CIO STRATEGY COUNCIL

HealthCareCAN
Leading. Innovation. Together.

SoinsSantéCAN
Leadership. Innovation. Collaboration.

INITIAL WORKSHOP SUMMARY

CAN/CIOSC 118

Cyber Resiliency in Healthcare

March 30, 2022
OTTAWA, CANADA

Table of Contents

EXECUTIVE SUMMARY 3
METHODOLOGY 3
RESULTS 4
NEXT STEPS 5

EXECUTIVE SUMMARY

The CIO Strategy Council and Healthcare*CAN* hosted a series of 2 workshops on March 9th, 2022 (English) and March 10th, 2022 (French) with the goal of acquiring feedback from healthcare technology leaders across the country on their concerns, issues and needs around cyber security. This initial feedback would form the basis and starting point for CIO Strategy Council Technical Committee 5- Cyber security to develop the National Standard for Cyber Resiliency in Healthcare in Canada. The secondary goal of the workshops was to raise awareness about the project and solicit participation from the user group on the technical committee.

As healthcare has become more digitized, automated, and connected, exposure to cyber threats is a recognized and growing threat to public security and patient safety in Canada. Health leaders recognize that cybersecurity is a patient safety issue and that the sector possesses certain traits that make cyber risk mitigation in healthcare a particular challenge to be protected. Promoting resilient critical infrastructure requires the development of sector-specific national cybersecurity standards for healthcare organizations to address cybersecurity vulnerabilities in healthcare.

The workshops saw representation from nearly 120 healthcare technology leaders from across Canada, with a diverse representation of the sector and in both official languages. During the session the participants were given an introduction and background on the project and its objectives, then divided into breakout rooms to facilitate discussion around 5 pre-determined questions. Following the break-out rooms, participants were given instructions on next steps and notified that they could provide additional feedback, until March 30th, 2022.

METHODOLOGY

Canada's healthcare system has become a prime target for cyber-attacks. The added pressure on the healthcare system, legacy and antiquated systems used at frontline institutions and the value of the data held by these institutions has allowed for easy targets for bad actors. Risks today present not only at the corporate level (e.g., fraud, ransom) and the social level (e.g., unauthorized exposure of private health information leading to blackmail, identity theft or loss of public trust), but also at the point of care itself.

Data however is not the only high-value target for attackers. Should attackers be able to take over critical infrastructure, lives could be at risk. For patients in the hospital on life-saving equipment and those that are in need of surgeries or other procedures, the results would be severe.

In a recent article from the CBC, the attack on the Newfoundland and Labrador Healthcare system was described as the "worst in Canadian history" and states that "more than 400 hospitals in Canada and the United States have been subject to ransomware attacks since the beginning of the pandemic."

The emerging trend of healthcare services moving to "virtual" or "telemedicine" is another reason why cyber security in healthcare is becoming an ever-increasing critical issue. Unprotected or legacy systems are not only a risk for the patient, but for the direct healthcare provider as well. With more and more services being made available remotely every day, safeguards are required to ensure the safety of all participants.

With the challenges delivered from the pandemic, along with fervent pace of technology, now is the time for Canada to have an established national set of guidelines to ensure the protection of healthcare infrastructure and Canadian citizens.

To kick the project off effectively, the CIO Strategy Council and HealthCare*CAN* recognized that it was imperative to solicit feedback from the end users to inform project objectives, as well as ensure their needs and requirements were met. This information would act as the foundation of the project for the technical committee to develop the Standard.

Focus Group Objectives

- Identify unique "healthcare specific" threats
- Identify what needs to be included in a healthcare specific national Standard

RESULTS

Participants were asked 5 key questions and the results are as follows:

QUESTION 1: What is your biggest area of concern if you become a target of a Cyber Attack?

Results/Trends:

- Patient safety, patient care, and ability to continue care, was by far the biggest concern among participants.
- Continuity of operations – how to continue to offer care/services during, after and attack
- Incident Response – Many participants do not have an incident response plan or know what to do in case of an attack, as well as a lack of resources to deal with an attack when it happens.
- Protection of Personal Health Information – The loss of incredibly sensitive and important data and information could have severe ramifications on the facility e.g., ability to deliver care, reputation, financial.
- Understanding what has been lost – how to determine the severity of the attack and what has been lost or comprised.
- Effect on partners/other care providers – how an attack could have a ripple effect through the ecosystem.

QUESTION 2: What is the biggest risk to the healthcare system today?

Results/Trends:

- Ransomware
- Legacy IT systems and infrastructure
- Business Continuity/Incident response plan
- Lack of funding
- Lack of leadership commitment to address cyber security
- Availability of cyber insurance – Sector is moving into a “high-risk” classification resulting in some providers not willing to provide coverage.
- Lacking alignment between security and clinical workforce – Difficult to integrate cyber security with front line workers. Solution providers lack an understanding of the sector and regulatory requirements.
- Lack of standards – predominantly in virtual care, IT procurement, cyber security frameworks. Also noting there is no “Canada”-wide approach.
- Staff shortages

QUESTION 3: What focus area(s) would you like to see included in a National Standard of Canada?

Results/Trends:

- Medical equipment/devices –Healthcare has unique needs due to medical devices, and IoT/IIoT security.
- IT Procurement – Due to regulatory requirements there are long purchase cycle time of devices (10-15 years) resulting in a lot of legacy technology in the market.
- Cloud governance – not properly defined in healthcare.
- Definition of virtual care and remote monitoring standards.
- Canadian healthcare specific and consistent across Canada.

- Staff competency – Tools to assess qualifications of IT personal e.g. certifications or accreditations.
- Tiered approach – Based on organization size and care being delivered. A “one-size-fits-all” approach will not work, and must be affordable for all organizations.
- How to incorporate/use existing cyber security standards and frameworks.

QUESTION 4: What are the critical success factors regarding the development and implementation of a national standard for the cybersecurity of Canada’s healthcare system?

Results/Trends:

- Tiered approach – Based on organizational size and type of care being delivered. A “one-size-fits-all” approach will not work and adoption must be affordable for all organizations.
- Buy-in – Healthcare organizations and supporting vendors must be willing to adopt.
- Accreditation/Verification – There must be program(s) in place to ensure that organizations are being verified by a third-party to ensure they are following the requirements as stated by them.
- Available and accessible in both official languages
- Achievable and adoptable requirements
- Informative supporting material e.g., checklists, plans, other tools
- Training

QUESTION 5: Does your organization currently use or looking to adopt any recognized information/cyber security standard? (e.g., ISO 27001, NIST CSF, Cybersecure Canada, Other)

Results/Trends:

Currently adopted frameworks and standards (Note: these have typically either been adopted by provinces or larger organizations)

- NIST Cyber security Framework
- ISO 27001
- CIS Controls
- Cybersecure Canada
- AICPA SOC2

Key Takeaways:

- Patient care and the ability to continue care is the paramount concern
- Approach must be tiered and accessible for all organizations in the ecosystem
- Strong need to address legacy systems
- Training and the ability to integrate security requirements into existing standard operating procedures is extremely important
- Most organizations will require additional resources to implement a program
- A Canada-wide, healthcare specific approach is needed.

NEXT STEPS

Work has commenced on drafting the seed document for Technical Committee review and this report will act as a strong input into that process. It should also be noted that contributions, submissions, and the ability to join the technical committee is open throughout the life of the project andstakeholders can engage at anytime.