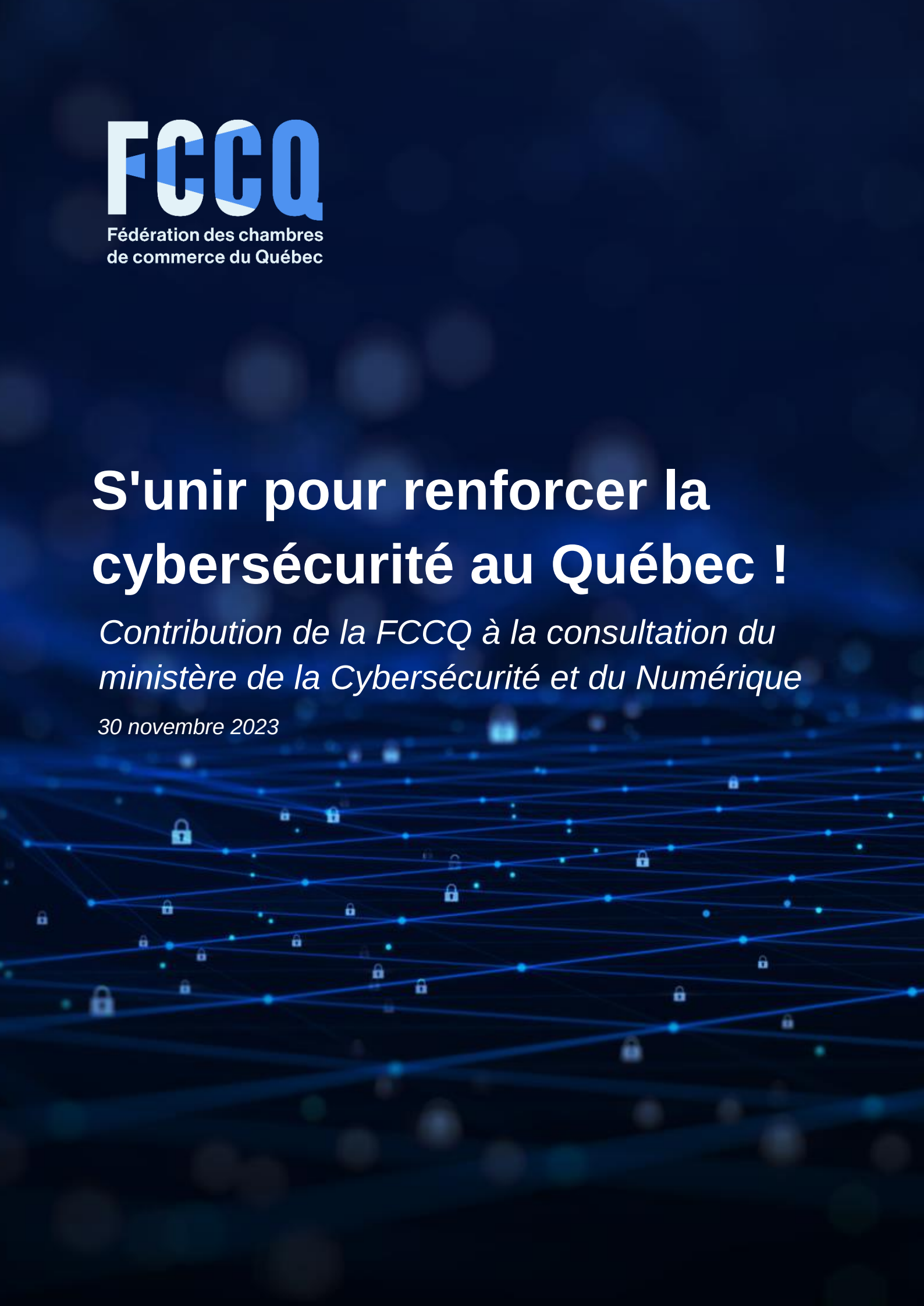
Fédération des chambres de commerce du Québec

S'unir pour renforcer la cybersécurité au Québec !

Contribution de la FCCQ à la consultation du ministère de la Cybersécurité et du Numérique

30 novembre 2023



Introduction

La Fédération des chambres de commerce du Québec (FCCQ) a pour mission d'appuyer le développement des entreprises de l'ensemble des secteurs économiques du Québec et des régions. Grâce à son vaste réseau de près de 120 chambres de commerce et plus de 1 000 membres corporatifs, la Fédération des chambres de commerce du Québec (FCCQ) représente plus de 45 000 entreprises exerçant leurs activités dans tous les secteurs de l'économie et sur l'ensemble du territoire québécois. Plus important réseau de gens d'affaires et d'entreprises du Québec, la FCCQ est à la fois une fédération de chambres de commerce et une chambre de commerce provinciale. Ses membres, qu'ils soient chambres ou entreprises, poursuivent tous le même but : favoriser un environnement d'affaires innovant et concurrentiel.

Au cours des dernières années, les incidents majeurs de cybersécurité se sont multipliés et devenus monnaie courante. Comme pour bien d'autres phénomènes émergents, la pandémie de la COVID-19 et l'adoption du télétravail n'aura qu'exacerbé les risques de cybermenace et placé les entreprises dans une position encore plus vulnérable. La meilleure illustration de cette exacerbation est qu'en 2020, 445 millions cyberattaques avaient été répertoriées à travers le monde, le double de ce qui avait été enregistré en 2019.

En plus d'être plus courantes, les cyberattaques deviennent de plus en plus sophistiquées. Dans l'économie numérisée d'aujourd'hui, toutes les entreprises ont recours à la technologie dans leurs opérations. La protection des données, de l'infrastructure numérique, des opérations, des clients voire des tiers contre une cyberattaque constitue un défi grandissant.

À travers le monde, le volume de données corporatives générées a été multiplié par 18 au cours de la décennie 2011-2020 et continue de s'accroitre de plus en plus rapidement. Le nombre d'appareils intelligents, la facilité de l'accès à Internet, la baisse des coûts d'entreposage des données, l'émergence d'outils d'analyse de plus en plus puissants, et l'essor du commerce en ligne sont autant de facteurs qui ont contribué au développement des données massives

Les risques croissants liés à la cybersécurité sont illustrés par une série d'attaques perpétrées auprès d'entités publiques et théoriquement munis des ressources pour s'en protéger : des ministères et organismes des gouvernements du Québec et du Canada, mais aussi des centres de services scolaires et des établissements d'enseignement supérieur. Or, il s'avère qu'aucune organisation n'est à l'abris des cyberpirates, qui ont su adapter et sophistiquer leurs techniques.

Les cybercriminels cherchent à exploiter les points faibles des systèmes informatiques, ce qui semble d'ailleurs s'avérer une stratégie efficace lorsqu'on analyse la série d'attaques recensées au cours des dernières années contre des entités publiques au Québec et au Canada.

La FCCQ est préoccupée depuis plusieurs années par cette situation et ses impacts sur les entreprises œuvrant au Québec. Nous avons d'ailleurs publié une étude à ce sujet dès 2021 dont la plupart des constats demeurent d'actualité, si ce n'est qu'ils ont pris un caractère d'autant plus urgent que la transformation numérique de la société québécoise s'est accélérée depuis.

Le résultat de notre étude était clair : tant les entreprises que le gouvernement doivent se doter dès maintenant de mesures de prévention des cybermenaces. Ce n'est plus une question de savoir si une entreprise sera l'objet d'une cyberattaque, mais bien de quand elle sera attaquée, si ce n'est pas déjà arrivé. Au Québec, près de la moitié des entreprises sont conscientes d'avoir fait l'objet d'une ou de plusieurs cyberattaques. Cependant, le tiers de ces entreprises admettent ne pas avoir consacré de ressources afin de connaître leurs vulnérabilités et leurs risques. Pourtant, la vitesse d'évolution des techniques d'attaque rend nos entreprises de plus en plus vulnérables et ça ne concerne pas seulement le domaine de la haute technologie : le manufacturier, la logistique, le commerce de détail et la santé sont eux aussi ciblés par les cybercriminels.

Pour faire face à ces nouveaux défis, la FCCQ recommande aux entreprises d'appliquer dès maintenant les pratiques exemplaires en matière de cybersécurité, par exemple en se dotant d'un plan d'intervention et en formant adéquatement et continuellement leurs employés. Des investissements en infrastructures technologiques de cybersécurité sont également requis.

Pistes d'actions

Miser sur la force du réseau

La FCCQ considère que l'État québécois gagnerait à être davantage proactif face à cette menace en constante progression. La création du ministère de la Cybersécurité et du Numérique (MCN) constitue un pas important en ce sens, tout comme l'adoption d'une série de projets de loi :

- Projet de loi n° 14, *Loi favorisant la transformation numérique de l'administration publique* (2019)
- Projet de loi n° 95, *Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives* (juin 2021)
- Projet de loi n° 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (septembre 2021)
- Projet de loi n° 3, *Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives* (2023)

Deux fils conducteurs guident ces différents gestes législatifs : le renforcement des capacités de l'État lui-même ainsi que l'encadrement plus serré des pratiques du secteur privé. En parallèle de ces actions, l'expertise en matière de cybersécurité continue toutefois de se développer dans l'entreprise privée et dans le milieu académique. Il importe donc de soutenir les organisations disposant de cette expertise et de favoriser la mise en commun des pratiques pour faire de la cyberdéfense un projet dépassant le cadre de l'État seul ou d'une entreprise privée seule.

L'exemple d'Israël

Le gouvernement israélien a créé le programme d'incubateurs technologiques au début des années 1990. Aujourd'hui, il existe plus de 25 incubateurs à travers le pays, qui ont tous été privatisés. Les incubateurs offrent un financement gouvernemental allant jusqu'à 85% des coûts des projets en phase de démarrage. Israël investit environ 4,1 % de son PIB dans la R&D, la moyenne au sein de l'OCDE étant de 2,0 %.

La dynamique d'innovation se poursuit ; la société israélienne a produit quelque 300 start-ups de cybersécurité en 2015, contre 150 en 2012. Le secteur de la cybersécurité est particulièrement porteur. Les entreprises israéliennes de cybersécurité ont enregistré une croissance de 70 % de leur financement en 2020.

Les bases d'un tel incubateur existent déjà au Québec et ce, à plusieurs endroits différents. Par exemple, le nouveau Carrefour Cyber, de l'organisme Cybereco (dont le MCN est d'ailleurs membre), dans les locaux de l'École de technologie supérieure (ÉTS) à Montréal, pourrait constituer un excellent point de départ. De tels incubateurs devraient être développés ou créés dans plusieurs régions, en misant sur les forces déjà présentes, et être mis en réseau afin de collaborer dans le développement de nouveaux outils, mais aussi dans la surveillance des nouvelles tendances en matière de cyberrisques.

Recommandation 1 : Développer un véritable réseau de pôles d'expertises et d'incubateurs en cybersécurité, dotés d'un soutien financier mixte public-privé.

Mettre en place une Identité numérique unique

Le projet d'Identité numérique du gouvernement du Québec, lancé en 2019, est au cœur d'un des enjeux essentiels liés à la cybersécurité : la prolifération des usages de différents outils d'identification des citoyens afin d'obtenir des biens et des services. La transformation numérique des services gouvernementaux et institutionnels, l'essor fulgurant du commerce en ligne et l'omniprésence des réseaux sociaux et des appareils électroniques personnels dits « intelligents » a notamment pour conséquence que nos numéros de permis de conduire, nos coordonnées postales, nos cartes de crédit et nos données biométriques n'ont jamais autant circulé afin de nous identifier.

À l'heure où nos téléphones se déverrouillent par reconnaissance faciale et où nos institutions financières sont suffisamment confiantes dans leurs capacités de nous authentifier qu'elles nous permettent de procéder à d'importantes transaction en ligne par nous-mêmes, le manque d'informations sur l'avancement du projet d'Identité numérique du gouvernement du Québec devient anachronique.

Ce projet a le potentiel de simplifier le travail tant des entrepreneurs que des citoyens en mettant fin au fouillis actuel en matière de méthodes d'identification. Il permettrait également de diminuer l'attrait des autres renseignements personnels pour de la fraude de toute sorte.

Recommandation 2 : Accélérer le projet de mise en place de l'Identité numérique du gouvernement du Québec

Apprendre de nos leçons récentes

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (ou Loi 25, issue du projet de loi n° 64) oblige, depuis septembre 2022, toutes les entreprises à déclarer les incidents de confidentialité dont elles ont été victimes. Comme nous l'avions signalé pendant l'étude du projet et à nouveau lorsque cette disposition est entrée en vigueur, ce processus est loin d'être optimal. La définition d'incident de confidentialité étant très large, la Commission d'accès à l'information (CAI) se trouve à compiler à la fois des incidents anodins et des attaques graves dans un même registre. Un courriel envoyé au mauvais destinataire constitue un enjeu de confidentialité, mais il ne s'agit pas d'une cyberattaque.

De plus, ce registre étant public et étant géré par l'organisation qui est également chargée d'appliquer les sanctions prévues dans la loi, les entreprises doivent être très prudentes avant d'y faire un signalement. C'est tout à fait contraire à l'esprit de mise en commun de l'expérience et de l'expertise mentionnée précédemment. Le partage de bonnes pratiques des organisations affectées, de la prévention à la résolution des menaces, apparaît fondamental si l'on veut améliorer nos capacités de cyberdéfense.

Recommandation 3 : Mettre en place une plateforme dédiée à l'inventaire des cyberattaques subies par les organisations québécoises (et d'ailleurs dans le monde) afin d'en faire un lieu d'apprentissage systématique.

La lutte aux rançongiciels

Selon des données compilées par la FCCQ en 2021, 17% des organisations canadiennes avaient subi une cyberattaque de type rançongiciel au cours des derniers mois. 69% des entreprises ciblées par un rançongiciel disent qu'elles ont payé la rançon que leur demandaient les pirates informatiques. Le nombre de demandes de rançon a d'ailleurs été neuf fois plus élevé au début de la pandémie par rapport aux années antérieures. Les dommages financiers directs, au premier chef le paiement de rançons, constitue d'ailleurs l'impact négatif que craignent le plus les dirigeants d'entreprise en ce qui concerne les cyberattaques.

Le modèle économique des pirates informatiques est basé sur le fait que, individuellement, chaque entité visée par un rançongiciel s'expose à des pertes de revenus (liées notamment au blocage de leurs opérations) qui sont plus élevées que le montant à payer. La solution à un problème de ce type ne peut passer que par une action collective, puisque le modèle demeurera viable tant que des organisations continueront de payer des rançons, malgré le fait que les autorités policières et de sécurité nationale recommandent de ne pas payer.

Les États-Unis ont d'ailleurs lancé une initiative regroupant, entre autres, le Canada, l'Union européenne, le Royaume-Uni, Israël, l'Australie, le Japon, Singapour et l'Inde afin de convenir d'une interdiction des paiements. Le Québec doit, dans la mesure de ce qui relève de sa juridiction, joindre ce mouvement et signaler son intention d'appliquer ce pacte lorsqu'il aura été mis en place.

Recommandation 4 : Annoncer l'adhésion du Québec aux éventuelles mesures contenues dans un pacte mondial d'interdiction de paiements de rançons.

L'aide financière gouvernementale en cybersécurité

Tel que mentionné, le gouvernement du Québec a fait adopter la Loi 25 concernant la protection des renseignements personnels. Ce nouvel encadrement législatif plus rigoureux que dans n'importe quelle autre juridiction nord-américaine ajoute au besoin d'investissements technologiques des entreprises du Québec. Son impact financier est d'autant plus important pour les PME qui ne disposent souvent pas de ressources internes suffisantes en matière d'affaires juridiques, de communications et de technologies de l'information qui seront nécessaires afin de bien comprendre les nouvelles responsabilités que leur impose la Loi 25 et les mesures à mettre en place pour s'y conformer, surtout depuis l'entrée en vigueur des principales dispositions en septembre 2023. Celle-ci a des impacts financiers importants : mise à niveau des logiciels et plateformes web, soutien technique et expertise juridique, pénalités, etc. Cela pourrait freiner l'innovation et affaiblir la compétitivité des PME, disproportionnellement affectées par ces coûts additionnels.

Tant dans le cas de la cybersécurité que de la protection des données, le gouvernement du Québec dispose des leviers financiers et fiscaux qui peuvent rendre accessibles les investissements que devront faire les entreprises dans les prochaines années. Comme en témoigne notre étude, la prise de conscience des entreprises quant à l'importance de ces nouvelles réalités est bien amorcée, mais il faut maintenant leur donner les moyens de prendre ce virage rapidement et avec le moins d'impact possible sur leur capacité financière.

Recommandation 5 : Lancer un équivalent du « Programme de rehaussement de la cybersécurité » pour les PME du secteur privé destiné spécifiquement à couvrir une partie des coûts de conformité à la Loi 25.

L’aide financière doit aussi être vue sous un angle plus large que la conformité à la Loi 25. Les entreprises doivent être incitées à procéder aux investissements requis afin de rehausser l’ensemble de leurs capacités de cyberdéfense, incluant l’acquisition ou la mise à niveau des systèmes, le recours aux services-conseil en cybersécurité, etc. Cela doit devenir un incontournable : les investissements en cybersécurité doivent être les jumeaux siamois de ceux servant à déplacer en ligne et automatiser davantage d’opérations d’une entreprise. Cela concerne tant les programmes du ministère de l’Économie, de l’Innovation et de l’Énergie que ceux des différents ministères et organismes sectoriels qui subventionnent la nécessaire transformation numérique des différents secteurs de l’économie québécoise.

Recommandation 6 : Rendre admissible les dépenses liées à la cybersécurité dans le cadre de tous les programmes gouvernementaux d’aide financière dédiés à la transformation numérique.

Au-delà des programmes qui ont, de nature, souvent une durée limitée dans le temps, une mesure plus pérenne doit aussi être mise en place. La volonté du gouvernement de faire de la cybersécurité un enjeu de société devant préoccuper et mobiliser l’ensemble du Québec, y compris ses entreprises, est certainement louable, mais il demeurera incomplet si l’on ne donne pas les moyens à tous d’y contribuer. La situation des PME doit faire l’objet d’une attention particulière, étant donné leurs marges de manœuvres financières généralement plus limitées. Leurs investissements en cybersécurité devant être faits de manière récurrente, une aide récurrente doit être mise en place.

Recommandation 7 : Instaurer un crédit d’impôt remboursable pour investissement en cybersécurité des entreprises, en particulier les PME.

Sommaire des recommandations

Recommandation 1 : Développer un véritable réseau de pôles d'expertises et d'incubateurs en cybersécurité, dotés d'un soutien financier mixte public-privé.

Recommandation 2 : Accélérer le projet de mise en place de l'Identité numérique du gouvernement du Québec

Recommandation 3 : Mettre en place une plateforme dédiée à l'inventaire des cyberattaques subies par les organisations québécoises (et d'ailleurs dans le monde) afin d'en faire un lieu d'apprentissage systématique.

Recommandation 4 : Annoncer l'adhésion du Québec aux éventuelles mesures contenues dans un pacte mondial d'interdiction de paiements de rançons.

Recommandation 5 : Lancer un équivalent du « Programme de rehaussement de la cybersécurité » pour les PME du secteur privé destiné spécifiquement à couvrir une partie des coûts de conformité à la Loi 25.

Recommandation 6 : Rendre admissible les dépenses liées à la cybersécurité dans le cadre de tous les programmes gouvernementaux d'aide financière dédiés à la transformation numérique.

Recommandation 7 : Instaurer un crédit d'impôt remboursable pour investissement en cybersécurité des entreprises, en particulier les PME.