Le 10 juin 2022

L'honorable Jim Carr
Député et président
Comité permanent de la sécurité publique et nationale

BlackBerry Ltée est heureuse de présenter un mémoire au Comité permanent de la sécurité publique et nationale à propos des moyens nécessaires pour protéger les infrastructures critiques du Canada contre les menaces à la cybersécurité.

BlackBerry Ltée est un leader mondial en cybersécurité et en sécurité des TI.
Depuis plus de 35 ans, BlackBerry Ltée crée et met au point des solutions de sécurité pour permettre à des particuliers, des gouvernements et des entreprises de rester productifs en toute sécurité. Aujourd'hui, nos produits sont employés par tous les gouvernements des pays du G7, se retrouvent dans plus de 195 millions d'automobiles, et protègent plus de 500 millions d'appareils, y compris des cellulaires et des ordinateurs portables, de même que des systèmes des secteurs du transport, de l'énergie, de la médecine, de l'aérospatiale, et de la défense.

L'infrastructure critique du Canada est mal préparée à faire face à des cyberattaques.
C'est à partir de ces connaissances techniques et de l'engagement sans faille de BlackBerry Ltée en matière de sécurité et de protection des données privées que j'aimerais attirer l'attention du Comité sur les lacunes qui existent actuellement au Canada dans le domaine de la protection de l'infrastructure critique contre les cybermenaces. Dans tous les domaines d'activité, toute organisation court le risque de subir une cyberattaque, et très peu y prêtent autant le flanc que celles du secteur de l'infrastructure critique.

Des études montrent que des attaques par rançongiciels contre des infrastructures de transport en Amérique du Nord (il ne s'agit que d'un des aspects de notre infrastructure critique, et d'une catégorie de cyberattaques) se sont accrues de 186 %[1] entre juin 2020 et juin 2021. Cette menace ne peut que croître à mesure que notre infrastructure critique emploie de plus en plus de logiciels et de technologies connectées en soutien à ses opérations.

À l'heure actuelle, mises à part les obligations découlant de la LPRPDÉ, il n'y a pas de réglementation en place au Canada exigeant – et encore moins obligeant – les propriétaires et exploitants d'éléments d'infrastructure critique à signaler les incidents relatifs à la cybersécurité, à s'y préparer ou à les prévenir. Les administrations portuaires, les installations maritimes et les installations de traversiers doivent rapporter les cyberincidents aux autorités policières et à Transport Canada, mais ces obligations réglementaires ne sont pas assorties de périodes de référence précises, et ne contiennent aucune ligne directrice sur les mesures de sécurité devant être mises en place. La cyberattaque contre le système de

[1] Ontario Trucking Association, *Trucking Faces Rise in Cyberattacks* [Résurgence des cyberattaques au sein de l'industrie du camionnage]: *Report*, 10 déc. 2021, https://ontruck.org/trucking-faces-rise-in-cyberattacks-report/

soins de santé de Terre-Neuve et Labrador[2] devrait alerter les autorités canadiennes sur la nécessité de faire du renforcement de la protection informatique de l'infrastructure critique une priorité nationale.

En matière de cybersécurité, le Canada tire de l'arrière au sein du G7.

À la suite d'une vague de cyberattaques contre l'infrastructure critique des États-Unis (l'attentat contre le pipeline Colonial[3], la crise SolarWinds[4], les cyberattaques contre Microsoft Exchange[5], le fournisseur de viande JBS[6], et le réseau de métro de New York[7]), le président Biden a rapidement rehaussé les normes en matière de cybersécurité s'appliquant à l'infrastructure critique. Entre autres mesures, le Décret présidentiel visant l'amélioration de la cybersécurité de la nation[8], en mai 2021, a rendu obligatoire des mesures de prévention comme la mise en œuvre du modèle à vérification systématique dans toutes les agences gouvernementales américaines, et le renforcement de la sécurité de la chaîne d'approvisionnement du pays et des logiciels du gouvernement. En juillet 2021, le président a également chargé le gouvernement d'établir des objectifs en matière de cybersécurité que doivent respecter les propriétaires et exploitants d'éléments d'infrastructure critique. En avril 2022, le gouvernement américain a promulgué la Loi de 2022 sur le signalement de cyberincidents s'appliquant à l'infrastructure critique, en vertu de laquelle les éléments d'infrastructure critique désignés doivent signaler aux autorités tout cyberincident les touchant dans les 72 heures, et dans les 24 heures s'il s'agit d'une attaque par rançongiciel. Des exigences semblables s'appliquent en Europe aux propriétaires et exploitants d'éléments d'infrastructure critique par la Directive sur la sécurité des réseaux et de l'infrastructure. On y prévoit des amendes allant jusqu'à 10 millions d'euros ou 2 % du revenu annuel (selon le plus élevé de ces montants) en cas de non-conformité.

Au Canada, des entreprises et des regroupements de secteurs industriels ont soulevé des préoccupations à propos du nombre sans cesse croissant[9] de cybermenaces[10] au pays. Ils en ont appelé au

---

2 CBC, « N.L. health-care cyberattack worst in Canadian history, says cybersecurity expert » [La cyberattaque contre le système de soins de santé de T.-N. a été la pire de l'histoire du Canada, selon un expert], 4 nov. 2021: https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cyber-attack-worst-canada-1.6236210

3 Clifford Krauss, « Colonial Pipeline chief says an oversight let hackers into its system » [Le dirigeant du pipeline Colonial dit qu'une erreur a été exploitée par des pirates informatiques] The New York Times, 8 juin 2021: https://www.nytimes.com/2021/06/08/business/colonial-pipeline-hack.html

4 CISA, « Advanced Persistent Threat Compromises Government Agencies, Critical Infrastructure, and Private Sector Organizations » [Des menaces persistantes pèsent sur des agences gouvernementales, des éléments d'infrastructure critique, et des organisations du secteur privé]. 17 déc. 2020. https://www.nytimes.com/2021/06/08/business/colonial-pipeline-hack.html

5 Kate Conger et Sheera Frenkel, « Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China » [Des milliers de clients de Microsoft ont peut-être été victimes de pirates liés à la Chine]. The New York Times, 6 mars 2021: https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html

6 Tom Polansek et Jeff Mason, « U.S. says ransomware attack on world's largest meatpacker likely from Russia » [Les É.-U. déclarent que l'attaque au rançongiciel contre le plus grand transformateur de viande vient probablement de Russie] Reuters, 1er juin 2021: https://www.ctvnews.ca/business/u-s-says-ransomware-attack-on-world-s-largest-meatpacker-likely-from-russia-1.5451709

7 The Associated Press, « New York transit officials confirm cyberattack: say harm limited » [Les autorités de transport de New York confirment une cyberattaque dont les dommages ont été limités] 2 juin 2021: https://www.ctvnews.ca/sci-tech/new-york-transit-officials-confirm-cyberattack-say-harm-limited-1.5453569

8 Maison-Blanche, « Executive Order on Improving the Nation's Cybersecurity » [Décret sur l'amélioration de la cyber sécurité de la Nation], 12 mai 2021: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

9 Max Fisher, « Constant but Camouflaged, Flurry of Cyberattacks Offers Glimpse of New Era » [Constantes mais cachées – Une volée de cyberattaques permettent d'entrevoir l'avènement d'une nouvelle ère], The New York Times, 20 juillet 2021: https://www.nytimes.com/2021/07/20/world/global-cyberattacks.html?searchResultPosition=1

10 BlackBerry, « BlackBerry Uncovers Massive Hack-For-Hire Group Targeting Governments, Businesses, Human Rights Groups and Influential Individuals » [BlackBerry découvre un vaste groupe d'informaticiens mercenaires ciblant les gouvernements, les entreprises, les groupes de droits de la personne et des personnes influentes], 7 octobre 2020:

gouvernement[11] d'investir dans la cybersécurité à un niveau correspondant à ce qui se fait dans les pays du G7. Là-bas, dans des pays comme les États-Unis, le Royaume-Uni et des états européens, on a investi presque le double de ce que le Canada dépense par personne en matière de cybersécurité afin de renforcer l'infrastructure et protéger l'économie (Voir les Tableaux 1 et 2). Le Canada ne peut se permettre de laisser son infrastructure critique, dont une bonne partie est détenue et exploitée par le secteur privé, exposée à des cybermenaces.

https://www.blackberry.com/us/en/company/newsroom/press-releases/2020/blackberry-uncovers-massive-hack-for-hire-group-targeting-governments-businesses-human-rights-groups-and-influential-individuals

[11] Chambre de Commerce du Canada, *La cybersécurité dès maintenant*: https://chamber.ca/fr/campaign/cybersecuritedesmaintenant/?doing_wp_cron=1635977179.8352680206298828125000

Tableau 1 : Financement en cybersécurité des organismes civils – Pays sélectionnés du G7 (Excluant la Défense)

Pays	Financement en cybersécurité
États-Unis	10,95 milliards $ C (Source[12])
Royaume-Uni	4,45 milliards $ C (National Cyber Strategy[13])(Revue des dépenses[14]) – 2,6 milliards £
France	1,43 milliard $ C (Source[15]) –1 milliard €
Canada	875,2 millions $ C (Budget fédéral de 2022[16])

Tableau 2 : Dépenses par personne pour la cyberbase dans les budgets du Tableau 1

Pays	Financement par personne
États-Unis	34,22 $ C
Royaume-Uni	52,66 $ C
France	37,05 $ C
Canada	23,03 $ C

La cybersécurité doit être une priorité pour le gouvernement, les propriétaires et exploitants d'éléments d'infrastructure critique, et les entreprises canadiennes.
Remédier aux lacunes en matière de cybersécurité constitue une priorité élevée aux yeux des Canadiens. En particulier, être victime d'une cyberattaque arrive maintenant au deuxième rang derrière une perte d'emploi sur la liste de ce qui inquiète le plus les Canadiens[17], selon une enquête Edelman de 2021. Shelley Bruce, chef du Centre de la sécurité des télécommunications Canada (CSTC), a déclaré publiquement[18] que la criminalité informatique constitue « la menace la plus grande et la plus fréquente contre les particuliers et les entreprises au Canada ». Ce point de vue est appuyé par l'expérience. Au

[12] Bureau de la gestion et du budget de la Maison-Blance, « Budget of the U.S. Government: Fiscal Year 2022 » [Budget du gouvernement des É.-U. – Exercice 2022] https://www.whitehouse.gov/wp-content/uploads/2021/05/budget_fy22.pdf

[13] Gouvernement britannique, « National Cyber Strategy 2022 » [Cyberstratégie nationale 2022], https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyberstrategy-amend.pdf

[14] Gouvernement britannique, « Autumn Budget and Spending Review 2021 » [Budget de l'automne et revue des dépenses], https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1043688/Budget_AB2021_Print.pdf

[15] Gouvernement de la France, « Un plan à 1 milliard d'euros pour renforcer la cybersécurité » https://www.gouvernement.fr/actualite/un-plan-a-1-milliard-d-euros-pour-renforcer-la-cybersecurite

[16] Gouvernement du Canada, « Budget 2022 » https://budget.gc.ca/2022/report-rapport/toc-tdm-en.html

[17] Edelman, *2021 Edelman Trust Barometer* https://www.edelman.com/trust/2021-trust-barometer

[18] Mike Lapointe, « We Must Make Canadian Cyberspace a Harder Target, says CSE Chief » [Il faut renforcer le cyberespace canadien, déclare le chef du CSTC], *The Hill Times*, 31 mais 2021. https://www.hilltimes.com/2021/05/31/we-must-make-canadian-cyberspace-a-harder-target-says-cse-chief/298987

pays, autant des entreprises[19], des hôpitaux[20], des universités[21], des systèmes de transport[22], des villes[23] et des services gouvernementaux[24] ont subi des cyberattaques d'envergure[25].

BlackBerry Ltée s'est réjouie de la récente annonce[26] faite par le ministre Marco Mendocino au sujet d'une nouvelle loi qui établira un cadre pour mieux protéger les systèmes d'importance critique pour notre sécurité nationale, en particulier ceux des secteurs de la finance, de l'énergie, des télécommunications, et des transports. Toutefois, il est extrêmement important que ces mesures s'appliquent à tous les secteurs du Canada où l'on retrouve des éléments d'infrastructure critique, y compris ceux qui, pour l'instant, ne sont pas désignés comme tels, comme l'éducation et la recherche, l'industrie aérospatiale et les services d'urgence.

On peut prévenir les cyberattaques

Pour y arriver, il faut mettre en place de robustes mesures de résilience en matière de cybersécurité. À tout le moins, le Comité devrait songer à recommander que les exploitants d'éléments d'infrastructure critique fassent ce qui suit :

1. **Mettre en place des mesures éprouvées d'atténuation des risques et incidents**, y compris
    a. Poser un diagnostic continu en matière de vulnérabilités et de compromissions;
    b. Développer des évaluations sur la préparation en matière de cybersécurité, et des plans de réaction en cas de cyberincidents;
    c. Désigner un coordonnateur de la cybersécurité pour superviser les investissements et la charge de travail dans le domaine;
    d. Adopter un modèle de sécurité à vérification systématique requérant l'authentification en continu pour l'ensemble des usagers et des appareils, y compris les usagers de l'intérieur du périmètre du réseau, un suivi constant des risques et menaces, ainsi qu'une adaptation dynamique des politiques de cybersécurité en fonction de l'évolution constante du domaine.

[19] The Associated Press, « Major ransomware attack aimed at tech provider leaves other companies scrambling » [Une importante attaque au rançongiciel contre un fournisseur de services technologiques forces ses concurrents à agir], 4 juillet 2021: https://www.cbc.ca/news/world/cyberattack-ransomware-kaseya-1.6089578

[20] Maria Sarrough, Megan Ogilvie, « Cyberattack leads to computer system failure at Humber River Hospital, impacting patient care » [Une cyberattaque provoque une panne du système informatique de l'Hôpital Humber River – Les soins s'en ressentent] *Toronto Star*, 15 juin 2021: https://www.thestar.com/news/gta/2021/06/15/computer-system-failure-at-humber-river-hospital-impacts-patient-care.html

[21] Alex Coop, « York University cyber attack looks like ransomware, says security expert » [La cyberattaque contre l'Université York ressemble à une tentative d'extorsion, selon un expert en sécurité], IT World Canada, 6 mai 2020: https://www.itworldcanada.com/article/york-university-cyber-attack-looks-like-ransomware-says-security-expert/430370

[22] Ben Spurr, « TTC begins restoring systems after suspected cyber attack » [Restauration des systèmes du TTC après une cyberattaque probable] *Toronto Star*, 1er nov. 2021: https://www.thestar.com/news/gta/2021/11/01/fallout-from-suspected-cyber-attack-hits-ttc-for-fourth-day-while-agency-stays-silent.html

[23] Laura Lyall, « Hackers demanded $17 million worth of bitcoin as ransom from city of Saint John » [Des pirates exigent une rançon 17 millions en Bitcoins de la ville de Saint John] CTV News, 1er avril 2021: https://atlantic.ctvnews.ca/hackers-demanded-17-million-worth-of-bitcoin-as-ransom-from-city-of-saint-john-1.5372347

[24] Colin Freeze, « Newfoundland cyberattack an 'alarm bell' for Canada » [La cyberattaque contre Terre-Neuve : un signal d'alarme pour le Canada] *The Globe and Mail*, 1er novembre 2021: https://www.theglobeandmail.com/canada/article-newfoundland-cyberattack-an-alarm-bell-for-canada/

[25] Ian Austen, « As Hackers Take Down Newfoundland's Health Care System, Silence Descends » [Des pirates s'en prennent au système de soins de santé de Terre-Neuve, et le silence se fait], *The New York Times*, 12 novembre 2021: https://www.nytimes.com/2021/11/12/world/canada/newfoundland-cyberattack.html

[26] Catherine Tunney, Richard Raycraft, « Canada bans Chinese tech giant Huawei form 5G network » [Le Canada retire l'accès à son réseau 5G au géant chinois de la technologie Huawei] CBC, 19 mais 2022, https://www.cbc.ca/news/politics/huawei-5g-decision-1.6310839

2. **Partager de façon proactive l'information sur les risques et incidents** avec le gouvernement et les propriétaires et exploitants d'éléments d'infrastructure critique. Ceux-ci devraient avoir l'obligation de communiquer rapidement les risques et incidents relatifs à la cybersécurité (par exemple, dans les 72 heures);
3. **S'assurer que les propriétaires et exploitants d'éléments d'infrastructure critique déploient des technologies matures de cybersécurité fondées sur l'AI/AM** pouvant :
    a. Protéger de façon proactive et continue les systèmes, réseaux, appareils et organisations d'infrastructure critique contre les maliciels, grâce à des modèles d'AI/AM entraînés pendant des années, à l'aide de milliards de fichiers (bons ou mauvais);
    b. Être installées dans n'importe quel système d'exploitation (Linux, Windows, etc.) et n'importe quel type d'appareils
    (ordinateurs portables, cellulaires); et
    c. Empêcher les maliciels de s'exécuter, peu importe l'état de connectivité à Internet de l'environnement (hors ligne/isolement physique). La chose prend une grande importance pour les systèmes d'infrastructure critique, dont beaucoup sont déconnectés.

4. **Renforcer la sécurité des logiciels utilisés dans l'exploitation de notre infrastructure critique.** La chaîne d'approvisionnement logicielle implique un réseau complexe de dépendances à l'égard de nombreux développeurs tiers et leurs composantes. Dans bien des cas, les exploitants d'éléments d'infrastructure critique ne connaissent que peu les composantes logicielles intégrées à leurs systèmes de contrôle. À cette fin, le gouvernement doit :

a. **Exiger des développeurs de logiciels employés dans le secteur de l'infrastructure critique qu'ils créent une nomenclature des logiciels[27] (SBOM) afin que les exploitants puissent repérer les vulnérabilités de leurs composantes logicielles.** Cette nomenclature aidera les exploitants à identifier facilement les nouveaux risques de sécurité et à y réagir, à abandonner les produits employant des logiciels qui ne sont plus soutenus par le fournisseur (par exemple, Windows XP), à réviser plus facilement les codes, et à éviter les composantes figurant sur la liste noire parce qu'elles présentent des problèmes en matière de sécurité, de rendement, ou de fiabilité. Cette exigence constituerait un outil de grande valeur[28] pour la gestion des risques de la chaîne d'approvisionnement des logiciels et la cybersécurité, et aiderait les développeurs et exploitants à découvrir des vulnérabilités intégrées dans des logiciels destinés à l'infrastructure critique que des gens mal intentionnés peuvent exploiter. La chose est importante, car d'après certains experts, l'application logicielle moyenne dépend de plus de 500[29] bibliothèques et composantes en libre accès. On a également révélé que plus de 90 %[30] des applications commerciales renferment des composantes en libre accès obsolètes ou abandonnées. Une nomenclature des logiciels prendra une grande importance à mesure que le gouvernement du Canada investira des milliards dans la prochaine génération d'infrastructure, les villes intelligentes, la technologie de réseau intelligent, ainsi que les bornes de recharge de VE et leur infrastructure.

Le Canada doit améliorer sa gouvernance au sujet des risques relatifs à la cybersécurité

À l'heure actuelle, les responsabilités à cet égard sont partagées entre au moins 12 ministères et agences du gouvernement fédéral. Instaurer une certaine cohérence à cet égard au sein de l'appareil gouvernemental permettra d'assurer que tous les ministères fournissent un même effort vers un but commun, ce qui est essentiel pour favoriser une meilleure résilience contre les cyberattaques. Les États-Unis ont nommé leur premier directeur de la sécurité informatique nationale à la Maison-Blanche en juillet, pour qu'il soit le principal conseiller du président dans le domaine, et le Royaume-Uni a créé un poste de sous-secrétaire d'État parlementaire pour le numérique et la large bande qui est responsable de la cybersécurité et des compétences liées au cyberdomaine. **Le Canada doit réfléchir à l'établissement d'un poste, au sein du Cabinet, de responsable de la coordination et des mesures gouvernementales en matière de cybersécurité**. Un tel geste montrerait que le Canada prend la chose au sérieux et cherche à favoriser la résilience en insistant sur la cohérence et la collaboration au sein de l'ensemble du gouvernement relativement aux politiques et mesures de cybersécurité.

Le Canada doit également chercher à améliorer la collaboration entre les secteurs public et privé dans le but de prévenir les cyberattaques. On peut y arriver en établissant une Collaboration canadienne en matière de cybersécurité qui aurait pour mandat de rassembler des acteurs des secteurs public et privé afin qu'ils trouvent les meilleures façons de contrer les menaces en matière de cybersécurité. En 2021, le

---

[27] National Telecommunications and Information Administration, « Software Bill of Materials » https://www.ntia.gov/SBOM

[28] Voir National Telecommunications and Information Administration, « Software Bill of Materials: Transparency in the Software Supply Chain » [Nomenclature de logiciels – Transparence dans la chaîne d'approvisionnement des logiciels], 26 janvier 2021: https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_energy_jan2021overview_0.pdf

[29] Robert Lemos, « Dependency Problems Increase for Open Source Components » [Les problèmes de dépendances croissent pour les composantes en libre accès], *Dark Reading*, 14 avril 2021: https://www.darkreading.com/application-security/dependency-problems-increase-for-open-source-components/d/d-id/1340665

[30] Security, « Synopsys Study Shows 91% of Commercial Applications Contain Outdated or Abandoned Open Source Components » [Une étude de Synopsis montre que 91 % des applications commerciales renferment des composantes en libre accès obsolètes ou abandonnées], 12 mai 2020: https://www.securitymagazine.com/articles/92368-synopsys-study-shows-91-of-commercial-applications-contain-outdated-or-abandoned-open-source-components

Congrès américain a autorisé la création d'une Collaboration de la Défense en matière de cybersécurité. Cette entité, hébergée par l'Agence de sécurité de l'infrastructure et de la cybersécurité, a pour mandat de mener une planification collaborative des secteurs public et privé en matière de défense, une fusion de l'information au cœur de la cybersécurité, et une diffusion des lignes directrices en matière de cyberdéfense pour réduire les risques et accroître la résilience des fonctions nationales critiques des États-Unis. Cette entité s'est montrée efficace, particulièrement dans le sillage de la crise en Ukraine, en améliorant le partage d'informations et la collaboration publique-privée en matière de cybersécurité. Ces efforts ont été renforcés par des réunions de haut niveau sur la cybersécurité organisées par la Maison-Blanche. En août 2021, le président Biden a convié des leaders américains du monde des affaires et de l'éducation au Sommet de la Maison-Blanche sur la cybersécurité, où l'on a souligné l'importance d'une collaboration étroite entre le gouvernement et l'industrie en matière de cybersécurité de l'infrastructure. Ce sommet a été suivi par une seconde réunion à la Maison-Blanche avec des acteurs du secteur privé en matière de sécurité logicielle en janvier 2022, puis en mai 2022, à propos de la sécurité des logiciels en libre accès. Suivant cet exemple, le gouvernement canadien devrait inviter des intervenants du gouvernement et du secteur privé à discuter des possibilités de renforcement de la collaboration en matière de cybersécurité. Grâce à un tel sommet canadien, qui se réunirait à la demande du premier ministre, par exemple, le Canada pourrait profiter des connaissances d'experts et des talents du secteur privé du pays, afin d'étudier comment nous pourrions, de façon collective, renforcer la cybersécurité du pays.

Le Comité peut agir maintenant pour aider les propriétaires et exploitants d'infrastructure à prioriser les investissements en matière de cybersécurité, afin d'empêcher que des cyberattaques ne les mettent en danger. La cybersécurité est essentielle pour soutenir l'innovation et favoriser la confiance en un monde numérique et dépendant des données. Elle est au cœur de notre sécurité nationale et économique.

BlackBerry Ltée sera heureuse d'expliciter ces quelques idées et de poursuivre sa collaboration avec le gouvernement du Canada pour que le pays demeure sûr et prospère.

Veuillez agréer, Monsieur, l'expression de mes sentiments distingués,

John de Boer
Directeur principal, Affaires gouvernementales et politiques publiques
BlackBerry Limited