HealthCare*CAN* Leading. Innovation. Together. SoinsSanté*CAN* Leadership. Innovation. Collaboration.

Building a National Standard for Cyber Resiliency in Healthcare

OVERVIEW

Virtual health, telemedicine, smart medical devices, and electronic health records are just a few concrete examples of how digital transformation in healthcare is reshaping our healthcare system for the better. Yet, as healthcare becomes increasingly digitized, automated and connected, exposure to cyber threats is a growing concern.

Cyber criminals continue to take advantage of increased vulnerabilities due to remote work and pressure facing critical sectors to target healthcare institutions with ransom payment demands. The Canadian Centre for Cyber Security reported 235 ransomware attacks against Canadian organizations between January and November 16, 2021. According to the centre, more than half of the victims were in critical sectors such as healthcare, but because only the largest attacks make headlines, federal authorities lack data on the actual scale of the threat.[1]

[1] Global News, Canadian health, energy sectors increasingly targeted by ransomware attacks. https://globalnews.ca/news/8427930/canadian-health-energy-sectors-increasingly-targeted-by-ransomware-attacks/

In an age of increasing reliance on digital systems, healthcare organizations must maintain a high level of confidence in their ability to respond to cyber threats. Through ongoing consultation with HealthCare*CAN* members and strong working relationships with Public Safety Canada, Health Canada, and the Public Health Agency of Canada, HealthCare*CAN*'s advocacy work in the area of cybersecurity has focused on:

- Raising awareness of cybersecurity threats in the healthcare sector;
- Increasing resources for capacity building;
- Developing national standards for cybersecurity in healthcare organizations[2].

While HealthCare*CAN* continues to advocate for greater attention and investment in cybersecurity in the healthcare sector, the lack of clear standards has been recognized as a barrier to achieving cyber resilience in facilities across Canada. To correct this, HealthCare*CAN* is working with the CIO Strategy Council with support from Public Safety Canada's Cyber Security Cooperation Program to:

- Develop a new set of standards to support cyber resilience in Canada's healthcare system, and;
- Facilitate information sharing opportunities targeting healthcare staff providing direct care.

A clear framework and enhanced cybersecurity capabilities will better protect Canada's healthcare organizations from cybercrime and allow them to more effectively respond to evolving threats and defend critical infrastructure.

UNDERSTANDING THE CYBER THREAT LANDSCAPE

As the national voice of healthcare organizations and hospitals across Canada, HealthCare*CAN* continues to successfully convene key partners and stakeholders to discuss the evolving cyber threat landscape for Canada's healthcare organizations. HealthCare*CAN*'s efforts focus on:

- Increasing understanding the current and evolving cyber threat landscape in Canada's healthcare system;
- Enhancing opportunities to enhance cyber resilience and mitigate risk for healthcare organizations;
- Analysing current prevention and mitigation initiatives underway in Canada.

Use of information and communication technology is growing rapidly in the health sector. While a basic level of security awareness and assessment is recognized as essential, the degree of preparedness varies widely across the health sector. Meanwhile, many organizations report experiencing cyberattacks of various types on a regular basis.

The current landscape suggests that healthcare organizations are highly vulnerable to cyber attacks and data suggests that the health sector is increasingly valued as a target because of several key factors:

- Personal information;
- Financial resources;
- High profile and impact;
- Pandemic-related pressure[3].

[2] HealthCare*CAN*, COVID-19 and Cybersecurity: Cyber Criminals not Deterred by Lockdowns. https://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/PolicyDocs/2020/HCC/EN/PolicyBrief-COVIDCybersecurity_EN.pdf

[3] HealthCare*CAN*. Cybersafe Healthcare: Options for Strengthening Cybersecurity in Canada's Health Sector. https://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/Cyber%20Security/Options%20Brief%20Summit%20Report.pdf

Through extensive consultation with our members and other key stakeholders, HealthCare*CAN* has identified a number of opportunities to enhance cyber resilience. Chief among these recommendations is a commitment to fostering a culture of cybersecurity within Canada's healthcare system through consistent standards and taking a systematic approach to educate the health sector about cyber risks and their mitigation.

HEALTHCARE-SPECIFIC NEEDS IN DEVELOPING A NATIONAL STANDARD

Promoting resilient critical infrastructure requires the development of sector-specific national cybersecurity standards for healthcare organizations to address existing vulnerabilities and prepare for future incidents.

On March 9 and 10, 2022, HealthCare*CAN* and the CIO Strategy Council co-hosted a series of workshops in both official languages with the goal of acquiring feedback from healthcare technology leaders across the country on their concerns, issues and needs around cybersecurity. This feedback would inform the development of a National Standard for Cyber Resiliency in Healthcare in Canada.

The workshops included nearly 120 healthcare technology leaders from across Canada, including from HealthCare*CAN* member organizations. Participants were asked five key questions:

- What is your biggest area of concern if you become the target of a cyber attack?
- What is the biggest risk to the healthcare system today?
- What focus area(s) would you like to see included in a National Standard of Canada?
- What are the critical success factors regarding the development and implementation of a national standard for the cybersecurity of Canada's healthcare system?
- Does your organization currently use or is your organization looking to adopt a recognized information/cyber security standard?

Respondents participating in the workshops identified patient care, safety, protection of health information and the ability to ensure continuity of care as some of the most pressing areas of concern to participants. Those in attendance also felt that a Canada-wide, healthcare specific approach would be needed to address some of the most common risk factors to healthcare organizations, which include ransomware, legacy IT infrastructure, lack of funding, leadership commitment and standards.

As many organizations would require additional resources to implement such a program, participants felt that a tiered approach would ensure accessibility for all organizations within Canada's healthcare system. Participants emphasized the need for extensive training for frontline and clinical staff and supporting knowledge translation materials.

The final report from these focus groups can be found here.

CREATING A CULTURE OF CYBER HYGIENE

Extensive consultation with HealthCare*CAN* members, key partners and stakeholders suggests significant variation in the level of cyber resilience and preparedness among Canada's healthcare organizations. While a new set of established standards to support cyber resilience in Canada's healthcare system will ensure that healthcare organizations across Canada are consistently prepared, the development of knowledge translation materials will emphasize the importance of cyber hygiene to all staff, equipping them with the knowledge to avoid the most common and severe threats and enable them to respond when systems are breached.

In developing educational resources and knowledge translation materials, it will be important to consider various training formats and activities to keep individuals engaged and aware, including:

- Courses and training
- Practical exercises and simulations
- Videos, posters and flow charts
- Panel discussions, workshops and webinars
- Academic publication

Improving cyber hygiene is critical to ensuring that healthcare organizations can protect against security breaches and cyberattacks. The development of comprehensive education programs and resources on cybersecurity best practices, policies and procedures, will help to ensure that healthcare organizations across Canada are able to maintain a high level of confidence in their ability to respond to cyber threats.

NEXT STEPS

The CIO Strategy Council and HealthCare*CAN* are assembling a technical committee of select cybersecurity experts from private, public, government organizations, and HealthCare*CAN* member institutions to create the national standard on cyber resiliency in healthcare. HealthCare*CAN* and the CIO Strategy Council will also develop knowledge translation materials and initiate a campaign to educate providers at key events. HealthCare*CAN* members will be consulted during the development process and have opportunities to provide feedback on the standard and knowledge translation materials.

FOR MORE INFORMATION

If you have questions, feedback, or wish to discuss or get further involved, please contact:

Siri Chunduri
Policy and Research Analyst
schunduri@healthcarecan.ca

Jonathan Mitchell
Vice President – Research and Policy
jmitchell@healthcarecan.ca

Thank you to Claire Samuelson-Kiraly, Consultant, HealthCareCAN.