MÉMOIRE DU CPQ

Consultation sur la cybersécurité

Ministère de la Cybersécurité et du Numérique

Novembre 2023

PROSPÉRER ENSEMBLE
cpq.qc.ca

Table des matières

Introduction 3

I. Commentaires généraux 4

1) Résumé du mémoire - *Une nouvelle culture basée sur la prévention* 4
2) Sommaire des recommandations 5

II. Commentaires spécifiques 5

3) Enjeux et défis pour le Québec 5
4) Besoins prioritaires pour le Québec 6
5) Pistes d'actions prioritaires pour le Québec 7

Conclusion 9

Introduction

Le Conseil du patronat du Québec, organisation créée en 1969, est une confédération de près de 100 associations sectorielles et de plusieurs membres corporatifs qui représente les intérêts de plus de 70 000 employeurs, de toutes tailles et de toutes les régions du Québec, issus des secteurs privé et parapublic.

Les employeurs du Québec peuvent compter sur la participation active du CPQ partout où s'élaborent les politiques susceptibles de les affecter, tant au palier municipal, provincial que fédéral. Le CPQ intervient également sur de nombreuses tribunes pour faire entendre la voix des employeurs du Québec et faire reconnaître leur contribution à l'amélioration du niveau et de la qualité de vie des citoyens et plus spécifiquement aujourd'hui, leur sécurité.

Le CPQ salue d'emblée la volonté du gouvernement du Québec à travailler en synergie avec l'écosystème québécois par la mise sur pied d'une consultation publique sur la cybersécurité permettant à la population et les différents intervenants du Québec de suggérer des pistes de solutions et d'émettre leur point de vue relativement à leurs craintes et leur vision de la situation et ce, en corrélation avec leur réalité distinctive trop souvent ignorée.

Le présent mémoire expose les commentaires du CPQ sur les enjeux et les défis pour le Québec qu'engendrent les virages numériques s'opérant dans l'ensemble de la société. Les besoins ainsi que les pistes d'actions prioritaires pour le Québec seront également abordés dans ce document dans lequel les mentions *« S'unir pour renforcer la cybersécurité au Québec! »* et *« Unissons nos voix! »* prennent tout leur sens.

I. Commentaires généraux

1) Résumé du mémoire - *Une nouvelle culture basée sur la prévention*

Ces dernières années, le virage numérique a pris d'assaut le développement des entreprises au Québec touchant leur rendement et créant ainsi une obligation de la part de ces organismes à suivre la vague pour rester dans les rangs. En avril dernier, le gouvernement du Québec poursuivait son « Offensive de transformation numérique[1] » afin d'accélérer le processus du virage des entreprises québécoises en injectant près de 37 M$ en aide.

Malgré le soutien, les outils et l'information déjà en place afin de faire connaître les risques liés à l'implantation et à l'utilisation du numérique ainsi que les efforts des entreprises en ce sens, les cas de fraude et de vol de renseignements personnels ou confidentiels sont très présents causant des préjudices considérables et engendrant un historique problématique pour les entreprises et les personnes touchées.

Le CPQ est d'avis que le renforcement de la cybersécurité au Québec doit être basé sur la prévention, la sensibilisation et la formation du facteur humain. Fait inquiétant, en 2022 le mot de passe le plus utilisé pour une troisième année consécutive était « 123456[2] ». Il est donc nécessaire développer une nouvelle culture afin d'implanter d'emblée, la conscience du risque pour tous et il appert primordial d'unifier les forces et les ressources du Québec afin d'y parvenir stratégiquement et efficacement.

Le Québec pourrait se pencher sur l'élaboration d'un répertoire des outils déjà existants en matière de soutien et de prévention, en guise d'outils de références. Le CPQ est d'avis qu'il s'agit de l'élément clé quant aux solutions envisageables. À cet effet, plusieurs associations, entre autres celle des banquiers canadiens, ont développé et mis sur pied des mesures de prévention personnalisées pour leurs membres[3]. Aussi Le Centre canadien pour la cybersécurité[4] offre une multitude d'outils, d'information, de services pouvant aiguiller le Québec vers des pistes tangibles.

[1] https://www.economie.gouv.qc.ca/bibliotheques/strategies/offensive-de-transformation-numerique/
[2] https://ici.radio-canada.ca/nouvelle/1945677/123456-mot-de-passe-utilisation-canada-2022
[3] https://cba.ca/fraud-prevention-toolkit-older-adults?l=fr
[4] https://www.cyber.gc.ca/fr

2) Sommaire des recommandations

Sommaire des recommandations (100 caractères au maximum pour chacune des recommandations)	
RECOMMANDATION 1 :	S'adjoindre d'effectifs et de ressources qualifiées du Québec en matière de cybersécurité
RECOMMANDATION 2 :	Uniformisation – Création d'un manuel de base simple afin d'unifier le processus d'implantation
RECOMMANDATION 3 :	Formation – Optimiser la formation afin de développer de la main-d'œuvre qualifiée
RECOMMANDATION 4 :	Sensibilisation – Stratégie de sensibilisation à la cybersécurité dans l'utilisation des ressources numériques

II. Commentaires spécifiques

3) Enjeux et défis pour le Québec

De nombreux défis attendent le Québec dans cette lutte aux cyberattaques. Relevons tout d'abord que les petites et moyennes entreprises risquent d'être les plus ciblées par ce changement puisque les multinationales, les grandes entreprises et les organismes gouvernementaux ont, pour la plupart, déjà une sphère de sécurité mise sur pied relativement à la cybersécurité. Gardons cependant à l'esprit que nul n'est véritablement à l'abri, puisque plusieurs grandes plateformes, incluant celle de l'État, ont vu leur système de sécurité déjoué, laissant émerger un lot de données confidentielles malgré leur protection. Une fois un tel incident survenu, diverses informations qui ne sont pas toujours fiables se retrouvent à être médiatisées. Le Québec doit donc se questionner sur les actions à considérer face aux médias et à l'accès à l'information dans ces circonstances afin d'éviter, par exemple, de compromettre une enquête.

Poursuivons en parallèle avec la Loi 25 qui modernise le régime de protection des renseignements personnels au Québec. Les renseignements personnels et les données confidentielles doivent être sécurisés en respectant un cadre précis. L'infrastructure du système numérique se doit d'être adéquate pour rencontrer les exigences imposées. La désuétude des systèmes et des outils informatiques peut mettre en cause l'inefficacité du moyen de prévention mis en place. Une réalité pécuniaire doit être considérée dans cette avenue afin de supporter les entreprises.

En ce sens, le remplacement d'équipements et l'utilisation de nouvelles technologies nécessiteront la formation des effectifs. Cependant, aucune formation n'est efficace si

l'erreur humaine perdure par manque de jugement ou de connaissances. Cette évidence nous guide vers l'importance de la sensibilisation quant aux actions à poser afin d'éviter d'être touché par de potentielles cyberattaques. La réalité actuelle où la toile est accessible par tous, à partir d'appareils multiples parfois même liés au réseau de l'entreprise, préconise cette sensibilisation à être priorisée dans le cadre de l'éducation au Québec. Voilà un enjeu d'envergure pour le Québec de modifier la culture, la façon de penser et d'agir lorsqu'il s'agit de données numériques et de bannir la pensée magique que seuls les banques et les géants de l'industrie sont visés par ces attaques. « Il faut penser avant de cliquer! »

Les voix des membres du CPQ sont unanimes sur la priorisation du renforcement des actions en matière de cybersécurité au Québec. Cependant, le fardeau d'application de nouvelles dispositions peut être une charge démesurée pour certaines entreprises du fait que le projet se veut « pour tous ». Imposer une même structure à tous doit pouvoir prendre en considération la réalité du terrain, notamment de considérer la grosseur de l'entreprise, sa capacité financière et ses effectifs. Il faut également soulever la capacité organisationnelle de certaines de ces entreprises à répondre à un incident de cybersécurité, d'où que la formation du personnel en place est inévitable. Il faut donc mettre sur pied des balises claires et s'assurer que les demandes du gouvernement soient réalisables pour tous.

Le facteur main-d'œuvre est également préoccupant. Bien qu'au Québec nous ayons du personnel compétent ayant développé l'expertise nécessaire à l'application et le respect d'une structure de protection, ces personnes qualifiées sont peu nombreuses et souvent non accessibles pour les entreprises alors que cette ressource est la base même de l'aspect technique et de la réussite du projet.

4) Besoins prioritaires pour le Québec

La prévention est de l'avis du CPQ à prioriser dans ce défi et, pour y arriver, le Québec a un besoin urgent en personnel qualifié afin de soutenir et d'accompagner les entreprises vers l'implantation d'une plateforme qui se veut à la base uniforme et qui pourrait être adaptée selon les réalités de chacun par la suite. Afin de susciter de l'intérêt à ce titre, la sensibilisation pourrait jouer un rôle motivateur auprès du grand public en plus d'un rôle éducateur.

Il ne faut pas non plus oublier qu'avant de prêcher l'exemplarité en matière de cybersécurité, le Québec a besoin que l'État soit lui-même exemplaire en la matière. Ainsi, le CPQ est d'avis que l'implantation d'une nouvelle loi imposant de nouvelles obligations, n'est pas souhaitable à l'heure actuelle. Débutons tout d'abord par l'harmonisation des diverses lois déjà en vigueur et mettons sur pied un plan d'action qui pourrait avoir une incidence réelle et positive sur les entreprises.

Quant à l'harmonisation des lois, le Québec doit aussi se questionner sur la façon de traiter ce dossier avec les actions et les initiatives du palier fédéral. Nous constatons trop souvent un manque d'harmonisation entre les obligations du palier fédéral et celles du palier provincial entrainant ainsi une confusion pour les entreprises ainsi qu'un fardeau administratif additionnel pour celles-ci.

5) Pistes d'actions prioritaires pour le Québec

Formation d'une équipe efficace
Le CPQ demeure convaincu que si les joueurs se regroupent, si les ministères travaillent de pair, si les établissements d'enseignement supérieur du Québec sont sollicités pour leur expertise dans le domaine et que les multinationales ayant déjà implanté des ressources en cybersécurité par leur propre chef, donnent leurs commentaires sur leur expérience et agissent en guise de guide, le Québec ne peut qu'être gagnant et efficace dans cette lutte. La collaboration dans une voie commune, aura à coup sûr un impact positif sur les coûts rattachés à ce projet.

Mise sur pied d'un guide
Cet outil serait composé de lignes directrices de base, claires et définies sur les actions à poser pour l'implantation de mesures simples favorisant la cybersécurité au sein de toutes entreprises. Ce guide se voudrait un outil commun pour tous et adaptable selon les particularités de chacun.

Programme de formation
Offrir de la formation adaptée au besoin, pouvant être accessible pour tous.

Aussi, afin de préparer les travailleurs de demain, le CPQ suggère qu'une formation sur la cybersécurité soit développée et intégrée au cursus scolaire. Dès lors, les étudiants de niveau primaire par exemple, pourraient développer très tôt, une culture d'utilisation sécuritaire des ressources numériques pour ainsi notamment, contribuer au renforcement de la cybersécurité des entreprises à leur arrivée sur le marché du travail.

Campagne de sensibilisation
Sensibiliser le grand public sur l'impact du choix des mots de passe (au travail et à la maison), sur les textos et les courriels frauduleux, etc. La clientèle est sollicitée de plus en plus jeune à la création de comptes et portails nécessitant des connaissances de sécurité minimales souvent inconnues. Une campagne de sensibilisation aurait un impact positif favorable.

Soutien financier

Épauler les entreprises au niveau financier afin que le projet de renforcement de la cybersécurité se réalise.

Conclusion

En conclusion, bien que le risque zéro n'existe pas en matière de cybersécurité, nous en serons assurément plus près si nous travaillons ensemble pour prévenir, sensibiliser et accommoder nos ressources d'ici.

En espérant que ces commentaires et recommandations vous seront utiles, nous vous remercions de l'attention que vous y porterez.

Si des interventions supplémentaires s'avèrent pertinentes, soyez assurés de l'entière disponibilité de l'équipe du CPQ.

Karl Blackburn, président et chef de la direction
Conseil du patronat du Québec

1010, rue Sherbrooke Ouest, bureau 510
Montréal (Québec) H3A 2R7
Téléphone : 514-288-5161
Sans frais au Québec : 1-877-288-5161

Courriel : president@cpq.qc.ca

cpq.qc.ca

CPQ
PROSPÉRER ENSEMBLE