CONSULTATION PUBLIQUE CONCERNANT LA CYBERSÉCURITÉ AU QUÉBEC

APPEL DE MÉMOIRES

Mémoire présenté par ESI Technologies
À l'attention du ministère de la Cybersécurité et du Numérique
Le 30 novembre 2023

INSTRUCTIONS

Le présent gabarit comprend six sections :

1. Résumé du mémoire;
2. Sommaire des recommandations;
3. Enjeux et défis pour le Québec;
4. Besoins prioritaires pour le Québec;
5. Pistes d'actions prioritaires pour le Québec;
6. Autres commentaires.

Il n'est pas obligatoire de remplir toutes les sections. Il est suggéré de remplir prioritairement les sections « Résumé du mémoire » et « Sommaire des recommandations ».

Des annexes, comprenant par exemple des références bibliographiques et des tableaux statistiques, peuvent également y être jointes.

Le mémoire doit être soumis au plus tard à la date limite de dépôt, soit le 30 novembre 2023 à 23 h 59, à l'adresse suivante : consultation.cybersecurite@mcn.gouv.qc.ca.

RENSEIGNEMENTS SUR LA PERSONNE QUI DÉPOSE LE MÉMOIRE	
Nom :	**Patrick**
Naoum	**Naoum**
Titre : M. ☒ M^{me} ☐ Autre ☐ Fonction :	**Vice-président exécutif, ESI Technologies et PDG, Gardien Virtuel**
Nom de l'organisation ou de toute autre entité que vous représentez :	**ESI Technologies de l'information Inc.** **Gardien Virtuel Inc.**
Description de l'organisation ou de toute autre entité que vous représentez :	**SERVICES-CONSEILS ET CYBERSÉCURITÉ EN TECHNOLOGIES DE L'INFORMATION.**
Numéro de téléphone (bureau) :	
Adresse courriel (bureau) :	

Autorisez-vous le ministère de la Cybersécurité et du Numérique à communiquer avec vous aux coordonnées mentionnées ci-dessus pour obtenir, au besoin, des renseignements complémentaires?

- **Oui**

RÉSUMÉ DU MÉMOIRE ET SOMMAIRE DES RECOMMANDATIONS

Résumé du mémoire (5000 caractères au maximum)

L'importance cruciale de la cybersécurité pour les entreprises québécoises ne peut être surestimée à l'heure actuelle. La numérisation croissante de nos activités commerciales a entraîné une dépendance accrue à l'égard des technologies de l'information, créant ainsi une exposition plus grande aux menaces cybernétiques. Malheureusement, de nombreux organismes ont fait face à des difficultés majeures lors de la mise en œuvre des directives du ministère de la Cybersécurité et du Numérique, ce qui s'est traduit par une certaine réticence envers la migration vers l'infonuagique. Cette stagnation a connu des conséquences préoccupantes, comme l'augmentation des vulnérabilités, exposant ainsi ces entreprises à un risque élevé de perturbation des services essentiels pour la population.

Pour les entreprises québécoises, investir dans la cybersécurité ne se limite pas à l'adoption de technologies de pointe, mais englobe également la sensibilisation, la formation continue et la collaboration avec des experts en la matière. Les défis posés par la migration vers l'infonuagique ont souligné le besoin de formation et de communication sur les risques liés à la cybersécurité. Les employés et les dirigeants doivent reconnaître et signaler les menaces, renforçant ainsi la posture de sécurité de l'entreprise contre les attaques.

Le gouvernement peut jouer un rôle crucial dans la promotion de la cybersécurité et de la cyberrésilience en offrant des services de surveillance à un plus grand nombre d'organismes, en particulier ceux qui ne bénéficient pas actuellement d'un tel soutien. Il est essentiel d'identifier des partenaires qualifiés et reconnus pour faciliter l'accès à des services de surveillance 24/7 au Québec, surtout pour des organisations comme les cégeps et les municipalités qui pourraient bénéficier grandement d'une telle initiative. En s'appuyant sur des firmes québécoises de renom, ces organisations pourraient renforcer leur résilience face aux menaces émergentes tout en contribuant à l'économie locale.

Les enjeux de cybersécurité exigent une approche proactive et collaborative. Il est impératif que les entreprises québécoises reconnaissent la nécessité d'investir dans des solutions de cybersécurité efficaces, de renforcer la sensibilisation au sein de leurs équipes et de s'engager dans des partenariats stratégiques pour garantir la protection de leurs activités et préserver la confiance de leurs clients.

En somme, la cybersécurité est un pilier fondamental pour la pérennité des entreprises québécoises.

Sommaire des recommandations (100 caractères au maximum pour chacune des recommandations)	
RECOMMANDATION 1 :	Créer un sentiment d'urgence et d'obligation en utilisant la loi 25 et lier le tout aux bonnes pratiques pour protéger nos organisations contre la cybercriminalité (p. ex., le vol d'identité, les attaques par déni de service, la prise en otage des données pour exiger le versement d'une « rançon », et l'extorsion).
RECOMMANDATION 2 :	Sensibiliser la sécurité en mode continu. Trop nombreuses sont les entreprises qui considèrent la loi 25 comme une tâche à compléter. Même certaines sociétés légales l'abordent en ce sens.
RECOMMANDATION 3 :	Rendre le processus d'approvisionnement du secteur public plus agile pour protéger plus rapidement nos organisations. Mettre en place un processus de vérification diligente en gestion de cybersécurité pour tous les investissements faits par l'état par les principaux acteurs issus du privé au Québec.

Enjeux et défis pour le Québec

À votre avis, quels sont les principaux enjeux et défis, actuels ou émergents, en matière de cybersécurité que le Québec devrait prendre en considération ?

(5000 caractères au maximum)

Par souci du respect de l'anonymat et de la confidentialité, pour tous les choix de réponses comportant des champs variables à remplir, il est recommandé de ne jamais inscrire de renseignements personnels ou sensibles, permettant de vous identifier ou d'identifier une autre personne, ni des données de nature médicale, financière, familiale, etc.

La pénurie de main-d'œuvre qualifiée en cybersécurité est un problème mondial, et le Québec n'est pas épargné. Dans un monde de plus en plus numérisé, la cybersécurité est devenue une nécessité pour protéger les informations privées et sensibles. Cependant, le nombre de professionnels qualifiés en cybersécurité ne parvient pas à répondre à la demande croissante. Cette situation est exacerbée par l'évolution constante des menaces numériques, ce qui nécessite de la formation et une mise à jour régulière des compétences. Le déficit en expertise qualifiée en cybersécurité au Québec et à l'échelle mondiale est un défi majeur qui nécessite une attention immédiate, des initiatives d'éducation ciblées et des programmes de formation adéquats.

La cybersécurité est un domaine en constante évolution, et il est essentiel que les professionnels de ce secteur disposent des connaissances et des compétences nécessaires pour faire face aux nouvelles menaces émergentes. Cela exige une formation continue tout au long de leur carrière, ainsi qu'un accès à des outils et à des ressources de pointe pour rester à l'affût des dernières innovations en matière de sécurité numérique.

En plus de protéger les informations confidentielles, la cybersécurité offre de nombreuses opportunités professionnelles prometteuses. Cela nous pousse à croire qu'il serait bénéfique d'investir dans la formation, la modernisation et la sécurisation des environnements informatiques des petites et moyennes entreprises. Des subventions et des mesures incitatives pourraient être mises en place pour encourager et aider ces initiatives et pour favoriser la disponibilité de la main-d'œuvre qualifiée comme ce fut le cas notamment dans le domaine de la santé durant la pandémie.

Les programmes de formation au collège et à l'université sont complètement dépassés en matière de cybersécurité et d'utilisation efficace et sécurisée des solutions modernes d'infrastructure, qu'elles soient basées sur l'infonuagique ou non. De plus, ces formations sont principalement axées sur les profils de programmeurs et ne permettent pas aux diplômés de démontrer une connaissance suffisante des méthodes de protection adéquates dans les écosystèmes actuels.

Les cours existants, tels que ceux offerts à l'Université Laval dans le domaine de la cybersécurité, reposent sur des principes, des concepts et des techniques orientés vers les réseaux traditionnels, sans aborder les notions de validation ou de recherche de vulnérabilités selon les techniques modernes.

De plus, les formations et les cours sur plusieurs années peuvent parfois représenter un défi, car les connaissances acquises risquent de devenir obsolètes à la fin de leur parcours. Les avancées rapides dans divers domaines rendent essentiel pour les apprenants de rester à jour avec les dernières tendances et les technologies émergentes. Cela requiert une volonté constante d'apprendre et de s'adapter afin de rester pertinents dans un monde en constante évolution. Il est donc primordial de revoir régulièrement les programmes et leur structure pour répondre aux besoins changeants des apprenants.

L’essor des outils de cybersécurité a créé une multitude d’options pour protéger les données et les systèmes. Des pare-feu aux logiciels EDR, en passant par les plateformes de gestion des menaces, ces différents outils offrent divers degrés de protection. Toutefois, la multiplication de ces outils constitue un défi en matière de maximisation de leur efficacité. Les professionnels de la cybersécurité sont confrontés à la tâche complexe de déterminer quels outils sont les plus adaptés à leurs besoins spécifiques, comment les intégrer efficacement dans leur infrastructure existante, et comment les gérer et les mettre à jour régulièrement pour faire face aux nouvelles menaces. Cette tâche requiert une expertise technique profonde, une compréhension des risques de sécurité, et une capacité à évoluer rapidement dans un paysage numérique en constante évolution.

L’utilisation croissante des outils numériques et des technologies avancées accroît considérablement les défis auxquels sont confrontées les entreprises en matière de main-d’œuvre qualifiée, en particulier pour les petites et moyennes entreprises (PME). Ces dernières, étant souvent limitées par des contraintes budgétaires, ne peuvent pas se permettre d’avoir plusieurs spécialistes en cybersécurité en raison des coûts élevés qui y sont associés. Malheureusement, même de nombreuses grandes organisations ne sont pas en mesure d’embaucher un spécialiste en cybersécurité pour répondre à leurs besoins croissants dans ce domaine crucial. Cette situation crée une vulnérabilité accrue face aux menaces et aux attaques cybernétiques, mettant en péril la sécurité et la confidentialité des données sensibles. Il est donc impératif de trouver des solutions innovantes et abordables pour renforcer la posture de sécurité des entreprises de toutes tailles et de tous secteurs d’activité.

En plus de la mise en place d’un programme de formation et du recrutement de main-d’œuvre qualifiée, il est essentiel de faire des progrès concrets dans la sensibilisation et l’engagement de toutes les parties prenantes. Cela inclut la communication régulière, la collaboration étroite et la promotion active des avantages et des opportunités liés à cette initiative. En renforçant ces efforts, nous pourrons efficacement mobiliser et impliquer tous les acteurs clés, créant ainsi un environnement propice à la réussite et à la croissance durable.

Il est frappant de constater les parallèles entre les organisations et les individus au Québec qui tombent fréquemment dans le piège des escroqueries et de l’extorsion de fonds. Ces individus, qui forment l’épine dorsale de la main-d’œuvre de nos organisations, mettent en évidence un déficit flagrant en matière de sensibilisation et de formation.

L’importance de la sensibilisation à la cybersécurité au niveau personnel et au niveau professionnel ne peut être sous-estimée. Chaque individu est un maillon potentiel de vulnérabilité dans la chaîne de sécurité et, sans une culture de sécurité robuste, une organisation est à risque. La sensibilisation à la cybersécurité permet aux individus de comprendre les risques et les menaces en ligne, de reconnaître les signes d’une attaque potentielle, et d’agir de manière appropriée tant au niveau de leur vie personnelle qu’au niveau professionnel.

Les gens doivent être formés pour reconnaître les signes d’hameçonnage, d’ingénierie sociale et autres techniques utilisées par les cybercriminels pour accéder aux données sensibles et confidentielles des organisations.

Parfois, la menace vient de l’interne, qu’elle soit intentionnelle ou non. La manipulation des renseignements personnels est un danger omniprésent dans le monde numérique d’aujourd’hui, d’où l’importance d’une sensibilisation accrue sur ce qu’est un renseignement personnel et comment le manipuler.

Il est essentiel d’intensifier les efforts dans le domaine de la sensibilisation à la cybersécurité pour faire de nos employés la première ligne de défense, plutôt que la porte d’entrée. Ça aura comme effet de renforcer la sécurité de nos données et de nos systèmes.

Besoins prioritaires pour le Québec

À votre avis, quels sont les besoins prioritaires pour renforcer la cybersécurité du Québec ?

(5000 caractères au maximum)

Par souci du respect de l'anonymat et de la confidentialité, pour tous les choix de réponses comportant des champs variables à remplir, il est recommandé de ne jamais inscrire de renseignements personnels ou sensibles, permettant de vous identifier ou d'identifier une autre personne, ni des données de nature médicale, financière, familiale, etc.

La cybersécurité au Québec a longtemps été négligée par nos organisations québécoises, ce qui signifie que la moitié des entreprises du Québec, en particulier les PME, ne sont pas suffisamment équipées pour relever les défis numériques. De plus, un tiers des entreprises de plus de 200 employés n'ont pas de plan documenté en matière de sécurité de l'information selon les dernières données de Cybereco.

L'absence d'un plan documenté de sécurité de l'information peut avoir des conséquences désastreuses pour une entreprise. Au-delà des pertes financières directes dues à des attaques informatiques, il y a des impacts indirects comme la perte de confiance des clients, l'atteinte à la réputation de l'entreprise et la perturbation des opérations commerciales.

L'entrée en vigueur de la loi 25 au Québec a jeté un éclairage inédit sur l'absence criante de plans de sécurité de l'information dans nombre d'entreprises. Cette loi, qui impose des sanctions juridiques en cas de violation des données personnelles, expose la vulnérabilité des entreprises mal préparées et met en évidence l'importance cruciale d'un plan de sécurité de l'information documenté. Pour les entreprises québécoises, notamment les PME, cette loi agit comme un signal d'alarme, les incitant à renforcer leurs mesures de cybersécurité pour éviter les conséquences coûteuses et dommageables d'une violation de données.

Par contre, le manque de force et de sensibilisation à la loi 25 est une problématique majeure contribuant au manque de considération des entreprises en matière de cybersécurité. Plusieurs entreprises ne sont pas pleinement conscientes des implications et des exigences de cette loi, et certaines ne la prennent pas au sérieux, voulant simplement s'y conformer avec le moins d'effort possible. Il est donc essentiel d'intensifier les efforts de sensibilisation pour faire comprendre aux entreprises l'importance cruciale de la conformité à la loi 25.

À mesure que les menaces évoluent, se transforment et se modernisent, il est impératif pour les organisations de rester à jour et de s'adapter en conséquence. La loi 25 n'y fait pas exception, il est impératif de la réviser constamment et de prendre des mesures supplémentaires pour assurer une protection optimale des individus et de leurs données.

Ceci dit, l'importance de la loi 25 prend toute sa dimension face à l'augmentation exponentielle des menaces cybernétiques. En effet, l'univers numérique dans lequel nous évoluons est infesté de fraudeurs, de pirates informatiques et de cybercriminels de partout dans le monde qui cherchent à exploiter les failles de sécurité. Leur but ? Voler des données sensibles et perturber l'infrastructure numérique des entreprises.

Le Québec, son gouvernement, ses organismes et ses entreprises sont aujourd'hui une cible de choix avec l'arrivée de l'intelligence artificielle malicieuse, de l'automatisation des attaques et de la démocratisation voire la commercialisation de ceux-ci. Il est plus facile aujourd'hui pour les acteurs malicieux de cibler de plus petits organismes moins bien protégés que ce ne l'était par le passé où le travail était principalement manuel, ce qui forçait les acteurs malicieux à choisir leurs cibles.

Le monde de la technologie est plus dynamique que jamais, les entreprises les utilisent plus que jamais ce qui cause des angles morts, du rattrapage et des vulnérabilités exploitables. Cette notion est importante, car elle met en lumière des enjeux majeurs en plus du manque de main d'ouvre, de sensibilisation cybernétique et de force de la loi 25 pour nos organismes publics et parapublics.

La prolifération des logiciels-services (SaaS), de la réseautique en nuages et du travail à distance, a considérablement élargi l'étendue du parc informatique des entreprises, augmentant ainsi leur exposition aux risques cybernétiques. Cette expansion a créé une multitude de vulnérabilités et d'angles morts que les acteurs malveillants peuvent exploiter pour accéder aux systèmes et aux données sensibles. Les environnements de réseautique en nuages, par exemple, peuvent être complexes à gérer et à sécuriser, offrant plusieurs points d'entrée potentiels pour les cybercriminels. De plus, le travail à distance accroît le nombre de dispositifs connectés en dehors du réseau sécurisé de l'entreprise, chacun d'eux constituant un point d'accès potentiel pour les attaques. Les organisations doivent donc redoubler de vigilance et investir dans des outils de sécurité robustes et des stratégies de gestion des risques pour sécuriser leur infrastructure informatique de plus en plus étendue.

Premièrement, l'approvisionnement par appel d'offres est un processus commun pour de nombreuses entreprises et organisations, mais ce processus peut entraîner des retards importants dans la mise en place de mesures de cybersécurité efficaces. Ces retards peuvent être coûteux, non seulement en termes de temps, mais aussi en exposant l'entreprise à des risques cybernétiques pendant la période de transition.

Deuxièmement, le problème des solutions à bas coût dans le cadre d'un processus d'appel d'offres est souvent un sujet de préoccupation en matière de cybersécurité. En effet, dans un monde en constante transformation numérique, la recherche du plus bas soumissionnaire peut se traduire par l'adoption de solutions de sécurité bon marché qui n'offrent pas une protection suffisante contre les menaces cybernétiques actuelles. Ce choix pourrait ainsi exposer l'organisation à des risques plus importants, rendant ses systèmes et ses données sensibles plus vulnérables aux attaques. Il est donc crucial, dans un monde numérique en constante évolution, de ne pas sacrifier la qualité et l'efficacité des mesures de cybersécurité au profit d'économies de court terme, mais plutôt de privilégier une approche de sécurité robuste et adaptative qui protège de manière proactive contre les menaces.

Finalement, il est impératif de comprendre qu'il n'y a pas de solution unique ou magique en matière de cybersécurité. Chaque organisation a ses propres besoins, risques et vulnérabilités spécifiques qui nécessitent une approche personnalisée et dynamique. De plus, la création d'ententes financières avec les principaux acteurs du marché, dans le but de réaliser des économies, peut nuire à une gestion de risque efficace. Ces accords peuvent souvent conduire à une dépendance excessive à l'égard d'un fournisseur unique, réduisant la résilience et la flexibilité en cas de menace. Il est donc crucial de mettre l'accent sur une stratégie de sécurité bien équilibrée qui allie des partenariats stratégiques à une gestion de risque rigoureuse, plutôt que de chercher à minimiser les coûts.

Pistes d'actions prioritaires pour le Québec

À votre avis, quelles pistes d'actions concrètes et prioritaires permettraient de renforcer la cybersécurité au Québec ?

(5000 caractères au maximum)

Par souci du respect de l'anonymat et de la confidentialité, pour tous les choix de réponses comportant des champs variables à remplir, il est recommandé de ne jamais inscrire de renseignements personnels ou sensibles, permettant de vous identifier ou d'identifier une autre personne, ni des données de nature médicale, financière, familiale, etc.

Subventions et incitations pour la modernisation/sécurisation des environnements informatiques des petites et moyennes entreprises, en particulier.

1. **Investissement dans les infrastructures critiques :** Orienter les ressources vers la sécurisation des infrastructures critiques, en travaillant en étroite collaboration avec des partenaires du secteur privé pour renforcer les services essentiels contre les cyberattaques.
2. **Campagnes de sensibilisation à la cybersécurité :** Lancer des campagnes de sensibilisation du public pour éduquer les individus et les entreprises sur les menaces cybernétiques, promouvant une bonne hygiène de cybersécurité et les meilleures pratiques.
3. **Incitations à la recherche et au développement :** Offrir des incitations aux entreprises du secteur privé pour investir dans la recherche et le développement de technologies de cybersécurité. Cela peut stimuler l'innovation et nous maintenir en avance sur les menaces émergentes.
4. **Développement de la main-d'œuvre en cybersécurité :** Élargir les programmes éducatifs et les initiatives pour former une main-d'œuvre qualifiée en cybersécurité. Cela inclut des bourses, des programmes de formation et des partenariats avec des établissements d'enseignement.
5. **Soutien aux petites entreprises :** Offrir une assistance et des ressources aux petites et moyennes entreprises pour renforcer leur posture en matière de cybersécurité. De nombreux cybercriminels ciblent des entités plus petites, les considérant comme des proies plus faciles.
6. **Surveillance et évaluation en mode continu :** Mettre en place un système robuste de surveillance et d'évaluation continue des mesures de cybersécurité. Évaluer régulièrement l'efficacité de nos stratégies et les ajuster en réponse à l'évolution des menaces.

Autres commentaires pouvant nourrir notre réflexion afin de rendre le Québec cyberrésilient

(5000 caractères au maximum)

Par souci du respect de l'anonymat et de la confidentialité, pour tous les choix de réponses comportant des champs variables à remplir, il est recommandé de ne jamais inscrire de renseignements personnels ou sensibles, permettant de vous identifier ou d'identifier une autre personne, ni des données de nature médicale, financière, familiale, etc.

Forcer les entreprises à intégrer la cybersécurité dans tous les produits et tous les services par le biais d'une loi. En ce moment, trop de produits et solutions sortent sur le marché avec peu d'égard pour la protection des données. S'il n'y a aucune loi qui force un manufacturier à intégrer des mesures de cybersécurité dans son produit, il ira la plupart du temps vers le moyen le moins cher ; c'est la loi du moindre effort. Un parallèle pourrait être fait avec la fabrication d'item à obsolescence préprogrammée. Pourquoi utiliser les meilleurs matériaux et les meilleurs processus de fabrication alors que le marché accepte des versions de moins bonne qualité ? Voilà que nous nous retrouvons avec des produits qui ont un impact très négatif sur la planète en faisant fi du développement durable. Or, nous voici en 2023 et des lois commencent à apparaître un peu partout sur la planète pour contrer ce phénomène. Nous en sommes à un point critique avec la cybersécurité. En ce moment, tout se fait pirater. Vous connaissez sûrement la phrase : « Ce n'est pas une question de SI on va se faire pirater, mais bien une question de QUAND ça va arriver ! » Je crois que le gouvernement peut certainement aider à améliorer la cyberrésilience avec, entre autres, des moyens législatifs.