EDITORIAL

Cybersecurity in Health: A 21st-Century Imperative

Locked filing cabinets are no longer enough to ensure security of research data and results. In the 21st century, cybersecurity is foundational to the ethical conduct of research and its application to health services and policy. It matters for ensuring the confidentiality of personal data, for integrity of research systems, for safety of digital interventions that are being studied, for protection of intellectual property, and more.

The challenge is real, not theoretical. The National Research Council has experienced state-sponsored cyberattacks (Moens et al. 2015). Universities have reported ransomware attacks (CBC News 2016). And cyberattacks are relatively frequent in the health sector, a potential source of vulnerability that is recognized by health sector leaders and citizens alike (Zelmer 2018). For instance, multiple organizations have reported malware, spyware or ransomware attacks; phishing and cyber fraud; denial of service attacks; and human error that affected critical systems. On a global scale, the World Medical Assembly has stated that "cyber-attacks on healthcare systems and other critical infrastructure represent a cross-border issue and a threat to public health" (WMA 2016).

Addressing these challenges depends on both individual and collective action. At a recent national Summit, health leaders and cyber experts explored options for strengthening the health sector's resilience to cyber threats (HealthcareCAN 2018a). Building on the *National Strategy for Critical Infrastructure* endorsed by federal, provincial and territorial governments, participants declared a shared commitment to cybersecurity and to six tangible actions to increase preparedness:

- *Championing* cybersecurity in Canada's health sector;
- *Contributing to shared action plans* that build collective resilience to cyberattacks;
- *Sharing information, best practices, and tools* with others within and beyond the health sector to build collective capacity and resilience;
- *Informing* leaders, staff and partners about the scope of the challenge and opportunities to mitigate risk;
- *Progressing cybersecurity in ways consistent with each signatory's mandate*, considering opportunities for prevention, mitigation, preparedness, response and recovery; and
- *Ensuring transparency* in the context of each signatory's unique circumstances and capacity by confirming how it will apply these commitments in its unique context and/or with its community by Cybersecurity Awareness Month in October 2018 (HealthcareCAN 2018b).

I worked with HealthcareCAN and its many partners to arrive at this *Declaration*. This editorial is part of my commitment to spreading the word about the challenges that we face and the importance of taking proactive action to address them. I invite you to join us in this effort to foster robust, safe and effective health and health research systems that benefit those we serve. For more information about the *Declaration*, how to take part in the collective effort and to get access to a range of associated resources, please visit http://www.healthcarecan.ca/what-we-do/health-policy/infrastructure/.

The need for shared commitment and mutual support to make progress is not unique to cybersecurity; collaboration and collective contributions are equally important for producing a journal like *Healthcare Policy/Politiques de Santé*. As this is the last issue of this volume of the journal, I would like to express my thanks to the team responsible for its production. The Editorial Board steers the journal's direction, as well as the path of individual submissions. They work closely with the reviewers who volunteer their time to ensure that the quality of papers we publish is high (see page 84 for a list of reviewers over the past year). Both interact directly with Ania Bogacka, the Managing Editor, and the team at Longwoods Publishing, who are core to the journal's production and distribution. And, of course, scholarly journals depend on the creative and thoughtful efforts of the authors who publish in our pages.

My sincere thanks to everyone involved, as well as to our readers who thoughtfully reflect on how to use the insights published here to continue to improve health and healthcare.

JENNIFER ZELMER, PhD
Editor-in-Chief

References

CBC News. June 7, 2016. "University of Calgary Paid $20K in Ransomware Attack: No Evidence Cyberattackers Released Personal or University Data to Public." Retrieved May 20, 2018. <http://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979>.

HealthcareCAN. 2018a. *Declaration of Commitment to Cybersafe Healthcare: Options for Strengthening Cybersecurity in Canada's Health Sector*. Retrieved May 20, 2018. <http://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/Cyber%20Security/Options%20Brief%20Summit%20Report.pdf>.

HealthcareCAN. 2018b. *Declaration of Commitment to Cybersafe Healthcare*. Retrieved May 20, 2018. <http://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/Cyber%20Security/Declaration%20of%20Commitment%20to%20Cybersafe%20Healthcare.PDF>.

Moens, A., S. Cushing and A.W. Dowd. 2015. "Cybersecurity Challenges for Canada and the United States." Retrieved May 20, 2018. <https://www.fraserinstitute.org/sites/default/files/cybersecurity-challenges-for-canada-and-the-united-states.pdf>.

World Medical Assembly (WMA). 2016. *WMA Statement of Cyber-Attacks on Health and Other Critical Infrastructure: Adopted by the 76th WMA, Taipei, Taiwan, October 2016*. Retrieved May 20, 2018. <https://www.wma.net/policies-post/wma-statement-on-cyber-attacks-on-health-and-other-critical-infrastructure/>.

Zelmer, J. 2018. *Issue Brief: Critical Infrastructure in Canada's Health Sector – Part B: A Focus on Cybersecurity*. Retrieved May 20, 2018. <http://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/IssueBriefs/2017/EN/IssueBrief_CriticalInfrastructure_B.pdf>.

ÉDITORIAL

La cybersécurité dans le secteur de la santé : une réalité du XXIe siècle

Les classeurs fermés à clef ne sont plus suffisants pour assurer la sécurité des données et des résultats de recherches. Au XXIe siècle, la cybersécurité est en effet un aspect incontournable de la recherche et ses applications aux politiques ou services de santé. La cybersécurité est essentielle, entre autre, pour assurer la confidentialité des données personnelles, pour l'intégrité des systèmes de recherche, pour la sécurité des interventions numériques à l'étude et pour la protection de la propriété intellectuelle.

Les défis sont bien réels et non théoriques. À preuve, le Conseil national de recherches a été victime de cyberattaques appuyées par des États (Moens et al. 2015). Des universités ont indiqué faire l'objet de rançongiciels (CBC News 2016). Et les cyberattaques sont relativement fréquentes dans le secteur de la santé; c'est là une source de vulnérabilité reconnue par les dirigeants et la population (Zelmer 2018). Par exemple, plusieurs organisations font état d'attaques par logiciels malveillants, espions ou rançonneurs; d'hameçonnage ou cyberfraude; d'attaques par déni de service et d'erreurs humaines qui affectent des systèmes névralgiques. À l'échelle mondiale, l'Association médicale mondiale a affirmé que « les attaques cybernétiques des systèmes sanitaires et autres infrastructures essentielles constituent un problème dépassant les frontières et une menace pour la santé publique » (Association médicale mondiale 2016).

Faire face à ces défis demande une action individuelle et collective. Lors d'un récent sommet, des cadres de la santé et des cyberspécialistes ont exploré les façons de renforcer la résilience face aux cyberattaques dans le secteur de la santé (SoinsSantéCAN 2018a). En s'inspirant de la Stratégie nationale sur les infrastructures essentielles cautionnée par les gouvernements fédéral, provinciaux et territoriaux, les participants au sommet ont rédigé une déclaration d'engagement commun pour la cybersécurité, laquelle comprend les six actions concrètes suivantes qui visent à accroître le degré de préparation :

- *Plaider en faveur* de la cybersécurité dans le système de santé du Canada;
- *Contribuer aux plans d'action communs* qui créent la résilience collective aux cyberattaques;
- *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;
- *Informer* les dirigeants, employés et partenaires de l'étendue du défi et des possibilités d'atténuer le risque;

- *Assurer la progression de la cybersécurité de manière cohérente avec le mandat de chacun des signataires* et tenir compte des occasions de prévention, d'atténuation, de préparation, de réaction et de rétablissement;
- *Faire preuve de transparence* selon le contexte et les capacités de chacun des signataires, en confirmant les mesures prises pour concrétiser ces engagements dans ledit contexte et/ou auprès de la collectivité, et ce, dans le cadre du Mois de la sensibilité à la cybersécurité, en octobre 2018 (SoinsSantéCAN 2018b).

J'ai participé avec SoinsSantéCAN et ses nombreux partenaires à la rédaction de la *Déclaration*. Cet éditorial s'inscrit donc dans le cadre de mon engagement pour faire connaître les défis présents et signaler l'importance de gestes proactifs pour y faire face. Je vous invite tous et toutes à vous joindre à l'effort afin de rendre solides, sécuritaires et efficaces nos systèmes de santé et de recherche, et ce, pour le bien de ceux que nous desservons. Pour obtenir plus de renseignements sur la *Déclaration*, sur la façon de contribuer à l'effort collectif ou sur une gamme de ressources en ce sens, veuillez consulter http://www.healthcarecan.ca/fr/ce-que-nous-faisons/politiques-en-sante/linfrastructure/.

Le besoin d'engagement commun et de soutien réciproque n'est pas le fief de la cybersécurité; la collaboration et l'effort collectif sont aussi importants pour produire une revue comme *Politiques de Santé/Healthcare Policy*. Puisqu'il s'agit du dernier numéro de ce volume, j'aimerais remercier l'équipe responsable de sa production. Le comité éditorial dirige l'orientation de la revue ainsi que le parcours des propositions d'article. Le comité travaille étroitement avec les évaluateurs qui offrent bénévolement leur temps afin d'assurer la qualité supérieure des articles que nous publions (consulter la liste des évaluateurs pour l'année écoulée à la page 84). Le comité et les évaluateurs interagissent directement avec Ania Bogacka, directrice de rédaction, et avec l'équipe de Longwoods Publishing qui œuvre à la production et à la distribution de la revue. Et, bien sûr, une revue scientifique comme la nôtre dépend de la créativité et du travail des auteurs qui publient dans nos pages.

Mes sincères remerciements à ceux et celles qui y travaillent, de même qu'aux lecteurs et lectrices qui réfléchissent aux façons d'utiliser les pistes publiées ici afin de continuer à améliorer la santé et les soins.

JENNIFER ZELMER, PhD
Rédactrice en chef

Références

Association médicale mondiale (AMM). 2016. *Prise de position de l'AMM sur les attaques cybernétiques des infrastructures de santé et autres infrastructures essentielles : adoptée par la 67e AMM, Taipei, Taiwan, octobre 2016*. Consulté le 20 mai 2018. <https://www.wma.net/fr/policies-post/prise-de-position-de-lamm-sur-les-attaques-cybernetiques-des-infrastructures-de-sante-et-autres-infrastructures-essentielles/>.

CBC News. 7 juin 2016. "University of Calgary Paid $20K in Ransomware Attack: No Evidence Cyberattackers Released Personal or University Data to Public." Consulté le 20 mai 2018. <http://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979>.

Moens, A., S. Cushing et A.W. Dowd. 2015. "Cybersecurity Challenges for Canada and the United States." Consulté le 20 mai 2018. <https://www.fraserinstitute.org/sites/default/files/cybersecurity-challenges-for-canada-and-the-united-states.pdf>.

SoinsSantéCAN. 2018a. *Declaration of Commitment to Cybersafe Healthcare: Options for Strengthening Cybersecurity in Canada's Health Sector*. Consulté le 20 mai 2018. <http://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/Cyber%20Security/Options%20Brief%20Summit%20Report.pdf>.

SoinsSantéCAN. 2018b. *Déclaration d'engagement pour les soins de santé cybersécuritaires*. Consulté le 20 mai 2018. <http://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/Cyber%20Security/Declaration%20of%20commitment%20cybersafe_fr.pdf>.

Zelmer, J. 2018. *Issue Brief: Critical Infrastructure in Canada's Health Sector – Part B: A Focus on Cybersecurity*. Consulté le 20 mai 2018. <http://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/IssueBriefs/2017/EN/IssueBrief_CriticalInfrastructure_B.pdf>.