R-D, ouvrir de nouveaux marchés, accroître les liquidités ou toute autre raison.]
Q.23	**Selon vous, quel est le principal obstacle que doit affronter l'industrie de la sécurité ?**

	Au Québec	Dans le reste du Canada	À l'étranger
Concurrence domestique…….……..	☐	☐	☐
Concurrence étrangère……..….	☐	☐	☐
Protectionnisme américain……..……..….	☐	☐	☐
Recrutement de personnel qualifié……..….	☐	☐	☐
Financement……..	☐	☐	☐
S**outien gouvernemental**……..	☐	☐	☐
Pas d'obstacle particulier	☐	☐	☐
Autre raison……	☐	☐	☐

Q.24	**Pour ceux qui ont répondu "Autre raison", veuillez expliquer, SVP.** *[Ceux qui ont fait d'autres réponses, peuvent aussi commenter leurs choix.]* …… …… ……

PRIÈRE DE RENVOYER LE QUESTIONNAIRE

PAR COURRIEL SERVICE@CATA.CA - PAR TÉLÉCOPIE (514) 313 5751

MERCI !

Annexe 3 : Sigles et acronymes

ASIS	American Society for Industrial Security
ATM	Automatic Teller Machine
BIS	Bank for International Settlements
BPIEPC	Bureau de la protection des infrastructures essentielles et de la protection civile (voir OCIPEP)
CANASA	Canadian Alarm and Security Association
CCTV	Closed Circuit Television
CGEIT	Certified in the Governance of Enterprise IT
CIPS	Canadian Information Processing Society
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CNRC	Conseil national de recherches Canada
CobiT	Control Objectives for Information and related Technolog
CRIM	Centre de recherche informatique de Montréal
CRIQ	Centre de recherche industrielle du Québec
DES	Data Encryption Standard
ECC	Elliptic curve cryptography
EPPR	Emergency Prevention, Preparedness and Responses
PGI	Progiciel de gestion intégrée
FDA	Food and Drug Administration (États-Unis)
ISP	Information Systems Professi
ITCP	Information Technology Certified Professional
TIC	Technologies de l'information et communications
ISC	International Security Conference
UIT	Union internationale des télécommunications
OCIPEP	Office of Critical Infrastructure Protection and Emergency Preparedness (voir BPIEPC)
Octave	Operationally Critical Threat, Asset, and VulnerabilityEvaluation
OSSTMM	Open Source Security Testing Methodology Manual
PME	Petites et moyennes entreprises
PMP	Project Management Professional
PIPEDA	Personal Information and Electronic Documents Act
PKI	Public Key Infrastructure
R-D	Recherche et développement
RFID	Radio Frequency Identification
SCC	Standards Council of Canada
SSCP	Systems Security Certified Practitioner
TSCP	Transglobal Secure Collaboration Program
RVP	Réseau virtuel privé

À propos de l'*Alliance* CATA

Mandat et mission

L'*Alliance* canadienne pour les technologies avancées (CATA) a pour mission d'aider ses membres à accroître leur chiffre d'affaires en leur conférant un avantage coopératif – une valeur ajoutée qui s'étend à tous les innovateurs canadiens, qu'ils soient commerçants, utilisateurs ou professionnels.

Plus importante association de technologies de pointe au Canada, l'*Alliance* CATA met à la disposition des entreprises des occasions d'affaires dans tous les secteurs économiques ou presque – de façon à ce que nous puissions faire affaires ensemble. Au-delà du marché local, l'*Alliance* CATA met ses membres en rapport avec le potentiel de partenariat et d'investissement des principales multinationales qui font affaires au Canada. Plus de 80% des membres de l'*Alliance* CATA sont des exportateurs ; ils représentent la fine pointe de l'expansion économique.

Dans le cadre du programme « Innovation Nation », les chefs d'entreprises sont invités à se réunir pour favoriser la création d'un environnement d'affaires favorable. L'*Alliance* CATA est à l'origine de tout un ensemble de canaux de distribution, d'études de marché, de réseautage, d'événements publics, de liaison avec d'autres associations, ainsi que de perfectionnement professionnel, à travers le pays.

Partagez votre excellence avec notre avantage coopératif – nous avons le gout de parler affaires avec vous !

Soutenez l'industrie des technologies de pointe et participez au développement des affaires, devenez membre de l'Alliance CATA !

Pour toute information, contactez Cathi Malette :
cmalette@cata.ca
613-236-6550
http://www.cata.ca/

Sécurité avancée Québec 2010

Les attaques ciblant les données de l'entreprise ont presque doublé. Sommes-nous protégés ? Est-ce que le Québec compte une industrie, voire une grappe industrielle en sécurité ? Quelles sont ses forces et ses faiblesses ?

En 2010, l'*Alliance* canadienne des technologies avancées (CATA) a fait le recensement de toutes les entreprises de sécurité avancée au Québec, elle les a interrogés par voie de sondage et a interviewé ses chefs de file.

Environ 90 entreprises de sécurité avancée ont répondu. Leurs noms et coordonnées sont disponibles sur le site de l'*Alliance* CATA : http://www.cata.ca

L'étude couvre plus précisément :

- ✓ Le profil de l'industrie
- ✓ Les stratégies du marché
- ✓ Le commerce hors Québec
- ✓ L'indispensable R-D
- ✓ Le financement
- ✓ Les enjeux

À qui s'adresse cette étude ?

- ✓ Les cadres de l'industrie de la sécurité
- ✓ Les utilisateurs de biens et services de sécurité
- ✓ Les investisseurs publics et privés
- ✓ Les décideurs gouvernementaux
- ✓ Les partenaires étrangers actuels ou potentiels
- ✓ Les médias spécialisés

Prix version papier : **320,00$** + taxes
Prix version électronique : **280,00$** + taxes
Rabais de 20% pour les membres des associations partenaires.
Par courriel : **service@cata.ca** *ou par télécopie* : 514.313.5751

Contact :
Huguette Guilhaumon, associée principale
36, place Trafalgar, Montréal, QC, H3H 1T3
Tél. **514.656.3254**

Québec

Développement économique Canada pour les régions du Québec
Canada Economic Development for Quebec Regions

Avec la coopération du ministère du développement économique, de l'innovation et de l'exportation (MDEIE) et de l'Agence de développement économique du Canada (DEC)

Dépôt légal :
Bibliothèque et Archives nationales du Québec, 2010
Bibliothèque et Archives Canada, 2010
ISBN 978-2-9812174-0-0