Gouvernement du Canada | Government of Canada

Cadre de gestion des incidents cybernétiques pour le Canada

Août 2013

Canada

Table des matières

Introduction

Les Canadiens – les particuliers, l'industrie et le gouvernement – exploitent les nombreux avantages qu'offre le cyberespace, ce qui améliore notre économie et notre qualité de vie. Cependant, notre dépendance accrue à la technologie cybernétique augmente notre vulnérabilité à ceux qui attaquent notre infrastructure numérique pour compromettre la sécurité nationale, la prospérité économique et la sécurité publique.

Les cybermenaces et les risques de cyberattaques sont devenus une dure réalité qui nous touche tous. Les gouvernements, l'industrie et les Canadiens ont la responsabilité de protéger leur portion du cyberespace. Toutefois, il est impossible d'atteindre une cybersécurité efficace en s'isolant. Nous pourrons améliorer l'état de cybersécurité de nos réseaux uniquement par le partenariat et l'échange de renseignements. Les organisations doivent être en mesure de réagir aux cyberincidents d'une façon bien coordonnée en travaillant avec des partenaires locaux, provinciaux-territoriaux et fédéraux.

La gestion des urgences au Canada est bien définie et documentée, la plupart des urgences étant de nature locale et gérées par les administrations municipales ou les gouvernements provinciaux ou territoriaux. Les gouvernements fédéral, provinciaux et territoriaux (FPT) ont créé en 2007 un cadre de sécurité civile pour le Canada (CSCC) afin d'unifier les initiatives de sécurité civile FPT. Le Cadre reconnaît que chaque gouvernement FPT a la responsabilité de la gestion des urgences et de la sécurité publique au Canada. Le Système national d'intervention d'urgence (SNIU) incorpore et opérationnalise les principes de gestion des urgences établis dans le CSCC. Par ailleurs, le SNIU sert à l'harmonisation des interventions d'urgence des gouvernements FPT et facilite la coordination entre tous les ordres de gouvernement, le secteur privé, les organisations non gouvernementales (ONG) et les intervenants internationaux.

La gestion des urgences au Canada est fondée sur une approche tenant compte de tous les risques, qui a été élaborée pour comprendre toutes les urgences indépendamment de leur cause sous-jacente. Cette approche bien établie serait adoptée si un incident cybernétique 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. Cette approche tous risques est déterminée par des experts de divers milieux qui se penchent sur la gamme étendue d'urgences possibles — catastrophes naturelles, incidents dans le domaine des transports ou de la santé publique, défaillance des infrastructures, etc. — pour lesquelles des mécanismes et des procédures sont en place afin de prendre en charge les aspects de l'urgence spécifiques de l'incident.

Le concept de cybersécurité, en particulier la façon d'intervenir en cas de cyberincidents importants, introduit des complications aux structures de gestion des urgences en place, car le cyberespace est indépendant des frontières physiques et géographiques. Le cyberespace est conçu, réglementé, maintenu, exploité, détenu et sécurisé par divers ordres de gouvernement et par l'industrie privée. Le CSCC et le SNIU fournissent des principes directeurs globaux d'intervention en cas d'évènements

cybernétiques. Un cadre spécifique des cyberincidents servant de complément aux politiques, aux cadres, aux procédures et aux plans actuels de gestion est cependant nécessaire.

Le Canada est privilégié d'avoir un milieu d'experts qualifiés en cybersécurité, mais jusqu'à maintenant les moyens de coordonner les activités ne sont ni structurés ni documentés, en partie en raison de la complexité inhérente au cyberespace. De nombreux intervenants travaillent au sein des gouvernements fédéral, provinciaux et territoriaux, ainsi que dans les secteurs public et privé. La situation est compliquée du fait que les cybermenaces et les cyberattaques peuvent venir d'hameçonneurs amateurs, d'hacktivistes, d'organisations criminelles, d'États nationaux qui, traditionnellement, sont pris en charge par des autorités différentes. En outre, ceux qui s'occupent de gestion des urgences et de cybersécurité ne sont pas reliés de façon uniforme dans l'ensemble des territoires administratifs du pays.

Il y a de plus en plus d'ententes bilatérales et communautaires qui forment le fondement d'un cadre sur les incidents cybernétiques. Sécurité publique Canada a établi des partenariats avec de nombreuses organisations, et beaucoup d'entre elles collaborent avec des associations régionales, sectorielles ou professionnelles. Ces partenariats sont des structures évolutives qui constituent un ensemble d'instruments utiles (critères de présentation, seuils, mécanismes de communication et gravité des répercussions) et qui pourraient servir de fondement pour le milieu de la cybersécurité au Canada.

Le Cadre de gestion des incidents cybernétiques (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 de gestion des urgences déjà en place aux échelons fédéral, provincial et territorial ainsi que les plans d'urgence des propriétaires et des exploitants d'infrastructures essentielles.

Sécurité publique Canada a rédigé le CGIC à l'aide d'une approche fondée sur la collaboration; il sollicite les suggestions des intervenants du milieu de la cybersécurité au Canada et tire profit des structures et des comités de l'industrie qui sont déjà en place. Le CGIC se veut un document évolutif, modifié lorsque cela s'avère nécessaire pour répondre aux besoins du milieu de la cybersécurité à mesure que des interventions sont réalisées pour contrer les incidents et que des leçons en sont tirées. La participation au CGIC est optionnelle, mais conformément aux pratiques exemplaires internationales, tous les intervenants sont encouragés à l'adopter pour la gestion des cyberincidents et l'échange d'information. La réussite du CGIC dépend de l'engagement des intervenants de la cybersécurité des gouvernements provinciaux et territoriaux et du secteur privé.

Portée du Cadre de gestion des incidents cybernétiques

Le but du Cadre est de fournir une approche consolidée « pancanadienne » pour la gestion et la coordination en cas de menaces ou d'incidents cybernétiques réels ou potentiels. Il attribue les rôles et les responsabilités de tous les ordres de gouvernement, de tous les propriétaires et exploitants d'infrastructures essentielles ainsi que d'autres partenaires des secteurs public et privé dans une intervention coordonnée en matière de prévention, d'atténuation, de préparation, d'intervention et de rétablissement par suite d'incidents qui touchent la portion canadienne du cyberespace. Le Cadre a pour but de permettre à chaque organisation de participer entièrement et efficacement à une intervention nationale coordonnée pour contrer un cyberincident.

Le CGIC étaie les dispositions non officielles existantes qui relient les relations opérationnelles du niveau inférieur aux grands mécanismes de gestion des urgences, et ce, pour trois raisons, qui sont les suivantes :

1. Préciser les rôles, les responsabilités, les autorités et les capacités des intervenants en matière de cybersécurité;
2. établir des attentes à l'égard de ce que les intervenants devraient être prêts à faire et décrire l'aide qu'ils pourraient obtenir;
3. servir d'instrument d'amélioration de la gestion des cyberincidents et de promotion de la coordination.

Rôles et responsabilités des intervenants

Capacités en matière de cybersécurité

En plus du rôle central relatif au CGIC, toutes les organisations sont responsables de leur propre cybersécurité. Les organisations auront vraisemblablement établi une capacité robuste et efficace en matière de cybersécurité, proportionnelle à leurs risques et étayée par les pratiques exemplaires de l'industrie. Bon nombre de secteurs sont en train d'élaborer ou ont déjà en place des normes et des règlements relativement à la protection de l'information, à la résilience opérationnelle et à la sécurité qui doivent également être respectés et qui peuvent fournir une orientation, même s'ils ne sont pas obligatoires. Parmi les mesures adéquates, mentionnons des capacités et des plans d'intervention, des configurations protégées pour le matériel et les logiciels, des configurations protégées pour les périphériques réseau, des activités de surveillance et d'analyse des rapports des vérifications de sécurité, des plans de rétablissement en cas de catastrophe, des procédures et paliers d'intervention relatifs à la haute direction, des liens avec des organismes de réglementation gouvernementaux et des organisations de gestion des urgences provinciales et territoriales ainsi que des plans de communications et d'affaires publiques.

Bien qu'il soit reconnu que la capacité en matière de cybersécurité varie d'une organisation à l'autre, l'expérience montre que l'aide externe qui arrive en temps de crise est bien moins efficace qu'une capacité interne robuste.

Gouvernement fédéral

Il y a de nombreux ministères fédéraux qui jouent un rôle actif dans la coordination de l'intervention en cas d'incidents cybernétiques. Les ministères et les organismes tels que Sécurité publique Canada, le Service canadien du renseignement de sécurité, le Centre de la sécurité des télécommunications Canada (CSTC), et la Gendarmerie royale du Canada ont des rôles et des mandats en ce qui concerne l'intervention en cas d'incidents cybernétiques. Le gouvernement fédéral travaille continuellement à améliorer la coordination interne de manière à assurer une intervention cohésive; cette coordination est en grande partie assurée grâce au Centre canadien de réponse aux incidents cybernétiques (CCRIC).

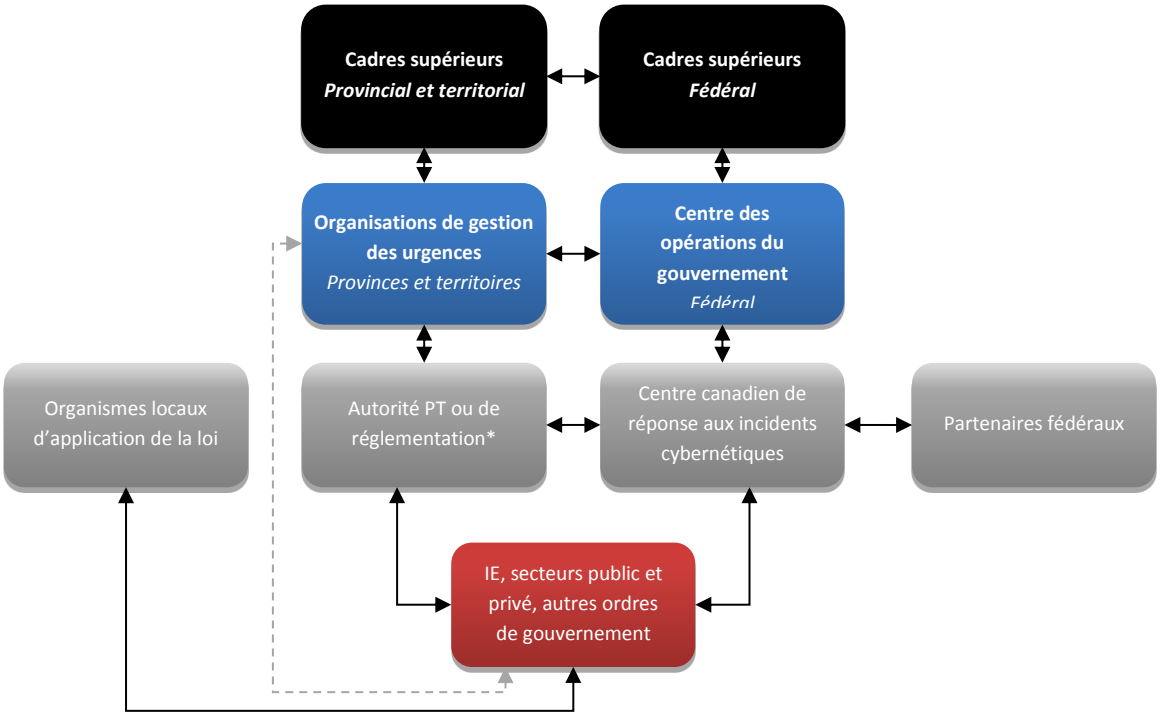
En tant qu'équipe de préparation aux urgences informatiques du Canada, le CCRIC le centre de coordination nationale du Canada pour la prévention, l'atténuation, la préparation, l'intervention et le rétablissement en matière d'incidents cybernétiques. Dans la plupart des cas, le premier contact d'une organisation avec le gouvernement fédéral afin d'obtenir des ressources en réponse à un incident cybernétique se fera par l'intermédiaire du CCRIC. Le CCRIC, qui fait partie de Sécurité publique Canada, a établi des liens de travail sur le plan fédéral avec la Gendarmerie royale du Canada, le Service canadien du renseignement de sécurité, le Centre de la sécurité des télécommunications Canada et d'autres organismes fédéraux. Il travaille étroitement avec les alliés importants du Canada, particulièrement avec les équipes nationales d'intervention en cas d'urgence informatique des États-Unis, du Royaume-Uni, de l'Australie et de la Nouvelle-Zélande, de même qu'avec les équipes nationales d'intervention en cas d'urgence informatique représentant des pays du monde entier. Le CCRIC a également établi des contacts avec les centres de protection de l'information des gouvernements provinciaux et territoriaux, les propriétaires et les exploitants d'infrastructures essentielles et le personnel responsable de la cybersécurité d'organismes des secteurs public et privé. C'est ainsi que, grâce à ces relations, le CCRIC est bien positionné pour émettre des alertes et des conseils en matière d'atténuation et pour diffuser de l'information qui profitera à tous les intervenants en vue d'améliorer la posture de cybersécurité de leurs systèmes informatiques et de l'information qu'ils contiennent.

Vous trouverez de plus amples renseignements au sujet du CCRIC ainsi que des instructions sur la façon de participer sur le site Web de Sécurité publique Canada, à l'adresse www.securitepublique.gc.ca.

Dans les cas où l'organisation touchée estime qu'un crime a été commis, elle doit s'adresser aux autorités d'application de la loi locales. Dans les cas où l'organisation touchée est d'avis que la sécurité nationale est menacée, elle doit s'adresse au Service canadien du renseignement de sécurité. Il pourrait s'avérer impossible de savoir si un évènement comporte des incidences criminelles ou visant la sécurité nationale. Au besoin, le CCRIC conseillera de prendre contact avec une autorité d'application de la loi ou une autorité de sécurité nationale.

Dans l'éventualité où un incident cybernétique important résulterait en des conséquences physiques (p. ex. une cyberattaque visant des installations électriques engendrera des pannes de courant), le Centre des opérations du gouvernement (COG) prendra vraisemblablement le rôle de direction pour ce

qui est de la gestion des conséquences. À ce point, divers accords de gestion des urgences peuvent entrer en jeu, y compris des liens avec des organisations de gestion des urgences au niveau provincial-territorial, tel qu'il est montré dans la Figure 1, ci-dessous.



* Certaines organisations pourraient ne pas avoir d'exigences relatives aux rapports de surveillance.

Figure 1 : Déclaration théorique d'incidents cybernétiques ayant des conséquences non cybernétiques

Provinces, territoires et autres ordres de gouvernement

Les provinces, les territoires et les autres ordres de gouvernement ont la responsabilité de protéger leurs propres systèmes informatiques. Ils ont également des responsabilités en matière de réglementation ou de surveillance pour un grand nombre d'industries et, au besoin, ils intègreront divers aspects de la cybersécurité dans leurs règlements et lignes directrices. Certains gouvernements provinciaux et territoriaux ont établi avec leurs homologues et des intervenants fédéraux et municipaux des relations en matière de gestion des urgences, et quelques-unes de ces ententes comprennent des mesures liées aux incidents cybernétiques. Les organisations auront probablement déjà mis en place un système de sécurité cybernétique efficace et robuste, comme précisé plus haut, dans les Capacités en matière de cybersécurité.

Propriétaires et exploitants d'infrastructures essentielles et autres organismes des secteurs public et privé

Les propriétaires et exploitants d'infrastructures essentielles, de même que les organismes des secteurs public et privé, sont responsables de la protection de leurs propres systèmes informatiques. Dans certains cas, ils peuvent avoir déjà établi des relations avec divers ordres de gouvernement pour la

coordination des incidents cybernétiques, comme précisé plus haut, dans les Capacités en matière de cybersécurité.

Les organisations qui font partie d'une industrie réglementée (p. ex. télécommunications, électricité, pétrole et gaz) peuvent s'attendre à une attention accrue à l'égard des questions de cybersécurité et de résilience dans les règlements et les normes qui s'appliquent à elles. Ces organisations auront déjà des liens avec le ministère responsable de la réglementation de leur secteur (fédéral ou provincial) ainsi qu'avec l'organisation responsable des mesures d'urgence de leur province. En plus d'être utilisés pour gérer une situation d'urgence dans le domaine physique, ces liens serviront à l'échange d'information et à la coordination de l'intervention pendant un cyberincident. On incite également les organisations touchées à entretenir des contacts avec le CCRIC dans le but de transmettre et de recevoir de l'information et des directives précises touchant les aspects cybernétiques de l'incident. En ce moment, il n'est pas réaliste qu'une organisation soumise à un régime réglementé ayant été touchée par un incident établisse un contact avec une seule entité (p. ex. organisme provincial ou CCRIC) dans le cas d'un cyberincident grave. Les organisations auront besoin des processus de gestion interne nécessaires à la coordination de ces multiples contacts.

Beaucoup d'organismes des secteurs public et privé ont des structures de gestion des crises en place au sein de leur organisation, lesquelles facilitent une intervention interne coordonnée en cas d'urgence; peu importe la cause ou la nature d'une urgence. De tels mécanismes font en sorte que les cadres supérieurs soient mis au courant des incidents, d'une façon appropriée et coordonnée. Il est important que toutes les organisations s'assurent que les mécanismes sont adaptés à la gestion des cyberincidents également. Les cadres supérieurs devraient établir des liens avec leurs homologues des ordres de gouvernement adéquats, y compris des organisations de réglementation et de gestion des urgences, et ce, afin d'accroître l'efficacité des communications et de la coordination pendant les situations de crise.

Organismes locaux responsables de l'application de la loi

Les organismes locaux responsables de l'application de la loi sont chargés de faire respecter la loi et de maintenir la paix, l'ordre et la sécurité. Si une organisation croit être victime d'un crime cybernétique, elle doit immédiatement le rapporter à son organisme local d'application de la loi.

Contexte du Cadre de gestion des incidents cybernétiques

Tel qu'il a été mentionné précédemment, l'objectif du CGIC consiste à présenter les rôles et les responsabilités de tous les ordres de gouvernement et des propriétaires et exploitants d'infrastructures essentielles pour l'intervention coordonnée en cas d'incident cybernétique touchant la portion canadienne du cyberespace. Ainsi, le CGIC définit le cadre stratégique de l'intervention coordonnée et les efforts d'atténuation, tandis que d'autres documents fournissent des plans et des procédures plus détaillés. Le contexte du CGIC prévu, montrant tous les types de documents requis pour une intervention robuste aux incidents cybernétiques, est présenté à la Figure 2.

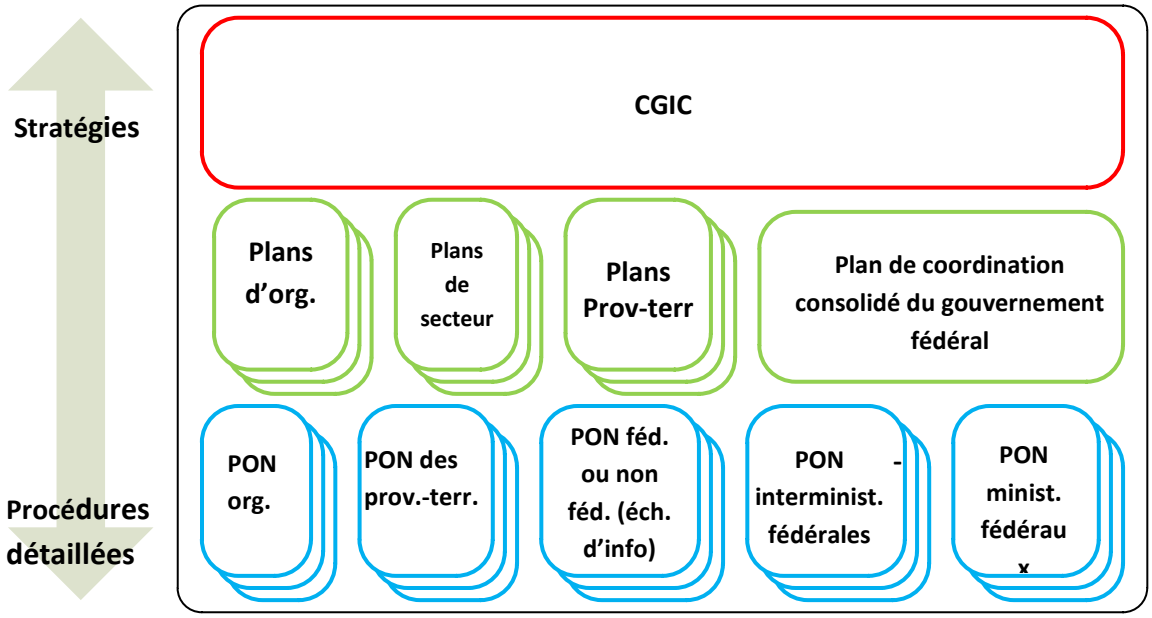


Figure 2 : Contexte du CGIC

Chaque organisation devrait avoir des plans en place en matière de prévention, d'atténuation, de préparation, d'intervention et de rétablissement en cas d'incidents cybernétiques. Par ailleurs, les gouvernements provinciaux et territoriaux ainsi que les secteurs des infrastructures essentielles doivent utiliser ces plans, au besoin, pour assurer une coordination et une collaboration efficaces. Dans de nombreux cas, ces plans existent, mais sont à des niveaux d'avancement différents. Le gouvernement fédéral, pour sa part, déploie des efforts soutenus pour s'assurer que ses mécanismes de coordination interne sont efficaces et adaptés aux besoins.

Des procédures opérationnelles normalisées (PON) détaillées sont également requises au sein de chaque organisation participante, lesquelles servent à orienter les activités quotidiennes du personnel technique, notamment en ce qui concerne la production de rapports et l'échange d'information ainsi que d'autres aspects opérationnels. Certaines PON seront propres à chaque organisation participante visée par le CGIC; d'autres détailleront l'échange d'information entre les organisations participantes, y compris le gouvernement fédéral.

Concept des opérations

Le CGIC est fondé sur le principe directeur que les personnes qui sont les mieux à même d'intervenir en cas d'incident cybernétique dans le réseau de l'organisation sont les membres de cette organisation, puisqu'ils sont ceux qui sont ultimement responsables du fonctionnement de leur réseau et de la protection de leurs biens. Même en cas d'attaque généralisée ayant une incidence sur de nombreux réseaux, chaque organisation est ultimement responsable de sa propre défense. Il est entendu qu'en raison de la complexité et du caractère unique des réseaux individuels, il est difficile pour tout

organisme externe d'apprendre les particularités d'un réseau assez rapidement pour organiser une défense robuste. Toutefois, aucune organisation ne devrait tenir pour acquis qu'elle peut dépendre uniquement d'une aide externe en cas de cyberincident. L'expérience montre qu'une capacité complexe et une bonne préparation à l'interne aux cyberincidents, accompagnée d'une collaboration avec des partenaires spécialistes externes comme le CCRIC, donne les meilleurs résultats. Plus les demandes d'aide et les questions d'une organisation sont précises, plus c'est probable qu'elle recevra de l'aide utile et les réponses à ses questions.

Le CCRIC a établi un tableau de gravité (voir annexe) afin de catégoriser les cyberincidents en fonction de plusieurs facteurs, notamment la diffusion d'information, le bien-être économique, la santé et la sécurité, la confiance du public, et les services essentiels. La structure fournit le fondement pour l'organisation du concept et des activités liés au CGIC. Bien que les seuils présentés puissent ne pas être appropriés dans tous les cas, chaque organisation est invitée à adapter une structure à niveaux multiples similaire, qui orientera leurs processus internes et facilitera la coordination avec les intervenants de tout le milieu. Le tableau contient cinq niveaux de gravité distincts, qui vont de « très faible » à « très élevée ».

La classification initiale du niveau de gravité pour tout incident donné sera effectuée par le client qui signale l'incident; le CCRIC évaluera les incidents signalés et, au besoin, travaillera de concert avec le client pour déterminer les répercussions potentielles de l'incident. Le niveau de répercussions déterminé orientera les mesures prises par le client ayant signalé l'incident, le CCRIC et les partenaires.

Dans la plupart des cas, l'intervention en cas d'incident cybernétique spécifique sera dirigée par l'organisation touchée, qui bénéficiera de l'aide de partenaires externes, sur demande. Les incidents qui correspondent aux seuils établis peuvent nécessiter de l'aide en matière de coordination ou l'intervention du milieu de la cybersécurité à l'échelle nationale. Par ailleurs, il est à noter qu'un incident de cybersécurité peut déclencher des effets de deuxième et de troisième ordres (notamment du domaine matériel; par exemple des usines de traitement des eaux). De tels incidents relèveraient alors du domaine de la gestion des conséquences et seraient assujettis aux politiques, aux cadres et aux accords actuels de gestion des urgences.

Opérations normales de cybersécurité

Le maintien de la cybersécurité est un processus opérationnel continu qui doit être traité comme une activité quotidienne. Les cyberattaques simplistes et automatisées se produisent souvent (de nombreuses fois par seconde dans un réseau de grande envergure), et on s'attend à ce que toutes les organisations protègent leurs réseaux et systèmes informatiques contre ces attaques, comme précisé plus haut dans les Capacités en matière de cybersécurité.

Il est attendu que toutes les organisations participant au CGIC vont signaler au CCRIC tous les incidents cybernétiques, peu importe leur niveau de gravité. Ce n'est que par la signalisation uniforme et exhaustive de tous les incidents que nous pourrons établir un portrait d'ensemble des incidents de cybersécurité au Canada. Les organisations qui prennent l'engagement d'échanger de l'information sur les cyberincidents avec le CCRIC et, par extension, avec les intervenants du domaine de la cybersécurité au Canada, contribuent à une sensibilisation commune aux cyberincidents, qui profite à elles-mêmes,

aux autres organisations ainsi qu'à tous les Canadiens. Le signalement de cyberincidents au CCRIC ne remplace pas des signalements transmis dans le cadre d'ententes et de dispositions préétablies.

Les organisations peuvent également communiquer avec le CCRIC si elles ne sont pas certaines que le cyberincident est d'origine criminelle ou qu'il a des incidences sur la sécurité nationale ou si elles ont besoin d'aide pour atténuer le cyberincident.

Le CCRIC s'engage à assurer la confidentialité et l'anonymat de l'organisation qui fait le signalement. Dans la mesure du possible, l'information présentée aux intervenants du milieu de la sécurité doit être dépourvue de tous renseignements permettant d'identifier l'organisation, ou encore les renseignements doivent être présentés de façon regroupée.

Incidents à incidence très faible

Comme précisé dans le tableau de gravité, les incidents à incidence très faible touchent un nombre très petit de personnes et ne résultent pas en la parte de services essentiels ou en des incidences économiques importantes. Ce type d'incidents est courant, et la plupart des organisations sont à même de les gérer sans aide ou coordination externe. Toutefois, l'absence d'incidence directe pour l'organisation qui constate l'incident ne signifie pas qu'il n'y a pas d'autres organisations qui sont touchées. Pour les cyberincidents qui consistent en le vol de données, par exemple, il est possible que l'incident reste non détecté pendant un certain temps pour de nombreuses organisations. C'est pourquoi le signalement des incidents au CCRIC est si important : il permet à la collectivité de bénéficier de la diligence collective de tous ses membres.

Mesures attendues – organisation touchée : L'organisation touchée devrait signaler ces incidents au CCRIC à titre d'information et d'analyse des tendances uniquement. Les associations sectorielles et autres collectivités pourraient souhaiter être mises au courant de tels incidents.

Mesures potentielles – milieu de la cybersécurité : Les incidents avec répercussions très faibles ne nécessitent généralement pas la participation de partenaires externes à l'organisation touchée. Le CCRIC surveillera les incidents avec répercussions très faibles et préparera les rapports des intervenants du milieu afin de déterminer si l'incident en question fait partie d'une campagne élargie touchant plus d'une organisation; dans ce cas, le niveau de gravité de l'incident pourrait être accru. En fonction de la nature de l'incident, le CCRIC pourrait également formuler des conseils en matière d'atténuation ou des recommandations.

Incidents à incidence faible

Les incidents à incidence faible sont les incidents qui sont perçus comme touchant un petit groupe ou un petit milieu, et ce, pour une durée limitée (« durée limitée » peut varier de façon considérable en fonction de la nature de l'organisation). En cas d'incident à incidence faible, il est prévu qu'il y aurait peu de conséquences, voire aucune, pour les services essentiels offerts à la population.

Mesures attendues – organisation touchée : L'organisation touchée réaliserait des activités d'intervention standard afin de gérer l'incident. L'organisation devrait signaler ces incidents au CCRIC, et

ce, afin que les conseils et les observations puissent être diffusées dans le milieu en général de façon anonyme.

Mesures potentielles – milieu de la cybersécurité : En fonction des détails de l'incident, le CCRIC peut préparer des notifications et aviser les partenaires de la situation. Comme c'est le cas pour les incidents à incidence très faible, le CCRIC surveillera les incidents à incidence faible et préparera les rapports des intervenants du milieu afin de déterminer si l'incident en question fait partie d'une campagne élargie touchant plus d'une organisation; dans ce cas, le niveau de gravité de l'incident pourrait être accru. Les organisations qui reçoivent les signalements d'incidents de la part d'une organisation touchée, ou d'une association sectorielle, ou du CCRIC devraient vérifier leurs propres systèmes pour s'assurer qu'ils n'ont pas été atteints par un incident semblable, rajuster leur position de risque et transmettre de l'information pertinente, au besoin. Le CCRIC gérera les incidents à incidence faible conformément aux PON, et pourra fournir des conseils pour l'atténuation ou d'autres recommandations. Le CCRIC pourrait émettre un avis à d'autres partenaires pour les informer de la situation, mais il ne mettra pas en œuvre d'autres mécanismes d'intervention.

Incidents à incidence moyenne

Les incidents à incidence moyenne sont les incidents qui sont perçus comme touchant un groupe ou une collectivité de taille moyenne, et pour lesquelles il y aurait une interruption prolongée des services. Les pertes financières seraient importantes et il pourrait y avoir l'interruption de certains services essentiels, mais aucune blessure grave ou perte de vie humaine.

Mesures attendues – organisation touchée : L'organisation touchée réaliserait des activités d'intervention standard afin de gérer l'incident et informeraient probablement la gestion interne. On s'attend également à ce que l'organisation signale l'incident au CCRIC et à d'autres organismes de réglementation et organismes de gestion des urgences à l'échelon municipal et/ou provincial, au besoin. À ce niveau de gravité, il est probable que les affaires publiques seront mobilisées, puisque les incidences et les mesures d'atténuation devront être communiquées au public, aux intervenants, aux clients et aux fournisseurs.

Mesures potentielles – milieu de la cybersécurité : Il est presque certain qu'un incident à incidence moyenne exigerait l'échange d'information entre les acteurs du milieu de la cybersécurité, et c'est le CCRIC qui coordonnera le tout. Le COG entamera probablement la planification pour s'assurer qu'il est prêt à aider à l'aide d'une intervention de gestion des urgences, au besoin. Le CCRIC informera les autres partenaires fédéraux de la situation ainsi que d'autres fonctionnaires de la cybersécurité de la situation et des répercussions potentielles. En parallèle, les organismes de gestion des urgences locaux et régionaux pourront communiquer avec les organisations touchées pour gérer les répercussions. En fonction de la nature de l'incident, les fournisseurs de services Internet, les sociétés de télécommunications, et d'autres fournisseurs experts pourront participer.

Incidents à incidence élevée ou très élevée

Pour ce qui est des niveaux de gravité élevé et très élevé, les conséquences sont plus graves et comprennent la perte potentielle de vies humaines et des répercussions financières importantes.

L'incident ne sera plus catégorisé comme un cyberincident, puisque les conséquences générales prescriront l'activation de procédures d'intervention d'urgence. Donc, les incidents à incidence élevée ou très élevée seraient coordonnés par l'organisme de gestion des urgences de l'administration touchée. Au niveau fédéral, ce serait le COG à l'appui du CCRIC.

Mesures attendues – organisation touchée : Un incident de cette gravité recevrait une attention importante de la part des médias, du public et des représentants des organismes de réglementation. De nombreux représentants de l'organisation touchée seront mobilisés, sans égard au fait qu'un cyberincident était à l'origine des conséquences, et le rôle de chef de file et d'intervention ne sera plus celui des experts de la cybersécurité. Par conséquent, il est essentiel que les experts de la cybersécurité soient en mesure de communiquer des concepts de cybersécurité à des personnes qui ne sont pas expertes qui pourraient devoir diriger les efforts d'intervention globaux. Des intervenants internationaux seront vraisemblablement présents, et la coordination avec ceux-ci pourra être nécessaire. Par ailleurs, il y aura un besoin important en ce qui a trait aux affaires publiques. Même si ce sont probablement d'autres organismes de gestion des urgences qui dirigeront les efforts d'intervention, l'organisation touchée doit signaler ces incidents au CCRIC, qui servira de point de coordination pour la gestion des aspects cybernétiques de ces problèmes.

Mesures potentielles – milieu de la cybersécurité : À l'échelon fédéral, les activités d'intervention seraient coordonnées par le COG conformément au SNIU. Parallèlement, le CCRIC continueraient de coordonner les aspects cybernétiques de l'intervention pour appuyer le COG, et de mobiliser d'autres partenaires fédéraux et fonctionnaires de la cybersécurité, selon les besoins.

Autres mesures possibles

En fonction des détails du cyberincident, d'autres mesures peuvent être prises à tout niveau de gravité, y compris les suivantes :

1. Enquête de sécurité à l'échelon national;
2. Enquête par un organisme d'application de la loi;
3. Échange d'information sur le cyberincident avec d'autres intervenants, conformément à des modalités d'utilisation entre le CCRIC et l'organisation qui signale l'incident, et ce, pour accroître la sensibilisation et améliorer la gestion des cyberincidents.

Ces activités se réalisent souvent en parallèle avec les efforts déployés pour la gestion d'un incident et l'atténuation de ses répercussions.

Conclusion

Comme mentionné précédemment, le CGIC a été conçu à l'aide d'une approche de collaboration supposant la participation des intervenants du milieu de la cybersécurité du Canada. Sécurité publique Canada espère que d'autres contributions seront apportées au Cadre à mesure que nous travaillons de concert pour améliorer la résilience cybernétique du Canada.

ANNEXE – TABLEAU DE GRAVITÉ DU CCRIC

Ce tableau est fourni à titre de référence uniquement; chaque organisation est encouragée à établir son propre tableau de gravité à l'aide de seuils qui sont adaptés à la taille, à la complexité et à la nature de l'organisation.

Tableau de gravité

Incidence	Divulgation d'information	Perte de vie/blessures	Économie	Santé et sécurité	Services essentiels	Confiance du public / médias
Très faible *Effet négligeable*	Information publique = Non classifiée	Malaises mineurs - certaines personnes	*Incidence faible sur les PME/incidence moyenne sur les personnes* Dommages < 1 k$	Les administrations FTP et municipales et les IE peuvent assurer le bien-être des Canadiens	Petit groupe = interruption temporaire (< 24 h)	Effet négligeable
Faible *Effet mineur*	Information de nature légèrement délicate = Protégé A	Malaises modérés à graves - certaines personnes	Incidence faible sur le secteur économique du Canada et incidence importante sur les PME 1 k$ < Dommages < 100 k$	L'organisme d'intervention responsable a besoin de ressources d'appoint pour gérer le problème / Aucune répercussion considérable sur les autres services de santé et de sécurité	Petit groupe / petite ville = interruption intermédiaire (de 24 à 72 h) / temporaire	Lettres ouvertes, plaintes électroniques, couverture médiatique locale
Moyenne *Effet majeur*	Information de nature délicate ou préjudice peu important à l'intérêt national	Malaises, blessures ou maladies graves - nombre important de personnes	Incidence moyenne sur le secteur économique du Canada et incidence très importante sur les PME 100 k$ < Dommages < 10 M$	L'organisme d'intervention responsable a besoin de ressources d'appoint pour gérer le problème / Répercussion négative sur les autres services de santé et de sécurité	SPetit groupe / petite ville / grande ville / interruption longue (>72 h) / intermédiaire / temporaire	Éditoriaux des médias, couverture médiatique nationale, débats ciblés au gouvernement
Élevée *Effet important*	Information de nature très délicate ou préjudice grave à l'intérêt national = Protégé C ou Secret	Risque de perte de vie humaine ou d'invalidité permanente	Préjudice à l'économie du Canada et aux objectifs économiques stratégiques 10M$ < Dommages < 1 G$	L'organisme d'intervention responsable est presque à sa capacité maximale pour la gestion du problème / Les autres services de santé et de sécurité deviennent inefficaces	LGrand groupe / grande ville / PT = Interruption longue / intermédiaire / temporaire	Contestation de la politique gouvernementale, vaste couverture médiatique internationale, manifestations de désobéissance civile
Très élevée *Effet catastrophique*	Préjudices exceptionnellement graves à l'intérêt national = Très secret	Perte de nombreuses vies potentielles	Préjudices importants à l'économie du Canada et aux objectifs économiques stratégiques Dommages > 1 G$	La capacité de gestion du problème de l'organisme d'intervention responsable est dépassée / Les autres services de santé et de sécurité sont interrompus	Grande ville / PT = interruption longue / intermédiaire	Pertubation des services gouvernementaux, manifestations violentes, couverture médiatique internationale ciblée, répercussions importantes sur les Canadiens