LA CYBERSÉCURITÉ AU QUÉBEC

Enquête sur la cybersécurité dans le secteur manufacturier et les infrastructures critiques

Par cybersécurité, on entend la préservation — par des politiques,
par la technologie et par l'éducation — de la disponibilité, de la confidentialité
et de l'intégrité de l'information et de son infrastructure sous-jacente,
dans le but d'accroître la sécurité des personnes à la fois en ligne et hors ligne.
Freedom Online Coalition
(avec la contribution du gouvernement du Canada)[1]

Faits saillants

1. Introduction

a) Une nouvelle menace

Quand les centrifugeuses iraniennes ont été détruites en 2010 par des hackers anonymes, la cybersécurité a changé de nature : désormais, il ne s'agit plus simplement de préserver l'intégrité de données informatiques, mais des équipements physiques et, à la limite des vies humaines. Or, 21% des entreprises canadiennes sont touchées par des cyberattaques ayant provoqués des dommages. La menace vise en priorité les infrastructures critiques (surtout pétrole et gaz, électricité et secteur financier) et les entreprises industrielles. Il s'agit d'une menace protéiforme qui peut venir aussi bien de loups solitaires et d'employés mécontents que de criminels organisés, voire de services secrets étatiques.

b) La cybersécurité dans le monde

Impossible de répondre à ces forces diffuses en ordre dispersé. Depuis 2004, le Groupe d'experts gouvernementaux (GGE) des Nations Unies a essayé d'organiser la cybersécurité au niveau mondial. En vain. Au même moment, le Conseil de l'Europe a conclu son propre traité sur la cybersécurité, connu sous le nom de Convention de Budapest, qui a été ratifié par 69 pays, dont le Canada. C'est le seul traité international en vigueur, même si une majorité de pays refusent toujours d'y adhérer. Devant cet échec de la communauté internationale, le secteur privé a essayé de réagir au moyen de deux initiatives majeures : le *Cybersecurity Tech Accord* lancé par Microsoft en avril 2018 et la *Charter of Trust* lancée par Siemens en février 2018.

c) Place du Canada sur la scène internationale

Le Canada occupe une place de choix sur la scène de la cybersécurité internationale. Classé dans le peloton de tête des pays les plus sûrs par les différentes études comparatives existantes, le Canada investit chaque année 14 milliards de dollars en cybersécurité (Statistique Canada).

d) Objet et organisation de l'étude

La présente étude vise (1) à évaluer le niveau d'adoption d'industrie 4.0 dans les entreprises manufacturières et les infrastructures critiques, (2) à analyser l'intensité de la cybersécurité dans les entreprises 4.0 et (3) à faire connaître les meilleures pratiques de cybersécurité.

[1] Cité par Holly Porteous, *Cybersécurité : défis techniques et stratégiques*, Bibliothèque du Parlement, Ottawa, 16 février 2018. La Freedom Online Coalition (FOC) est un groupe constitué de 30 gouvernements déterminés à travailler ensemble pour défendre la liberté sur Internet et protéger les droits fondamentaux de la personne. La Coalition a été créée en décembre 2011 et son siège social est situé à Londres (Grande-Bretagne). Le Canada est un des membres fondateurs de la Coalition.

e) 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 Siemens Canada et CyberNB. L'*Alliance* CATA a fourni des services dans la production de l'étude.

2. Profil de l'industrie

a) Situation géographique des répondants
Le sondage CATA/Sciencetech couvre tout le Canada à fins de comparaison (*benchmarking*). Toutefois, le Québec est surreprésenté avec plus de la moitié des réponses, ce qui nous permet de mieux détailler les variations de la cybersécurité dans cette province.

b) Taille et nature des entreprises ayant répondu au sondage
D'une manière générale, les entreprises visées dans cette enquête représentent le secteur le plus avancé de l'économie québécoise : la moitié des répondants sont des grandes entreprises (plus de 500 employés). Près de la moitié exploitent des infrastructures critiques, les autres étant composés d'entreprises industrielles.

c) Dimension internationale des entreprises
Peu de multinationales au sein de cette population et un niveau d'exportations relativement bas. C'est un comportement prévisible en raison de la surreprésentation des infrastructures critiques qui, en fonction de leur mission même, n'exportent généralement pas. La minorité qui exporte le fait principalement à destination des États-Unis.

3. Caractéristiques de la numérisation

a) Numérisation des TI dans les entreprises
La grande mutation des entreprises québécoises est bien entamée. Plus de 90% des entreprises ont déjà numérisé les processus basés sur des technologies informationnelles (TI) et le plus souvent de manière intensive.

b) Numérisation des TO dans les entreprises
Par contre, la numérisation des technologies opérationnelles (TO) est moins avancée. Si près des deux-tiers des entreprises ont déjà numérisé leurs TO, la grande majorité l'est de manière marginale. C'est néanmoins un début significatif.

c) Entreprises qui ont franchi le seuil Industrie 4.0
Par contre, une fois qu'elles ont numérisé leurs TO, les entreprises ont tendance à les relier à leurs TI. Les deux tiers des répondants ont ainsi adopté le paradigme Industrie 4.0. On pénètre ainsi dans un nouveau monde industriel où des capteurs ont envahi les usines et où les robots ont cessé d'être l'exception pour devenir un outil de base.

4. Position de la cybersécurité dans l'organisation

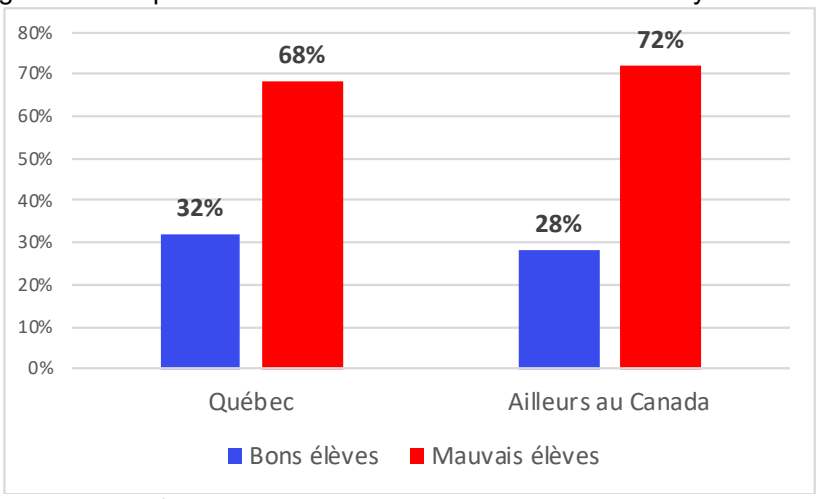
a) Les trois paramètres essentiels de la cybersécurité

Il y a trois paramètres essentiels pour évaluer la cybersécurité dans une organisation : y a-t-il un responsable de la sécurité des systèmes d'information (RSSI)? Existe-t-il un programme écrit de cybersécurité? L'organisation a-t-elle déjà procédé à un audit de cybersécurité de ses systèmes? Les 2/3 des entreprises québécoises ont nommé un RSSI; la moitié ont un programme formel de cybersécurité; un peu plus de 40% ont procédé à un audit de ses systèmes TI.

b) Les « bons » et les « mauvais élèves » de la cybersécurité

Les « bons élèves » de la cybersécurité sont les organisations qui satisfont à ces trois critères simultanément : moins du tiers sont dans ce cas au Québec (taux comparable au reste du Canada). Cela signifie que les 2/3 des entreprises québécoises sondées sont à risque. Or, nous rappelons qu'il s'agit des entreprises les plus avancées du Québec en matière de numérisation.

Figure i - Entreprises satisfaisant à 3 critères de base de la cybersécurité



Source : Sondage Alliance CATA/Sciencetech communications – janvier - avril 2019 (respectivement 109 et 99 répondants)

c) Entreprises ayant nommé un RSSI

Si on examine le détail de la gouvernance de la cybersécurité, on peut distinguer d'autres points faibles. Ainsi, dans plus du tiers des entreprises, il n'y a pas de responsable de la cybersécurité ou bien une personne à temps partiel. Les entreprises qui ont créé un poste de RSSI, l'ont en majorité confié à un informaticien. Seuls 13% des RSSI relèvent de la haute direction. Plus de la moitié de ceux-ci relèvent du service des TI, tandis que les autres relèvent d'autres services (finances, affaires administratives, exploitation, etc.) D'une façon générale, on peut dire que les entreprises québécoises n'ont pas encore pris la mesure de l'importance de la cybersécurité et de la nature polyvalente de la fonction de RSSI.

d) Impartir ou non la cybersécurité ?

Le recours à l'impartition compense en partie la faiblesse des équipes internes de cybersécurité. En effet, il convient de signaler que l'impartition est une pratique généralisée au sein des entreprises québécoises : la moitié confie une partie de sa cybersécurité à des firmes spécialisées, 12% en confie la totalité.

5. Les cyberattaques et leurs impacts

a) Ampleur du phénomène

Plus du tiers des répondants ont déclaré que leurs entreprises avaient déjà subi une ou plusieurs cyberattaques ayant occasionné des dommages (35%). Ces sont les grandes entreprises qui sont les plus susceptibles d'être attaquées.

b) Nature des cyberattaques

La grande majorité des cyberattaques vise les TI, tandis que les TO ne sont affectées que de façon marginale. Une autre façon de classifier les attaques consiste à distinguer le vandalisme (attaques virales, piratage de site web) des fraudes motivées par le gain. Il apparaît qu'au moins la moitié des cyberattaques ont le gain pour finalité.

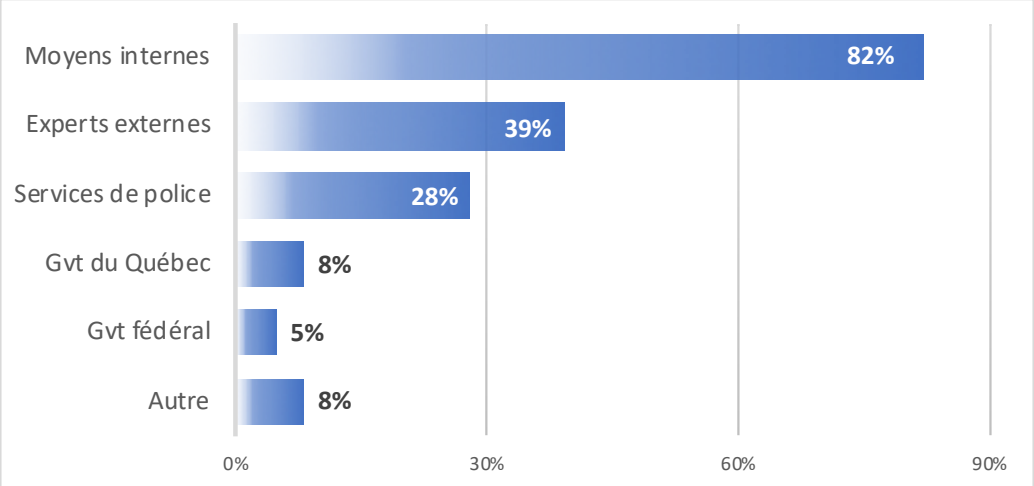
c) Coût des cyberattaques

Plus de la moitié des cyberattaques ont causé des dégâts inférieurs à 100 000 $. La modicité des montants déclarés a deux raisons. Une grande partie des cyberattaques est non ciblée (virus) et parvient à être bloquée avant d'avoir fait des dégâts significatifs. Les cyberattaques ciblées sont relativement rares, mais occasionnent des dégâts pouvant se chiffrer à plusieurs millions de dollars.

d) Réaction aux cyberattaques

La plupart des entreprises comptent avant tout sur leurs ressources internes pour contrer les cyberattaques. Une grande partie fait appel à des consultants externes (39%) et à la police (28%). Par contre les ministères et organismes gouvernementaux sont les grands absents de cette riposte aux cyberattaques.

Figure ii - À qui l'entreprise a-t-elle fait appel en réaction aux cyberattaques ?
(le total n'est pas égal à 100, car certaines entreprises ont fait appel à plusieurs catégories d'intervenants)



Source : Sondage Alliance CATA/Sciencetech communications – janvier - avril 2019 (61 répondants)

6. Réglementation, normalisation et gestion de la cybersécurité

a) Normes ou règlements en vigueur

Moins du tiers des entreprises déclarent avoir adopté des normes de cybersécurité (29%). Encore s'agit-il d'une évaluation « optimiste » car une grande confusion règne dans l'esprit des répondants qui citent volontiers des normes étrangères à la cybersécurité ou encore des normes internes qui sont plutôt des règles d'éthique.

b) Qui fait partie des infrastructures critiques ?

Phénomène *surprenant* : plusieurs RSSI ne savent pas si leur organisation est une infrastructure critique ou non. Cette ignorance de la part des cadres qui sont concernés au premier chef souligne que bien du travail reste à faire en matière de sensibilisation des infrastructures critiques.

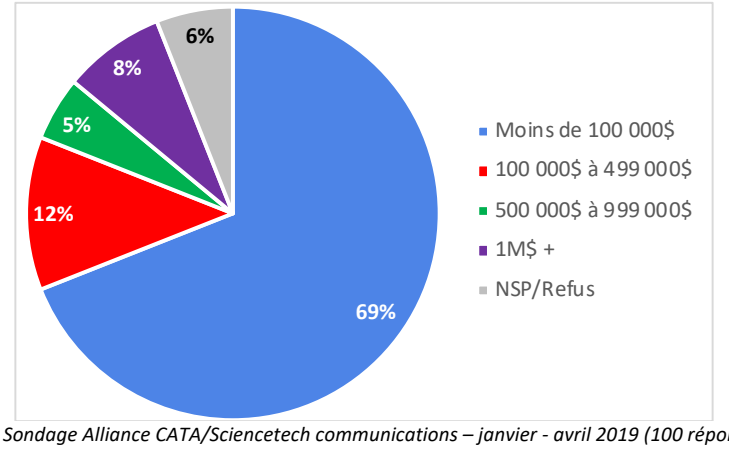
c) Processus de consultation du gouvernement fédéral

Les répondants placent de grands espoirs dans le rôle des pouvoirs en matière de cybersécurité : elles réclament pêle-mêle des crédits d'impôts, des subventions, de l'aide technique et de la formation. Bref, la majorité du secteur privé attend une implication plus active des gouvernements.

d) Investissement en cybersécurité

D'une manière générale, les entreprises consultées investissent peu en cybersécurité : 69% des répondants situent leurs budgets sous la barre des 100 000 dollars – à l'exception des banques qui ont toutes atteint un très haut degré de maturité. Ce sous-investissement est d'autant plus préoccupant que les budgets ont tendance à stagner.

Figure iii - Montant investi en cybersécurité (base annuelle)



Source : Sondage Alliance CATA/Sciencetech communications – janvier - avril 2019 (100 répondants)

e) Assurance de cybersécurité

Un peu plus du quart des entreprises ont déjà pris une assurance de cybersécurité. Cette faible pénétration découle du manque d'empressement à adopter des normes de cybersécurité ainsi que du sous-investissement chronique en la matière. En effet, les assureurs exigent des preuves de « bonne conduite » de cybersécurité que nombre d'entreprises sont incapables de respecter.

f) Degré de préparation générale de l'entreprise à la cybersécurité
Enfin, 35% des répondants se déclarent satisfaits du niveau de préparation à la cybersécurité de leur entreprise. Or, certains de ces « optimistes » de la sécurité n'ont même pas de RSSI ni de programme formel de cybersécurité. Ces entreprises à la fois mal préparées et satisfaites d'elles-mêmes sont les plus à risque.

7. Enjeux et pistes de solution

Le passage au paradigme Entreprise 4.0 est bien engagé, pourtant nombreuses sont les entreprises qui n'ont pas pris la mesure du risque accru que cela implique.

Enjeu et piste de solution No 1 : Partage d'information.
Aucune organisation ne peut lutter isolément contre le cybercrime. Voici pourquoi, il convient de systématiser le partage d'information entre les entreprises et entre les gouvernements. Le modèle de concertations a fait ses preuves dans de nombreuses institutions internationales – le Québec a une place à occuper.

Enjeu et piste de solution No 2 : Pénurie de main d'œuvre.
Toutes les entreprises sont d'accord pour déplorer le manque de ressources qualifiées. Deux solutions s'imposent : recyclage systématique des employés TI ou même non-TI en experts de cybersécurité et, au-delà du renforcement de la formation, une mobilisation totale des réseaux universitaires et collégiaux sur le modèle d'Israël et, plus près de nous, du Nouveau-Brunswick.

Enjeu et piste de solution No 3 : Valoriser la fonction de RSSI
Le RSSI n'est pas un spécialiste sous les ordres du DSI, mais un cadre polyvalent qui doit avoir un statut de vice-président ou équivalent avec accès au comité de direction de l'entreprise.

Enjeu et piste de solution No 4 : Inscrire la cybersécurité dans la description de tâche des employés
Puisqu'on demande aux employés de participer à la cybersécurité de l'entreprise, il faut inscrire cette activité dans leur description de tâche avec tout ce que cela implique en termes d'évaluation annuelle, de niveau de performance, d'évolution de carrière et de promotion, de conditions salariales, etc.

Enjeu et piste de solution No 5 : Vulnérabilité des logiciels.
De même, tous les intervenants sont d'accord pour déplorer l'existence de vulnérabilités dans les systèmes d'exploitation et les logiciels applicatifs. Un code de bonne conduite pourrait être imposé aux éditeurs de logiciels afin de les tenir responsables pour les vulnérabilités des produits.

Enjeu et piste de solution No 6 : Le cas particulier des PME industrielles.
La PME est l'enfant pauvre de la cybersécurité. Elles sont moins susceptibles d'avoir un responsable en cybersécurité que la moyenne québécoise. Une forme d'incitatif financier devrait être conçu à leur intention, à condition que ce ne soit pas une mesure isolée, mais un élément intégré dans un cadre d'accompagnement général. Plusieurs intervenants ont cité les crédits d'impôt à la cybersécurité.

Enjeu et piste de solution No 7 : Importance stratégique de la cyberassurance.
De plus en plus, les assureurs acquièrent une expertise en cybersécurité et accompagnent leurs clients dans le renforcement des processus sécuritaires et l'adoption de normes nationales ou internationales. Toute stratégie nationale de cybersécurité doit compter avec l'effet multiplicateur des assureurs en la matière.

Enjeu et piste de solution No 8 : Question de souveraineté.
Question de souveraineté. - Avec la migration en cours des centres de données vers des solutions infonuagiques, la cybersécurité prend une nouvelle dimension. La protection des données québécoises, en particulier celles du secteur public, devraient être hébergées par des entreprises québécoises. À cette fin, il conviendrait de créer une cellule d'accompagnement au sein du Centre des services partagés du Québec (CSPQ) et de créer un bâtiment résistant aux catastrophes, avec alimentation de secours et Internet destinée à héberger en mode colocation les fournisseurs québécois de solutions infonuagiques – sur le modèle du Cyber Park de CyberNB à Fredericton.