2020

CFP – 009M
C.P. – PL 53
Agents d'évaluation de crédit

Commission des finances publiques

Consultations particulières et auditions publiques sur le projet de loi No.53 – Loi sur les agents d'évaluation du crédit

MEMOIRE

CAPT(RET) STEVE WATERHOUSE, CD

INFOSECSW

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

Sommaire exécutif

Le projet de loi 53 a pour objectif de baliser les actions que doit prendre un agent d'évaluation du crédit envers les informations qu'il détient / manipule / gère : Le gel de sécurité, l'alerte de sécurité et la note explicative.

Dans mon exposé, j'apporte un point de vue plus technique que de gouvernance, car malgré les meilleures intentions, si ces dernières ne peuvent être mises en place et contrevérifiées, ce n'est qu'un exercice de bien paraître,

Selon une étude de Price Waterhouse Cooper de 2018[1], 44% des cyberattaques de fuites d'information aux États-Unis sont attribuables à des agents de menace interne à l'organisation. Seulement 10% des malfaisants ont exhibé des signes, des changements de comportement avant le méfait, ce qui les rend encore plus difficiles à détecter.

De l'enquête canadienne sur la cybersécurité et le cybercrime 2017 de la Sécurité Publique du Canada[2], il n'est pas surprenant de constater que seulement 20.8% des entreprises ont été victime d'un cyber incident, et moins de 10% le rapporte aux services policiers. De ces incidents rapportés, 26,5% sont des demandes de rançon (à la hausse) suivie du vol de renseignements personnels ou financier (17.4%) et des accès non autorisés (15.6%). Il est fréquemment constaté que plus de la moitié des compagnies sondées règlent à l'interne les incidents.

Pour y voir clair, il faut tout d'abord connaître les protagonistes qui sauront influencer l'évaluation des menaces et des risques (ÉMR), outil qui guide les décideurs des organisations quant au choix des moyens de détection / défense envers les fuites de données, tel que présenté dans l'étude du rapport « Insider Threat Report 2018 » de Verizon[3]. Ces acteurs sont :

A. Le travailleur insouciant (*Utilisation à mauvais escient du matériel);*
B. L'agent interne (*vol de l'information pour des demandes externes*);
C. L'employé mécontent (*destruction de matériel ou d'information*);
D. L'employé interne malveillant (*vol d'information pour gain personnel*);
E. Le tiers incapable (*partenaire d'affaires qui compromet la sécurité par négligence ou malice*);

Pour mitiger ce risque de compromission, les dirigeants des entreprises de toute grandeur, doivent reconnaître ce risque existe et prendre les moyens de vérifier à l'interne si l'organisation est vulnérable, intégrer des contre-mesures (technique et/ou humaine) contre toutes menaces et

revoir fréquemment si ces mesures sont appropriées et recommencer. Ce sont là des principes fondamentaux dans la cybersécurité dans n'importe quelle sphère d'activité[4].

Alors que c'est des cas de fuite d'information comme c'est arrivé chez AOL (É-U), Equifax (Can-ÉU-G-B), Desjardins (Can), ou chez l'armée américaine en opération en Irak (U.S. Army) (ÉU-Irak), les vieilles façons de travailler de la « sécurité par l'obscurité » n'ont plus sa place au 21e siècle. Tout finit par se savoir, surtout dans le domaine des fuites d'information, comme l'ont appris les entreprises où il y a eu brèche. Ce sont toujours les citoyens/clients/utilisateurs qui en paient le prix dans le futur, pas ces institutions.

Dans le rapport de février 2020 de Ernst and Young d'un sondage global sur la sécurité de l'information[5], qui est de plus en plus adoptée par les compagnies proactives en matière de protection des renseignements personnels et de la vie privée, l'approche « security by design » est préconisée et mise de l'avant afin de favoriser un environnement de travail axé sur la culture de la sécurité de l'information qui est clé à éviter et à anticiper les fuites de données par différents acteurs de menace envers ces données, dont la menace à l'interne. Et même au Gouvernement fédéral où cette culture de gestion de l'information est présente depuis plus de 50 ans, il y a quand même des manquements et incidents de sécurité[6] et il faut constamment entretenir ces notions de protection de l'information et non imposer et/ou adopter une solution unique dans une organisation, et consignée au dossier qu'une solution a été mise en place et satisfaire la/les norme(s) ou les actionnaires et oublier le tout jusqu'au prochain incident. Car les moyens techniques de prévention de pertes de données (DLP[7]) existent et sont disponibles depuis plus de 10 ans, ayant moi-même installé par le passé ces types de moyens de défense dans des organisations de moyenne et grande taille, dans le but de réduire les fuites de données, tel que soutenu par leur ÉMR.

Je suis d'avis que les organisations se doivent d'user surtout de gros bon sens dans la sécurité de l'information. L'université Carnegie-Mellon d'ailleurs a publié en 2016[8] un excellent papier à cet effet qui peut servir de ligne directrice aux organisations qui veulent bien développer leurs règles à l'interne et sensibiliser / former leur personnel. Sans une formation / sensibilisation adéquate des agents, une transparence des actions d'intervention et une direction claire des dirigeants envers la sécurité des données détenues / manipulées (basé sur une meilleure connaissance des menaces et vulnérabilités), les incidents de fuites de données ne feront se répéter et s'amplifier dans un futur rapproché.

Discutons-en ensemble. 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[9] 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. 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.

Les incidences des mauvaises pratiques

À la fin du 20e siècle, tous découvraient la puissance de l’Internet, de ses capacités. N’importe qui était fasciné de tout ce qui est disponible à lire et voir. L’utilisation du courrier électronique était à ce moment-là tendance du jour. Des services en lignes comme la compagnie américaine AOL venaient d’effectuer son virage technologique de l’ère de l’accès commuté via modem vers des services « en ligne ». Ce qui maintenant donnait un avantage pour les pirates, car la vitesse d’accès venait de doubler, voire quadrupler (pour les chanceux). Qui dit vitesse plus élever d’échange d’information, apporte aussi plus grande vitesse pour le vol d’information. AOL l’a appris à ses dépens par de mauvaises pratiques de sécurité des systèmes à l’interne qui leur a valu une vingtaine d’incidents de sécurité seulement de 1995 à 2003[10]. Puis vint la fuite majeure de 92 millions d’adresses de courriel de 35 millions d’usagers. Pourtant, l’accès à cette base de données était protégé avec une authentification fiable à 2 facteurs (RSA SecurID)[11] que pour des administrateurs internes, un de ceux-ci s’est compromis en ouvrant un courrier électronique avec un « cheval de Troie »[12], livrant ainsi un virus informatique d’accès à distance (RAT)[13] donnant accès au

réseau interne et permettant aux pirates de télécharger la base de données des usagers pour ensuite la revendre à un individu pour fins de campagne de publicité d'un casino « offshore »[14].

L'exemple d'AOL est saisissant par la répétition des incidents jusqu'à ce jour, par des failles techniques dans les plateformes, mais aussi de façon non volontaire, avec l'assistance de personnel à l'interne. Plus récemment et plus près de nous, le vol de données chez Desjardins en 2019 a démontré qu'il ne faut pas trop de connaissances techniques (principalement due à l'absence de système de journalisation d'accès aux données à ce moment) pour mettre la main sur l'information des usagers dans le but de revente[15]. Dans ce cas précis, le sujet d'intérêt avait pleinement accès aux données de l'entreprise dans le cadre de son travail et aucun système ne documentait l'accès aux données, mise à part l'heure et la date l'usager s'authentifiait au réseau informatique pour travailler. Un constat qui m'a interpelé au cours des dernières années en consultation au Québec est le fait que beaucoup de professionnels en TI ne se documentent pas régulièrement sur des sites d'information technique anglophones, faute de la maîtrise de la langue anglaise. Ceci résulte souvent en un manque d'opportunités d'être rapidement informé alors que les sites francophones tardent à faire circuler l'information due à la traduction. Depuis sa mise en opération il y a quelques années, le Centre de Cybersécurité du Canada publie davantage de documentation dans les deux langues officielles pour ainsi faciliter l'accès à l'information névralgique pour tous, comme les meilleures pratiques pour contrer les menaces à l'interne publiées en février 2020[16].

Un cas type de ces incidents en provenance de l'interne des organisations est celui du soldat Bradley Manning (après condamnation en 2013 est renommé Chelsea Manning) de la U.S. Army alors déployée comme analyste au renseignement en Irak en 2010. Ce dernier de sa position a eu accès à de l'information classifiée et hautement sensible d'opérations en cours des organisations militaires et diplomatiques américaines dans le monde et a volontairement retiré des systèmes informatiques classifiés pour l'acheminer à Julian Assange (WikiLeaks)[17]. Suite à cet incident, le directorat du renseignement (DNI) a mis sur pied un programme de sensibilisation national (National Insider Threat Task Force[18]), conjointement avec le FBI, par ordre exécutif du prédisent Obama en novembre 2012. Cinq ans plus tard, un cadre de travail, est livré à tout le gouvernement fédéral ce programme de sensibilisation / normalisation dans le but évident de raffermir la sécurité envers tous les usagers qui manipulent et le traitent de l'information classifiée[19].

L'enquête de la fuite de Manning qui a mené à la création de ce programme et a mis aussi en lumière les traits de personnalité qui caractérise le malfaisant interne[20] :

A. L'avidité des difficultés financières
B. Mécontent ou veut se venger
C. Idéologie
D. Loyauté divisée
E. Vulnérable au chantage
F. Égo / image de soi
G. Intégration
H. Famille / problèmes personnelle

Ces traits caractériels sont là des références à considérer dans l'analyse du comportement louche de collègues de travail qui mène au vol de biens ou de données afin de satisfaire un ou plusieurs

de ces manques. Or, dans le cas du sujet d'intérêt dans l'incident Desjardins, ce dernier dit avoir volé l'information pour remplir une commande pour des connaissances « d'affaire » (et être peu rémunéré a-t-on appris par la suite)[21]. Des sources affirment que c'était chose courante pour des employés de Desjardins sortent des listes de noms pour soit aider des connaissances à se partir en affaire ou pour un paiement en argent[22]. Malgré le travail ardu de bon nombre de professionnels à la sécurité des systèmes d'information chez Desjardins, je suis d'avis que certains dirigeants à la direction de Desjardins ont sous-estimé la menace à l'interne envers l'information des membres depuis bon nombre d'années en ne journalisant pas les accès à ces données des membres et tardant d'aviser tous ceux et celles qui ont étés impactés dès la fuite connue. De plus, en collaborant peu avec les services policiers, et surtout en allant saisir la preuve SANS coordination avec les services policiers[23] contrairement aux autres cas mentionnés dans ce mémoire, le sujet d'intérêt n'a toujours pas été accusé, faute de preuve judiciaire. Desjardins a alors mené une gestion du risque de sa réputation, au lieu en amont d'appliquer une gestion du risque informationnel plus rigoureuse qui aurait réduit les chances à une menace interne d'exploiter des vulnérabilités connues : l'absence de surveillance d'accès des données et des droits d'accès trop ouverts. Les façons de faire et les meilleures pratiques sont là, connues et disponibles.

Dans une autre extrémité du spectre des fuites de données, il y a pour des raisons techniques, mais aussi des raisons de mauvaises gestions des fuites d'information. Comme dans le cas de la fuite de données chez Equifax en 2017[24] où en plus de ne pas avoir pris connaissance rapidement de la situation qui affectait le reste du monde (dont l'ARC et StatsCan[25] en début mars), le CIO et un autre officier de cette compagnie ont commis des délits d'initiés 2 semaines avant l'annonce publique de la brèche d'information affectant plus de 140 millions d'identifiants[26] [27], sois le 6 septembre 2017 alors que les systèmes n'étaient même pas corrigés. À l'annexe « C » est présentée une ligne du temps illustrant les évènements avec la vulnérabilité de certaines fonctionnalités de serveurs Web (Apache Struts 2)[28], qui ont éventuellement atteint Equifax. La cause à effet ici démontré est celle d'une mauvaise gestion des vulnérabilités et gestion de crise de la part d'Équifax et non pas d'agents d'information malveillants, comparé à la réaction rapide des autorités canadiennes[29] avec conférence de presse explicative. L'information sur les vulnérabilités est amplement disponible, et le CIO d'Équifax avait décidément les idées tournées ailleurs que sur le bien-être de l'entreprise. Aucun moyen technique n'aurait pu prévenir cet incident, mais dans la stratégie de cette compagnie, la notification et la documentation des vulnérabilités auraient dû sonner l'alarme que les systèmes étaient à risque dès le mois de mars et non à la fin du mois d'août.

Par ailleurs, l'exploitation de cette brèche a été attribuée au service de renseignement chinois par le département de la justice américaine qui a porté des accusations contre 4 officiers de l'armée chinoise[30] appartenant à la 54^{e} institut de recherche[31] et sont recherchés par le FBI[32]. Il n'est pas impossible que ces mêmes individus (ou du moins l'unité 54^{e} institut de recherche) soient aussi derrière l'attaque envers l'ARC et StatsCan en mars 2017.

Responsabilité de protection des données partagée

Beaucoup de dirigeants considère la prévention des fuites et la protection des données en entreprise comme une responsabilité uniquement informatiques. Or, peu d'organisation réalise que c'est une responsabilité collective, par une synergie interdépartementale comme ce tableau illustre[33] ici-bas afin de déceler une menace à l'interne qui présente des signes avant-coureurs :

A. Les Ressources Humaines sont en mesure d'interpréter les évaluations de rendement;
B. Les opérations au quotidien peuvent constater que le travailleur est mécontent ou n'offre pas un rendement optimal;
C. La sécurité verra des entrées / sortie anormale même possiblement dans des lieux hors du commun;
D. Les Technologies de l'Information verront des activités anomales d'accès / déplacement d'information (considérant que les systèmes sont bien surveillés) voir même l'utilisation de moyens de stockage externe non autorisé;
E. Les avocats seront souvent tard dans la prévention d'actes malveillants alors qu'ils seront habileté à préparer les procédures légales après le méfait accompli et intercepté;

Sans mener des chasses aux sorcières, dès qu'un des départements documente / est rapporté un des signes perçus, il est à l'avantage des collègues de se communiquer entre les intervenants et produire un plan d'intervention qui devra inclure tous les intervenants (autant que possible).

Quelques pratiques dans l'industrie

Finalement (Annexe C)[34], il y a un recueil de pratiques exemplaires proposées par la Sécurité Publique du Canada recommandé à mettre en pratique par les organisations de toutes tailles, qui aidera à prévenir des fuites de données et agrémenter le travail des agents. En voici les grandes lignes:

A. Établir une culture de sécurité
B. Élaborer des politiques et des procédures de sécurité claires
C. Réduire les risques des partenaires et des tiers fournisseurs
D. Mettre en œuvre un cycle de vie de filtrage de sécurité du personnel
E. Offrir de la formation, accroître la sensibilisation et mener des exercices
F. Déterminer les biens essentiels et les protéger
G. Réagir aux comportements inhabituels, les surveiller et les atténuer
H. Protéger vos données

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 les projets de loi 64 et 53 qui complèteront les types d'outils nécessaire à diminuer le risque d'exposition des données des citoyennes et décourager d'éventuelles tentatives d'exfiltration de données de n'importe quelles organisations.

Recommandations

Dans l'esprit du présent projet de loi 53, je propose que ces recommandations soient considérées pour doter le Québec soit à l'avant-garde de la protection et gestion de l'information :

A. Mettre en place un programme de certification envers gestion des données supervisée par l'AMF ou la CAI (avec besoin de re-certification aux 3 ans), non seulement dans les processus de gestion de l'information, mais avec en complément, l'inventaire et la démonstration qu'un système est en place et en service dans le réseau informatique de l'organisation, qui vient renforcer la section « IV » du présent projet de loi, sous forme d'audit;

B. Exiger de l'organisation que les agents affectés à la manipulation / gestion de l'information soient instruits sur les pratiques de la gestion de l'information telles que par exemple le cours au collégial 412-302 - Gestion de l'information administrative[35];

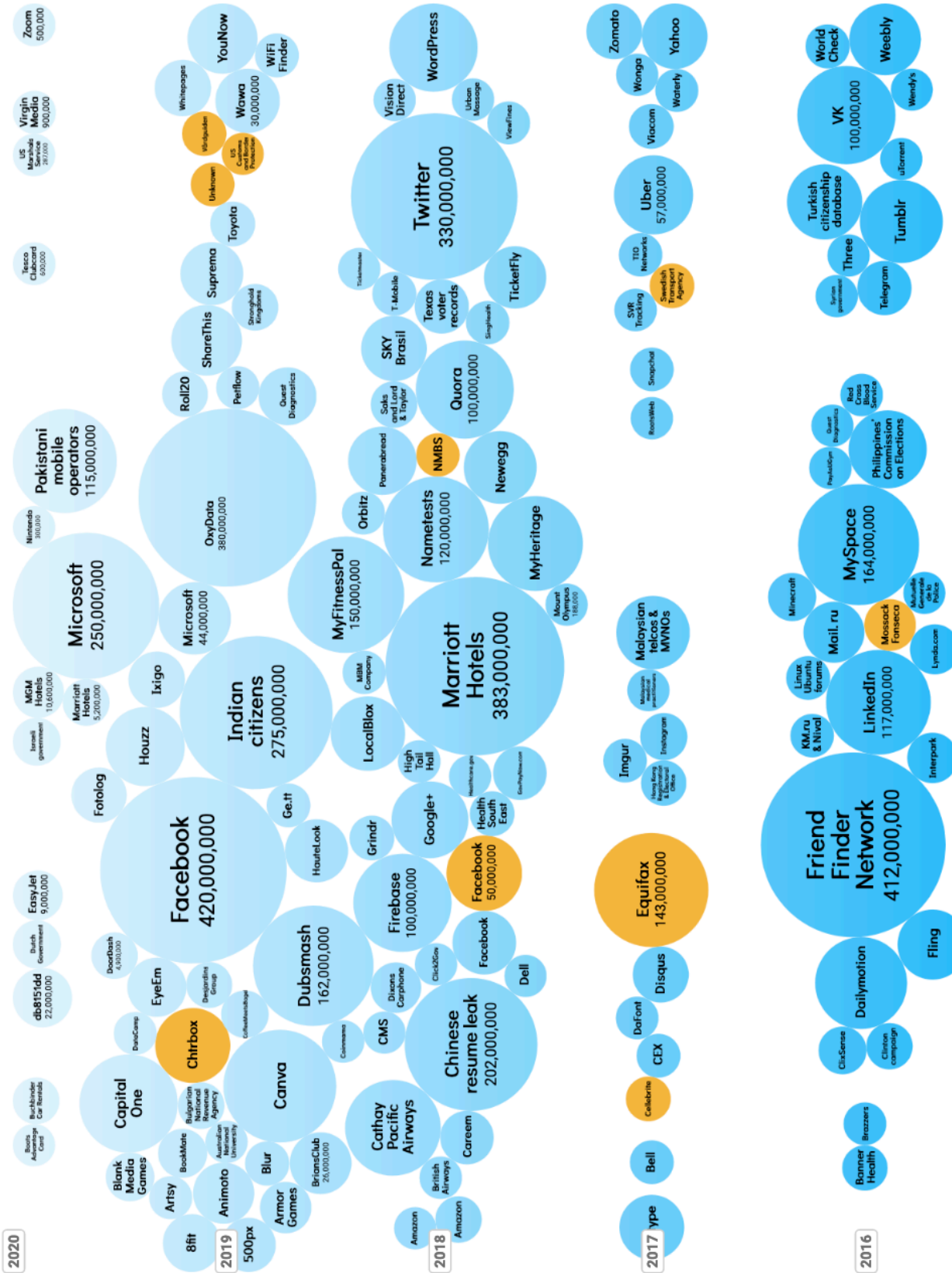
C. Exiger des organisations que le responsable de la protection des renseignements personnels soit détenteur d'une certification professionnelle propre au rôle (CISSP[36], CISM[37], CDPSE[38], CIPM[39], garantissant que la personne en poste a toutes les connaissances nécessaires à jour pour remplir son mandat;

D. Tel que présenté à la section II.1 du projet de loi 64[40], 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;

E. 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;

F. Octroyer aux services policiers davantage de spécialistes en crime technologique ainsi que les ressources (techniques et financières) nécessaire à aider les enquêteurs dans les nombreuses demandes et croissantes d'enquête et d'expertises judiciaire 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 desservit 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



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

La résilience aux risques internes

8 mesures de sécurité recommandées

Établir une culture de sécurité

- ☐ Établir l'engagement et la responsabilisation de la haute direction
- ☐ Désigner un cadre supérieur responsable de la gestion des risques internes
- ☐ Établir un engagement de l'ensemble de l'organisation à l'égard de la sécurité et mettre l'accent sur le leadership à tous les niveaux

Élaborer des politiques et des procédures de sécurité claires

- ☐ Définir des attentes et des résultats clairs
- ☐ Déterminer les niveaux de risques des postes au sein de l'organisation
- ☐ Harmoniser l'accès des employés avec les niveaux de risque des postes

Réduire les risques des partenaires et des tiers fournisseurs

- ☐ Comprendre les principaux biens et systèmes
- ☐ Connaître vos partenaires
- ☐ Connaître vos risques

Mettre en œuvre un cycle de vie de filtrage de sécurité du personnel

- ☐ Effectuer les vérifications préalables à l'emploi
- ☐ Mettre en place un filtrage de sécurité continu des employés
- ☐ Incorporer les procédures de départ et de roulement interne
- ☐ Établir des politiques de sécurité transparentes

Offrir de la formation, accroître la sensibilisation et mener des exercices

- ☐ Offrir une formation régulière pour réduire les risques d'infractions non intentionnelles à la sécurité
- ☐ Accroître la sensibilisation aux signes avant-coureurs
- ☐ Favoriser une culture de vigilance et responsabiliser les employés

Déterminer les biens essentiels et les protéger

- ☐ Cerner et classer les principaux biens et systèmes
- ☐ Sécuriser les principaux biens et systèmes
- ☐ Exploiter la signalisation et les moyens de dissuasion visibles pour contrer l'accès
- ☐ Appliquer le principe de droit d'accès minimal
- ☐ Séparer les fonctions

Réagir aux comportements inhabituels, les surveiller et les atténuer

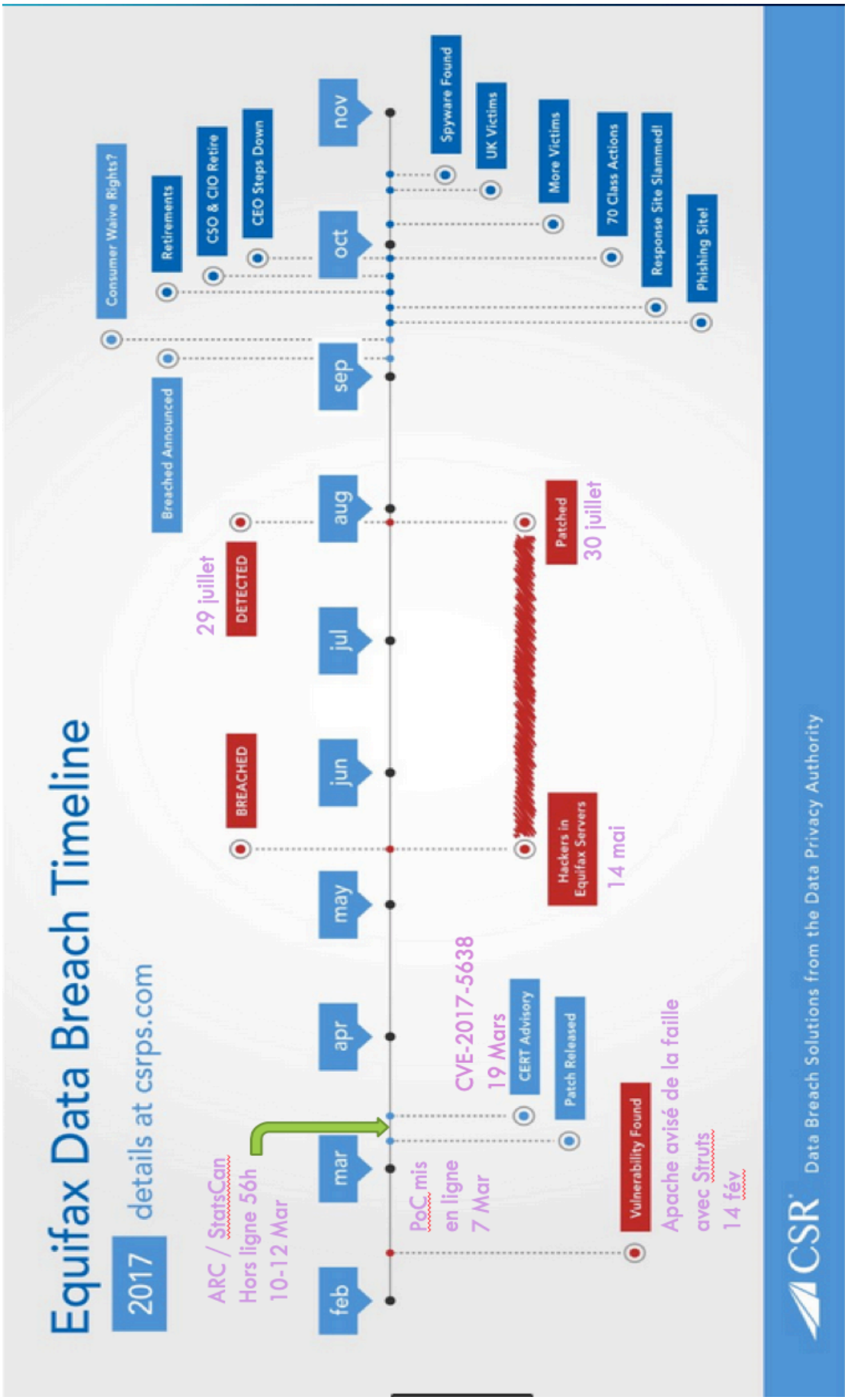
- ☐ Assurer un suivi de l'accès à distance et surveiller les dispositifs d'extrémités
- ☐ Établir des mesures efficaces de signalement, de suivi et d'intervention en cas d'incident
- ☐ Sensibiliser aux meilleures pratiques concernant l'utilisation des sites de réseautage social

Protéger vos données

- ☐ Établir et mettre à l'essai des plans et des procédures de continuité des activités
- ☐ Mettre en œuvre des procédures pour limiter les points de sortie de l'information

Sécurité publique Canada | Public Safety Canada

Canada


Equifax Data Breach Timeline
2017 details at csrps.com
feb
mar
apr
may
jun
jul
aug
sep
oct
nov
ARC / StatsCan
Hors ligne 56h
10-12 Mar
PoC mis
en ligne
7 Mar
Vulnerability Found
Apache avisé de la faille
avec Struts
14 fév
CVE-2017-5638
19 Mars
CERT Advisory
Patch Released
BREACHED
29 juillet
DETECTED
Hackers in
Equifax Servers
14 mai
Patched
30 juillet
Breached Announced
Consumer Waive Rights?
Retirements
CSO & CIO Retire
CEO Steps Down
Spyware Found
UK Victims
More Victims
70 Class Actions
Response Site Slammed!
Phishing Site!
CSR
Data Breach Solutions from the Data Privacy Authority

Annexe D
Références

---

[1] Audit Committee update – Insider threat (https://www.pwc.co.uk/audit-assurance/assets/pdf/insider-threat-for-google.pdf)
[2] Sécurité Publique Canada - L'Enquête canadienne sur la cybersécurité et le cybercrime de 2017 (https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2019-r006/index-fr.aspx)
[3] 2018 Verizon – Insider threat Report (https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf)
[4] Principes fondamentaux de cybersécurité à l'intention du milieu des infrastructures essentielles du Canada (https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-fr.aspx)
[5] EY Global Information Security Survey 2020 (https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-single-pages.pdf)
[6] Des milliers de brèches à la vie privée (https://www.journaldemontreal.com/2019/07/08/des-milliers-de-breches-a-la-vie-privee)
[7] Reviews for Enterprise Data Loss Prevention (DLP) Market (https://www.gartner.com/reviews/market/enterprise-data-loss-prevention/vendors)
[8] 2016 – Carnegie-Mellon University - Common Sense Guide to Mitigating Insider Threats, Fifth Edition (https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf)
[9] 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/)
[10] 2003-02-23 AOL hacked…again (http://xenogere.com/2003/02/22/aol-hackedagain/)
[11] 2003-02-21 Hackers Run Wild and Free on AOL (https://www.wired.com/2003/02/hackers-run-wild-and-free-on-aol/)
[12] Qu'est-ce qu'un Cheval de Troie ? (https://www.kaspersky.fr/resource-center/threats/trojans)
[13] Trojan RAT (https://www.malekal.com/rat-remote-access-tool-botnet/)
[14] Biggest data breaches in history 2004 - (AOL) (https://www.comparitech.com/blog/information-security/biggest-data-breaches-in-history/#2004)
[15] Radio-Canada - Fuite de données chez Desjardins : quels sont les risques et que doit-on faire? (https://ici.radio-canada.ca/nouvelle/1193373/fuite-donnees-desjardins-fraude)
[16] Comment protéger votre organisation contre les menaces internes (ITSAP.10.003) (https://cyber.gc.ca/fr/orientation/comment-proteger-votre-organisation-contre-les-menaces-internes-itsap10003-0)
[17] Chelsea Manning: government anti-leak program a 'blank check for surveillance' (https://www.theguardian.com/us-news/2016/mar/18/chelsea-manning-insider-threat-surveillance-government-employees)
[18] National Insider Threat Task Force Mission Fact Sheet(https://assets.documentcloud.org/documents/2768026/National-Insider-Threat-Task-Force-Fact-Sheet.pdf)
[19] Insider Threat Guide - A COMPENDIUM OF BEST PRACTICES TO ACCOMPANY THE NATIONAL INSIDER THREAT MINIMUM STANDARDS (https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf)
[20] The Insider Threat: Bradley Manning (https://assets.documentcloud.org/documents/2766933/Chelsea-2.pdf)
[21] TVA JE – Rencontre avec le suspect dans le vol de Desjardins (https://video.tva.ca/details/_6094031024001)
[22] Fuite de données au Mouvement Desjardins : 40 000 $ pour acquérir des listes (https://ici.radio-canada.ca/nouvelle/1519744/desjardins-fuite-donnes-liste-informations-personnelles-representant-quebec)
[23] Vol de données: Desjardins et la police se sont marché sur les pieds (https://www.lapresse.ca/actualites/2019-07-31/vol-de-donnees-desjardins-et-la-police-se-sont-marche-sur-les-pieds)
[24] Equifax Breach Response Turns Dumpster Fire (https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/)
[25] CRA, Statscan services back online after shutdowns due to hacking vulnerability (https://www.theglobeandmail.com/news/national/hacking-threat-prompts-cra-to-take-some-online-services-down/article34275578/)
[26] Former Equifax employee indicted for insider trading - Jun Ying (https://www.justice.gov/usao-ndga/pr/former-equifax-employee-indicted-insider-trading)
[27] Charges filed against second defendant for insider trading related to the Equifax data breach - Sudhakar Reddy Bonthu (https://www.justice.gov/usao-ndga/pr/charges-filed-against-second-defendant-insider-trading-related-equifax-data-breach)
[28] The Apache Struts 2 Vulnerability and the Importance of Patch Management (https://securityintelligence.com/the-apache-struts-2-vulnerability-and-the-importance-of-patch-management/)

[29] «La mesure qu'il fallait», estime un expert (https://www.tvanouvelles.ca/2017/03/12/la-mesure-quil-fallait-estime-un-expert)
[30] Chinese military personnel charged with computer fraud, economic espionage and wire fraud for hacking into credit reporting agency Equifax (https://www.justice.gov/usao-ndga/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud)
[31] INSS - China's Strategic Support Force: A Force for a New Era (https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf)
[32] CHINESE PLA MEMBERS, 54th RESEARCH INSTITUTE (https://www.fbi.gov/wanted/cyber/chinese-pla-members-54th-research-institute)
[33] How to Combat the Insider Threat Through Process Improvement (https://cdn2.hubspot.net/hubfs/283820/How_to_Combat_the_Insider_Threat_Through_Process_Improvement_-_Big_Sky_Associates_2015.pdf)
[34] Sécurité Publique Canada – La résilience aux risques internes - 8 mesures de sécurité recommandées- (https://www.securitepublique.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/rslnc-nsdr-rsk-ctns-fr.aspx)
[35] CEGEP Maisonneuve – Formation continue - 412-302 Gestion de l'information administrative (https://fc.cmaisonneuve.qc.ca/syllabus/412-302-gestion-de-l-information-administrative)
[36] ISC2 Certified Information Systems Security Professional (https://www.isc2.org/Certifications/CISSP)
[37] ISACA Certified Information Security Manager (https://www.isaca.org/credentialing/cism)
[38] ISACA Certified Data Privacy Solutions Engineer (https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer)
[39] IAPP Certified Information Privacy Manager (https://iapp.org/certify/cipm/)
[40] 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)