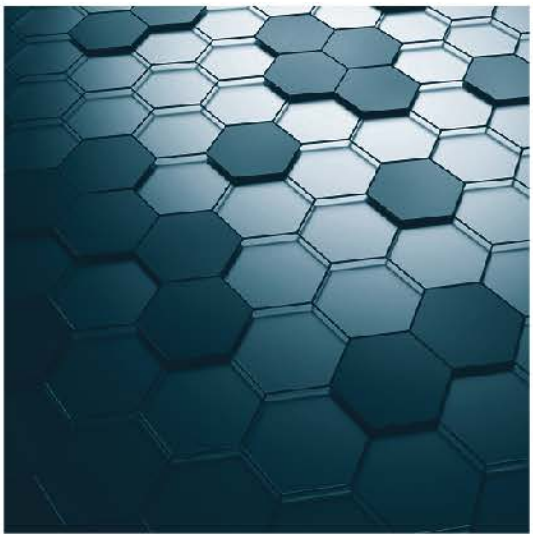
Sécurité publique Canada | Public Safety Canada

BÂTIR UN CANADA SÉCURITAIRE ET RÉSILIENT



Principes fondamenteaux de cybersécurité à l'intention du Milieu des infrastructures essentielles du Canada

1RE ÉDITION

Canada

Page vierge

Table des matières

Sommaire

La sécurité nationale du Canada dépend du fonctionnement ininterrompu de ses infrastructures essentielles, dont la perturbation peut avoir de graves répercussions sur les vies, la sécurité des collectivités et l'économie. Les organisations responsables des infrastructures essentielles utilisent le vaste éventail de réseaux et de systèmes interdépendants, notamment les technologies de l'information (TI) et les systèmes de contrôle industriel (SCI), pour appuyer leurs activités et faire en sorte que les Canadiens ont accès aux produits et services essentiels. Toutefois, ces systèmes sont vulnérables à la perturbation accidentelle et à l'exploitation intentionnelle, lesquelles peuvent engendrer des conséquences dévastatrices.

Le présent document propose des directives pragmatiques et des mesures d'atténuation concrètes en vue d'accroître la sensibilisation et d'entreprendre des activités visant à atteindre un niveau de base de cybersécurité. Ne constituant toutefois pas un guide exhaustif décrivant tous les aspects de la cybersécurité, ce document doit être consulté en parallèle avec d'autres publications, telles que les lignes directrices de l'industrie, les normes internationales et d'autres documents du gouvernement du Canada, le cas échéant. Les organisations devraient également envisager de consulter des spécialistes de la cybersécurité, qui répondront à leurs besoins et à leurs situations particulières.

Le présent document a été élaboré par un groupe de travail du Forum national intersectoriel sur les infrastructures essentielles en vue de recommander une intervention appropriée à l'égard des cybermenaces en constante évolution. Les lignes directrices ont été conçues pour répondre à la nécessité d'adopter une orientation pragmatique pour accroître la cybersécurité.

L'établissement d'une résilience réelle nécessite généralement la mobilisation active de différents intervenants. À titre d'équipe d'intervention nationale en cas d'incident de cybersécurité, le Centre canadien de réponse aux incidents cybernétiques (CCRIC) œuvre au carrefour du secteur public et du secteur privé afin de renforcer les cybersystèmes qui sous-tendent notre sécurité nationale, en plus d'être favorable aux partenariats avec des propriétaires et des exploitants canadiens d'infrastructures essentielles. En outre, Sécurité publique Canada adhère au Cadre du NIST, qui a été conçu par le département de la Sécurité intérieure des États-Unis, en collaboration avec le National Institute for Standards and Technology (NIST), et reconnaît sa pertinence et son applicabilité dans le contexte canadien.

Compte tenu du caractère évolutif du contexte des cybermenaces, les secteurs des infrastructures essentielles, et les partenaires qui les soutiennent, se doivent d'examiner et d'analyser régulièrement leur état de préparation sur le plan de la cybersécurité et de mesurer les progrès réalisés par rapport aux mesures prises. Le présent document décrit plusieurs instruments de mesure, de nature tant réactive que proactive, qui peuvent servir à évaluer les progrès de la résilience d'une organisation aux cybermenaces, tant à l'échelle nationale qu'au sein de chaque organisation.

Cybersécurité : Pierre angulaire de l'économie numérique du Canada

L'univers cybernétique du Canada connaît une croissance rapide et se complexifie un peu plus chaque jour[1].

L'intégration accrue de la technologie et la dépendance croissante à celle-ci, ainsi que l'accroissement des vecteurs de menace et des vulnérabilités en matière de sécurité, font comprendre aux gouvernements et aux citoyens toute l'importance de la cybersécurité et la nécessité de prendre les mesures qui s'imposent pour se protéger contre toute atteinte et exploitation.

L'information constitue souvent l'actif le plus précieux d'une organisation. Par conséquent, la cybersécurité – la protection de ce précieux actif – doit être intégrée aux principaux processus opérationnels et administratifs. Les secteurs des infrastructures essentielles sont interconnectés et dépendent de cybersystèmes sécurisés. Les perturbations cybernétiques des infrastructures essentielles peuvent avoir des conséquences économiques importantes, notamment en engendrant de lourdes pertes pour les entreprises et en entraînant des retombées négatives sur l'économie locale, nationale et mondiale.

Proposition de valeur

Par ailleurs, les conséquences indirectes d'une cyberattaque peuvent entraîner une perte de production et une perturbation des ventes, en plus de miner la confiance des consommateurs. Des coûts économiques indirects tels que ceux-ci peuvent être tout aussi importants que les dommages à l'équipement et aux infrastructures et avoir de lourdes conséquences à long terme sur l'emploi, l'innovation et la croissance économique.

Les cybersystèmes sont désormais indispensables dans presque tous les secteurs de l'économie. Bon nombre d'industries ont été révolutionnées par l'informatique et les systèmes électroniques, y compris pour la fabrication, l'expédition et l'exploitation des ressources naturelles. Même au sein des industries où l'utilisation des cybersystèmes est moins manifeste, une cyberattaque réussie a le potentiel de perturber les activités ou de compromettre des renseignements de nature délicate.

Portée

Le présent document offre aux secteurs des infrastructures essentielles des orientations adaptables et pragmatiques qui permettront aux organisations d'atteindre un niveau minimal de cybersécurité avec peu d'investissement. En fin de compte, en posant quelques questions simples et en adoptant une approche stratégique pour combler les lacunes, les organisations seront en mesure d'améliorer leur situation générale en matière de cybersécurité, et ainsi de

[1] La cybersécurité est l'un des composants clés de *Canada numérique 150*, la stratégie relative à l'économie numérique du Canada. Pour de plus amples renseignements, voir le http://www.ic.gc.ca/eic/site/028.nsf/fra/accueil.

contribuer à accroître la solidité et la résilience des infrastructures et à améliorer la qualité de vie des Canadiens.

Contexte actuel de la menace

Le stockage infonuagique, l'informatique mobile, l'automatisation accrue, de même que la connectivité accrue à Internet des systèmes organisationnels et des systèmes de contrôle des processus augmentent tous les éventuelles vulnérabilités aux cybermenaces des organisations responsables d'infrastructures essentielles. Plusieurs domaines de risques croissants ont été mis en lumière par des recherches dans le cadre desquelles des entrevues ont été menées auprès de centaines de propriétaires et d'exploitants d'infrastructures essentielles. En fait, les études et les rapports portent à croire que la prévalence de la cybercriminalité, les coûts associés aux compromissions, les risques pour les systèmes de contrôle industriel et la sophistication des attaques sont tous à la hausse.

Un grand nombre de cyberattaques ont ces caractéristiques en commun :

- **peu coûteuses** – bon nombre des outils servant aux attaques peuvent être achetés à bas prix ou téléchargés gratuitement;

- **efficaces** – même les attaques mineures peuvent causer d'importants dommages;

- **peu risquées** – les pirates informatiques peuvent échapper à la détection et aux poursuites en masquant leurs traces à l'aide d'un réseau complexe d'ordinateurs et en tirant profit des lacunes des régimes juridiques nationaux et internationaux.

Les auteurs de la majorité des cyberincidents qui touchent l'économie numérique d'aujourd'hui appartiennent aux catégories ci-dessous.

• **Espionnage industriel** – Personnes ou organisations qui cherchent à obtenir de l'information classifiée et exclusive, notamment des stratégies commerciales et de prix, des données sur la situation financière d'entreprises, des renseignements sur les clients, des modèles ou des formules de produits, des données de recherche et des vulnérabilités organisationnelles.

• **Cyberespionnage parrainé par des États –** Personnes bien financées et soutenues par des programmes nationaux disposant de capacités de pointe et capables de compromettre et d'exploiter des systèmes vulnérables.

• **Criminels** – Personnes cherchant à obtenir des données qui pourront être vendues ou utilisées en vue de toucher un profit.

• **Cybermilitants et pirates informatiques amateurs** – Pirates informatiques, expérimentés ou non, qui utilisent des techniques et outils dernier cri pour attaquer un réseau, parfois à des fins personnelles ou pour un groupe organisé.

• **Menace interne** – Personnes évoluant déjà – légalement ou non – au sein d'organisations où elles peuvent causer de graves problèmes.

Sécurité des systèmes administratifs

Comme toutes les organisations, les propriétaires et les exploitants d'infrastructures essentielles utilisent des systèmes de TI pour gérer les aspects administratifs de leurs activités. Ces systèmes servent notamment à exécuter des tâches courantes, comme celles qui relèvent de la gestion des relations avec les clients, des ressources humaines, des finances, de la facturation, ainsi que de la recherche et du développement.

Les renseignements personnels et les données financières stockées dans les systèmes administratifs peuvent constituer des cibles de choix pour des gens mal intentionnés, tout comme la propriété intellectuelle, un actif encore plus précieux également conservé dans de tels systèmes. L'infrastructure administrative peut donc représenter une cible particulièrement attirante pour les groupes criminels qui espèrent toucher un avantage financier.

Les propriétaires et les exploitants d'infrastructures essentielles utilisent des systèmes de TI dans l'ensemble de leurs activités, qu'il s'agisse de l'administration ou de l'exploitation. Ces deux volets ont toujours été gérés séparément, mais ils sont désormais de plus en plus interconnectés. C'est pourquoi les propriétaires et les exploitants doivent mettre en place de rigoureux mécanismes de contrôle dans l'ensemble de leurs activités et porter une attention particulière aux points d'interconnexion.

Sécurité des systèmes de contrôle industriel

Des systèmes de TI ont été ajoutés pour améliorer la gestion des systèmes de contrôle industriel (SCI) qui exécutent des fonctions mécaniques essentielles, ainsi que celle des systèmes de surveillance et d'acquisition de données (SCADA) qui les surveillent et les contrôlent. Ces systèmes sont utilisés dans de nombreuses applications et industries essentielles, notamment les secteurs de l'énergie et des services publics, du transport, de la santé, manufacturier, de l'alimentation et de l'eau. Cela a mené à une amélioration des services, à une réduction des coûts et à des percées technologiques comme les réseaux intelligents. Par contre, ces avancées en TI ont aussi exposé les infrastructures essentielles aux vulnérabilités des logiciels. L'accroissement de la connectivité entraîne la multiplication des points d'accès, ce qui accentue l'exposition éventuelle aux cybermenaces.

Principes fondamentaux de cybersécurité

L'institutionnalisation de la cybersécurité est la responsabilité de tout un chacun. Le fait de suivre quelques principes fondamentaux clés peut considérablement augmenter la résilience d'une organisation.

1) Accroître la sensibilisation à la sécurité

Même les technologies de sécurité les plus pointues seront inutiles si on ne les utilise pas correctement. Comme les pirates informatiques se tournent de plus en plus vers le leurre d'employés pour avoir illégalement accès aux actifs des organisations, un robuste programme de sensibilisation à la sécurité est essentiel pour être en mesure de livrer bataille sur le front en constante évolution de la cybersécurité. Prévoyant d'abord une formation de base pour le personnel, un tel programme devrait ultérieurement intégrer des rappels portant sur les politiques et les pratiques exemplaires, ainsi que de l'information sur les plus récents moyens que les pirates prennent pour leurrer les employés (voir l'annexe 1, qui présente des ressources utiles). Le plan de sensibilisation peut aussi comprendre des examens prévus à intervalles réguliers et visant à actualiser les mesures de sécurité existantes, y compris l'adoption de nouveaux moyens de protection, au besoin.

2) Définir les rôles et les responsabilités

Bien que la cybersécurité soit la responsabilité de tous, la reddition de comptes, elle, doit débuter aux échelons les plus élevés de l'organisation.

Les dirigeants d'organisations jouent donc un rôle essentiel relativement aux principales responsabilités. Ils sont particulièrement bien placés pour favoriser une culture de sensibilisation et de prévention, et veiller à ce que les vulnérabilités soient évaluées, que des plans de cybersécurité soient établis et que des mesures de responsabilisation soient mises en place.

Chaque organisation devrait désigner au moins une personne-ressource en matière de cybersécurité ayant les responsabilités suivantes :

- s'informer sur les menaces, les tendances et les options de sécurité :
  - en adhérant à une association de cybersécurité, les organisations peuvent se tenir informées de l'actualité du domaine (voir l'annexe 1 pour obtenir des exemples);
- planifier, acquérir et mettre en œuvre des mesures de sécurité;
- aider les autres membres du personnel à comprendre les politiques et les pratiques exemplaires en matière de cybersécurité;
- faire appliquer les politiques et les pratiques exemplaires en matière de cybersécurité avec l'aide de la direction;
- maintenir les mesures de sécurité utilisées par l'organisation et les mettre à jour.

La cybersécurité devrait faire partie des obligations de reddition de comptes des gestionnaires, qui devraient également s'acquitter des responsabilités suivantes :

- donner des directives aux employés sur l'importance de la cybersécurité en tant qu'élément des activités, y compris des politiques décrivant la responsabilisation en matière de cybersécurité;
- appuyer et surveiller les projets de cybersécurité;
- consulter des experts, comme des conseillers juridiques, au sujet des obligations externes, par exemple, à l'égard des lois fédérales ou provinciales.

3) Élaborer des politiques et des normes

Une ***politique*** de sécurité est un document qui explique ce que les employés peuvent ou ne peuvent pas faire en ce qui a trait à la cybersécurité, par exemple accéder à Internet ou aux réseaux sociaux à partir des réseaux organisationnels. Les politiques de cybersécurité sont donc essentielles pour aider les employés à comprendre leurs rôles et leurs responsabilités.

Une politique sur l'utilisation acceptable pourrait, par exemple, indiquer que :

- *les employés **ne peuvent pas** brancher un ordinateur ou un dispositif mobile personnel au réseau de l'entreprise;*
- *les employés qui accèdent au réseau de l'entreprise à partir de la maison **doivent** le faire en utilisant les outils de sécurité approuvés.*

Quant à elle, la ***norme*** est un document qui explique comment une tâche particulière doit être effectuée. Dans le domaine cybernétique, les normes s'appliquent le plus souvent à la mise en place et à l'utilisation de systèmes techniques. Par exemple, une norme relative aux mots de passe décrirait exactement ce qu'un mot de passe acceptable peut et ne peut pas comprendre, sa longueur et la fréquence à laquelle il doit être changé.

Les éléments suivants devraient être pris en considération lors de l'élaboration et de l'utilisation de politiques et de normes en matière de cybersécurité :

1) Commencer avec une politique générale et simple pour établir clairement les principes et les règles.

2) Relever les normes existantes et les adapter à certaines questions de cybersécurité ou technologies de l'organisation ou rédiger ses propres normes.

3) Expliquer les normes et les politiques aux membres du personnel afin qu'ils comprennent ce qui justifie les règles, à qui elles s'appliquent et quelles sont les conséquences si elles ne sont pas respectées.

4) Une fois que la politique de cybersécurité initiale et les normes connexes sont en vigueur, les revoir et ajouter au besoin de l'information plus détaillée ou précise.

4) Élaborer un plan de cybersécurité

La mise au point d'un plan de cybersécurité devrait être une priorité pour toute organisation. Un tel plan permet de cerner les mécanismes de contrôle de base qui constituent la pierre d'assise de la cybersécurité de toute organisation. En outre, il décrit en détail les actifs qui nécessitent une protection accrue, les menaces et les risques particuliers auxquels les activités sont exposées, ainsi que les mesures de protection à mettre en place. Il convient de garder à l'esprit qu'il est toujours possible de revoir le plan et de l'élargir au fil du temps. En outre, le Centre canadien de réponse aux incidents cybernétiques (CCRIC) offre des ressources pour aider les organisations dans leurs activités de planification en matière de cybersécurité. Une fois que l'organisation a établi son plan, celui-ci devrait être approuvé par un membre de la haute direction, passé en revue à intervalles réguliers et assorti d'un budget. Comme les plans de cybersécurité peuvent contenir de l'information de nature délicate, il convient de les libeller, de les manipuler, de les entreposer, de les diffuser et de les éliminer d'une façon qui tient compte des impératifs de sécurité.

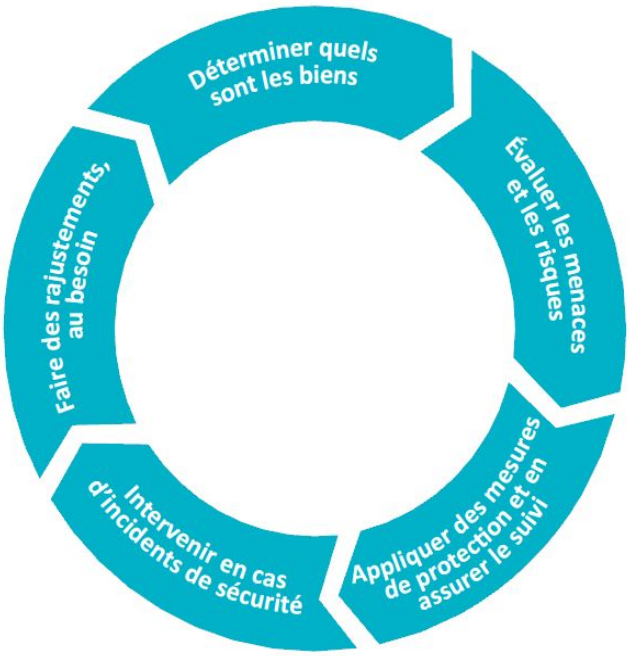
5) Établir un budget pour la cybersécurité

L'efficacité des contrôles de sécurité est optimale quand une organisation en tient compte dès les premières étapes d'un projet et les ajuste tout au long du cycle de vie de ce projet. Les organisations devraient donc faire en sorte que la sécurité fasse partie intégrante de tous leurs exercices d'établissement de budget. Les activités de cybersécurité doivent être prises en compte au moment d'établir des plans d'activités et des budgets annuels. Certaines politiques ou certains documents peuvent être créés à l'interne, à coût minime. Par contre, d'autres mesures de sécurité devront être achetées, et elles peuvent comporter des frais d'abonnement annuels. À titre d'exemple, contrairement aux logiciels dont les coûts sont habituellement ponctuels, les renouvellements de licences d'utilisation de logiciels antimaliciel devront vraisemblablement être achetés annuellement. Les investissements dans les activités d'atténuation et de préparation peuvent être hautement profitables. Les budgets alloués à la cybersécurité devraient également tenir compte de la valeur des actifs à protéger. Investir dans la cybersécurité, c'est comme souscrire une police d'assurance, c'est-à-dire que l'organisation met des mesures en place en espérant qu'elle n'aura pas à s'en servir, tout comme le propriétaire d'une maison souscrit une assurance contre les inondations en souhaitant que sa résidence ne soit jamais inondée. On recommande aux organisations de prévoir des ressources pour les cinq aspects suivants :

1) les coûts fixes des outils de sécurité;
2) les frais continus ou annuels de mise à jour (p. ex. logiciels);
3) les coûts rattachés au soutien, aux services-conseils et à la formation;
4) les coûts de vérification;
5) les fonds de prévoyance.

Les fonds de prévoyance sont importants pour composer avec les urgences imprévues (comme une infection par un programme malveillant). Certaines assurances peuvent couvrir les pertes dues à un incident de cybersécurité. Il importe donc d'en discuter à l'avance avec l'assureur.

Figure 1 – Principes fondamentaux de la



Bon nombre d'organisations des secteurs public et privé sont dotées de structures de gestion des crises pour faciliter une intervention interne coordonnée en cas d'urgence, peu importe la cause ou la nature de ces urgences. De tels mécanismes font aussi en sorte que les cadres supérieurs sont mis au courant des incidents, d'une façon appropriée et coordonnée. Il est important de s'assurer que ces mécanismes sont aussi adaptés à la gestion des cyberincidents.

Tous les actifs nécessitent un niveau minimal de protection, mais il est possible que certains requièrent des mesures supplémentaires. Même lorsque de telles mesures sont en place, les organisations doivent être prêtes à intervenir au moment où des incidents de sécurité se produisent, ainsi qu'à modifier les mesures de protection en réaction aux changements constatés relativement aux actifs, aux menaces et aux risques.

Les organisations peuvent prendre les mesures suivantes pour cerner les actifs à protéger et en établir l'ordre de priorité, évaluer les menaces et déterminer quand il convient d'appliquer les mesures de protection appropriées (voir la figure 1).

1. **Déterminer les actifs –** Quels sont les actifs qui nécessitent des mesures de sécurité renforcées ou spécialisées? *Il convient de tenir à jour une liste de tous les actifs essentiels aux activités d'exploitation.*

2. **Évaluer les menaces et les risques –** Quelles *menaces* et quels *risques* pourraient toucher ces actifs ou ces activités organisationnelles? Quelles mesures de protection devraient être mises en place pour atténuer les risques et protéger les actifs?

3. **Appliquer et surveiller les mesures de sécurité –** Surveiller les mesures de sécurité et les actifs afin de prévenir ou de gérer toute atteinte à la sécurité.

4. **Intervenir en cas d'incident de sécurité –** Traiter les problèmes de cybersécurité à mesure qu'ils surviennent.

5. **Faire les ajustements nécessaires –** Mettre à jour et adapter les mesures de sécurité selon les changements qui touchent les actifs, les risques et les menaces.

Quatre principales mesures de protection

La mise en œuvre de contrôles de cybersécurité peut constituer un défi de taille pour les propriétaires et les exploitants, surtout à la lumière des longues listes de contrôles nécessaires et de la complexité de la terminologie propre au domaine. Il existe une vaste gamme de listes de contrôles de cybersécurité reconnus par l'industrie et les gouvernements qui peuvent fournir une protection de base dans l'ensemble des organisations. Les stratégies d'atténuation des cyberintrusions ciblées (notamment les quatre premières stratégies d'une liste qui en compte trente-cinq) de l'Australian Signals Directorate (ASD) et d'autres listes semblables proposent des conseils judicieux pour les organisations de tous les types.

Il a été déterminé que les quatre mesures de protection ci-dessous permettent d'éviter la grande majorité des attaques.

1) **Établir la liste des applications autorisées (liste blanche)** – Indiquer les programmes précis qui peuvent être exécutés sur un système donné et mettre en application une politique de sorte que seules les composantes mentionnées puissent être utilisées.

2) **Utiliser des systèmes d'exploitation et des applications modernes** – Installer les versions les plus récentes des systèmes et des programmes et mettre en place une approche fondée sur le cycle de vie en vue de la migration vers de nouvelles versions.

3) **Installer les correctifs des systèmes d'exploitation et des applications** – Installer le correctif dans les deux jours de l'annonce publique d'une vulnérabilité à risque élevé.

4) **Limiter les privilèges administratifs** – Restreindre le nombre d'utilisateurs possédant des droits d'accès administratifs locaux ou de domaine à un système ou à un appareil.

Ressources du gouvernement du Canada

Le gouvernement fédéral offre de nombreux produits et services à l'appui du renforcement des infrastructures essentielles au Canada, y compris des cybersystèmes qui sous-tendent ces infrastructures. Des ressources supplémentaires sont présentées à l'annexe 1. Le tableau qui suit énumère les 10 secteurs des infrastructures essentielles et les ministères et organismes fédéraux qui y sont associés, que l'on appelle les « ministères principaux ». En cas d'incident, le ministère principal désigné est responsable de coordonner l'intervention du gouvernement fédéral.

Secteur	Ministères et organismes fédéraux responsables
Énergie et services publics	Ressources naturelles Canada
Technologies de l'information et de la communication	Innovation, Sciences et Développement économique Canada
Finances	Ministère des Finances Canada
Santé	Agence de la santé publique du Canada
Alimentation	Agriculture et Agroalimentaire Canada
Eau	Environnement et Changement climatique Canada
Transports	Transports Canada
Sécurité	Sécurité publique Canada
Gouvernement	Sécurité publique Canada
Secteur manufacturier	Innovation, Sciences et Développement économique Canada /Défense nationale et Forces armées canadiennes

Ressources du gouvernement du Canada (suite)

✓ *Loi sur la gestion des urgences*

Au Canada, la gestion des urgences est fondée sur une approche tous risques conçue pour comprendre toutes les urgences, indépendamment de leur cause sous-jacente. Cette approche bien établie serait adoptée si un cyberincident entraînait des conséquences matérielles (par exemple, une cyberattaque qui empêcherait le fonctionnement de l'usine de traitement des eaux d'une grande ville). L'approche contribuerait à faire en sorte que les conséquences de l'incident soient gérées efficacement. Le concept de cybersécurité introduit des complications au sein même des structures de gestion des urgences en place, car le cyberespace est indépendant des frontières physiques et géographiques.

✓ Cadre de gestion des incidents cybernétiques (CGIC)

Afin de tenir compte de certains des aspects de la cybersécurité qui brouillent les frontières entre les différents domaines de responsabilité, Sécurité publique Canada a élaboré un *Cadre de gestion des incidents cybernétiques (CGIC)*. Le CGIC est un document d'orientation qui vise les gouvernements provinciaux et territoriaux, les propriétaires et les exploitants d'infrastructures essentielles, ainsi que d'autres partenaires des secteurs public et privé. Le CGIC est conçu pour compléter et intégrer les plans et les cadres fédéraux, provinciaux et territoriaux de gestion des urgences déjà en place, ainsi que les plans d'urgence des propriétaires et des exploitants d'infrastructures essentielles.

✓ Stratégie nationale et plan d'action sur les infrastructures essentielles

La Stratégie nationale sur les infrastructures essentielles a pour objectif d'accroître la sûreté, la sécurité et la résilience du Canada. À cette fin, elle assure une plus grande cohérence d'action et une plus grande complémentarité des initiatives des gouvernements fédéral, provinciaux et territoriaux et des dix secteurs des infrastructures essentielles.

Les concepts et principes fondamentaux énoncés dans la Stratégie nationale découlent du Cadre de sécurité civile pour le Canada, lequel établit une approche de collaboration à l'égard des initiatives fédérales, provinciales et territoriales de gestion des urgences. Conformément à ce Cadre et en considération des interconnexions qui existent entre les infrastructures essentielles, la Stratégie nationale favorise l'établissement de partenariats entre les gouvernements fédéral, provinciaux et territoriaux et les secteurs des infrastructures essentielles, soutient une approche de gestion tous risques et met en place des mesures pour améliorer l'échange et la protection de l'information.

Pour suivre l'évolution rapide des risques, il faut, comme élément essentiel de l'approche nationale du Canada, un Plan d'action qui se fonde sur les thèmes principaux de la Stratégie, soit :

- des partenariats durables avec les gouvernements fédéral, provinciaux et territoriaux, ainsi qu'avec les secteurs des infrastructures essentielles;
- des mécanismes améliorés de protection et d'échange de l'information;
- un engagement relativement à la gestion tous risques.

Le Plan d'action est mis à jour régulièrement pour permettre aux partenaires de prévoir les nouveaux risques et de s'employer à les contrer.

✓ Examen canadien de la cyberrésilience (ECCR)

Si un propriétaire ou un exploitant a besoin d'aide pour évaluer son organisation, Sécurité publique Canada propose l'Examen canadien de la cyberrésilience (ECCR). Il s'agit d'un atelier d'un jour présenté sur place et conçu pour évaluer l'approche globale d'une organisation à l'égard des pratiques et des procédures en matière de cybersécurité. Pour en savoir plus sur l'ECCR, il suffit d'écrire à l'adresse électronique suivante : rrap_perr@ps-sp.gc.ca.

✓ Centre canadien de réponse aux incidents cybernétiques

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) offre toute une gamme de documents d'orientation, de bulletins de sécurité et de rapports techniques portant sur des questions de cybersécurité, ainsi que des renseignements opportuns et exploitables en réaction à des cyberincidents.

Portail communautaire : En 2012, le CCRIC a lancé son portail communautaire sécurisé. Cet outil destiné aux partenaires des secteurs public et privé vise à améliorer le signalement des

incidents, à fournir des liens vers des outils utiles et à stimuler les échanges entre les secteurs. Le portail fournit aux intervenants du secteur des infrastructures essentielles une plateforme collaborative qui favorise l'échange d'information. Il propose également des sous-sites classés par secteur ou par communauté d'intérêts.

Le portail communautaire contient la version archivée de tous les produits opérationnels et techniques du CCRIC, y compris ceux qui ne sont pas publiés sur son site public. Les partenaires sont donc invités à s'inscrire à ce portail communautaire.

Rapports opérationnels : Cet ensemble de produits professionnels vise à sensibiliser les principaux dirigeants d'infrastructures essentielles au sujet des incidents et des tendances d'intérêt que le CCRIC observe, et à souligner les études de cas et les pratiques exemplaires en matière de sécurité. Ces produits sont publiés sur une base mensuelle, trimestrielle et annuelle. De plus, le CCRIC publie ponctuellement un rapport intitulé *Pleins feux sur…*, qui met en évidence les enjeux courants ou nouveaux en matière de cybersécurité.

Ensemble de produits techniques : Le CCRIC met à la disposition de ses partenaires des secteurs public et privé un ensemble complet de produits techniques qui présentent des renseignements opportuns sur la détection et l'atténuation des menaces au sujet des enjeux immédiats en matière de sécurité. De plus, le CCRIC publie régulièrement divers documents traitant de sécurité sur son site Web, comme des **notes d'information**, des **rapports techniques**, des **alertes** et des **avis**.

Le CCRIC publie régulièrement des **bulletins cybernétiques** pour informer ses partenaires des secteurs public et privé des menaces cybernétiques potentielles, imminentes ou réelles. Il produit aussi un **rapport technique hebdomadaire** destiné à ses partenaires de confiance. Ce rapport comprend un sommaire des incidents et des indicateurs de compromission qui leur sont associés, ainsi que des nouvelles d'intérêt. Ces deux produits sont affichés dans le portail communautaire sécurisé du CCRIC.

Coordination d'interventions : Coordination des interventions en cas d'incident cybernétique en cours 24 heures par jour, sept jours par semaine.

Conseils en matière d'atténuation : Prestation de conseils pour améliorer la posture de cybersécurité des clients.

Analyses techniques : Analyses et rapports techniques sur des échantillons de maliciels, analyses des médias numériques et analyses judiciaires.

Notification aux victimes : Le Système national de notification de cybermenace du CCRIC utilise le résultat des analyses effectuées au laboratoire de maliciels du

POUR JOINDRE LE CCRIC :

Pour obtenir de l'information sur le portail communautaire du CCRIC et les produits disponibles, communiquez avec le CCRIC au cyber-incident@ps-sp.gc.ca.

L'agent de cybersécurité de service du CCRIC est le point de contact des responsables des infrastructures essentielles pour signaler des incidents au Centre et obtenir de l'aide pour les gérer.

CCRIC pour fournir périodiquement des avis personnalisés aux parties intéressées.

✓ Passerelle d'information canadienne sur les infrastructures essentielles

La Passerelle d'information sur les infrastructures essentielles du Canada est un forum destiné aux propriétaires et exploitants d'IE qui vise à favoriser l'échange rapide d'information et la collaboration entre les secteurs des infrastructures essentielles. Les utilisateurs ont un accès rapide et efficace à des documents, à des hyperliens, à des fils RSS, à des documents géospatiaux et à des coordonnées relatifs à tous les secteurs des infrastructures essentielles. Ils ont également la possibilité de recommander ou de proposer du contenu à communiquer au reste des membres de la Passerelle (en écrivant à cigateway@ps-sp.gc.ca).

✓ Ateliers et formation sur la sécurité des systèmes de contrôle industriel (SCI)

Les ateliers sur la sécurité des systèmes de contrôle industriel (SCI) de Sécurité publique Canada réunissent des experts reconnus et des représentants du gouvernement fédéral qui présentent des exposés sur les menaces les plus récentes et sur les mesures à prendre pour renforcer la sécurité des SCI.

La formation sur la sécurité des systèmes de contrôle industriel (SCI) de Sécurité publique Canada est axée sur l'acquisition de compétences de base liées à la gestion des incidents dans l'environnement des SCI. Cette formation prend la forme d'un apprentissage pratique qui fait appel à l'utilisation d'outils et de cibles tangibles.

Surveillance et mesure des progrès

Mesurer l'efficacité des mécanismes de cybersécurité demeure un défi de taille. Le fait qu'aucun événement négatif ne se produise ne signifie pas nécessairement que le programme de cybersécurité d'une organisation fonctionne adéquatement. Pour mesurer l'efficacité d'un programme de cybersécurité, on doit se pencher non seulement sur les activités réactives négatives, mais également sur les activités proactives positives.

Sécurité publique Canada recommande l'adoption d'une approche multidimensionnelle afin de surveiller et de mesurer les progrès réalisés relativement à l'atteinte de l'objectif clairement défini qui consiste à accroître la résilience des infrastructures essentielles cybernétiques. En recueillant des indicateurs de niveau organisationnel et national, les organisations devraient être en mesure de suivre les progrès réalisés quant à la hausse de la résilience tant dans les détails que du point de vue global. Les organisations peuvent adapter les indicateurs organisationnels énumérés ci-dessous afin de mesurer leur propre rendement.

Indicateurs de mesure	
Mesure réactive	**Source**
Taux relatifs d'infections par des maliciels au Canada	Mesure nationale – *Security Intelligence Report: Worldwide Threat Assessment* de Microsoft
Rang occupé par le Canada au sein des principaux pays ayant des adresses URL d'hameçonnage	Mesure nationale – *Labs Threats Report* de McAfee
Pourcentage de la population globale de robots au Canada et position du Canada en matière de classement annuel de robots à l'échelle internationale	Mesure nationale – *Internet Security Threat Report* de Symantec Corporation
Taux de logiciels malveillants recensés et d'infections au Canada	Mesure nationale – *Security Intelligence Report: Worldwide Threat Assessment* de Microsoft
Taux de rétablissement[2]	Mesure organisationnelle – Données recueillies à des fins internes par les organisations.
Mesures proactives	**Sources**
Taux de mise en œuvre des principales mesures d'atténuation recommandées (CCRIC)	Mesure organisationnelle – Données recueillies à des fins internes par les organisations.
Notes globales de l'Examen canadien de la cyberrésilience de Sécurité publique Canada	Mesure nationale et organisationnelle
Taux de trafic sur les réseaux[3]	Mesure organisationnelle – Données recueillies à des fins internes par les organisations.
Taux de récence des logiciels[4]	Mesure organisationnelle – Données recueillies à des

[2] Délai nécessaire au rétablissement, après une attaque, des services essentiels, puis des services secondaires, et enfin de la totalité des services.
[3] Trafic légitime sur le réseau, par rapport au trafic généré par des réseaux de robots (pourriel).
[4] Mesure de la rapidité avec laquelle une organisation met en œuvre les mises à jour et les nouvelles versions d'un logiciel.

fins internes par les organisations.

Conclusion

Les conseils fournis dans le présent document ne constituent pas une liste exhaustive des moyens que peut prendre une organisation pour accroître sa cybersécurité. Ils visent plutôt à compléter, à améliorer et, dans bien des cas, à amorcer l'approche des organisations à l'égard de la cybersécurité, un domaine dynamique, complexe et en constante évolution.

Un investissement précoce dans des mesures de prévention et de protection en matière de cybersécurité peut aider à atténuer les services coûteux associés à l'intervention et au rétablissement.

Il est crucial d'adopter une approche collaborative nationale à l'égard des défis associés à la cybersécurité, puisque les systèmes et les réseaux sont de plus en plus intégrés et interreliés, et qu'une cyberattaque à l'endroit d'un intervenant est susceptible d'avoir des répercussions sur tous les intervenants. Collectivement, le gouvernement, les partenaires d'affaires et les citoyens s'attendent à ce que les organisations et les institutions avec lesquelles ils font affaire soient suffisamment solides pour résister aux cyberincidents et éviter les réactions en chaîne dans un même secteur et d'un secteur à l'autre. *La cybersécurité est la responsabilité de tous.*

Plus nous agissons maintenant pour améliorer collectivement la cybersécurité des infrastructures essentielles, plus nous serons prêts à relever les défis d'aujourd'hui et de demain.

Annexe 1 : Ressources supplémentaires

Ressources du gouvernement du Canada

Loi canadienne anti-pourriel

- http://www.fightspam.gc.ca/eic/site/030.nsf/fra/h_00241.html

Centre antifraude du Canada pour la prévention et le signalement de la fraude (y compris la cybercriminalité)

- Numéro sans frais : **1 888-495-8501** ou courriel : info@antifraudcentre.ca
- Site Web : http://www.antifraudcentre-centreantifraude.ca/index-fra.htm

Centre canadien de réponse aux incidents cybernétiques (CCRIC)

- Principes de prévention contre les menaces sophistiquées et persistantes : http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-002-fr.aspx
- Formation, orientation et conseils techniques en matière de cybersécurité : http://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/tchncl-dvc-gdnc-fr.aspx
- Principes de prévention contre les attaques par déni de service : http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-001-fr.aspx
- Guide Pensez cybersécurité pour les petites et moyennes entreprises : http://www.pensezcybersecurite.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-fr.aspx
- Guide de rétablissement à la suite d'une infection par un logiciel malveillant : http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-001-fr.aspx
- Systèmes SCADA et SCI : http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-002-fr.aspx

Site de signalement des arnaques du Conseil de la radiodiffusion et des télécommunications canadiennes :

- http://www.crtc.gc.ca/fra/info_sht/g9.htm

Centre de la sécurité des télécommunications (CST)

- Guides GSTI d'architecture : https://www.cse-cst.gc.ca/fr/publication/list
- Évaluation des menaces et des risques (EMR) : https://www.cse-cst.gc.ca/fr/publication/tra-1

Stratégie *Canada numérique 150*

- https://www.ic.gc.ca/eic/site/028.nsf/fra/h_00569.html

Pensez Cybersécurité – Site Web où l'on trouve des nouvelles et des directives sur la cybersécurité destinées aux particuliers et aux entreprises.

- www.pensezcybersecurite.gc.ca

Commissariat à la protection de la vie privée du Canada

- Un programme de gestion de la protection de la vie privée – La clé de la responsabilité :

https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_f.asp

- Protéger les renseignements personnels – Un outil d'auto-évaluation à l'intention des organisations : https://www.priv.gc.ca/resource/tool-outil/security-securite/francais/AssessRisks.asp?x=1

Ressources des partenaires internationaux

Australie

- **Stratégies d'atténuation des cyberintrusions ciblées de l'Australian Signals Directorate** (en anglais seulement) : http://www.asd.gov.au/infosec/top-mitigations/mitigations-2014-table.htm
- *Manuel de sécurité de l'information du gouvernement australien* (en anglais seulement)

Royaume-Uni

- *Guide en dix étapes à l'intention des cadres* (en anglais seulement)
- Lignes directrices essentielles sur la cybersécurité (en anglais seulement)

États-Unis

- Pratiques recommandées par l'équipe d'intervention en cas d'urgence cybernétique touchant les systèmes de contrôle industriels (Industrial Control Systems Cyber Emergency Response Team, ICS-CERT) du département de la Sécurité intérieure (en anglais seulement) : https://ics-cert.us-cert.gov/Introduction-Recommended-Practices
- Base nationale de données sur les vulnérabilités, version 2.2 (en anglais seulement) : http://nvd.nist.gov/
- Cadre d'amélioration de la cybersécurité des infrastructures essentielles du National Institute for Standards and Technology (NIST) (en anglais seulement) : http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Nouvelle-Zélande

- Considérations relatives à la cybersécurité et à la gestion du risque à l'intention des cadres (en anglais seulement) : http://www.ncsc.govt.nz/assets/cyber-security-risk-management-Executive.pdf
- Normes volontaires de cybersécurité des systèmes de contrôle industriels du National Cyber Security Centre (en anglais seulement) : http://www.ncsc.govt.nz/assets/NCSC20voluntary20cyber20security20standards20for20ICD20v.1.0.pdf

Autres ressources (associations, normes, rapports, etc.)

Un large éventail d'organisations diffuse de l'information utile au sujet des cybermenaces. En voici quelques exemples.

Échange canadien de menaces cybernétiques (ECMC)

- Organisme indépendant à but non lucratif qui a pour mission d'aider les entreprises et les consommateurs canadiens à se protéger contre les cyberattaques : https://cctx.ca/?lang=fr

Associations membres d'organismes de cybersécurité œuvrant au Canada

- American Society for Industrial Security (ASIS) : www.asis-canada.org/
- High Technology Crime Investigation Association (HTCIA) : www.htcia.org/
- Association des professionnels de la vérification et du contrôle des systèmes d'information : www.isaca.org/Membership/Local-Chapter-Information/Browse-by-List/Pages/North-America-Chapters.aspx
- Information Systems Security Certification Consortium, Inc. (ISC2) : https://www.isc2.org/chapters/Default.aspx
- Information Systems Security Association (ISSA) : https://www.issa.org/?page=ChaptersContact

Norme sur la gestion de la sécurité de l'information de l'Organisation internationale de normalisation (ISO)

- http://www.iso27001security.com/html/27032.html

***Security Intelligence Report* de Microsoft**

- https://www.microsoft.com/security/sir/default.aspx

Publications de McAfee

- http://www.mcafee.com/ca/apps/view-all/publications.aspx

Kaspersky Internet Security Center

- http://www.kaspersky.com/internet-security-center

***Annual Threat Report* de FireEye**

- https://www.fireeye.com/current-threats/annual-threat-report.html

Publications sur les interventions de sécurité de Symantec

- https://www.symantec.com/security_response/publications/

Contrôles de sécurité critique du SANS Institute

- https://www.sans.org/critical-security-controls/

Les normes énumérées dans le tableau ci-dessous peuvent faciliter la gestion et la planification efficaces de la cybersécurité, ainsi que la prise de décisions éclairées en la matière.

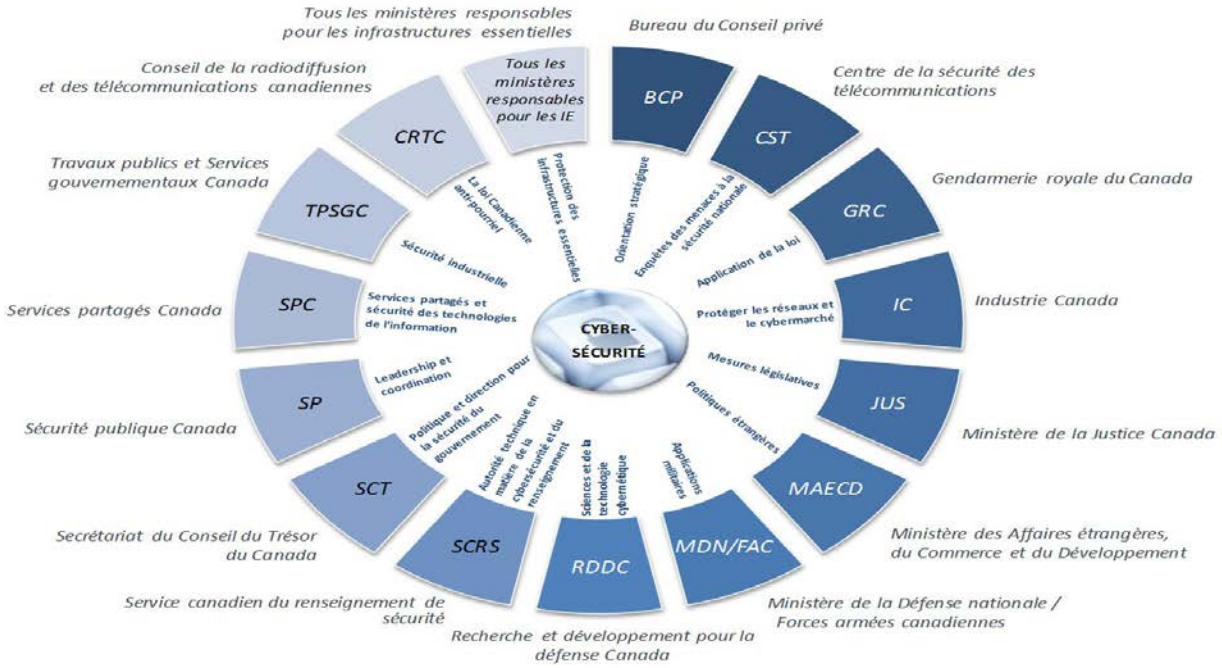
Normes et directives *(hyperliens)*
Cadre d'amélioration de la cybersécurité des infrastructures essentielles (National Institute for Standards and Technology, en anglais seulement)
Partenariat pour la cyberrésilience (Forum économique mondial, en anglais seulement)
Guide de pratiques exemplaires en matière de cybersécurité à l'intention des courtiers membres de l'OCRVM (Organisme canadien de réglementation du commerce des valeurs mobilières)
Guide de planification de la gestion des cyberincidents à l'intention des courtiers membres de l'OCRVM (Organisme canadien de réglementation du commerce des valeurs mobilières)
Stratégies d'atténuation des cyberintrusions ciblées (Australian Signals Directorate, en anglais seulement)
Norme sur la gestion de la sécurité de l'information (Organisation internationale de normalisation, en anglais seulement)
Risque et responsabilité dans un monde hyperconnecté : Les voies de la cyberrésilience mondiale (Forum économique mondial, en anglais seulement)

Annexe 2 : Rôles et responsabilités des ministères et organismes du gouvernement du Canada en matière de cybersécurité

Bien que la grande majorité des infrastructures essentielles cybernétiques du pays appartiennent à des intérêts privés, les risques pour la sécurité nationale et économique associés à ces actifs exigent des partenariats étroits entre le gouvernement et le secteur privé, ainsi que des mesures concertées pour protéger ces actifs. Publiée en 2010, la *Stratégie de cybersécurité du Canada* constitue le plan du gouvernement du Canada pour aider à protéger les cybersystèmes essentiels contre les attaques et les Canadiens contre la cybercriminalité, ainsi qu'à protéger les réseaux du gouvernement.

Il convient que les secteurs des infrastructures essentielles comprennent les rôles et les responsabilités des ministères et organismes fédéraux participant à la Stratégie de cybersécurité (voir la figure 1), et établissent des liens avec les partenaires compétents pour gérer efficacement les risques cybernétiques en constante évolution.

Figure 1 – Ministères et organismes du gouvernement du Canada responsables de la sécurité



Sécurité publique Canada joue un rôle important et unique dans le domaine de la cybersécurité. Le Ministère est responsable de la coordination et de la mise en œuvre de la

Stratégie de cybersécurité. Il doit notamment collaborer avec les secteurs des infrastructures essentielles pour les sensibiliser aux cybermenaces, cibler les vulnérabilités et élaborer des stratégies d'atténuation.

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) fonctionne au sein de

Sécurité publique Canada. À titre d'équipe d'intervention en cas d'incident lié à la sécurité informatique du Canada, le CCRIC est responsable de la surveillance des cybermenaces et de la formulation de conseils sur les mesures d'atténuation pertinentes, ainsi que de la coordination de l'intervention nationale en cas d'incident de cybersécurité. Son mandat consiste à protéger les infrastructures essentielles nationales contre les incidents de cybersécurité. Cela étant dit, les propriétaires et exploitants ont accès aux produits et services du Centre.

Sécurité publique Canada a aussi récemment lancé le Programme de coopération en matière de cybersécurité (PCCS) en vue d'accroître la sécurité des cybersystèmes essentiels du Canada. Le programme accorde des subventions et des contributions aux propriétaires et aux exploitants de cybersystèmes essentiels, ainsi qu'à d'autres intervenants, en appui à des projets qui renforcent la résilience des cybersystèmes essentiels du Canada. Pour en savoir plus sur le PCCS ou pour présenter une demande de financement, veuillez consulter le site Web du Programme.

Voici une liste d'autres ministères et organismes, ainsi qu'un résumé de leurs rôles et responsabilités en matière de cybersécurité.

Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)

- Veiller à ce que les Canadiens aient accès à un système de communication de calibre mondial, tout en protégeant les Canadiens des communications non sollicitées et en contribuant à accroître la sécurité du cyberenvironnement pour les consommateurs et les entreprises.

Service canadien du renseignement de sécurité (SCRS)

- Effectuer des enquêtes portant sur la sécurité nationale. Signaler au gouvernement du Canada les activités constituant une menace contre la sécurité du pays aux termes de la *Loi sur le Service canadien du renseignement de sécurité*, et le conseiller à cet égard.
- Fournir au gouvernement du Canada des analyses afin de l'aider à comprendre les cybermenaces, ainsi que les intentions et les capacités des cyberacteurs menant leurs activités au Canada et à l'étranger et constituant une menace pour la sécurité du pays.
- Grâce à ces renseignements, le gouvernement du Canada peut améliorer sa connaissance générale de la situation, mieux cerner les cybervulnérabilités, empêcher les actes de cyberespionnage et les autres cybermenaces et prendre des mesures pour protéger ses infrastructures essentielles.

Centre de la sécurité des télécommunications (CST)

- Surveiller les réseaux du gouvernement du Canada et en assurer la défense en détectant des cybermenaces contre le gouvernement, en protégeant les réseaux contre ces menaces, ainsi qu'en offrant aux institutions fédérales et aux propriétaires et exploitants d'infrastructures essentielles des services pour les aider à atténuer les répercussions de ces menaces ou pour se rétablir après coup.
- Organisme responsable de la collecte de renseignements cybernétiques étrangers et point de contact avec la collectivité cryptologique du Groupe des cinq.
- Effectuer des recherches et mettre sur pied des projets dans le domaine de la cybersécurité.
- Mettre sur pied des programmes d'assurance pour les technologies commerciales.

- Travailler en partenariat avec Services partagés Canada et Industrie Canada afin d'assurer l'intégrité de la chaîne d'approvisionnement électronique pour l'équipement et les services du gouvernement du Canada.
- Échanger de l'information sur les cybermenaces et les vulnérabilités avec le CCRIC, aux fins de diffusion aux propriétaires et exploitants d'infrastructures essentielles.

Recherche et développement pour la défense Canada (RDDC)

- Diriger l'élaboration du volet militaire de la cybersécurité en matière de sciences et de technologies (S et T) en appui aux Forces canadiennes.
- Diriger le volet national de S et T de Sécurité publique Canada pour les mesures n'ayant pas été attribuées spécifiquement à un autre ministère ou organisme par le Centre des sciences pour la sécurité, en collaboration avec des partenaires nationaux en matière de sécurité dans le cadre du Programme technique de sécurité publique. S'acquitter de ces tâches en partenariat avec le gouvernement, l'industrie, le milieu universitaire et les alliés.

Affaires mondiales Canada

- Appuyer des organismes étrangers dans le cadre de leurs mesures d'atténuation des cybermenaces et aider les gouvernements étrangers à améliorer leur profil et leurs capacités dans le domaine de la cybersécurité.
- Contribuer à l'engagement diplomatique pour aider à élaborer l'espace réglementaire multilatéral prenant forme en matière de cybersécurité. Permettre au gouvernement de donner au Canada une meilleure position sur la scène internationale afin qu'il défende sa politique étrangère et ses intérêts liés à la cybersécurité et en fasse la promotion.

Ministère de la Justice Canada

- Appuyer les initiatives des ministères et organismes clients en leur fournissant des conseils juridiques sur des questions relatives aux lois et aux politiques sur la cybersécurité.
- Jouer un rôle de premier plan au sujet de certaines questions, particulièrement celles qui sont liées aux politiques en matière de droit pénal et à l'échange d'information. Les services juridiques du Centre de la sécurité des télécommunications Canada ont été désignés comme le centre d'excellence sur les lois relatives à la cybersécurité.

Défense nationale et Forces canadiennes

- Communiquer des renseignements de défense afin d'éclairer le processus d'évaluation des menaces et des risques du gouvernement du Canada.
- Aider le gouvernement du Canada à bien connaître la situation pendant les étapes de surveillance, d'analyse, d'atténuation et d'intervention du Plan de gestion des incidents de TI du gouvernement du Canada en lui fournissant de l'information sur la cybersécurité venant de sources militaires alliées, en surveillant et en signalant les menaces contre la technologie de l'information, ainsi qu'en présentant des analyses et des options liées à des interventions militaires possibles.

Innovation, Sciences et Développement économique Canada (ISDE)

- Gérer le spectre du Canada et héberger un système de télécommunications robuste et fiable. Élaborer des politiques pour veiller à ce que les marchés en ligne soient sécuritaires.

Contribuer à assurer la continuité des télécommunications en cas d'urgence.

Bureau du Conseil privé (BCP)

- Héberger les bureaux du conseiller en matière de sécurité nationale auprès du premier ministre et apporter du soutien à ce dernier.
- Coordonner les activités des membres du milieu de la sécurité et du renseignement et encourager l'adoption d'une démarche concertée dans le domaine de la sécurité nationale.

Services publics et Approvisionnement Canada

- Agir à titre de fournisseur de services partagés et communs. Dans le cadre du Programme de sécurité industrielle, assurer la sécurité des contrats attribués par le Ministère ou à la demande d'autres ministères.
- Assurer la protection des renseignements classifiés de gouvernements étrangers et de l'OTAN au sein du secteur privé au Canada.
- Le Secteur de la sécurité industrielle maintient des relations avec des alliés et négocie des protocoles d'entente sur les questions relatives à la sécurité industrielle, y compris la cybersécurité, dans le cadre du processus contractuel.

Gendarmerie royale du Canada (GRC)

- Diriger les enquêtes criminelles en cas de cyberincident présumé mettant en cause les infrastructures d'information essentielles (p. ex. utilisation non autorisée d'un ordinateur ou méfait mettant en cause des données). Mener les enquêtes criminelles sur les incidents présumés touchant la cybersécurité nationale.
- Conseiller et orienter les partenaires nationaux et internationaux au sujet des cybermenaces criminelles.

Services partagés Canada (SPC)

- Simplifier et consolider les technologies de l'information et des communications en ce qui a trait au courriel, aux centres de données et aux réseaux, afin de veiller à ce que les services communs des technologies de l'information (TI) offerts aux ministères demeurent confidentiels, intègres et accessibles.
- Offrir des services de sécurité des TI et d'autres solutions afin de permettre aux ministères d'échanger de l'information avec les citoyens, les entreprises et les employés.
- Recueillir, analyser et colliger l'information sur les menaces et les vulnérabilités opérationnelles ayant trait aux services communs et aux infrastructures essentielles gouvernementales de TI dont il est responsable, et faciliter la divulgation de ces renseignements et communiquer cette information au CCRIC et, s'il y a lieu, aux ministères et aux partenaires de la cybersécurité.

Annexe 3 : Glossaire et sigles

Glossaire

Actif : Tout ce qui appartient à l'entreprise et qui a de la valeur (y compris les renseignements sous toutes leurs formes et les cybersystèmes).
Attaque : Tentative d'accéder de façon non autorisée à des renseignements professionnels ou personnels, aux cybersystèmes ou aux réseaux à des fins (habituellement) criminelles. Une attaque réussie peut entraîner une *faille* de la sécurité ou être classée de façon générique, comme un « incident ».
Authentification : Mesure de sécurité mise en place (normalement au moyen de logiciels de contrôle) pour confirmer l'identité d'une personne avant de lui accorder l'accès aux services de l'entreprise, à ses ordinateurs ou à ses renseignements.
Sauvegarde : Processus consistant à copier des fichiers dans un outil de stockage secondaire afin que ces copies soient disponibles en cas de besoin pour une restauration future (p. ex. après une panne d'ordinateur).
Faille : Une faille de sécurité est une lacune qui émerge en raison d'une négligence ou d'une attaque délibérée. Elle peut aller à l'encontre d'une politique ou d'une loi et est souvent exploitée pour réaliser des actions nuisibles ou criminelles.
Cyber : Qui se rapporte aux ordinateurs, aux logiciels, aux systèmes de communication et aux services utilisés pour accéder à Internet et y interagir.
Chiffrement : Conversion d'information en un code que seules les personnes autorisées peuvent lire, c.-à-d., celles qui ont reçu la « clé » (habituellement unique) et le logiciel spécial qui leur permettront de renverser le processus (déchiffrement) et d'utiliser l'information.
Pare-feu : Genre de barrière de sécurité placée entre divers environnements réseau. Il peut s'agir d'un dispositif spécialisé ou d'un ensemble de plusieurs composantes et techniques. Seule une transmission autorisée, telle qu'elle est définie par la politique de sécurité locale, peut avoir droit de passage.
Vol d'identité : Copie des renseignements personnels d'une autre personne (comme son nom et son numéro d'assurance sociale) pour ensuite se faire passer pour elle et commettre une fraude ou une autre activité criminelle.
Maliciel : Logiciel conçu pour infiltrer ou endommager un système informatique sans le consentement éclairé de l'utilisateur. C'est un terme général utilisé par les professionnels de l'informatique pour désigner toutes les formes possibles de logiciels ou de programmes hostiles, intrusifs ou nuisibles. L'intention du créateur, et non les caractéristiques particulières du logiciel, détermine si celui-ci est considéré malveillant. Les maliciels comprennent les virus, les vers, les chevaux de Troie, la plupart des programmes furtifs, les logiciels espions, les logiciels de publicité malhonnêtes et d'autres logiciels non sollicités. Les maliciels diffèrent des logiciels défectueux, qui eux, sont légitimes, mais contiennent des bogues nuisibles.
Mot de passe : Mot secret ou combinaison de caractères utilisés pour authentifier la personne qui le détient.
Correctif : Mise à niveau ou réparation d'un logiciel appliquée sans qu'il soit nécessaire de remplacer le programme original en entier. Les correctifs sont souvent fournis par le développeur de logiciels pour corriger les vulnérabilités de sécurité connues.
Hameçonnage : Tentative, par une tierce partie, d'obtenir des renseignements confidentiels

d'une personne, d'un groupe ou d'un organisme, en imitant ou en se faisant passer pour une marque particulière et généralement bien connue, habituellement afin d'en tirer un profit financier. Les hameçonneurs tentent, par la ruse, d'amener les utilisateurs à leur transmettre des données personnelles comme des numéros de cartes de crédit, des identifiants de connexion à des sites bancaires et d'autres renseignements sensibles à l'aide desquels ils pourraient commettre des actes frauduleux.
Risque : Exposition à des conséquences négatives si une *menace* se concrétise.
Mesure de protection : Processus de sécurité, mécanisme physique ou outil technique visant à lutter contre des menaces particulières. Parfois appelée « contrôle ».
Serveur : Ordinateur installé dans un réseau, destiné à fournir des ressources à d'autres cybersystèmes rattachés au réseau (il stocke et « sert » des données et des applications).
Pourriel : Courriel poubelle ou non sollicité provenant d'un tiers. Considérés comme une nuisance par les utilisateurs et les administrateurs, les pourriels soulèvent d'importantes préoccupations en matière de sécurité, car ils peuvent servir à introduire des chevaux de Troie au sein des systèmes ou tenir lieu de tentatives d'hameçonnage. Ils peuvent également entraîner des pertes de service ou perturber le fonctionnement des ressources et des passerelles de messagerie des réseaux.
Menace : Toute action ou tout événement potentiel (délibéré ou accidentel) qui représente un danger pour la sécurité de l'entreprise.
Vulnérabilité : Faiblesse d'un logiciel, du matériel, de la sécurité matérielle ou pratique humaine pouvant être exploitée pour commettre des attaques à la sécurité.
Wi-Fi : Réseau local qui emploie des signaux radio pour transmettre et recevoir des données à des distances de quelques centaines de mètres.

Sigles

CCRIC : Centre canadien de réponse aux incidents cybernétiques
CSTC : Centre de la sécurité des télécommunications Canada
DSD : déni de service distribué
ECCR : Examen canadien de la cyberrésilience
EMR : évaluation des menaces et des risques
FNI : Forum national intersectoriel
GSTI : Guide de sécurité de la technologie de l'information
HTTPS : Protocole de transfert hypertexte sécurisé
NIST : National Institute for Standards and Technology
PCCS : Programme de coopération en matière de cybersécurité
PERR : Programme d'évaluation de la résilience régionale
RPV : réseau virtuel privé
SCADA : système d'acquisition et de contrôle des données
SCI : système de contrôle industriel
SE : système d'exploitation
TI : technologies de l'information
URL : localisateur de ressources uniformes