Aller de l'avant pour des soins de santé cybersécuritaires

CONCLUSIONS DU SOMMET CANADIEN SUR LA CYBERSÉCURITÉ DANS LES SOINS DE SANTÉ

Par: Charles Thompson

SoinsSantéCAN
Leadership. Innovation. Collaboration.

Contexte

Les nouvelles technologies pénètrent toutes les facettes de la santé et des soins de santé et cette tendance ne fera que s'accentuer au cours des prochaines années. En soi, c'est une très bonne chose. Par ailleurs, les infrastructures numériques deviennent de plus en plus les piliers d'une gamme étendue de services de santé quotidiens. D'un point de vue plus général, le nouveau paysage numérisé et réseauté est en train de devenir un élément déterminant d'un système de santé moderne, adapté aux besoins et résilient.

Pourtant, ce qui nous apparaît comme le meilleur des mondes en soins de santé pose aussi de nouveaux défis effarants pour les leaders des soins de santé, les gouvernements, les patients et le grand public. Le laxisme en matière de cybersécurité menace d'affaiblir la sécurité des infrastructures essentielles dont nous dépendons tous et de compromettre la sécurité des patients et des collectivités que nous servons. Au bout du compte, ces nouvelles technologies peuvent s'avérer la plus grande vulnérabilité de notre secteur dans un moment de crise, si elles ne sont pas gérées et sécurisées adéquatement.

SoinsSanté*CAN* est consciente de l'importance de promouvoir des infrastructures résilientes; un projet grandement lié à la consolidation de la position de notre secteur en matière de cybersécurité. Nos efforts pour améliorer la cyberrésilience du système de soins de santé du Canada ne sont qu'un volet de nos efforts élargis pour promouvoir la *Stratégie nationale sur les infrastructures essentielles*. SoinsSanté*CAN* s'engage dans cette démarche en partenariat avec l'Agence de la santé publique du Canada, en tant que représentant du secteur de la santé au sein du Forum national intersectoriel (FNI) sur les infrastructures essentielles. Le FNI dans son ensemble, maintient quant à lui une approche canadienne exhaustive et concertée envers les infrastructures essentielles en fournissant un mécanisme permanent pour la discussion et l'échange d'information au sein des gouvernements fédéral, provinciaux et territoriaux et des secteurs des infrastructures essentielles et entre ceux-ci.

Dans le cadre de ce travail, nos partenaires et nous avons commencé à nous soucier de la stagnation du dialogue sur la cybersécurité dans les soins de santé. Nous avons déterminé qu'il faudrait réunir les principales parties de notre secteur pour ranimer la discussion et dynamiser notre communauté autour d'une compréhension commune de nos risques et d'un ensemble d'engagements clés à aller de l'avant. C'est ainsi que SoinsSanté*CAN* a organisé le Sommet canadien sur la cybersécurité des soins de santé à Toronto (Ontario), le 22 février 2018.

La tenue de ce Sommet a été rendue possible grâce au généreux soutien de Sécurité publique Canada par l'entremise du Programme de coopération en matière de cybersécurité. Le Comité directeur sur les infrastructures essentielles et la cybersécurité du secteur de la santé, qui est présidé conjointement par SoinsSanté*CAN* et l'Agence de la santé publique du Canada, a orienté le programme du Sommet. SoinsSanté*CAN* désire exprimer sa gratitude à ses partenaires sans qui ce projet n'aurait pu être réalisé.

Des leaders de plusieurs disciplines ont participé au Sommet, y compris des cadres supérieurs en soins de santé; des responsables de cliniques; des spécialistes des domaines pertinents du droit, de l'assurance et de la recherche; des partenaires gouvernementaux; des associations de l'industrie; et des experts techniques de la cybersécurité au Canada et ailleurs dans le monde. Une liste complète des participants est incluse à l'Annexe A.

Pour qu'ils puissent se préparer au Sommet, nous avons remis aux délégués un mémoire d'options intitulé *Cybersafe Healthcare : Options for Strengthening Resilience in Canada's Health Sector (Options pour renforcer la cybersécurité dans le secteur de la santé au Canada).* Ce mémoire décrit l'état actuel de la cybersécurité dans la santé d'un point de vue mondial et au Canada; il présente la *Déclaration d'engagement pour des soins de santé cybersécuritaires* et il cerne les possibilités d'action collective pour renforcer la résilience du secteur. Le mémoire a été mis à jour pour tenir compte des discussions lors du Sommet et est inclus à l'Annexe B.

Le présent rapport documente les débats du Sommet canadien sur la cybersécurité dans les soins de santé. Il compile également les principales réflexions reliées aux discussions de cette journée et qui en ont découlé. Nous espérons sincèrement que les leaders en soins de santé, les partenaires gouvernementaux, les parties prenantes et les autres parties intéressées utiliseront ces idées et ces réflexions au cours des prochains mois et des prochaines années. Bien des risques auxquels notre secteur est exposé sont obscurs ou techniques. Toutefois, dans le cadre de notre travail nous avons été frappés de constater dans quelle mesure une grande partie de la bataille doit se mener en territoire familier en tenant compte des questions de leadership et de culture. Nous avons tous un rôle à jouer en cette matière. Notre objectif est de donner à nos partenaires les outils pour le faire.

Introduction

Le Sommet canadien sur la cybersécurité dans les soins de santé a commencé par les observations luminaires du président du conseil d'administration de SoinsSanté*CAN* et du président et chef de la direction d'Eastern Health, David Diamond (Annexe C). Ces observations ont été immédiatement suivies par l'allocution d'ouverture du président et chef de la direction de SoinsSanté*CAN*, Paul-Émile Cloutier (Annexe D). Le Sommet, selon M. Cloutier, poursuivait les trois objectifs suivants :

1. Sensibiliser les participants à la menace actuelle par rapport à la cybersécurité dans les soins de santé;

2. Lancer une déclaration qui souligne une même compréhension de l'importance de la cybersécurité dans le secteur de la santé au Canada et qui fait preuve d'un engagement commun, en principe, en faveur du renforcement de la résilience du secteur;

3. Examiner et étoffer des options potentielles pour promouvoir la résilience du secteur et cerner d'autres options qui n'ont pas été soulevées antérieurement.

L'allocution de M. Cloutier a été suivie de celle de M. Craig Oldham, directeur général de la coordination des infrastructures essentielles à Sécurité publique Canada.

La facilitatrice du Sommet, la Dre Jennifer Zelmer, présidente d'Azimuth Health Group, a présenté le programme de la journée (joint à l'Annexe E) qui comprend l'ordre du jour de l'activité et les biographies des conférenciers.

Discussions de groupe et présentations

Principes de la cybersécurité dans les soins de santé

La première activité du Sommet a été une discussion de groupe d'experts dont certains membres provenaient de l'étranger. L'objectif était d'obtenir des idées d'intervenants d'ailleurs dans le monde et d'autres secteurs dans l'espoir d'aider les leaders des soins de santé canadiens à tirer parti des leçons apprises et à éviter les erreurs commises par d'autres. Après avoir discuté des ramifications des menaces croissantes expérimentées à l'étranger et en dehors du secteur des soins de santé, le Sommet a porté son attention sur des préoccupations plus locales et plus spécifiques ayant trait à la cyberrésilience dans le secteur de la santé du Canada. Le nom et le titre des participants aux deux panels sont indiqués ci-dessous.

Ces discussions ont été suivies d'une présentation de Kevin Magee, directeur national pour les technologies infonuagiques émergentes intelligentes chez Microsoft Canada et ancien membre du conseil d'administration de Brant Community Healthcare System. M. Magee a parlé de l'importance de planifier les activités de cybersécurité et d'accroître les compétences et les connaissances à l'échelle des cadres supérieurs.

Dans les évaluations remises après le Sommet, les participants ont indiqué que ces discussions avaient une valeur considérable pour les aider à mieux comprendre comment les questions de cybersécurité influent sur le secteur des soins de santé et à définir leurs propres plans et stratégies pour accroître la résilience. Les principaux éléments de ces présentations ont été regroupés en une série de principes visant à aider les leaders des soins de santé à mieux comprendre la nature des risques à la cybersécurité dans les soins de santé; les menaces auxquelles nous sommes exposés; et les mesures à prendre pour les contrer.

PANEL Nº 1 Apprendre à partir des points de vue d'autres intervenants d'ailleurs dans le monde et d'autres secteurs	**PANEL Nº 2:** État actuel de la cybersécurité dans le secteur de la santé du Canada
Dan Taylor Directeur de la sécurité, National Health Service Digital	**Ray Boisvert** Conseiller provincial en matière de sécurité Gouvernement de l'Ontario
Cédric Arcos Directeur général adjoint pour la région de Paris, Fédération hospitalière de France	**Jeff Curtis** Chef de la protection des renseignements personnels Centre des sciences de la santé Sunnybrook
John Riggi Conseiller principal en matière de cybersécurité et de risque American Hospital Association	**Jim Patterson** Associé Bennett Jones LLP
Francis Bradley Chef de l'exploitation Association canadienne de l'électricité	**Brendan Seaton** Président, Division de la santé de l'Association canadienne de la technologie de l'information

Principe nº 1 : La cybersécurité dans les soins de santé est une question de sécurité des patients

Le profil de risque en matière de cybersécurité dans le secteur des soins de santé est souvent perçu comme étant relié à la détention de renseignements, le pire scénario étant celui de la perte ou du vol de données précieuses. Les risques de notre secteur s'étendent toutefois bien au-delà de la perte ou de l'interruption des données. Le secteur des soins de santé fait également face à d'importants risques potentiels à la sécurité des patients découlant de lacunes dans la sécurité du système. Comme le secteur est de plus en plus numérisé, automatisé et connecté, les risques liés à une cybersécurité inadéquate sont de plus en plus privés. À titre d'exemple, il n'est pas impossible que des lacunes dans les stimulateurs cardiaques ou les ventilateurs utilisant l'Internet des objets (IdO) soient exploités par des acteurs malicieux avec les incidences terrifiantes que l'on peut imaginer. Ces possibilités établissent clairement un lien entre la cybersécurité dans les soins de santé et la sécurité des patients. Les participants au Sommet ont bien saisi que le laxisme en matière de cybersécurité pose un risque réel à la sécurité des patients.

> *« Si la cybersécurité n'a traditionnellement pas fait partie des activités cruciales de notre secteur, ce n'est plus le cas aujourd'hui, qu'on le veuille ou non »*
>
> - Panéliste

Principe nº 2 : Les organisations de soins de santé sont des cibles de choix

Les panélistes du Sommet ont expliqué clairement que le secteur de la santé a des caractéristiques particulières qui le rendent très attrayant pour les criminels.

L'une de ces caractéristiques est le milieu de soins de santé en lui-même. Les organisations des soins de santé ont tendance à utiliser de nombreux logiciels et systèmes informatiques qui doivent bien fonctionner ensemble, mais qui n'ont pas toujours été conçus dans un but précis de compatibilité. Dans un tel environnement, les décisions se prennent souvent au détriment des bonnes pratiques de gestion des correctifs, car l'installation des correctifs augmente généralement le risque de conséquences imprévues pour les logiciels ou les systèmes qui doivent être accessibles en tout temps. Par conséquent, les organisations de soins de santé doivent établir un équilibre entre le risque technique de la gestion des correctifs et le risque clinique pour les patients qui peut en résulter. Dans les grands établissements de soins de santé qui peuvent faire fonctionner des milliers de dispositifs connectés – dont des ordinateurs, des téléphones et des dispositifs médicaux – l'installation de correctifs n'est pas une question futile qui peut être effectuée pendant la nuit. Ces vulnérabilités sont amplifiées par les questions de sécurité induites par l'utilisation fréquente et souvent inévitable des dispositifs personnels en milieu de soins de santé.

Les pratiques de segmentation des réseaux dans les organisations de soins de santé sont un problème connexe. Certains systèmes ne sont pas segmentés, de sorte qu'à peu près tout ce qui est dans le réseau est interconnecté. Cela simplifie les choses pour le personnel clinique qui, en raison de la nature de son travail, doit pouvoir accéder aux dossiers ou aux systèmes où qu'il soit dans l'organisation. Mais cela signifie aussi que l'intrus a un accès considérable au système. Il y a des façons de concevoir les environnements numériques pour atténuer ces risques (p. ex., par l'utilisation de solutions du Network Access Control, un contrôleur d'accès au réseau), mais elles requièrent une connaissance très pointue des biens de l'organisation et des besoins de son personnel.

La nature des données de santé fait de leurs gardiens des cibles attrayantes pour les intérêts criminels. Les données relatives aux soins de santé ont notamment les caractéristiques suivantes :

Vitales – Comme elles sont susceptibles d'améliorer l'accès aux soins, la qualité des services de santé et l'efficacité du système de santé, les organisations de santé se fient de plus en plus aux solutions numériques. Certains systèmes de santé dépendent tellement d'une infrastructure numérique que sa compromission peut nuire sérieusement à la prestation des soins. Par exemple, le piratage et le cryptage de renseignements médicaux pour obtenir une rançon pourraient sérieusement nuire à la capacité de certaines organisations de donner des soins ou d'offrir des services. Cela s'est déjà produit au Canada.

Personnelles – Les dossiers médicaux comprennent des données permanentes très sensibles, y compris des diagnostics confidentiels et des identifiants personnels, comme les noms, adresses et numéros d'assurance sociale. Ces données peuvent être des cibles de grande valeur pour les demandes de rançon ou le vol d'identité.

Rentables – Les organisations de soins de santé détiennent des renseignements importants sur les médecins, les employés et les patients. Ces renseignements peuvent être utilisés de manière inappropriée, par exemple pour faire des demandes frauduleuses de services de santé ou de médicaments et d'équipement médical destiné à la revente. Les organisations de soins de santé, à l'instar des organisations œuvrant dans d'autres secteurs, ont été victimes de compromission de courriel d'affaires, ce qui a entraîné des détournements de fonds par virements et a même obligé au minage des Bitcoins.

Denses en information – Les données de soins de santé peuvent servir à bien des fins, selon l'entreprise criminelle en cause. Par exemple, elles sont à risque élevé d'espionnage. Les instituts de recherche peuvent aussi être victimes du vol de la propriété intellectuelle de grande valeur, que ce soit pour en tirer un avantage commercial ou pour toute autre fin malveillante.

Comme les données de soins de santé comportent tellement de caractéristiques précieuses, les organisations et les travailleurs de la santé ne peuvent se permettre de laxisme en matière de cybersécurité. Et si la cybersécurité n'a traditionnellement pas fait partie des activités cruciales de notre secteur, ce n'est plus le cas aujourd'hui, qu'on le veuille ou non, comme l'a dit un panéliste.

Principe nº 3 : Aucune organisation et aucun secteur ne peuvent faire cavalier seul

Les partenariats sectoriels et intersectoriels sont essentiels au développement de la cyberrésilience. Comme on l'a souligné, le secteur de la santé fait face à diverses menaces à la cybersécurité en raison de ses activités et des données qu'il détient. Mais notre secteur a aussi des dépendances avec une gamme beaucoup plus élargie des secteurs d'infrastructures (par exemple, les secteurs de l'eau et de l'énergie) qui font face eux aussi à des menaces. Ces autres secteurs, réciproquement, dépendent du bon fonctionnement du système de santé.

En l'état actuel des choses, il n'est pas défendable pour un secteur de faire « cavalier seul »; il faut encourager le partage sectoriel et intersectoriel des menaces et des stratégies. Les partenariats sont un facteur de résilience déterminant, puisqu'il est essentiel que les propriétaires et les exploitants occupent une position centrale dans les flux d'information pour être en mesure de se préparer aux menaces, de les détecter et d'y réagir. Ces partenariats peuvent être encouragés par les gouvernements, mais ils exigent aussi un engagement profond des secteurs des infrastructures essentielles eux-mêmes.

Dans ce contexte, les exercices de simulation de cyberattaques et d'autres plateformes de partage de l'information sont particulièrement importants. Le secteur de l'énergie du Canada participe à des exercices qui s'étendent sur tout le continent, ce qui lui a permis d'acquérir des connaissances très utiles. Le secteur de la santé devrait examiner sérieusement comment il pourrait être un partenaire plus actif dans le milieu élargi des infrastructures essentielles en participant à des exercices semblables à l'échelle régionale, provinciale ou fédérale.

Principe nº 4 : Le secteur des soins de santé a besoin de leadership et de capacité pour réagir aux menaces

La vulnérabilité du secteur de la santé a attiré l'attention mondiale en mai 2017, lors de la cyberattaque WannaCry qui a perturbé les soins dans les fiducies du NHS au Royaume-Uni. L'attaque a affecté le tiers des fiducies, ce qui a entraîné l'annulation de quelque 19 000 rendez-vous dans les hôpitaux. Elle a aussi touché 603 organisations de soins primaires et 595 bureaux de médecins généralistes. WannaCry a sensibilisé le monde à l'importance des défis auxquels les systèmes de santé font face, mais un panéliste a mis en garde contre l'accent indu porté à cet événement en soulignant qu'en se concentrant sur WannaCry au détriment des autres menaces, on peut limiter l'imagination et nuire à une pleine évaluation des risques.

> *« Ne sous-estimez jamais la menace interne, vous pouvez faire confiance, mais vérifiez toujours. »*
>
> - Ray Boisvert, conseiller provincial en matière de sécurité au gouvernement de l'Ontario

L'incident de WannaCry met toutefois en évidence le fait que les partenariats ne sont utiles que si les organisations de soins de santé peuvent réagir à l'information qu'elles reçoivent.

L'incident de WannaCry était prévisible et prévu. La vulnérabilité qui l'a rendu possible avait en fait été détectée par NHS Digital plusieurs mois avant l'attaque de mai. Des avis avaient été envoyés aux fiducies du NHS avec des instructions sur la nature de la vulnérabilité et des conseils sur les façons d'atténuer le risque.

Toutefois, les fiducies n'ont pas toutes suivi les conseils. À ce moment-là, plusieurs d'entre elles travaillaient avec des versions de Windows 7 qui n'étaient pas à jour ou avec des versions de Windows XP pour lesquelles il n'y avait plus de soutien, deux versions qui étaient vulnérables face à l'exploit de WannaCry. Cette situation était une conséquence de décisions budgétaires et autres prises dans les années antérieures. En conséquence, bien des fiducies du NHS ont trouvé qu'elles n'étaient pas en position de réagir dans les délais qu'elles avaient, alors que d'autres n'ont pas accordé la priorité à cette question dans la période qui a précédé l'incident.

Principe nº 5 : La cyberrésilience et la réponse aux cyberincidents sont une responsabilité de toute l'entreprise

D'autres secteurs des infrastructures essentielles (par exemple, les secteurs de l'énergie et de la finance) comprennent que la cybersécurité est une responsabilité qui touche toute l'entreprise. Le secteur de la santé, au contraire, a souvent une perspective limitée du problème et considère la cybersécurité comme une question de TI. Dans ce modèle, la résilience et l'intervention sont déléguées au directeur de la technologie, au directeur des systèmes d'information ou au titulaire d'un poste semblable. Cette façon de voir les choses peut empêcher les conseils d'administration et les cadres supérieurs d'une organisation d'acquérir les connaissances et l'expertise nécessaires pour assurer une solide résilience et préparer des plans d'intervention qui concernent toutes les activités de l'organisation.

Les panélistes ont souligné qu'en considérant la sécurité comme une question de TI, on cache le fait que la menace interne est un facteur majeur de risques à la sécurité. Ces menaces peuvent être accidentelles ou intentionnelles. « Ne sous-estimez jamais la menace interne », a recommandé Ray Boisvert, conseiller provincial en matière de sécurité au gouvernement de l'Ontario. « Vous pouvez faire confiance, mais vérifiez toujours. » Les solutions techniques ne suffiront pas à elles seules à protéger contre ces situations de menace interne; une stratégie qui vise toute l'entreprise doit tenir compte du comportement des utilisateurs tout autant que de la défense des systèmes.

La planification à la grandeur de l'entreprise doit se faire à l'avance. Le pire moment pour élaborer une stratégie, c'est pendant une attaque, lorsque le niveau de stress est élevé et que l'information est rare. Comme pour les autres menaces aux infrastructures essentielles, les organisations de soins de santé doivent avoir établi un plan qui traite de prévention et d'intervention en cas de cyberattaques sous toutes leurs formes.

Les mesures préventives pour améliorer la résilience peuvent inclure des mesures pour s'assurer que les sauvegardes sont fréquentes et isolées des menaces externes; des programmes d'éducation; et des exigences visant à assurer la cybersécurité dans l'approvisionnement en matériel informatique pour favoriser la résilience et prévenir les attaques. Au-delà de ces mesures, le plan doit aussi comprendre une série de critères pour déterminer à qui demander de l'aide; s'il y a lieu de payer une rançon et, le cas échéant, dans quelles situations; et comment communiquer avec le personnel et les parties intéressées.

Le plan de résilience et d'intervention d'une organisation doit aussi traiter des conséquences juridiques d'un manquement. Comme l'a souligné Jim Patterson, les enquêtes ou les mesures que prend une organisation avant d'avoir engagé un conseiller juridique ne sont pas couvertes par le privilège. L'organisation peut être tenue de les divulguer pendant un recours collectif ou une autre action en justice. C'est pourquoi il faut engager un conseiller juridique le plus tôt possible dans le processus.

Principe nº 6 : La formation est essentielle et la simplicité est la clé

Comme la cybersécurité doit être considérée comme une responsabilité de toute l'entreprise, tous les dirigeants et les employés d'une organisation devront être sensibilisés à la cybersécurité, à divers niveaux de technicité. Pour qu'ils reçoivent une formation adéquate, il n'est pas nécessaire d'engager des coûts élevés ou d'aller dans la complexité. En fait, la simplification de l'information est souvent considérée comme une première étape essentielle de la formation.

Les meilleures pratiques en matière d'hygiène numérique sont relativement simples. Le langage trop technique peut être un obstacle à leur adoption. Comme l'a fait remarquer un panéliste, « dès que vous êtes technique, vous perdez la bataille ». John Riggi, conseiller principal en matière de sécurité et de risque pour l'American Hospital Association, a souligné qu'en tant que formateur de cadres supérieurs en milieu hospitalier, il « agit principalement comme un traducteur ». Kevin Magee, directeur national pour les technologies infonuagiques émergentes intelligentes chez Microsoft Canada, a insisté sur les rôles que jouent la terminologie et le jargon pour rendre la formation et l'intervention plus compliquées qu'elles ne doivent l'être : « En les qualifiant de 'pirates', c'est comme si ces personnes étaient intouchables. Je préfère le terme 'criminel' qui fait référence à un concept que les membres des conseils d'administration comprennent et auquel ils peuvent adhérer. »

Les participants ont souligné que la formation est importante pour tous les employés, à tous les niveaux, puisque la cybersécurité est la responsabilité de tous les services et de tous les intervenants dans l'organisation. Les stratégies d'audit et de rétroaction sont souvent utilisées à l'intérieur et à l'extérieur du milieu des soins de santé. Dans la plus grande mesure possible, il faudrait les utiliser pour amener les employés à adopter de meilleures pratiques d'hygiène numérique plutôt que de les fustiger pour leur piètre comportement. Le personnel devrait avoir la possibilité de participer à des approches de formation personnalisées et interactives, car les séances de formation de routine sont rarement mémorables. La formation pourrait aussi être dynamisée pour en faire une séance mémorable, par exemple en offrant des récompenses à ceux qui identifient des attaques par hameçonnage.

> *« Dès que vous êtes technique, vous perdez la bataille ».*
>
> – John Riggi, conseiller principal en matière de sécurité et de risque, l'American Hospital Association

Il en va de même pour le partage d'information sur les menaces à la cybersécurité et les mesures à prendre pour les éviter. La simplicité est gage de succès. Les gouvernements peuvent réglementer ou offrir des mesures incitatives pour favoriser la déclaration et l'amélioration de la résilience collective du secteur.

Principe nº 7 : L'expertise en cybersécurité est rare

Il n'y a pas de panacée technique qui améliorera de manière significative la résilience en cybersécurité en l'absence de personnel possédant l'expertise adéquate. Comme les autres secteurs, le secteur des soins de santé dans son ensemble peine à attirer le talent nécessaire en matière de cybersécurité, tant au Canada qu'à l'étranger. Au Royaume-Uni, il y a trois postes pour chaque candidat qualifié dans l'écosystème de la cybersécurité des soins de santé.

Face à cette pénurie de talent, le Royaume-Uni a adopté des modèles de réseaux en étoile lorsque c'est possible, qui sont organisés autour de centres d'excellence qui offrent leur expertise aux partenaires. Les participants du sommet ont souscrit à cette stratégie qu'ils considèrent comme prometteuse pour le secteur de la santé du Canada. Pour y parvenir, il faudra d'abord identifier les centres d'excellence régionaux, puis encourager des partenariats solides et fiables entre les organisations.

Principe nº 8 : Les normes de cybersécurité sont importantes, mais se sont avérées difficiles à déployer dans les soins de santé

L'adoption de normes cohérentes dans tout le secteur est une stratégie couramment utilisée pour lutter contre les failles de cybersécurité dans les soins de santé. Par exemple, le Royaume-Uni oblige les organisations qui font affaire avec le gouvernement à obtenir la certification de la plateforme appelée Cyber Essentials. Cette plateforme permet l'autoévaluation de la cyberrésilience en se basant sur cinq contrôles clés de la sécurité. On estime que cette certification prévient environ 80 % des attaques courantes sur Internet. Cyber Essentials a fait son entrée au Canada par l'entremise de CyberNB, établie au Nouveau-Brunswick, qui est considérée comme une option viable pour les organisations de soins de santé qui désirent évaluer leur niveau de risque.

Les conférenciers ont souligné qu'il est aussi important de comprendre son niveau actuel de résilience et de préparation que de savoir quelles sont les étapes suivantes. Il semble toutefois que ce niveau de certification soit très difficile à atteindre pour les organisations de soins de santé. En date de février 2018, 200 évaluations sur place ont été effectuées dans les fiducies du NHS et aucune n'a mené à la certification. Parmi ces évaluations, la note moyenne était de 59 % (allant de 23 % à 74 %) alors qu'il faut obtenir une note de conformité de 100 % pour obtenir la certification.

Cela pose des défis à l'échelle des politiques publiques. Comme l'a souligné un participant : « S'il en coûte X milliards de $ pour amener nos hôpitaux aux niveaux de sécurité prévus dans la norme Cyber Essentials, nous devons nous demander si cet investissement fait vraiment une différence et nous devons avoir une conversation honnête sur les mesures que nous prendrons pour que les hôpitaux respectent cette norme d'ici cinq ans. »

> *« Croyez-le ou non, les fournisseurs canadiens ont pleinement adhéré à la doctrine de la protection de la vie privée. Nous avons maintenant besoin de règles de conduite qui s'appliquent équitablement. »*
>
> - Brendan Seaton, président de la Division de la santé de l'Association canadienne de la technologie de l'information

Principe nº 9 : La cybersécurité des dispositifs médicaux doit être gérée comme une question de politique

L'utilisation accrue de technologies médicales connectées à Internet offre de nombreux avantages pour les soins aux patients, mais peut aussi causer divers problèmes du point de vue de la cybersécurité avec des risques connexes pour la sécurité des patients. Par exemple, un dispositif médical implanté ne peut être remplacé sur simple demande s'il est considéré comme étant une menace à la sécurité pour la personne ou pour l'établissement de soins. L'intégration d'exigences relatives à la sécurité dès le début, que l'on appelle parfois la « sécurité dès la conception » est une pratique exemplaire reconnue en ce domaine. Brendan Seaton, président de la Division de la santé de l'Association canadienne de la technologie de l'information avise les participants : « Croyez-le ou non, les fournisseurs canadiens ont pleinement adhéré à la doctrine de la protection de la vie privée. Nous avons maintenant besoin de règles de conduite qui s'appliquent équitablement. »

Les gouvernements ont certainement un rôle à jouer dans la réglementation des dispositifs médicaux, mais l'étendue de ce rôle n'est pas encore claire au Canada. Les organisations de soins de santé peuvent aussi jouer un rôle dans l'endiguement des menaces en établissant des exigences de cybersécurité dans le processus d'approvisionnement. Cette mesure contribuerait à garantir que seuls les dispositifs satisfaisant à un certain standard sont utilisés dans l'écosystème des soins de santé et orienterait le marché vers des solutions toutes prêtes comportant des dispositions de cybersécurité adéquates. Il est aussi possible de tirer parti des lignes directrices de Digital Health Canada sur la protection des renseignements personnels et de la sécurité dans la technologie de l'information en santé pour orienter des politiques à l'échelle de l'hôpital.

La déclaration d'engagement pour des soins de santé cybersécuritaires

Dans une volonté de renforcer la résilience de notre secteur en matière de cybersécurité, SoinsSanté*CAN* a profité de l'occasion pour présenter une *Déclaration d'engagement pour des soins de santé cybersécuritaires*. Le but de la séance était d'abord d'obtenir les commentaires des participants, mais plus important encore, d'évaluer la volonté et la capacité des organisations de signer la *Déclaration* et d'en adopter l'esprit. La *Déclaration* engage les signataires à prendre six mesures concrètes pour améliorer la préparation et la résilience en cybersécurité :

1. **Plaider en faveur** : plaider en faveur de la cybersécurité dans le système de santé du Canada;
2. **Informer** : s'assurer que nos dirigeants, nos employés et nos partenaires sont informés de l'étendue du défi et des possibilités d'atténuer le risque;
3. **Contribuer** : contribuer aux plans d'action communs qui créent la résilience collective aux cyberattaques;
4. **Progresser** : assurer la progression de la cybersécurité de manière cohérente avec notre mandat et tenir compte des occasions de prévention, d'atténuation, de préparation, de réaction et de rétablissement;
5. **Partager** : partager l'information, les pratiques exemplaires et les outils avec d'autres intervenants du secteur de la santé et d'autres secteurs pour bâtir la capacité et la résilience collectives;
6. **Faire preuve de transparence** : comme la situation et la capacité de chaque organisation sont uniques, nous confirmerons d'ici le Mois de la sensibilité à la cybersécurité, en octobre 2018, les mesures que nous prendrons pour concrétiser ces engagements dans notre contexte particulier et/ou avec notre collectivité.

Les participants ont été invités à exprimer la mesure dans laquelle ils étaient à l'aise avec la *Déclaration* et son déploiement dans le secteur de la santé. Les participants ont en général réagi positivement, mais certains ont souligné qu'ils avaient besoin de temps avant de signer la *Déclaration* au nom de leurs organisations.

Au cours des prochains mois, le *Déclaration* servira de pierre angulaire pour une coalition canadienne sur la cybersécurité en santé qui amènera ses membres à unir leurs efforts pour offrir de l'éducation, du partage d'information et d'autres marques de cyberrésilience. Conscients que cette coalition naissante devrait inclure des membres qui n'étaient pas représentés au Sommet, les participants ont été invités à nommer les autres organisations qui devraient en faire partie pour sensibiliser davantage aux cyberrisques et pour accroître l'efficacité des efforts d'atténuation des cyberrisques. Les participants ont mentionné les organisations ou structures dirigeantes suivantes :

- Le milieu universitaire
- Les associations cliniques et les autorités réglementaires
- La supergrappe des technologies numériques
- Les assureurs
- Les responsables de l'application de la loi
- Les ministères de la Santé
- Les administrations municipales qui offrent des services de santé
- Les fournisseurs de soins de santé et les autorités sanitaires régionales
- Les associations de patients
- Les commissariats à l'information et à la protection de la vie privée
- Les dépositaires de données en santé autres que le fournisseur ou les réseaux gouvernementaux
- Les organisations qui offrent des services d'approvisionnement et des services partagés
- Les associations et les syndicats d'employés en santé
- Les ministères pertinents à l'extérieur du secteur de la santé
- Héma-Québec
- Les organisations de normalisation
- Les intervenants du secteur des technologies en santé
- Les incubateurs et les accélérateurs de l'innovation

D'autres options menant à un progrès collectif

Le document sur les options préparé avant le Sommet identifiait des mesures pouvant être prises à divers niveaux pour promouvoir collectivement la cyberrésilience dans le secteur de la santé, sur la base de l'expérience d'autres pays et d'autres industries. Ces mesures comprenaient :

- **Normes** : intégrer des normes de cybersécurité dans les processus d'agrément ou d'audit;
- **Formation étendue** : offrir des incitatifs à une formation ordinaire ou à de perfectionnement en cybersécurité par des crédits universitaires ou d'autres mesures;
- **Obligation de divulgation et d'intervention** : obliger les organisations à divulguer les cyberrisques ou les cyberattaques et/ou à réagir aux risques identifiés;
- **Évaluation de l'état de préparation** : investir dans des évaluations des niveaux actuels de préparation et les capacités d'intervention dans tout le secteur, faire le suivi des changements au fil du temps;
- **Exercices pratiques** : organiser des exercices conjoints pour tester l'état de préparation à la cybersécurité et les capacités d'intervention;
- **Certification** : étendre la certification ou la réglementation en cybersécurité aux produits de santé numériques, aux dispositifs médicaux connectés à Internet et aux systèmes connexes.
- **Engagement moral** : s'engager à ne pas payer de rançon à la suite des cyberattaques pour que le secteur devienne moins attrayant pour les criminels – tout en équilibrant cet engagement par rapport aux responsabilités légales des organisations et des prestataires de soins de santé;
- **Réseau d'intervention** : identifier les responsables de la sécurité dans les organisations de santé à des fins de partage de l'information et pour savoir qui contacter avant, pendant et après d'importantes cyberattaques.

Au-delà de ces mesures, les participants ont été invités à générer leurs propres idées pour réussir à augmenter substantiellement la cyberrésilience dans le secteur de la santé. Voici les idées retenues – celles qui ont obtenu une moyenne de 3 sur 5 selon une échelle d'évaluation établie par les participants au Sommet :

- **Normes** : établir des normes cohérentes, des mesures de responsabilisation et des procédures de fonctionnement normalisées qui transcendent les mandats organisationnels et s'engager à les respecter.
- **Réseau en étoile** : identifier les Centres d'excellence pour exercer un leadership et déterminer « à quoi ressemble ce qui est bien » et orienter les autres, notamment par des projets pilotes sur l'adoption de la norme et la promotion de son adoption dans la communauté élargie;
- **Culture de la cybersécurité** : favoriser une culture de la cybersécurité dans les soins de santé en recourant à des approches systématiques pour sensibiliser aux cyberrisques et aux mesures permettant de les atténuer;
- **Collaboration** : faire participer les intervenants publics et privés des 10 secteurs d'infrastructures essentielles à des efforts nationaux, y compris en fournissant des fonds pour faire face aux risques prioritaires;
- **Législation** : adopter une loi relative à la sécurité de l'information, semblable par son concept à la Health Information and Protection of Privacy Act des États-Unis;
- **Simulation** : simuler une cyberattaque pour sensibiliser aux impacts potentiels et renforcer l'état de préparation au sein de l'organisation de santé;
- **Analyse comparative** : établir une base de référence pour la cybersécurité dans le secteur de la santé et déterminer des cibles mesurables que les organisations devront atteindre en 24 mois;
- **Éducation des conseils d'administration** : créer un modèle d'éducation en cybersécurité qui s'adresse aux administrateurs en soins de santé de toutes les autorités;
- **Échanges sur les menaces** : étendre radicalement la participation du secteur de la santé au Canadian Cyber Threat Exchange.

Les gouvernements, les organismes de réglementation, les fabricants de dispositifs médicaux et les organisations de soins de santé devraient examiner toutes ces options lorsqu'ils étudient leurs propres stratégies pour améliorer la résilience de la cybersécurité tant sur la scène locale que dans tout le secteur de la santé.

Conclusion

Ce rapport décrit les débats du Sommet canadien sur la cybersécurité des soins de santé 2018 et énonce les principes de gestion de la cybersécurité des soins de santé basés sur les discussions de la journée. Nous espérons sincèrement que les lecteurs le trouveront utile et y trouveront un relevé des forces et faiblesses de notre secteur et des défis auxquels il fera face au cours des mois et des années à venir.

En plus de sensibiliser les participants et le public élargi qui lira ce rapport, le Sommet a donné aux leaders des soins de santé une occasion de poser un jalon en déclarant leur engagement envers le progrès en matière de cybersécurité des soins de santé. Nous invitons les lecteurs à juger la force de notre engagement dans la réussite de nos prochaines étapes. Dans un proche avenir, SoinsSanté*CAN* communiquera avec les participants du Sommet et d'autres parties intéressées de l'intérieur et de l'extérieur du secteur de la santé afin d'augmenter le nombre de signataires de la *Déclaration* d'engagement pour des soins de santé cybersécuritaires. D'ici octobre 2018, les signataires de la *Déclaration* sont invités à publier leurs propres plans pour accroître la préparation et la résilience à la cybersécurité. Cela permettra d'explorer plus à fond l'état de préparation de notre secteur et ses opportunités pour aller de l'avant.

Alors que nous établissons le groupe intéressé au changement, il appartient aux signataires de juger comment ces changements s'inscriront dans nos organisations, notre secteur et notre pays. Comme l'a dit un conférencier lors du Sommet : « Nous faisons actuellement face à l'inévitable et il est impossible d'éviter l'inévitable ». Nous avons tous un rôle à jouer. Ce rapport décrit certaines mesures qui méritent d'être étudiées par les gouvernements, la liste des signataires de la *Déclaration* et celle des alliés dans l'effort d'isoler le secteur de la santé contre les menaces à la cybersécurité. Nous espérons que ces acteurs examineront ces mesures attentivement lorsqu'ils définiront les stratégies visant à améliorer la résilience et à atténuer le risque pour assurer des soins de santé cybersécuritaires.

Outils et liens utiles

Les participants ont souligné des outils et des ressources actuellement disponibles pour orienter et soutenir la détection des cybermenaces et les mesures d'intervention. Des descriptions annotées de certains de ces outils sont présentées ci-dessous :

Échange canadien de menaces cybernétiques (ECMC) – ECMC est un organisme indépendant à but non lucratif lancé en 2016 pour aider les entreprises et les consommateurs canadiens à détecter et à atténuer les cyberattaques. ECMC agit comme un point de contact dans lequel l'information sur les menaces de divers secteurs et industries peut être analysée, au bénéfice de tous les membres. Les partenaires d'ECMC donnent accès à des données internes qu'ECMC collige, analyse, résume et rend anonymes pour leur distribution dans le réseau. Toutes les menaces détectées par ce processus sont identifiées et tous les membres en sont informés et reçoivent des conseils sur les stratégies d'atténuation.

Cyber Essentials - Cyber Essentials Canada est une plateforme qui permet aux firmes d'autoévaluer leur cyberrésilience en se basant sur cinq mesures de contrôle essentielles : (1) pare-feu et passerelles Internet, (2) configuration sécuritaire, (3) contrôle d'accès, (4) protection contre les maliciels, (5) gestion des correctifs. Ces cinq contrôles de sécurité peuvent prévenir environ 80 % des cyberattaques courantes. La certification de Cyber Essentials est obligatoire au Royaume-Uni pour les firmes qui font affaire avec le gouvernement.

Centre canadien de réponses aux incidents cybernétiques (CCRIC) - Le CCRIC est un centre national de coordination dont la responsabilité consiste à atténuer les risques d'origine cybernétique auxquels sont exposés les systèmes et les services vitaux du Canada et fonctionne au sein de Sécurité publique Canada, en partenariat avec les provinces, les territoires, les municipalités, des organisations du secteur privé et des homologues internationaux. Il coordonne également la réponse nationale à tout incident grave menaçant la cybersécurité.

Passerelle d'information canadienne sur les infrastructures essentielles - La Passerelle d'information canadienne sur les infrastructures essentielles est un espace de travail non classifié, axé sur la collaboration et destiné aux intervenants du milieu des infrastructures essentielles, qui vise à faciliter l'échange d'information afin de bâtir un Canada plus sécuritaire et plus résilient. Les propriétaires ou les exploitants d'infrastructures essentielles peuvent profiter de l'expertise commune et d'un accès rapide à de l'information sur les cybermenaces en se joignant à la Passerelle et en y participant.

Health Insurance Reciprocal of Canada (HIROC) – HIROC est une mutuelle d'assurance à but non lucratif au service des organisations de soins de santé du Canada qui offre une couverture d'assurance économique et exhaustive et des solutions de gestion du risque afin d'aider les adhérents à prendre de meilleures décisions. HIROC a publié un guide sur la gestion des cyberrisques dans les organisations canadiennes de soins de santé qui comprend des conseils sur les mesures à prendre pour protéger une organisation contre des attaques, des menaces et des vulnérabilités.

Firstreceivers.ca – Firstreceivers.ca est une communauté de pratique qui offre aux professionnels de la santé des liens vers des ressources et des nouvelles récentes en réponse à des catastrophes qui affectent les infrastructures essentielles des soins de santé. La communauté est administrée par le Centre for Excellence on Emergency Preparedness, qui promeut l'excellente et les normes de diligence en matière de préparation et de la capacité de réaction aux situations d'urgence.

American Hospital Association – L'AHA est un chef de file en matière d'amélioration de la résilience des systèmes de santé des États-Unis par rapport aux cybermenaces. Dans sa série sur la cybersécurité et les hôpitaux : Questions Hospital Leaders Should Ask et What Hospital Trustees Need to Know, l'AHA offre des commentaires pertinents et des conseils sur le leadership en cybersécurité des soins de santé.

10 meilleures mesures de sécurité des TI – Le Centre de la sécurité des télécommunications (CST) publie une série des 10 meilleures mesures de sécurité des TI qui reposent sur l'analyse effectuée par le CST des tendances en matière de cybermenaces ayant une incidence sur les réseaux connectés à Internet. Lorsqu'elles sont mises en œuvre conjointement, les 10 mesures de sécurité permettent de minimiser les intrusions ou les impacts d'une cyberattaque sur les réseaux.

SoinsSanté*CAN*
17 rue York, bureau 100
Ontario (Ottawa) K1N 5S7

(613) 241-8005
1 (855) 236-0213

www.soinssantecan.ca