Une norme nationale pour la cybersécurité en santé

SoinsSanté*CAN* et le Conseil de gouvernance numérique, avec le soutien du Programme de coopération en matière de cybersécurité de Sécurité publique Canada, ont publié conjointement la première norme nationale sur la cybersécurité adaptée particulièrement pour le secteur des soins de santé. Intitulée *Cybersécurité : cyberrésilience en santé,* la norme est le point culminant d'un projet échelonné sur trois ans et il offre un autre outil s'inscrivant dans les efforts de SoinsSanté*CAN* pour remédier aux lacunes cruciales dans la cybersécurité des soins de santé.

PLAIDER EN FAVEUR DE PLUS GRANDES MESURES DE CYBERSÉCURITÉ

SoinsSanté*CAN* s'efforce depuis bien des années de sensibiliser à la nécessité d'une action et de ressources concertées pour améliorer la cybersécurité et la cyberhygiène dans les soins de santé. Depuis 2017, nous avons élaboré des politiques, formulé des recommandations d'action et développé des outils pour aider les hôpitaux, les autorités sanitaires, les établissements de soins de santé et de recherche en santé à réduire le risque des cybermenaces.

En 2018, nous avons organisé le Sommet canadien sur la cybersécurité dans les soins de santé, parrainé par le Programme de coopération en matière de cybersécurité de Sécurité publique Canada. Les points de vue et les connaissances échangés par des leaders de la santé du Canada avec des experts du domaine des soins de santé et de la cybersécurité du Royaume-Uni, de la France et des États-Unis lors de ce sommet ont été saisis dans un rapport sur les conclusions du Sommet et un mémoire sur les options pour aider les dirigeants du domaine de la santé du Canada à comprendre et à relever les enjeux de cybersécurité. L'événement s'est conclu par une série d'ententes de principe sur une Déclaration d'engagement pour des soins de santé cybersécuritaires signé par plus d'une vingtaine d'organisations de soins de santé du Canada.

En 2019, SoinsSanté*CAN* et son membre, Eastern Health – la plus grande organisation intégrée de santé à Terre-Neuve-et-Labrador, se sont associés avec la Fondation Canada-Israël pour la recherche et le développement industriels (FCIRDI) afin de réunir des chefs de file israéliens de la cybersécurité et des spécialistes canadiens dans les domaines de la santé, de l'éducation, des technologies de l'information et

de la gestion avec des partenaires du secteur privé pour s'engager dans des discussions ciblées sur la cybersécurité dans les soins de santé au Canada. Ce partenariat a permis de se pencher sur les possibilités de développer de nouveaux projets dans les domaines de l'éducation, de la création de logiciels et de l'infrastructure numérique dans l'objectif de soutenir la cybersécurité des soins de santé au Canada.

Pendant la pandémie, nous avons soutenu nos membres en leur transmettant des documents d'information qui mettaient en évidence les diverses opportunités offertes par l'extension des soins virtuels, mais aussi les menaces qui en découlent pour leur structure de TI et leurs efforts de développement de vaccins. Nous avons régulièrement participé aux appels hebdomadaires COVID-19 du Centre canadien pour la cybersécurité (CCCS) pour le secteur de la santé afin d'être au courant des cybermenaces et d'en faire part à nos membres. Nous continuons d'assister aux réunions d'information sur les menaces organisées toutes les deux semaines par le CCCS afin de rester informés des nouvelles menaces qui pèsent sur le secteur de la santé.

TRAVAUX EN COURS

SoinsSanté*CAN* représente le secteur de la santé au sein du Forum national intersectoriel sur les infrastructures essentielles. Ce réseau multisectoriel est coprésidé par le sous-ministre de Sécurité publique Canada et est mandaté dans le cadre de la Stratégie nationale sur les infrastructures essentielles pour renforcer les partenariats intersectoriels, échanger et protéger de l'information et mettre en œuvre une approche de gestion tous risques – y compris les menaces à la cybersécurité. Notre rôle au sein de ce forum nous amène à travailler avec nos partenaires de l'Agence de la santé publique du Canada pour bâtir et maintenir un réseau pour les infrastructures essentielles du secteur de la santé qui répond aux besoins du secteur dans tous les domaines des infrastructures essentielles.

Nous avons souligné le besoin d'un plus grand investissement dans l'infrastructure numérique canadienne afin de transformer le système de santé pour en faire un système reposant sur une base solide et en mesure de soutenir les nouvelles technologies et les nouveaux outils et de mieux partager l'information entre les établissements et les juridictions. Nous avons également appuyé la Feuille de route commune de l'interopérabilité pancanadienne du gouvernement du Canada en participant aux consultations pour fournir nos conseils stratégiques.

Dans notre Mémoire prébudgétaire pour 2024 présenté au Comité permanent des finances, nous avons exhorté le gouvernement à établir un fonds de modernisation des infrastructures des soins de santé de 5 milliards de dollars sur trois ans, afin d'améliorer les infrastructures physiques et numériques et de créer un système de santé plus résilient, durable et équitable et d'améliorer les soins et la sécurité des patients.

LES ATTAQUES PAR RANÇONLOGICIEL CONTINUENT DE MENACER LES ORGANISATIONS DE SOINS DE SANTÉ

En octobre, cinq hôpitaux de l'Ontario ont été attaqués par rançonlogiciel, ce qui a entraîné une interruption de services de santé essentiels, y compris des traitements contre le cancer et des interventions chirurgicales[i]. Les pirates ont diffusé des renseignements médicaux privés sur le Web clandestin (le « dark web ») après que les hôpitaux ont refusé de payer la rançon. Aujourd'hui, des semaines plus tard, les hôpitaux peinent encore à s'en remettre et à rétablir pleinement leurs services. Ce n'est qu'un des exemples récents de cyberattaques, une menace qui continuera à peser sur les hôpitaux et les établissements de soins de santé, selon le Centre canadien pour la cybersécurité[ii].

[i] https://www.cbc.ca/news/canada/windsor/windsor-hospital-ransomware-attack-cybercriminal-group-1.7017176
[ii] https://www.cyber.gc.ca/fr/orientation/bulletin-sur-les-cybermenaces-incidence-de-la-covid-19-sur-les-cybermenaces-pesant-sur

QUE PEUT FAIRE LE SECTEUR HOSPITALIER POUR SE PROTÉGER CONTRE DE TELLES CYBERMENACES?

Les hôpitaux, les autorités sanitaires, les centres de recherche en santé et les organisations de soins de santé peuvent adopter la norme *Cybersécurité : cyberrésilience en santé*, une norme nationale du Canada, afin d'être mieux équipés. Cette norme, adaptée au secteur des soins de santé, a été orientée par le vaste réseau de dirigeants du secteur de la santé de SoinsSanté*CAN* et le vaste réseau d'experts en technologies numériques et en technologies de l'information du Conseil de gouvernance numérique (CGN – anciennement connu sous le nom de Conseil stratégique des DPI).

ÉLABORATION DE LA NORME – PHASE 1 : GROUPES DE DISCUSSION

Avec le soutien du Programme de coopération en matière de cybersécurité de Sécurité publique Canada, le projet d'élaboration de la norme a débuté avec la tenue d'une série de groupes de discussion en anglais et en français, organisée par SoinsSanté*CAN* et le CGN, dans le but de recueillir les commentaires des dirigeants des soins de santé et des responsables des technologies de la santé sur leurs préoccupations, leurs problèmes et leurs besoins en matière de cybersécurité dans les soins de santé. Vous trouverez un supplément d'information sur ces groupes de discussion et les résultats obtenus en cliquant ici. Plus de 100 dirigeants des technologies de la santé et bien d'autres intervenants clés de tout le Canada ont participé à ces groupes de discussion. Il s'agissait notamment de représentants d'hôpitaux et d'organisations de soins de santé, d'établissements universitaires et d'instituts de recherche, des gouvernements fédéral, provinciaux et territoriaux, du secteur, de la profession juridique et du milieu des assurances.

Les participants membres de SoinsSanté*CAN* et du CGB ont été invités à répondre aux cinq questions suivantes :

- Quel est votre principal sujet d'inquiétude si vous devenez la cible d'une cyberattaque?
- Quel est le plus grand risque pour le système de santé aujourd'hui?
- Quel(s) domaine(s) d'intérêt aimeriez-vous voir inclus dans une norme nationale du Canada?
- Quels sont les facteurs de réussite concernant l'élaboration et la mise en œuvre d'une norme nationale pour la cybersécurité du système de santé canadien?
- Votre organisation utilise-t-elle actuellement ou cherche-t-elle à adopter une norme reconnue en matière d'information et de cybersécurité?

Les participants ont fait part de leurs préoccupations concernant les soins aux patients, la sécurité, la protection des informations personnelles sur la santé et la capacité à assurer la continuité des soins. Les participants ont également noté que parmi les principaux facteurs de risque à prendre en compte dans une norme spécifique aux soins de santé figuraient les rançongiciels et l'infrastructure informatique existante. Les participants ont estimé qu'une approche par paliers garantirait l'accessibilité pour toutes les organisations et ont souligné la nécessité d'une formation approfondie pour le personnel de première ligne et le personnel clinique, avec du matériel d'appui informatif.

Un projet de norme a été achevé en novembre 2022, orienté par les commentaires des groupes de discussion et avec l'expertise d'un comité technique et d'une équipe de rédaction composée d'experts en cybersécurité issus d'organisation de soins de santé, de gouvernements et du secteur privé.

ÉLABORATION DE LA NORME – PHASE 2 : CONSULTATIONS ET EXAMENS

Le comité technique a tenu une série de consultations et d'examens avec des représentants des dirigeants du secteur de la santé, des patients et des soignants de tout le Canada, de janvier à mars 2023. Les membres de SoinsSanté*CAN* ont fait part de leurs commentaires sur le projet de norme, oralement et par écrit. Parmi les principaux sujets sur lesquels ils ont insisté, mentionnons le rôle important du leadership dans la gestion des risques de cybersécurité et le renforcement de la sensibilisation à la cybersécurité, la clarification du rôle et des responsabilités de l'équipe de direction, ainsi que l'identification et la réalisation de politiques et d'objectifs en matière de cybersécurité.

L'ébauche de la norme a été affichée sur le site Web du CGN et une consultation publique de 60 jours a été menée du 27 avril au 27 juin 2023. Cette consultation ouverte a offert une occasion supplémentaire de fournir leurs commentaires sur la norme aux experts de la cybersécurité, dirigeants de la santé et parties prenantes de tout le Canada. Vous trouverez un supplément d'information sur le processus, ainsi que les principales conclusions qui en ont été tirées dans l'article *Enhancing patient safety: A national standard for cyber resiliency in healthcare* publié en ligne avant la publication de l'édition de décembre du magazine Healthcare Management Forum.

PRINCIPALES RECOMMANDATIONS DE LA NORME

La norme intègre des lignes directrices et des pratiques exemplaires à l'intention des organisations de soins de santé, allant des hôpitaux aux instituts de recherche et des cliniques médicales aux prestataires de soins virtuels. Elle porte sur un large éventail de sujets et de considérations, et elle traite notamment de gestion des risques organisationnels, de leadership, de sensibilisation, de réponse aux cyberincidents et de planification des urgences. La norme fournit des conseils sur la façon d'identifier, d'évaluer et de gérer les cyberrisques dans les organisations de soins de santé du Canada.

La norme insiste sur le rôle de l'équipe de haute direction, qui doit s'assurer d'offrir les ressources nécessaires, de définir la politique et les objectifs en matière de cybersécurité et de superviser le programme de cybersécurité de l'organisation.

Parmi les principales recommandations de la norme, mentionnons les responsabilités suivantes :

- Élaborer et mettre en place un programme de cybersécurité à l'échelle de l'organisation qui couvre les contrôles de base.
- Rédiger et diffuser des politiques et procédures de sécurité de l'information.
- Coordonner la création et la mise en place d'un programme organisationnel de sensibilisation et de formation sur la sécurité de l'information.
- Déterminer le degré de cyberrisque ciblé pour l'organisation et transmettre une recommandation à cet effet à la direction.
- Suivre les progrès vers la cible et rendre régulièrement des comptes sur l'avancement.
- Coordonner l'intervention en cas d'atteinte réelle ou présumée à la confidentialité, à l'intégrité ou à la disponibilité des systèmes et des données de l'organisation.
- Recenser les risques organisationnels et en prioriser l'atténuation selon leur probabilité et la gravité de leurs répercussions potentielles.
- Déléguer les fonctions de sécurité de l'information au besoin.

De plus, la norme comprend un modèle de plan d'intervention en cas d'incident, un questionnaire d'évaluation des risques de cybersécurité et d'autres modèles qui aideront les utilisateurs à comprendre où ils se situent en matière de cybersécurité et à créer un plan adapté pour leur organisation.

PROCHAINES ÉTAPES

La norme sera révisée tous les cinq ans et évoluera continuellement pour répondre aux besoins des organisations de soins de santé du Canada. SoinsSanté*CAN* et le Conseil de gouvernance numérique continueront à diffuser les principales conclusions et leçons tirées de ce projet auprès des dirigeants du secteur de la santé dans tout le Canada et encourageront toutes les organisations de soins de santé et nos membres à mettre la norme en œuvre. SoinsSanté*CAN* offrira également des documents d'application des connaissances en anglais et en français.

Vous pouvez télécharger gratuitement la norme en français et en anglais ici.

POUR UN SUPPLÉMENT D'INFORMATION

SoinsSanté*CAN* reste attentive à ces développements en ce qui concerne ses membres. Si votre organisation a des questions, des préoccupations ou des commentaires en lien avec ces développements, n'hésitez pas à nous contacter.

Siri Chunduri
Analyste de politiques et de recherches
schunduri@healthcarecan.ca

Jonathan Mitchell
Vice-président, Recherche et politiques
jmitchell@healthcarecan.ca