SoinsSantéCAN
Leadership. Innovation. Collaboration.

Document d'information

Document d'information – Infrastructures essentielles dans le secteur de la santé du Canada
Partie B – L'accent sur la cybersécurité

2017

Les solutions numériques et la connectivité numérique sont en forte croissance dans le secteur de la santé et au-delà. Les services indispensables dépendent de plus en plus de systèmes numériques et ces systèmes occupent une part toujours plus grande dans les infrastructures essentielles du pays. Les infrastructures essentielles du système de santé ne font pas exception. Dans le monde numérique d'aujourd'hui, plus de gens utilisent plus de systèmes, d'appareils et d'applications, de façons plus variées, pour effectuer des tâches encore plus fondamentales pour le système de santé. Les grandes organisations de la santé utilisent des centaines de systèmes cliniques et administratifs différents et doivent maintenir des interfaces entre ceux-ci. Le partage de l'information entre les fournisseurs des soins de santé est également en hausse pour améliorer la sécurité des patients et la continuité des soins. Toutefois, plus nous comptons sur ces solutions numériques, plus nous devenons vulnérables en cas de défaillance de celles-ci. Au moment de rédiger le présent document, le nombre, l'ampleur et la complexité des cyberattaques sont en hausse et ont des incidences importantes pour le secteur de la santé du Canada.

La cybersécurité n'en devient que plus importante pour assurer la résilience de nos infrastructures essentielles. Dans le secteur de la santé, elle consiste à s'assurer que la continuité des opérations et la confidentialité des renseignements personnels sur la santé ne sont pas compromises par des cyberattaques.

Notre approche

SoinsSanté*CAN* a formé un comité directeur chargé d'orienter la création et la mise en œuvre d'un Réseau sur les infrastructures essentielles du secteur de la santé sous l'égide de la Stratégie nationale sur les infrastructures essentielles du Canada. Ce comité a supervisé la préparation du présent *Document d'information* et a prodigué ses conseils. D'autres sources d'information ont orienté le document :

- un survol de la littérature sur les infrastructures essentielles dans le secteur de la santé, avec une attention particulière à la cybersécurité;
- un sondage effectué auprès des membres de SoinsSanté*CAN* entre novembre 2016 et février 2017 (24 réponses, soit un taux de 46 %);
- des entrevues auprès d'intervenants clés : des leaders de la santé de partout au pays; des autorités en matière d'infrastructures essentielles et de préparation aux situations d'urgence; et des experts en cybersécurité;

Enjeu

Les services indispensables dépendent de plus en plus de systèmes numériques et ces systèmes occupent une part toujours plus grande dans les infrastructures essentielles du pays. Plus nous comptons sur ces solutions numériques, plus nous devenons vulnérables en cas de défaillance de celles-ci. Au moment de rédiger le présent document, le nombre, l'ampleur et la complexité des cyberattaques sont en hausse et ont des incidences importantes pour le secteur de la santé du Canada. La cybersécurité n'en devient que plus importante pour assurer la résilience de nos infrastructures essentielles.

Préparé par SoinsSanté*CAN* pour le Comité directeur sur les infrastructures essentielles et la cybersécurité du secteur de la santé (sous l'égide de la Stratégie nationale sur les infrastructures essentielles)

La Partie B du présent *Document d'information* présente un aperçu des aspects de cybersécurité à considérer par le secteur de la santé du Canada. La Partie A, quant à elle, traite de questions d'infrastructures essentielles de manière plus générale.

Par: Jennifer Zelmer, Ph. D.

Pour plus d'information :

Jennifer Kitts
Directrice, politiques et stratégie
jkitts@healthcarecan.ca

- la validation des résultats avec des personnes interviewées sélectionnées et les membres du comité directeur et du conseil d'administration de SoinsSanté*CAN*.

« Les cyberattaques comprennent l'accès involontaire ou non autorisé à des renseignements électroniques et/ou des infrastructures électroniques ou matérielles utilisés pour traiter, communiquer ou entreposer cette information, ainsi que leur utilisation, leur manipulation, leur interruption ou leur destruction (par voie électronique). La gravité des cyberattaques détermine le niveau d'intervention et les mesures d'atténuation nécessaires, c'est-à-dire la cybersécurité. »[1]

La cybersécurité dans le secteur de la santé

Les cyberattaques sont fréquentes dans le secteur de la santé du Canada. Lors d'un récent sondage effectué par SoinsSanté*CAN*, 86 % des répondants ont déclaré qu'ils avaient détecté une violation de données ou évité de justesse un incident, généralement mineur ou d'ampleur relativement faible. Bien des organisations mentionnent que leurs pare-feu détectent régulièrement des tentatives d'exploitation des vulnérabilités et les bloquent. Par exemple, une organisation avec laquelle nous nous sommes entretenus a fait état de millions d'attaques par année. La plupart étaient mineures et facilement bloquées par les mesures de protection existantes, mais l'organisation a décrit son risque global de cybersécurité comme étant « gérable, mais important ».

Plusieurs organisations ont rapporté les types de cyberrisques suivants :

- **les programmes malveillants, les logiciels espions, ou les rançongiciels :** des codes ayant une intention malveillante (p. ex., des virus ou des vers) qui peuvent dérober ou détruire des données;
- **l'hameçonnage et la cyberfraude :** des courriels ou d'autres communications qui, si l'on suit les instructions qu'ils contiennent (p. ex., cliquer sur un lien), peuvent donner accès à un système informatique, activer d'autres fonctions malveillantes ou demander des renseignements confidentiels;
- **les attaques par déni de service**, qui surchargent un réseau ou un site Web avec un volume de données ou un trafic très élevés dans une tentative de le neutraliser ou de le perturber;
- **les erreurs humaines qui ont touché des systèmes essentiels,** comme de brancher un téléphone de voix sur le protocole Internet (VoIP) dans une prise non câblée pour le service.

Les organisations de la santé du Canada ne sont pas les seules à subir des cyberattaques, comme le démontrent les récentes attaques à grand retentissement qui ont touché les services de santé au Royaume-Uni et ailleurs dans le monde. Aux États-Unis, on a rapporté plus d'une violation de données par jour au Département de la Santé et des Services aux personnes ou dans les médias, en 2016[2]. Ces violations des données ont touché plus de 27 millions de dossiers de patients. Deux sur cinq de ces violations (42 %) étaient le résultat de gestes posés par des initiés se répartissant en pourcentage à peu près égal en erreurs humaines et en actions fautives. De même, au Royaume-Uni, 27 des 94 groupes de la NHS (le Service national de santé) qui ont répondu à une récente demande d'information ont dit qu'un pirate de l'extérieur avait crypté un PC ou un appareil ou un réseau et demandé le paiement d'une rançon pour le décrypter.

Ces cas, et d'autres exemples semblables, indiquent qu'en plus des attaques aléatoires, les organisations de la santé peuvent être particulièrement ciblées pour diverses raisons, parmi lesquelles :

- les renseignements personnels qu'elles détiennent sur les patients et les employés peuvent être précieux et certains types d'information sur la santé ont une valeur permanente;
- de nombreux employés et cliniciens affiliés et de plus en plus de patients/clients ont besoin d'avoir accès à de l'information sensible, de sorte qu'il y a de nombreuses cibles potentielles pour des attaques de type hameçonnage;
- bien des organisations de la santé ont des ressources financières substantielles et sont de grands employeurs avec une masse salariale importante;

Figure 1 : Comment les leaders en soins de santé évaluent l'importance de la cybersécurité pour leurs organisations

(1 = pas importante du tout; 10 = extrêmement importante)

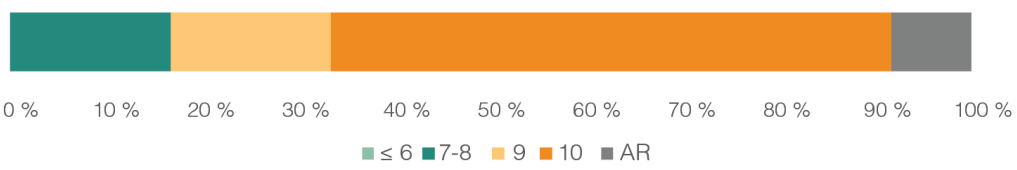
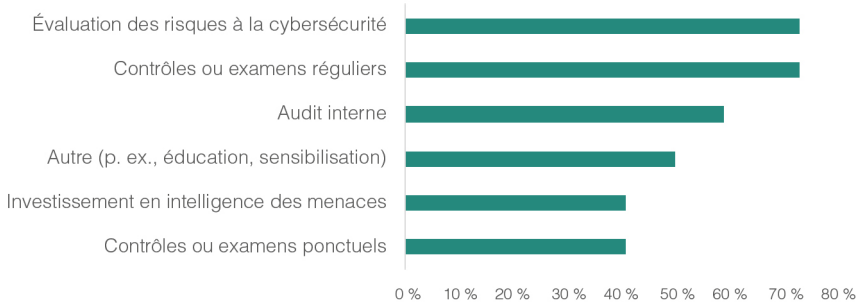


Figure 2 : Pourcentage des organisations de soins de santé qui disent avoir pris des mesures particulières pour évaluer ou prévenir les cyberattaques
(n = 21 répondants)



- les organisations de la santé ont souvent une grande notoriété dans les communautés et peuvent prendre des décisions que certaines personnes ou certains groupes n'approuvent pas;
- il y a un risque de perturbation des infrastructures et des services essentiels.

Dans ce contexte, il n'est pas étonnant que bien des leaders en santé considèrent la cybersécurité comme un élément extrêmement important pour leurs organisations (voir la Figure 1)[i]. Cela dit, les organisations sont aux prises avec de nombreuses priorités concurrentes et doivent prendre des décisions difficiles dans l'attribution des ressources.

État de préparation en matière de cybersécurité

La cybersécurité rend compte de l'interaction entre les menaces, les vulnérabilités, la probabilité d'un incident et ses incidences potentielles. Les organisations peuvent prendre bien des mesures pour améliorer l'état de préparation et atténuer les risques. Ainsi, le Framework for Improving Critical Infrastructure Cybersecurity du National Institute of Science and Technology des États-Unis recommande de déployer des efforts continus pour qu'une organisation puisse :

- **Cerner** les capacités et les risques et notamment, savoir qui a accès à l'information; exercer un contrôle sur ceux qui ont accès à l'information; utiliser des mots de passe appropriés; et mettre en œuvre des politiques et des procédures liées à la sécurité de l'information;
- **Protéger** contre un incident potentiel ou contre l'impact d'un tel incident relié à la cybersécurité en limitant l'accès aux données et à l'information; en utilisant des mesures techniques adéquates et en les mettant à jour; en cryptant des renseignements sensibles; en sensibilisant le personnel; et en prenant d'autres mesures de protection semblables;
- **Détecter** les incidents en temps opportun grâce à la mise en place des mécanismes appropriés;
- **Réagir** rapidement aux incidents grâce aux mesures de préparation aux cyberrisques mises en place;
- **Reprendre** les activités normales après un incident lié à la sécurité de l'information.

De même, Sécurité publique Canada[3] recommande de suivre les principes fondamentaux suivants : accroître la sensibilisation à la sécurité; définir les rôles et les responsabilités; élaborer des politiques et des normes; élaborer un plan de cybersécurité et établir un budget pour la cybersécurité. L'organisme attire également l'attention sur quatre mesures de protection particulières pour éviter la majorité des problèmes de cybersécurité :

- **Établir la liste des applications autorisées (liste blanche)** pour que seuls les programmes déterminés puissent être exécutés sur un système donné;
- **Utiliser des systèmes d'exploitation et des applications modernes**, et mettre en place une approche fondée sur le cycle de vie en vue de la migration vers les versions les plus récentes des systèmes ou des programmes;
- **Installer les correctifs des systèmes d'exploitation et des applications** dans les deux jours de l'annonce publique d'une vulnérabilité à risque élevé;
- **Limiter les privilèges administratifs.**

Les organisations de soins de santé du Canada disent qu'elles prennent diverses mesures pour évaluer ou prévenir les cyberattaques (voir la Figure 2). De plus, un peu moins de la moitié (45 %) des répondants ont déclaré que la cybersécurité était un point permanent à l'ordre du jour des réunions de leur conseil d'administration.

i. Selon un sondage réalisé auprès des membres de SoinsSantéCAN entre novembre 2016 et février 2017. SoinsSantéCAN a reçu 24 réponses, ce qui correspond à un taux de 46 %.

Évolution des risques et des interventions en matière de cybersécurité

Lors d'entrevues avec des intervenants clés, bien des leaders en santé ont insisté sur les risques en constante évolution auxquels ils font face. L'un d'entre eux a souligné que « plus de gens utilisent plus de systèmes d'une façon plus évoluée à plus d'endroits sur plus d'appareils différents. La menace évolue. Les attaques sont en forte croissance ». Il est clairement apparu dans ces discussions qu'il fallait adopter une approche stratégique à long terme basée sur une solide compréhension des risques et des opportunités. En examinant des cyberévénements graves, il faudra peut-être insister sur la continuité des activités et le relèvement après la catastrophe. En même temps, comme l'a souligné un responsable de systèmes d'information avec qui nous nous sommes entretenus, « sur une base quotidienne, nous devons équilibrer le bon accès à l'information et la sécurité; nous ne devons pas devenir ceux qui disent toujours non ».

D'autres questions d'intérêt commun ont été soulevées pendant les entrevues :

- **L'utilisation de la technologie de l'information et des communications connaît une croissance rapide dans le secteur de la santé.** Les personnes interviewées ont indiqué qu'elles s'inquiétaient davantage des vulnérabilités des applications que du matériel informatique, parce que certaines solutions cruciales sont obsolètes, n'ont plus de soutien ou sont sur le point de ne plus en avoir. C'est d'ailleurs ce qu'a dit l'une d'entre elles : « Nos plus grandes vulnérabilités sont dans les applications. C'est un élément critique pour nous. Plusieurs applications que nous utilisons sont fondamentalement obsolètes ou sur le point de l'être. » Certaines autorités se sont engagées dans des mises à niveau de grande portée – ou envisagent de le faire – mais ce n'est pas le cas partout. Passer aux procédures de sauvegarde manuelles (comme le prévoit le plan d'urgence) devient de plus en plus encombrant et insoutenable. En même temps, l'utilisation accrue de solutions numériques offre des possibilités de résilience, car elle favorise le partage des données et elle permet l'utilisation des soins virtuels pour continuer d'offrir des services en cas de perturbation de la prestation de services en personne dans un endroit donné.
- **La cybersécurité est sur l'écran radar de la plupart des organisations, mais pas de toutes.** Il est généralement reconnu que nous ne pouvons pas prévenir toutes les attaques, mais nous devons réduire le risque d'incidence et notamment détecter les attaques et nous en relever le plus tôt possible lorsqu'elles surviennent. Le leadership est la clé. Les organisations les plus grandes et les plus branchées ont généralement des plans et des mécanismes avancés en matière de cybersécurité. Plusieurs personnes interviewées ont souligné que les membres de leurs conseils d'administration proviennent souvent d'autres secteurs où la cybersécurité est une question importante et qu'ils ont contribué à en faire valoir l'importance dans le secteur de la santé. Comme l'a dit l'une d'entre elles, « nous avons beaucoup à apprendre des autres secteurs; je ne crois pas que les exigences [du secteur de la santé] soient particulièrement uniques. »
- **La sensibilisation et l'évaluation relatives aux niveaux de sécurité de base sont importantes.** Bien des personnes interviewées ont insisté sur l'importance de mieux comprendre les menaces, les risques, la préparation et les facteurs de résilience qui évoluent sans cesse. Il existe divers outils et services en appui à un processus d'évaluation structuré, comme le Programme d'évaluation de la résilience régionale de Sécurité publique Canada, des cadres d'évaluation du secteur privé et une carte de pointage sur la sécurité à l'intention des organisations de soins de santé[4]. Quoi qu'il en soit, la mesure dans laquelle de telles évaluations ont été faites, que les résultats en ont été partagés avec les intervenants appropriés et que les mesures de suivi ont été prises varie considérablement.
- **Bien des organisations disent faire l'objet de divers types de cyberattaques sur une base régulière,** la plupart d'entre elles étant toutefois détectées et prévenues. Les systèmes de santé et les systèmes financiers sont tous deux des cibles potentielles. Plusieurs violations des systèmes de dossiers de santé par des initiés ont été largement publicisées. Les hôpitaux canadiens ont aussi été victimes d'autres types de cyberattaques. Dans un cas, par exemple, des pirates informatiques se sont attaqués par hameçonnage aux fichiers de la paye d'un hôpital et ont effectué trois « transactions importantes à partir des comptes de la paye ». Bien que ce soit moins courant, certaines personnes interviewées ont également parlé des incidences éventuelles des interruptions généralisées de l'Internet et des services de données qui peuvent se produire lors de catastrophes naturelles et d'autres scénarios semblables.
- **Le degré de préparation varie grandement dans le secteur de la santé** et peu d'exigences standards sont en place. Presque toutes les organisations prennent certaines précautions de base (p. ex., les pare-feu). Il est de plus en plus reconnu que si ces couches de sécurité sont importantes, elles sont toutefois insuffisantes pour « bâtir un mur plus haut » autour de nos biens et de nos systèmes d'information. Certaines organisations investissent dans des stratégies plus vastes et plus intégrées, par exemple dans des activités d'éducation ou de sensibilisation à l'échelle de l'organisation;

l'analyse prospective proactive; l'évaluation des risques; la détection des menaces avancée et d'autres solutions technologiques; l'approche de sécurité à plusieurs niveaux et la redondance pour les systèmes ou les réseaux essentiels; les vérifications ponctuelles et les tests des mesures d'intervention; les plans de récupération ou de résilience suite à une défaillance; et le renforcement des capacités (voir la Figure 2). Les plus petites organisations, comme les cliniques individuelles, peuvent être plus vulnérables, mais le fait qu'elles sont réparties en plusieurs endroits leur procure peut-être des avantages sur le plan de la résilience. Compte tenu de l'évolution de l'environnement des risques, les personnes interviewées ont toutes exprimé une volonté d'améliorer l'état de préparation.

- **L'allocation de ressources pour des initiatives de cybersécurité pose un défi** parce que les organisations ont bien d'autres priorités qui ont des incidences directes sur les services de santé aux patients et aux collectivités et parce qu'on ne comprend pas toujours très bien les incidences potentielles des défaillances de la technologie de l'information sur la santé et la sécurité des personnes dans un monde numérique connecté. Dans au moins une province, les personnes interviewées ont dit craindre que les investissements en capitaux (que ce soit en cybersécurité ou en d'autres domaines) aient des effets pervers sur le financement du gouvernement en raison de la structure des modèles de financement actuels.
- **La cybersécurité n'est pas une compétence de base pour la plupart des prestataires et des organisations de soins de santé.** Bien des personnes interviewées ont recommandé de miser davantage sur l'expertise (p. ex., en matière d'évaluation de cyberrisques et de tests) et sur les solutions (p. ex., les solutions infonuagiques bien conçues) susceptibles d'améliorer l'état de préparation et d'atténuer les risques, y compris les modèles de services partagés et d'externalisation de services. L'une de ces personnes a dit « qu'il faut éviter de penser que l'on doit créer tous ces systèmes d'information par nous-mêmes. Il faut intégrer des solutions qui existent déjà et qui sont mises en œuvre dans le marché ».
- **Un certain nombre de personnes interviewées appellent à la collaboration** pour renforcer la capacité d'intervention et la résilience globales du secteur de la santé, en tenant compte du besoin d'une expertise spécialisée et de la nécessité de sensibiliser et d'éduquer dans tout le secteur. Certaines personnes ont demandé d'intégrer les capacités de relèvement de la cybersécurité avec une planification élargie de la continuité des affaires et des services.
- **Plusieurs considèrent que l'éducation en cybersécurité et l'état de préparation des citoyens et des professionnels de la santé posent des défis, mais sont des éléments déterminants** pour l'état de préparation général du secteur de la santé, particulièrement du fait que de plus en plus de personnes ont accès à de l'information en santé (p. ex., par l'entremise des portails des patients). Les gestes posés par inadvertance et les gestes délibérés des initiés qui compromettent la cybersécurité sont considérés comme des risques potentiels importants. Les personnes interviewées ont suggéré d'améliorer les canaux de communication et la sensibilisation pour atténuer ces risques. Par exemple, l'une d'entre elles a souligné qu'il y a « beaucoup d'outils et de technologies, mais que cela semble être la partie facile. Il est beaucoup plus difficile d'intégrer au processus la notion de sensibilisation, les comportements et les politiques et procédures. Il faut y porter au moins autant d'attention qu'aux outils et technologies. Et c'est rarement bien reçu ».
- **La croissance de l'Internet des objets** et la plus grande connectivité des appareils médicaux sont considérées comme des développements technologiques susceptibles d'accroître la vulnérabilité du secteur de la santé. Certains prétendent que le piratage des appareils médicaux comptera parmi les plus grandes menaces à la cybersécurité auxquelles le secteur de la santé fera face dans la prochaine décennie. Pour relever ce défi, il faudra porter attention aux cybervulnérabilités potentielles pendant toute la durée de vie des appareils médicaux, y compris dans le cadre de la gestion de leur post-commercialisation[5].
- **Nous devons partager nos expériences, mais aussi protéger nos stratégies et nos systèmes de sécurité.** La question du partage des leçons apprises, des stratégies efficaces, des outils et d'autres ressources entre les organisations de soins de santé a suscité beaucoup d'intérêt. En même temps, tous reconnaissent qu'il faut maintenir la confidentialité des renseignements détaillés sur les dispositions de cybersécurité. L'une des personnes interviewées a souligné que la législation provinciale n'est pas claire sur ce qui est permis ou non lorsqu'il y a une demande d'*Accès à l'information*.

ii. La Société canadienne du sang (SCS) gère l'approvisionnement en sang, en produits sanguins et en cellules souches pour les provinces et les territoires du Canada, sauf le Québec. Elle assure également la gestion des dons et des greffes d'organes pour l'ensemble du pays.

La cybersécurité à la Société canadienne du sang

Comme bien des organisations qui dépendent de solutions et de réseaux numériques, la Société canadienne du sang[ii] doit régulièrement faire face à de petits cyberévénements. Ces événements se produisent presque quotidiennement et ont généralement des incidences minimes en raison des contrôles et des processus de cybersécurité fondamentaux de la Société canadienne du sang (SCS). Cependant, il arrive parfois que des événements plus importants amènent la SCS à renforcer la priorité qu'elle accorde à la cybersécurité.

Par exemple, à la fin de 2015, la SCS a remarqué que les donneurs d'une région particulière ne se présentaient pas à leur rendez-vous. Après un examen des registres du système de gestion en ligne des rendez-vous, elle a réalisé qu'une série de faux rendez-vous avait été prise par une application du logiciel qui effectuait une tâche automatisée. Cela a entraîné une réduction temporaire des collectes de sang. Par ailleurs, en octobre 2016, le pendant australien de la SCS, la Croix rouge australienne, a fait l'objet de la plus grande fuite de renseignements personnels de tout temps en Australie. (Une personne à la recherche des vulnérabilités de la sécurité a réalisé qu'un fichier contenant des renseignements sensibles sur les donneurs avait été placé dans un endroit non sécurisé par une tierce partie qui développe et maintient le site Web des services. Une fois identifié, le problème a été résolu et un examen indépendant a déterminé qu'il y avait un faible risque de mauvais usage direct de l'information dans le futur.)

Aujourd'hui, la cybersécurité n'est plus une fonction administrative dirigée par les TI, mais un catalyseur de la stratégie d'entreprise de la SCS :

- la cybersécurité favorise une souplesse en permettant à la SCS d'exploiter la technologie en toute confiance pour interagir avec les donneurs et les partenaires;
- la cybersécurité sert de sentinelle pour la marque de l'organisation, car la SCS est de plus en plus identifiée par sa présence en ligne;
- la cybersécurité favorise le bon fonctionnement de la SCS – de la chaîne d'approvisionnement cruciale jusqu'à l'administration de l'organisation, la cybersécurité assure que les données et les systèmes sont disponibles au besoin et que les données de ces systèmes sont fiables, précises et complètes.

Cette remise en perspective établit la cybersécurité comme un élément essentiel aux activités fondamentales de l'organisation et à la réalisation de son mandat pour répondre aux besoins des patients canadiens.

En s'appuyant sur des cadres normatifs de l'industrie (p. ex., ISO/IEC 27001 et le Framework for Improving Critical Infrastructure Cybersecurity du National Institute for Science and Technology), la SCS a développé un cadre et un plan stratégique de la cybersécurité qui insiste sur la mise en œuvre des moyens lui permettant de rester engagée face à une menace qui évolue sans cesse et de se tenir prête à résister à un incident relié à la cybersécurité. Motivée par une évaluation de ses capacités et l'éventail des menaces, la SCS va de l'avant avec plusieurs initiatives clés qui renforceront la sensibilisation à la sécurité et les processus de cybersécurité rigoureux dans toute l'organisation, qui adapteront les contrôles de cybersécurité aux évaluations des risques et qui assureront une architecture de cybersécurité qui lui permettra de tirer parti de solutions numériques, en toute confiance, pour atteindre ses objectifs d'entreprise.

Dans une perspective d'avenir : Améliorer la coopération avec une table ronde du secteur de la santé

La préparation, la planification et la communication sont des catalyseurs fondamentaux de la résilience des infrastructures essentielles et par conséquent, du fonctionnement efficace du secteur de la santé face aux dangers potentiels. Pour appuyer ce processus, l'Agence de la santé publique du Canada et SoinsSanté*CAN* ont créé un comité directeur en 2016 pour orienter et diriger les éléments clés du développement d'un réseau pancanadien du secteur de la santé centré sur les questions d'infrastructures essentielles. Ce comité a fourni des conseils sur l'élaboration du présent *Document d'information*. Ses membres contribueront également à la définition des modalités et de l'effectif du réseau ainsi qu'à la définition de ses livrables et de ses priorités pour la première année.

Pour en savoir plus

- Stratégie nationale sur les infrastructures essentielles et Plan d'action sur les infrastructures essentielles (2014-2017) du Canada.
- La série sur la cybersécurité et les hôpitaux de l'American Hospital Association : Questions Hospital Leaders Should Ask et What Hospital Trustees Need to Know
- Le Guide Pensez cybersécurité pour les petites et moyennes entreprises de Sécurité publique Canada
- Les Bulletins et pratiques exemplaires en matière de cybersécurité de Sécurité publique Canada
- Healthcare Sector Cybersecurity Framework Implementation Guide (2016), élaboré aux États-Unis par HITRUST, the Healthcare and Public Health (HPH) Sector Coordinating Council (SCC) et le Government Coordinating Council (GCC)
- Conseils de Healthcare Insurance Reciprocal of Canada (HIROC) sur la gestion des cyberrisques
- National Institute for Science and Technology Framework for Improving Critical Infrastructure Cybersecurity

Bibliographie

1. Sécurité publique Canada, « Stratégie de cybersécurité du Canada : Renforcer le Canada et accroître sa prospérité », 2010. [En ligne]. Disponible à : https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-fra.pdf. [Consulté le 24 janvier 2017].
2. Protenus, Inc. en collaboration avec DataBreaches.net, « BREACH BAROMETER REPORT: YEAR IN REVIEW 2016 Averaged at Least One Health Data Breach Per Day, Affecting More Than 27M Patient Records », 2017. [En ligne]. Disponible : http://www.protenus.com/hubfs/Breach_Barometer/Protenus%20Breach%20Barometer-2016%20Year%20in%20Review-%20final%20version.pdf. [Consulté le 27 janvier 2017].
3. Sécurité publique Canada, « Principes fondamentaux de cybersécurité à l'intention du milieu des infrastructures essentielles du Canada », 2016. [En ligne]. Disponible à : tps://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/2016-fndmntls-cybr-Scrty-cmmnty-fr.pdf. [Consulté le 17 décembre 2016].
4. H. Elrefaey, E. Borycki et A. Kushniruk, « Developing a Security Metrics Scorecard for Healthcare Organizations », *Healthcare Quarterly*, vol. 18, no 3, pp. 61-68, 2015.
5. Food and Drug Administration, « Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff », 28 décembre 2016. [En ligne]. Disponible à : https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf. [Consulté le 6 mars 2017].

SoinsSantéCAN
Leadership. Innovation. Collaboration.

17 rue York, Bureau 100
Ottawa (Ontario) K1N 5S7
(613) 241-8005
www.soinssantecan.ca