A Shared Commitment to Cybersecurity

Jennifer Zelmer

President, Azimuth Health Group, Toronto, ON

Charles Thompson

Research and Policy Analyst, HealthCareCAN, Ottawa, ON

Patient safety today depends on cybersecurity, but readiness varies across Canada's health sector. The increasingly digitized and networked landscape is core to a modern, responsive, and resilient healthcare system. For instance, electronic data exchange and virtual care can be a source of resilience in the face of natural disasters or other emergencies, facilitating access to care even when local critical infrastructure is disrupted or overwhelmed. It is also the backbone of a broad range of everyday health services. As a result, when digital services are interrupted, patient care is affected.

Why is cybersecurity a large and growing concern for the health sector? Health authorities, hospitals, long term care facilities, and other organizations hold information about patients and employees that are sensitive, valuable, and easily commercialized. A small army of employees, clinicians, and increasingly patients/clients need to have access to this information. This information is viewed and shared between users via a growing number of connected devices, which may or may not have been designed with built-in security provisions. Health organizations also tend to have substantial financial resources and are large employers with significant payroll. They often have a high profile within their communities, and may make decisions that people disagree with and wish to react to. These factors in combination make the health sector a target for cyber attacks.

These risks are real, not theoretical. Experts stress that the healthcare sector will be a focal point for cyber attacks in the future, and that these attacks will likely increase in number and sophistication in the years to come. HealthCare*CAN* surveys fielded shortly after the widely-publicized May 2017 WannaCry ransomware attacks found that more than 8 in 10 health leaders and Canadians believe that Canada's health sector is vulnerable to cyberattacks. Likewise, 86% of HealthCare*CAN* members say that their organization has detected a breach or narrowly avoided an incident, typically minor or moderate in scale. According to public reports, Canadian organizations have been affected by malware, denial of service attacks, phishing, cyberfraud, and other cyber risks.

These risks need to be faced proactively. Cybersecurity decision-making requires a deep understanding of threats and vulnerabilities, as well as the likelihood and potential impact of security breaches. To enhance preparedness and mitigate risk, we need to identify capabilities and risks, detect incidents, respond quickly, and be in a position to recover normal operations swiftly following an incident.

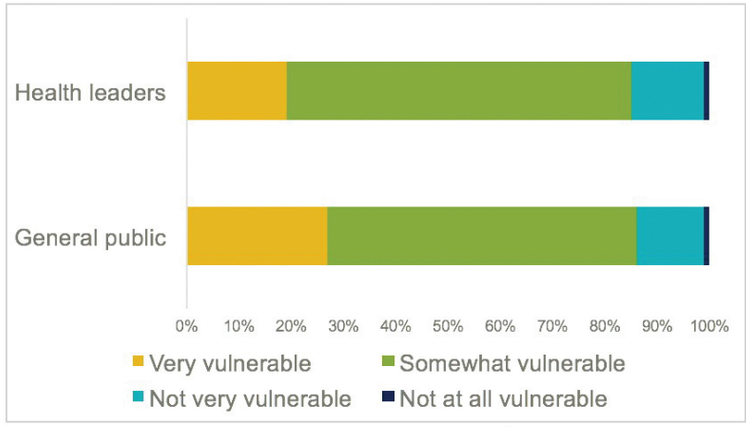
Earlier this year, HealthCare*CAN* issued a call to action to address strengthen cybersecurity preparedness in Canadian healthcare. We invite you to join us a growing list of organizations in a collective *Declaration of Commitment to Cybersafe Healthcare* to be launched this summer, as the first step in a shared effort to improve cybersecurity resilience in Canada's health sector.

Advance planning is imperative; the worst possible time to develop a strategy is during an attack. *Declaration* signatories recognize the importance and urgency of protecting critical infrastructure systems and data against cyber threats in Canadian health care organizations. Our approach is consistent with the National Strategy for Critical Infrastructure endorsed by federal, provincial, and territorial governments, as well as Canada's Action Plan for Critical Infrastructure.

There is much that individual organizations can do, and there is much that collective, collaborative action can achieve. Together, signatories commit

MORE THAN 8 IN 10 HEALTH LEADERS & CANADIANS SAY THE HEALTH SECTOR IS VULNERABLE TO CYBERATTACKS

Source: 2017 Ipsos online surveys of HealthcareCAN & CCHL Members and of Canadian adults



> *"...when digital services are interrupted, patient care is affected."*

to taking six steps to increase cybersecurity preparedness and resiliency:

1) Champion: Championing cybersafety in Canada's health sector;
2) Inform: Ensuring that leaders, staff, and partners are informed about the scope of the challenge and opportunities to mitigate risk;
3) Contribute: Contributing to shared action plans that build collective resilience to cyberattacks;
4) Advance: Progressing cybersafety in ways consistent with our mandate, considering opportunities for prevention, mitigation, preparedness, response, and recovery;
5) Share: Sharing information, best practices, and tools with others within and beyond the health sector to build collective capacity and resilience; and
6) Transparency: As each organization's circumstances and capacity are unique, we will confirm by Cybersecurity Awareness Month in October 2018 how we will apply these commitments in our unique context and/or with our community.

Whether you're working in a public, not-for-profit or private organization, we encourage you to be part of this collective effort to foster a robust, safe, and effective health system that benefits the individuals and communities that we serve. The *Declaration* is intended as the cornerstone for a coalition that will jointly pursue education, standardization, information sharing, and other hallmarks of cyber resilience.

For More Information

- Visit http://www.healthcarecan.ca/what-we-do/health-policy/infrastructure/ for the full text of the Declaration, more information about how to join the Coalition for Cybersecurity in Healthcare, and links to cybersecurity resources.
- Digital Health Canada's eSafety Community of Action: https://digitalhealthcanada.com/esafety/

e-Health 2018 IN THE SPOTLIGHT

Digital Health: A Launchpad to the Moon + Mars

Notes from "Driving the Future of Digital Health", October 30, 2017

The popular Space Panel from the Digital Health Canada "Driving the Future of Digital Health" Conference on October 30, 2017 will reconvene at e-Health 2018 Conference and Tradeshow Monday afternoon plenary session on Monday, May 28, 2018 from 1:30 pm – 3:00 pm. The panel features Dr. Robert Thirsk, Chancellor, University of Calgary and former astronaut, Canadian Space Agency; Isabelle Tremblay, Director, Astronauts, Life Science and Space Medicine, Canadian Space Agency; and Dr. Sonny Kohli, Physician in Internal Medicine & Critical Car, Founder, CloudDX, and finalist of the Qualcomm Tricorder XPRIZE.

Notes from "Driving the Future of Digital Health"

Dr. Thirsk noted that an anniversary approached, as November 2 was the first date humans inhabited the International Space Station (ISS), and that people have been in space uninterrupted since 2000.

The unique health challenges of space travel

The health challenges faced by the people aboard the ISS are unique, and include the effects of a new and harsher environment, where everything works against the body. Cardiovascular health is of prime importance, as the walls of the heart thin and the muscle itself becomes deconditioned with prolonged periods in space. Second to cardiovascular health is bone condition, as the absence of gravity causes bones to demineralize. Ocular and mental health are also affected, and landed astronauts require regular post-mission monitoring.