2020

CI– 010M
C.P. – PL 64
Protection des renseignements personnels

Commission des institutions

Consultations particulières et auditions publiques sur le projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

MEMOIRE

CAPT(RET) STEVE WATERHOUSE, CD

INFOSECSW

Capt (ret) Steve Waterhouse, CD
Expert en cybersécurité, CISSP

Sommaire exécutif

Le Gouvernement du Québec est bel et bien en voie d'accomplir sa mise à niveau technologique, accompagné des aspects judiciaires, plus que maintenant nécessaire. Le présent projet de loi devrait motiver aussi l'entreprise privé à emboiter le pas dans la prévention de fuites de données, devenu un enjeu sérieux au 21e siècle, comme tous ont étés témoins récemment.

Le rapport d'IBM sur le coût des brèches de données 2020[1] précise que 52% des brèches sont causées par des attaques malicieuses, à 23% par erreur humaine et à 25% par des erreurs système. 80% des incidents implique la compromission d'information personnelle nominative (PII). Le Canada dans ce rapport s'affiche comme le 3e pays qu'il y a eu le plus de brèches déclarées, au montant de $4,5M USD par incident à régler en moyenne. L'industrie qui est la plus perdante est le secteur des soins de la santé, comme c'est est la présente situation en temps de COVID, envers les chercheurs et hôpitaux[2], suivi du secteur de l'énergie, des finances et des pharmas.

Afin d'éviter ces situations, les entreprises, les fonctionnaires et les particuliers serait avantagés de développé et adopter une culture de la sécurité de l'information[3] qui se veut d'être définie comme suit :

1. Intégrer une culture d'entreprise plus large, composée d'actions quotidiennes encourageant les employés à prendre des décisions réfléchies et conformes aux politiques de sécurité;
2. Exiger du personnel qu'il connaisse le risque de sécurité et les processus permettant de l'éviter (sensibilisation);
3. Mettre en place et appliquer un processus de fonctionnement des tâches qui assure la sécurité de l'entreprise (rétroactions et exercices de validation);

Cette approche culturelle implique une combinaison de saines de connaissances et du suivi des tâches quotidiennes. Découlant d'une solide Évaluation des Menaces et des Risques (ÉMR), les priorités de travail sont établies et l'importance accordée aux manquements à corriger sont mis de l'avant tout en gardant en vue les menaces émergeantes. Cette façon de faire est certainement plus accessible pour les grandes entreprises et les gouvernements, par l'accès à du personnel dédié, alors que la PME typique se doit d'engager des consultants externes si ce n'est d'improviser un tel support qui souvent les laissent plus vulnérable.

J'ai été témoins de cette approche gagnante lors d'une visite en Israël au début de 2020. Quoi que ce pays soit constamment sur le qui-vive de menaces terroristes, les autorités ont apportés cette

philosophie de constante anticipation de la menace dans le monde informatique. Bien sûr le marchand de légume du coin ne s'en fait pas trop parce qu'il n'accepte que les paiements en argent, mais les autres entrepreneurs autours le sont certainement, contre la fraude mais aussi de la perte de données qui pourrait se retrouver entre les mauvaises mains. Avec le RGPD, l'Europe a débuté depuis plus de 2 ans une intensive promotion de la protection des renseignements personnelles et l'utilisation des technologies afin de protéger les échanges même par courriel en encourageant l'utilisation de courriels chiffrés comme avec le leader du marché « ProtonMail »[4].

Donc les exigences du présent projet de loi apporteront des défis importants afin d'adresser la conformité par ces PME ce qui selon moi, laissera des vulnérabilités dans la mise en pratique de la loi. Tous les entrepreneurs avec qui j'ai conversé récemment et je converse sur le sujet des fuites de données sont unanime : Tous sont pour la bonne vertu, mais signifient qu'il y a limite à combien ils dépenseront pour la protection des données personnelles. C'est mon interprétation qu'ils éclipsent l'impact réelle des fuites d'information (souvent en absence de la connaissance des menaces en cours contre le vol d'informations personnelle[5]) versus les dépenses de « conformités » qu'ils doivent engager et maintenir, sans compter la mise en place d'une possible réserve de fonds en cas de d'incident. N'en demeure pas moins que les entreprises et organismes publique possédant nombre élevé (à déterminé) d'informations personnelles, que leur soit obligatoirement exigé une journalisation des accès et transferts des données sur les systèmes d'entreposage des données, tel que proposé la norme ISO 27001[6]. Avec un système de surveillance en bonne et due forme, cette mesure aidera grandement à prévenir la consultation non-autorisé des données et leur exfiltration, tel qu'observé en 2019, lors de la fuites massive d'information client chez une importante institution financière importante au Québec.

Tous gardent espoir qu'au moment où une inévitable fuite de données frappe, les services policiers sauront être disponible à prêter assistance, documenter le cybercrime et réussir à traduire en justice les cyber-bandits. Comme j'en fais état dans le mémoire, c'est un travail en voie de développement, mais le temps presse, les corps policiers doivent rattraper le temps perdu à reconnaître le cybercrime dans son importance, et former rapidement une relève solide de cyber enquêteurs et des patrouilleurs à l'affût de la réponse à apporter aux citoyens et aux entreprises aux prises avec un cyber-incident.

Merci à nouveau pour cette opportunité. Je suis maintenant disponible à répondre à vos questions.

Capt (ret) Steve Waterhouse, CD
Expert en cybersécurité, CISSP

Introduction

C’est un honneur et un privilège de m’adresser à vous sur ce sujet important.

Tout d'abord, voici une brève introduction de mes origines. Après 23 ans de service avec les Forces armées canadiennes (R22eR et CIC) et au Ministère de la Défense Nationale (MDN), j'ai eu le privilège d'être parmi les premiers « cyber-soldats » au pays, passant par la gestion des systèmes d'information en réseau de la taille d'un réseau local (LAN - 250 utilisateurs), d’un réseau de campus (CAN - 650 utilisateurs) à celle d'un réseau métropolitain (MAN - plus de 5000 utilisateurs sur plusieurs sites), jusqu’aux premières phases d'intégration de la cybersécurité à titre d’Officier de Sécurité des Systèmes d’Information (OSSI) pendant 10 ans, principalement lors de la renaissance du Collège militaire royal de Saint-Jean (CMRSJ). Plus récemment, outre les divers mandats de consultation avec mon entreprise INFOSECSW, je continue cette mission d’éduquer et former tant les novices que les professionnels des technologies de l’information (TI) et à sensibiliser le public sur la manière d'appliquer les meilleures pratiques de sécurité envers les TI, principalement avec l’Université de Sherbrooke[7] et aussi via les médias d'information (locaux et nationaux) et par la présentation de conférences au pays et ailleurs dans le monde.

La situation

Au cours des 20 dernières années, nos habitudes de travail se sont vraiment tournées vers le cyber espace, y consignant beaucoup de données de toute sorte, tout comme en demandant un peu plus à chaque nouveau client / citoyens. Hebdomadairement, nous apprenons dans les nouvelles d’actualité qu’il y a de nouvelles fuites d’information, des vols de données personnelles. À titre d’exemple en annexe A, y figure un recueil de fuites de données de plus de 30 000 identifiants depuis 10 ans, afin de donner un aperçu de l’ampleur du phénomène et de l’augmentation constante de situations, malgré les leçons apprises.

Il est utopique aussi de penser que la présente structure de gestion de l’information au GQ est adéquate pour les besoins des années à venir afin répondre aux exigences du Projet de Loi 64. Cependant, la présente conjoncture de la transformation numérique va dans ce sens de restructuration nécessaire afin de soutenir et démontrer l’exemple.

Le PL64 fondamentalement

Toutes choses considérées, les fuites de données ne sont pas un phénomène nouveau, seulement rendu plus facile par les technologies incomplètes et par la quantité d’information que nous détenons et partageons parfois sans trop questionner. Le Gouvernement doit développer et maintenir un rôle phare dans ses opérations au quotidien et montrer le bon exemple envers les citoyens et les entreprises en matière de saine gestion des données sous sa responsabilité. La politique de cybersécurité du Gouvernement du Québec en est un bon exemple tout comme le projet de loi 64 qui complètera les outils

nécessaires à diminuer le risque d'exposition non voulu des données des citoyennes et décourager d'éventuelles tentatives d'exfiltration de données de n'importe quelles organisations.

Dans cette optique, appliquer le concept de « Privacy by Design »[8] dans le PL64 se veut d'être défini en 7 concepts :

1. Être proactif, et non réactif; Préventif au lieu d'être correctif;
2. La confidentialité (privacy) comme réglage par défaut;
3. La confidentialité (privacy) inclus dans les conceptions;
4. Pleine fonctionnalité – Somme positive, et non un résultat nul;
5. Sécurité bout en bout - Protection du cycle de vie complet de la donnée;
6. Visibilité et transparence – Demeurer ouvert, et;
7. Respect de la vie privée des usagers – Garder le tout centré sur le besoin usager

Afin de rendre possible ce « Design », les différentes organisations assujetties à la présente loi devront désigner un « responsable de la protection des renseignements personnels » et se doter, pour leur gouvernance, de politiques qui définiront bien cette gestion d'information. À titre d'exemple, une politique de confidentialité, de classification des données, de rétention des données, de destruction des données, de gestion des incidents, des audits que pour en nommer quelques-unes.

Devant toutes ces responsabilités, il serait souhaitable d'établir un échéancier de mise en application ferme, mais réaliste, qui tiendra compte de la nouvelle charge de travail à la PME typique. Afin de favoriser une mise en fonction rapide, je verrai très bien la Commission d'Accès à l'Information (CAI) établir des cadres et de la documentation type, afin que les PME n'aient à remplir en un format uniforme et rendra la tâche plus facile pour tous, voire même par des formules en ligne. À titre d'exemple de la documentation d'opérations pour tous :

A. Ligne directrice pour les sauvegardes, en anticipation des attaques de rançongiciels;
B. Lignes directrices quant à la gestion des mises à jour;
C. Lignes directrices développement sécuritaire s'ils font du développement;
D. Lignes directrices quant à l'entreposage des données locales et en infonuagique

Une majorité de la documentation ci-haut mentionnée existe déjà avec le Centre de Cybersécurité du Canada[9], qui pourrait être revu, si requis, par le Centre Gouvernemental Cyberdéfense du Québec (CGCQ) afin d'appuyer techniquement la CAI dans la production et la diffusion de l'information aux entreprises concernées dans le PL64.

Le PL64 et les organismes publics

Le concept d'opération d'Infrastructures Technologiques Québec[10] (ITQ) arrive au bon moment afin d'offrir la consolidation des actifs informationnels, mais aussi aller une étape plus loin : celle de réellement centralisé les données, ce qui aidera beaucoup à mieux gérer le risque de ces données, mais aussi mieux les sécuriser en ayant des moyens concentrés pour les chiffrer adéquatement l'entreposage selon leur niveau de sécurité. Considérant dans un avenir rapproché que les données ayant un niveau de sensibilité pouvant causer un préjudice à un bien ou un citoyen[11] seront hébergées chez des fournisseurs

d'infonuagique, soit à l'extérieur physiquement des serveurs du GQ, il sera important que des lignes directrices claires et fermes définissent les façons faire quant à l'entreposage sécuritaire les données et la configuration des accès soient émises, puis testées par un exercice de pénétration des systèmes, et ce de manière périodique, rapport à l'appui, réduisant ainsi les fuites potentielles.

Le PL64 et les entreprises privées

Considérant que toutes les entreprises se conforme au PL64 le lendemain de son dépôt, 10 d'entre elles déclarent une violation de confidentialité et/ou fuite de données, est-ce que les effectifs des services policiers sont en nombre suffisant ? Comme nous savons tous que notre économie repose sur les petites et moyennes entreprises, ces dernières n'ont pas de personnel dédié à assurer l'administration au quotidien des ressources informatique. Dans la majorité des cas, ce sont soit des employés connaissant qui y voit, ou les boutiques locales qui assurent un dépannage de base sans trop s'aventurer à offrir une stratégie de gouvernance ou de gestion d'information. Par la nature du travail dans les PME, l'achat de moyen informatisé est inévitable et la considération du stockage d'information demeure élémentaire et précaire. Pour encourager les entreprises de toutes grandeurs, Innovation, Science et Développement Économique du Canada (ISED) ont mis de l'avant en 2019 un programme de certification de conformité en cybersécurité[12] des entreprises afin que ces dernières affichent qu'elles respectent les meilleures pratiques de l'industrie, se voulant de donner confiance aux partenaires et clients. Malheureusement, cette brillante initiative est hors de portée pour les PME par les coûts exorbitants exigés pour évaluer la posture de sécurité d'une entreprise et le coût de la certification annuelle. Dommage... Toute fois, ça n'enlèvera rien au fait que les entreprises qui désirent conserver des données personnelles, devront considérer la forme sous laquelle ces données seront conservées (physique ou électronique) et qu'elle le soit conservées en accord du niveau approprié au niveau de sensibilité, pas plus longtemps du temps prévu selon l'entente signée.

Revenant sur le scénario des 10 entreprises ci-haut mentionnées, le quotidien des employés est voué à la production de leur entreprise, ou la livraison de services, avec très souvent plusieurs sous-tâches, dont l'informatique qui se veut de réparer lorsque brisé, donc en réaction. Avec très peu personnel technique compétent présent lors d'un incident de fuite de données par exemple, ces entreprises feront tout pour minimiser les coûts de rétablissement en l'absence souvent de marges financières d'opération suffisamment généreuse pour les imprévus informatiques, déjà difficile à quantifier. Avec une loi qui les obligera à documenter et rapporter les incidents dès que possible, je suis d'avis que les entreprises plus fragiles (en nombre d'employés et de ressources financières) seront peu réceptives à collaborer, ce qui érodera l'esprit de la présente loi en considération.

Le PL64 et la disponibilité des ressources judiciaires

Au cours des dernières années, j'ai eu à aider des clients qui ont été pris malgré eux, devant un fait tout autant inattendu que non désiré : celui du vol d'identité et d'information. Dans tous les cas, ils se sont malheureusement heurtés à des fins de non-recevoir de la part des services de police auxquels ils ont demandé assistance avec comme réponse qu'ils n'ont soit pas les effectifs suffisant pour prendre leurs dépositions, pas de personnel qualifié afin de documenter la preuve, malgré ce qui est officiellement diffusé et encouragé[13].

Ironiquement, 23 ans passés, ce même constat décris ci-haut était documenté dans un papier à l'Université de Harvard[14] qui pourtant ne se voulait pas d'être une prophétie, mais qui se déroule ainsi de nos jours. On ne peut que saluer la constance des services policiers dans leur façon de faire, mais malheureusement ça dénonce aussi une incapacité à s'adapter aux changements sociétaux menés par les technologies tout autant de l'allocation des ressources et nécessairement des budgets, car les dirigeants tant policiers que politiques ne reconnaissent pas le crime informatique en prévention, mais toujours en réaction[15]. Tout comme mon début de carrière en sécurité de l'information alors en service avec les Forces Armées canadiennes, c'est par passion que beaucoup de policiers se sont liés d'intérêt avec le cyber crime, et ce partout dans le monde par la force des choses. Aujourd'hui en 2020, le portrait est tout autre. Le collège canadien de police a maintenant un programme bien étoffé dédié aux crimes technologiques.[16] Les équipes d'interventions en matière de cybercrime ont beaucoup de succès à traduire devant les tribunaux de plus en plus de bandits grâce au raffinement des techniques d'enquête, l'accroissement des outils pour documenter les preuves et par la motivation de bien effectuer leur travail dans le cyber espace.

Chaque année, des réseaux criminels imposants sont découverts et neutralisés grâce à une collaboration internationale. Le premier avril 2020 a débuté le Groupe national de coordination contre la cybercriminalité (GNC3)[17] qui deviendra la dorsale nationale contre le cybercrime. Quoique la Sûreté du Québec demeure avant-gardiste à combattre le cybercrime[18], cette ressource nationale saura les appuyer davantage et ainsi soutenir le Centre Anti-Fraude[19] qui est en manque flagrant de ressource afin de faire face à l'augmentation constante de cybercrimes.

Le PL64 et les organismes de surveillance

Quelle joie de finalement de constater les pouvoirs accrus qui viendront appuyer la CAI dans la mise en application de la présente loi et lui donner des moyens plus juste à sa mission. Ce qui devrait aussi donner justification à la CAI de procéder à plus d'embauche pour cette augmentation de charge de travail, mais aussi pour diminuer les temps de résolution des cas en cours et à venir. Tous sont, je crois assez réaliste à comprendre qu'il ne sera pas possible de régler des cas de fuites de données en quelques semaines, mais ce serait un objectif réaliste de réduire à un délai de 6 mois alors que présentement la moyenne de résolution des cas tourne autour de 12-18 mois.

Recommandations

Dans l'esprit du présent projet de loi 64, je propose que ces recommandations soient considérées pour doter le Québec des moyens nécessaires pour une meilleure protection et gestion de l'information :

A. Considérer un partenariat avec le conseil canadien des normes afin de rendre plus accessible le programme « cybersécuritaire » aux entreprises du Québec, si ce n'est de parrainer la création d'un programme similaire en province. L'utilisation de ce programme de conformité offrira une solution gagnant-gagnant pour les entreprises à adopter et maintenir de saines pratiques de cybersécurité qui directement profiteront au GQ par possiblement moins de cas de mauvaise gestion d'information menant à des compromissions d'information citoyenne;

B. Exiger des organisations que le responsable de la protection des renseignements personnels soit détenteur d'une certification professionnelle propre au rôle (CISSP[20], CISM[21], CDPSE[22], CIPM[23], garantissant que la personne en poste a toutes les connaissances nécessaires à jour pour remplir son mandat, comme exigé à l'article 37(5) du RGPD[24];

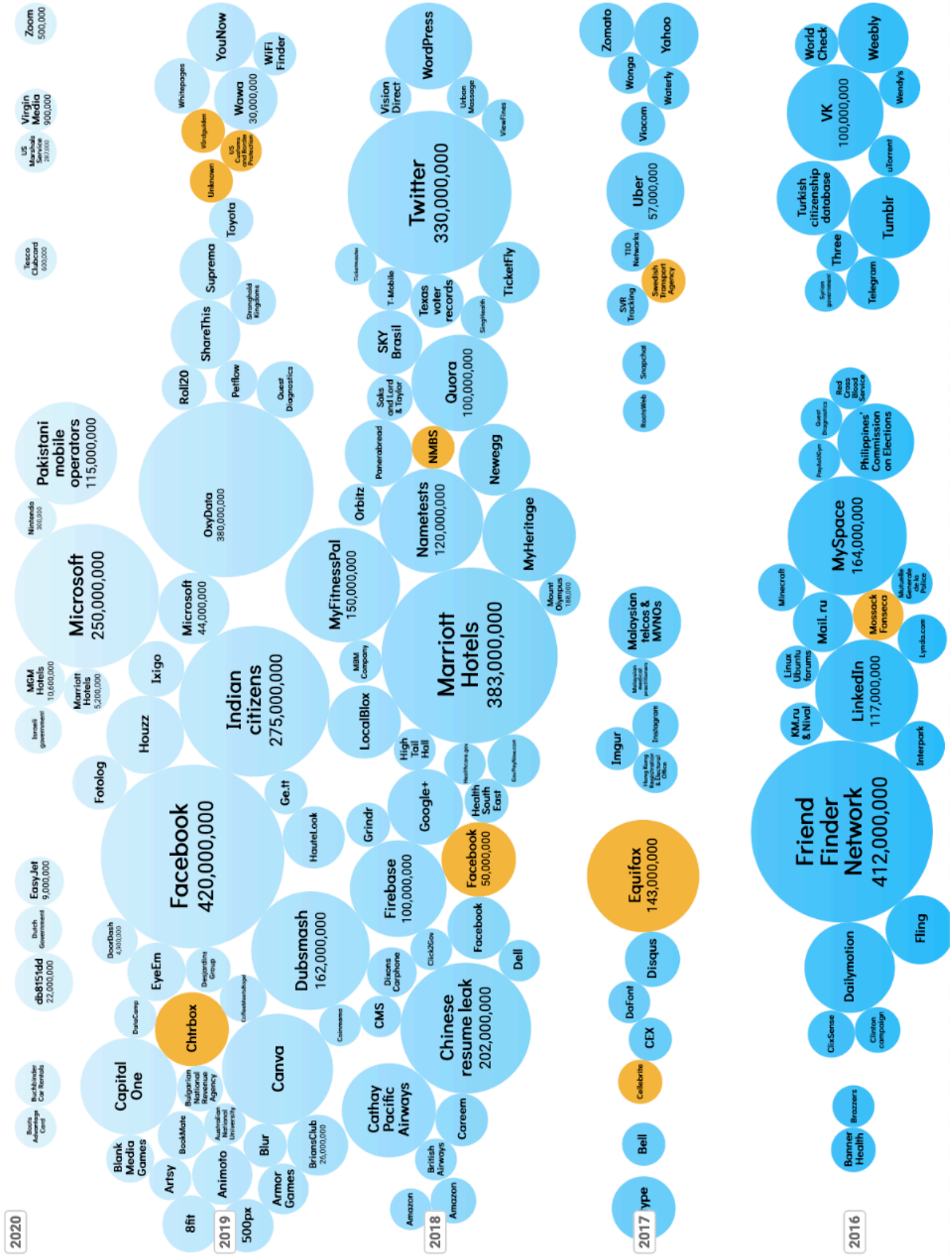
C. Tel que présenté à la section II.1 du projet de loi 64[25], légiférer que les dirigeants d'entreprise soient tenus responsable de la protection d'information et qu'ils en soient imputable de fuites d'information et intégrer dans un processus d'audit obligatoire (annuel peut-être sous la responsabilité de la CAI ou AMF) qu'il soit présenté les plans de gestion d'information et plan de responsabilité de l'information détenue;

D. La CAI doit augmenter son travail de prévention tant envers la population qu'envers les entreprises en ce qui concerne les bonnes pratiques de gestion de l'information comme les meilleures pratiques au traitement et à la transmission des données sensibles. Trop souvent les organisations n'utilisent pas les moyens sécuritaires disponibles pour transmettre l'information qui peut compromettre les renseignements personnels et affecter la vie privée (courrier électronique) par faute de formation / sensibilisation. Les organisations s'en remettent alors à ce qu'ils maîtrisent et se sentent confortables et (faussement) en sécurité avec : le FAX, et;

E. Octroyer aux services policiers davantage de spécialistes en crime technologique ainsi que les ressources (techniques et financières) nécessaires à aider les enquêteurs dans les nombreuses demandes et croissants d'enquête et d'expertises judiciaires avec la technologie. Sans quoi les délais ne cesseront de s'allonger et les criminels s'en sortiront sans payer de leur crime. Et le citoyen sera mieux desservi alors c'est actuellement un manque criant, surtout dans les corps policiers municipaux et régionaux.

Annexe A

Échantillon des fuites d'information mondiale de plus de 30 000 identifiants compromis 2016 - 2020



A1 de 1

World's Biggest Data Breaches & Hacks - Information is Beautiful – 11 May 2020
https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Niveaux de sécurité

Renseignements et biens de nature délicate du gouvernement

Protégé
Lorsque l'on peut raisonnablement s'attendre à ce qu'une divulgation non autorisée porte atteinte à un intérêt autre que l'intérêt national, c'est à-dire à l'intérêt d'une personne ou d'une organisation.

- **Protégé A** — Préjudice à une personne, une organisation ou un gouvernement.
- **Protégé B** — Préjudice grave à une personne, une organisation ou un gouvernement.
- **Protégé C** — Préjudice extrêmement grave à une personne, une organisation ou un gouvernement.

Classifié
Lorsque l'on peut raisonnablement s'attendre à ce qu'une divulgation non autorisée porte atteinte à l'intérêt national, c'est à-dire à la défense et au maintien de la stabilité sociopolitique et économique du Canada.

- **Confidentiel** — Préjudice à l'intérêt national.
- **Secret** — Préjudice grave à l'intérêt national.
- **Très secret** — Préjudice extrêmement grave à l'intérêt national.

Personnel

Cote de fiabilité
Exigée d'un employé qui travaille sur un contrat fédéral de nature délicate pour accéder aux renseignements et aux biens Protégés (A, B ou C).

Attestation de sécurité sur le personnel
Exigée d'un employé qui travaille sur un contrat fédéral de nature délicate pour accéder aux renseignements et aux biens Classifiés (confidentiel, secret, très secret) (peux aussi accéder aux renseignements et aux biens Protégés).

Organisation du secteur privé

Vérification d'organisation désignée (VOD)
Permet à une entreprise d'envoyer des employés avec un besoin de connaître et qui ont fait l'objet d'une enquête de sécurité appropriée sur des lieux de travail à accès réglementé et de leur donner accès à des renseignements et à des biens Protégés.

Attestation de sécurité d'installation (ASI)
Permet à une entreprise d'envoyer des employés avec un besoin de connaître et qui ont fait l'objet d'une enquête de sécurité appropriée sur des lieux de travail à accès réglementé et de leur donner accès à des renseignements et à des biens Protégés et Classifiés.

Organisation du Traité de l'Atlantique Nord (OTAN) : Les niveaux de sécurité classifiés du Canada correspondent à ceux de l'OTAN, mais nécessitent une séance d'information spéciale et un engagement à respecter les exigences applicables de l'OTAN.

Des attestations de sécurité supplémentaires peuvent être accordées aux organisations qui font l'objet d'une VOD ou d'une ASI.

Autorisation de détenir des renseignements (ADR) : autorisation de détenir, de traiter et de protéger des renseignements ou des biens Protégés ou Classifiés sur les lieux de travail. **Production :** autorisation de produire des biens de nature délicate. **Sécurité physique liée à la sécurité des TI et COMSEC/INFOSEC :** peut être un critère dans certains contrats.

Canada

Annexe C
Références

[1] IBM Security - Cost of a Data Breach Report 2020 (https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/)
[2] La cybersécurité pour les organismes de santé : se protéger contre des cyberattaques courantes (https://cyber.gc.ca/fr/orientation/la-cybersecurite-pour-les-organismes-de-sante-se-proteger-contre-des-cyberattaques)
[3] Building a Culture of Security (http://www.isacajournal-digital.org/isacajournal/2020_volume_5/MobilePagedArticle.action?articleId=1616197#articleId1616197)
[4] ProtonMail - GDPR (https://protonmail.com/gdpr)
[5] Évaluation des cybermenaces nationales 2018 (https://cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2018)
[6] ISO 27001 - Annex A.9: Access Control (https://www.isms.online/iso-27001/annex-a-9-access-control/)
[7] CeFTI - Centre de formation en technologies de l'information - Microprogramme de 2e cycle en sécurité informatique - volet prévention (À distance) (https://www.usherbrooke.ca/cefti/futurs-etudiants/microprogramme-de-2e-cycle-en-securite-informatique-volet-prevention-a-distance/)
[8] Privacy by Design - The 7 Foundational Principles (https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf)
[9] Centre de Cybersécurité du Canada – Publications (https://cyber.gc.ca/fr/publications)
[10] ITQ (https://www.quebec.ca/gouv/ministeres-et-organismes/infrastructures-technologiques-quebec/)
[11] TPSGC – Niveaux de sécurité (https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-fra.html)
[12] CyberSécuritaire Canada (https://www.ic.gc.ca/eic/site/137.nsf/fra/accueil)
[13] Sûreté du Québec – Prévention (https://www.sq.gouv.qc.ca/services/prevention/)
[14] Harvard Journal of Law & Technology Volume 10, Number 3 Summer 1997 WHY THE POLICE DON'T CARE ABOUT COMPUTER CRIME (http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech465.pdf)
[15] Cybercriminalité :enjeux, sources de données et faisabilité de recueillir des données auprès de la police - 2002 (https://www150.statcan.gc.ca/n1/pub/85-558-x/85-558-x2002001-fra.pdf)
[16] Collège Canadien de Police – Criminalité Technologique (https://www.cpc-ccp.gc.ca/programs-programmes/technological-technologique/index-fra.htm)
[17] Le Groupe national de coordination contre la cybercriminalité (GNC3) (https://www.rcmp-grc.gc.ca/fr/gnc3)
[18] La SQ met sur pied un grand centre de «cybersurveillance» (https://www.lapresse.ca/actualites/justice-et-affaires-criminelles/affaires-criminelles/201610/31/01-5036426-la-sq-met-sur-pied-un-grand-centre-de-cybersurveillance.php)
[19] Centre antifraude du Canada (https://antifraudcentre-centreantifraude.ca/index-fra.htm)
[20] ISC2 Certified Information Systems Security Professional (https://www.isc2.org/Certifications/CISSP)
[21] ISACA Certified Information Security Manager (https://www.isaca.org/credentialing/cism)
[22] ISACA Certified Data Privacy Solutions Engineer (https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer)
[23] IAPP Certified Information Privacy Manager (https://iapp.org/certify/cipm/)
[24] Article 37 EU RGPD "Désignation du délégué à la protection des données" (https://www.privacy-regulation.eu/fr/37.htm)
[25] Projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (http://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html)