Cybersafe Healthcare

Options for strengthening cybersecurity in Canada's health sector

February 2018

This report is over 5 years old and may contain out-of-date information

HealthCareCAN
Leading. Innovation. Together.

TABLE OF CONTENTS

INTRO

Pages 3–6

01 Current State

Pages 7–23

+ *Global: Current State of Cybersecurity in Health*
+ *Canada: Current State of Cybersecurity in Health*

02 Cyber Resilience

Pages 24–29

+ *Public Safety Canada recommendations*
+ *Asset map of multi-jurisdictional activities*
+ *Actions taken by health care organizations*

03 We Commit

Pages 30-35

+ *Declaration on cybersecurity in Canadian healthcare*

04 Moving Further

Pages 36-40

+ *Prompts for a dialogue regarding options for further strengthening cybersecurity*

"The great boon of the digital era has been that patients' medical data is becoming increasingly portable. This promises to make it vastly easier to collect and share data from all the players in health care in the years ahead. But, unfortunately, it also poses major cybersecurity risks.

- Rebecca Weintraub & Joram Borenstein, writing in Harvard Business Review, June 2017 (LINK)

IN THE 21ST CENTURY, SAFE CARE DEPENDS ON CYBER SAFETY

Cyber attacks have the potential to disrupt many, perhaps most, safety-critical systems in the health sector.

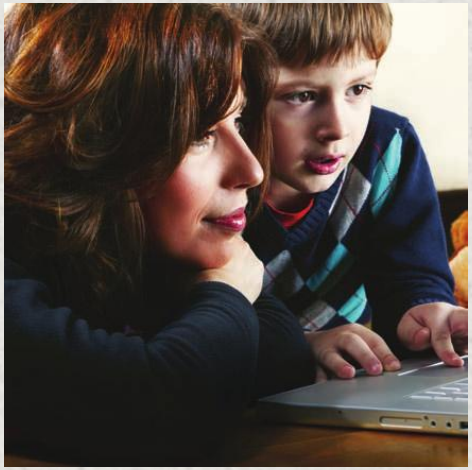
Digital solutions are increasingly common in healthcare. For example, electricity powers the lights in a clinic and the computers that help prescribers track the medications that their patients are taking. Medical devices provide critical life support and deliver chemotherapy; digital solutions enable clinicians to communicate with their patients and with their colleagues; and public health tools track the spread of outbreaks.

These tools and many others rely on reliable networked digital infrastructure. The more we rely on digital solutions, the more vulnerable we could be if they fail.

At the same time, it is important to remember that electronic systems can be a source of resilience for health sector critical infrastructure.

For instance, electronic data sharing and virtual care services can facilitate access to care even when local physical services are disrupted.

> ***Cyber attacks*** *include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate, and/or store that information. The severity of the cyberattack determines the appropriate level of response and/or mitigation measures, i.e.* ***cybersecurity****."*
>
> – *Canada's Cyber Security Strategy (LINK)*



Canada's Cyber Security Strategy

FOR A STRONGER AND MORE PROSPEROUS CANADA

ABOUT THIS BRIEF: OUR APPROACH & KEY INPUTS

The number, significance, and complexity of cyberattacks is increasing, both in Canada and around the world. This Options Brief is intended to prompt discussion of how we can increase the collective resilience of the Canadians health sector's critical infrastructure to cyber attacks. Its preparation was informed by a number of key inputs.

Preparation of this *Options Brief* was overseen by a *HealthCareCAN* Steering Committee formed to guide the development and implementation of a Health Sector Critical Infrastructure Network under the auspices of Canada's National Strategy for Critical Infrastructure. It was made possible by funding from Public Safety Canada.

The Brief is designed to complement previously published *Issue Brie*fs that provide overviews of critical infrastructure and cybersecurity considerations for Canada's health sector.

A **rapid review of the literature** on critical infrastructure in the health sector, with a focus on cybersecurity

Key informant interviews with health sector leaders, authorities on critical infrastructure and emergency preparedness, and cyber-security experts in Canada and other countries

Online surveys

(1) *HealthCareCAN* members conducted between November 2016 and February 2017 (24 responses for a response rate of 46%)

(2) *HealthCareCAN* and Canadian College of Health Leaders members conducted between May 17th and 26th, 2017 (227 responses)

(3) Adults living in Canada's provinces conducted between May 19th and 23rd, 2017 (n=1005)

An **asset map** of activities underway or planned with a focus on those undertaken by organizations with a pan-Canadian and/or cross-jurisdictional mandate to promote resilience in the face of cyber-security threats

Input from Cyber Security Summit held in February 2018 to bring together health sector and security experts from across Canada and beyond.

1a

GLOBAL

CURRENT STATE OF
CYBERSECURITY IN HEALTH

A GLOBAL CHALLENGE

Canadian health organizations are not alone in experiencing cyberattacks, as recent high-profile ransomware attacks that affected global health services demonstrate.

Some cybersecurity groups predict that healthcare sector will be a key focal point for cyber attacks in the coming year, with increasingly sophisticated attacks emerging.

"As attackers shift their focus, an increase in hospital breaches means the consequences for healthcare organizations that don't properly manage this risk will increase. Healthcare organizations of all sizes and types need to ensure they have proper, up to date security measures in place, including contingency planning for how to respond to a ransomware attack and adequate employee training about the importance of security." – Experian 2017 Fourth Annual Data Breach Industry Forecast

"Information governance - covering areas of privacy, confidentiality, security and informed consent - is becoming a defining issue of our times. In a global environment, the current complex sets of national laws and regulations are not enough to prevent the sale of health-search information, the exposure of health and other personal data online, and concerns over cybersecurity of medical devices and hospital networks."

World Health Organization ~ www.who.int/ehealth/programmes/governance/en/

WORLD MEDICAL ASSOCIATION STATEMENT ON CYBER-ATTACKS ON HEALTH AND OTHER CRITICAL INFRASTRUCTURE

Adopted by the World Medical Assembly in October 2016 (LINK)

"The WMA [World Medical Assembly] recognises that cyber-attacks on healthcare systems and other critical infrastructure represent a cross-border issue and a threat to public health." – *World Medical Assembly, 2016*

In October 2016, the World Medical Assembly recognized the importance of cybersecurity in healthcare. On a global basis, they noted that "current security procedures and strategies in the healthcare sector have generally not kept pace with the volume and magnitude of cyber-attacks."

The Assembly also came to consensus on seven recommendations to address this issue, ranging from improving awareness and education to implementing comprehensive systems for prevention of, and response to, cyber attacks.

HEALTH CYBERSECURITY IN THE UNITED STATES

In the United States, more than one health data breach per day was reported to the Department of Health and Human Services or in the media in 2016. These breaches affected more than 27 million patient records. Two in five of the breaches (42%) were the result of actions by insiders, about evenly split between those that resulted from human-error and those caused by wrong-doing.

A recent report by the Health Care Industry Cybersecurity Task Force, a group established by the *Cybersecurity Act of 2015*, identified a number of key challenges including:

- Shortage of security talent
- Legacy equipment and operating systems
- Premature/over-connectivity
- Vulnerabilities impacting patient care
- Large number of known vulnerabilities

The health care system cannot deliver effective and safe care without deeper digital connectivity…. Our nation must find a way to prevent our patients from being forced to choose between connectivity and security. - Health Care Industry Cybersecurity Task Force

HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE IMPERATIVES FOR IMPROVEMENT (US)

The 2017 report of this Task Force provided detailed recommendations to strengthen cybersecurity, organized according to the 6 imperatives listed below. LINK

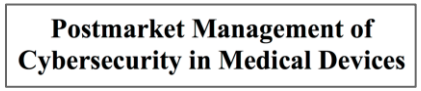
1. "Define and streamline leadership, governance, and expectations for health care industry cybersecurity
2. Increase the security and resilience of medical devices and health IT
3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities
4. Increase health care industry readiness through improved cybersecurity awareness and education
5. Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure
6. Improve information sharing of industry threats, weaknesses, and mitigations"

"Members of the health care industry report that without experiencing a breach or data loss, many security professionals and organizations have difficulty demonstrating the importance of cyber protections and how proactive risk mitigation can save money and protect against reputational damage in the long- term." - *Health Care Industry Cybersecurity Task Force*

OTHER US INITIATIVES RELATED TO STRENGTHENING CYBERSECURITY IN THE HEALTH SECTOR

Various federal government and non-government organizations have developed resources, regulatory tools, programs, and services that aim to strengthen cybersecurity in the health sector. Examples are shown below.

Healthcare Sector Cybersecurity Framework Implementation Guide, HITRUST More…



Food and Drug Administration guidance on post-market management of cybersecurity in medical devices More…

Critical Infrastructure Cyber Community or C³ (pronounced "C Cubed") Voluntary Program, including a cyber resilience self-assessment package More…

The American Hospital Association's Cybersecurity and Hospitals series: Questions Hospital Leaders Should Ask and What Hospital Trustees Need to Know

STRENGTHENING CYBERSECURITY ACROSS THE NATIONAL HEALTH SERVICE

The spring 2017 WannaCry ransomware attacks affected a number of NHS organizations that had unpatched or unsupported Windows operating systems. The National Audit Office (NAO) found that the attack led to disruptions in at least 34% of NHS trusts in England. Patients had thousands of appointments and operations cancelled and in five areas they had to travel further for emergency services. The NAO deemed these outcomes avoidable.

In addition to immediate actions taken to address issues related to the attacks, lessons learned reviews have led to a number of broader commitments, such as :

- **Standards:** Embedding requirements for local organisations to implement data security standards in the NHS Standard Contract;
- **Inspection**: Including the importance of meeting data security standards in the Care Quality Commission's inspection framework;
- **Transparency**: Requiring Chief Executive Officers to prepare an annual 'statement of resilience' confirming essential action being taken;
- **Reporting Attacks:** Compelling health and care organizations to report significant cyber attacks to a central body (CareCERT) as soon as possible following detection; and
- **Resources:** Investing in data and cybersecurity, with an initial £21 million of targeted capital funding;

"Only by leading cultural change and backing organisations to drive up security standards across the health and social care system can we build the resilience the NHS needs in the face of a global threat."– Health Minister Lord O'Shaughnessy

NATIONAL HEALTH SERVICE
2017/18 DATA SECURITY REQUIREMENTS

Steps that all health and social care organizations must take in 2017/18 to implement the data security standards. There are related requirements for general practices. LINK

Named senior executive responsible for data and cyber security

Measure progress using steps outlined in an Information Governance toolkit

Complete a process to ensure compliance with new May 2018 legal data protection obligations

All staff to complete annual data security and protection training

Act on CareCERT advisories, including confirming plans within 48 hours for High Severity advisories

Comprehensive business and continuity plan

Report data security incidents to CareCERT

Identify unsupported systems and have a plan to mitigate or manage risks

Participate in on-site cyber and data security assessments if invited by NHS Digital and act on outcomes

Ensure that IT suppliers and systems have appropriate certification

A FOCUS ON HEALTH CYBERSECURITY IN AUSTRALIA

As in other countries, Australian healthcare organizations have experienced a range of cyber incidents that have affected the operations of health services.

Australia's Digital Health Cyber Security Centre was established "to support secure operation of national digital health systems, and protection for Australian personal health information that is stored and transacted through the Australian Digital Health Agency." It also has a goal of raising security awareness and maturity across the country's digital health ecosystem. Its work focuses across the continuum of:

- ***Partnerships*** for proactively gathering information about cyber security threats;
- ***Securing*** national digital health services and systems;
- ***Informing*** the sector with guidance about cyber threats and mitigation strategies; and
- ***Responding*** in a coordinated way to cyber incidents related to national digital health systems or services.

Likewise, a 2017 audit by the Australian National Audit Office found that the Commonwealth Department of Human Services had achieved "cyber resiliency" (i.e. it had demonstrated "the ability to continue providing services while deterring and responding to cyber attacks").

"Cyber security is not simply a technology challenge. It is also a cultural challenge and one that extends beyond traditional information security practices.". - Enabling Australia's Digital Future: Cybersecurity Trends and Implications

1b

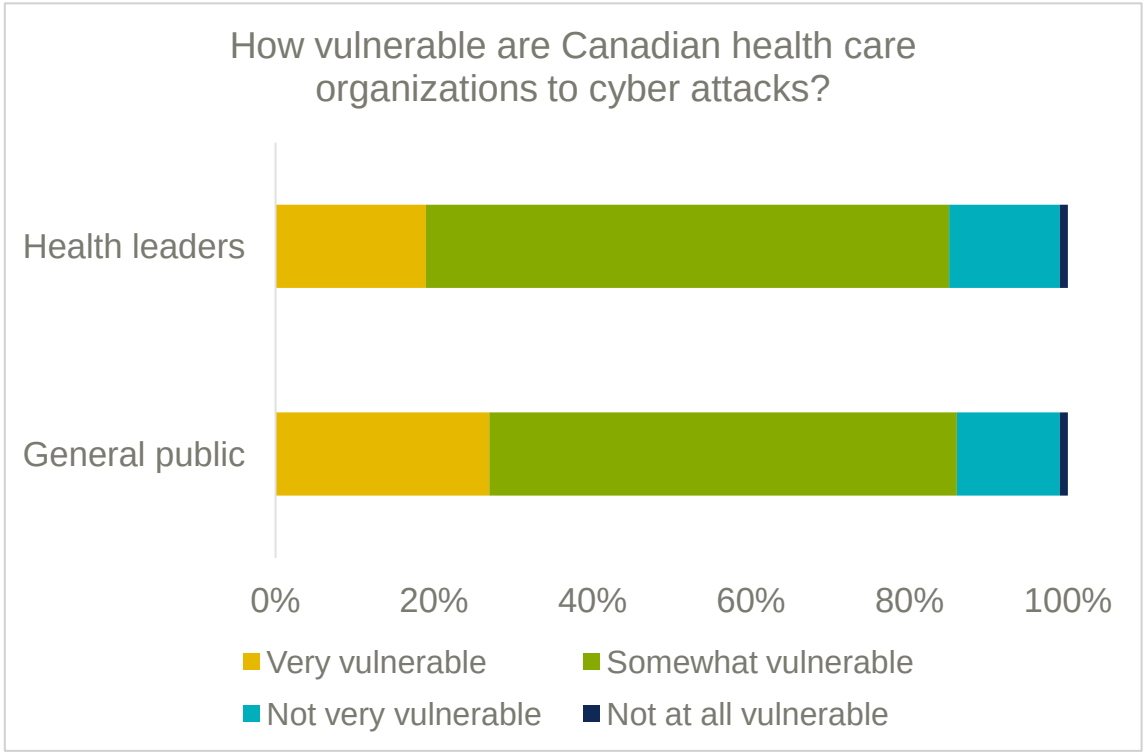
CANADA

CURRENT STATE OF
CYBERSECURITY IN HEALTH

CYBER ATTACKS ARE FREQUENT IN THE HEALTH SECTOR

In surveys which fielded shortly after the May 2017 WannaCry ransomware attacks, more than 8 in 10 health leaders and Canadians said that Canada's health sector is vulnerable to cyberattacks. Likewise, **86% HealthCareCAN members say that their organization has detected a breach or narrowly avoided incident**, typically minor or moderate in scale.

Many organizations report that their firewalls routinely detect probes for vulnerabilities that are handled on a routine basis. For instance, one organization we spoke with reported millions of attacks annually. Most were minor and readily addressed by existing safeguards, but the organization described its overall cybersecurity risk as "manageable but significant."



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

HEALTHCARE PROVIDERS VIEWS: 2018 SURVEY IN US & CANADA

Source: Losing the Cyber Culture War in Healthcare: Accenture 2018 Healthcare Workforce Survey on Cybersecurity (n=601 providers and 311 payers; survey in November 2017) *LINK*

29%

of healthcare employees are aware of someone within their organization selling access to patient data

21%

of healthcare providers said that they were willing to make a profit by providing unauthorized outsider access to confidential data

47%

of healthcare providers say that they are aware of patient data breaches in their organization

1 in 6

are unaware of cybersecurity training or it is not offered at their organization

WHY HEALTHCARE MAY BE A TARGET FOR CYBER ATTACKS

In addition to random attacks, there are a variety of reasons why healthcare organizations may face cybersecurity risks.

Financial Resources

Many health organizations have substantial financial resources and are large employers with significant payroll

Profile of Decisions

Health organizations often have a high profile and may make decisions that people disagree with and wish to react to

Personal Information

Health organizations hold information about patients and employees that can be valuable and some types of health information have enduring value

# of Access Points

Large numbers of employees, affiliated clinicians, and increasingly patients/clients need to have access to sensitive information, which means that there are many potential targets for attacks such as phishing. There are also increasing numbers of connected medical devices.

Critical Infrastructure

There is potential for disruption of critical infrastructure and services

EXAMPLES OF CYBER RISKS IN CANADIAN HEALTHCARE

Multiple healthcare organizations reported the types of cyber risks described below.

Malware, spyware, ransomware: Code with malicious intent (e.g. viruses or worms) that may steal or destroy data.

For example, malware designed to exploit a Windows XP and 2003 vulnerability led to temporary loss of systems at a hospital. Some servers and systems had to be replaced. More…

Phishing or cyberfraud: When instructions in emails or other communications are followed (e.g. a link is clicked), they may provide access to a computer system or activate malicious functions.

For instance, hackers using a phishing attack accessed hospital payroll files and made 'significant' transactions. More…

Denial of service attacks which overload a network or website with a high volume of data or traffic in an attempt to incapacitate or otherwise disrupt it.

For example, a software application running an automated task booked false Canadian Blood Services appointments to donate blood. The net impact was a temporary reduction in collections. More…

Hacking and similar attacks in which systems, websites, and/or networks are targeted for malicious purposes.

For example, hackers modified a healthcare organization's website to redirect job applicants to a site where they were asked to pay to process their job applications. More…

Human error affecting critical systems which may be inadvertent or unintentional.

For instance, one health care organization reported serious disruption when someone inadvertently plugged a Voice Over Internet Protocol (VOIP) phone into a jack not wired for the service. More…

EVOLVING CYBERSECURITY RISKS AND RESPONSES: WHAT WE HEARD VIA KEY INFORMANT INTERVIEWS

Many health leaders emphasized the evolving risk environment that they face. For example, one of the key informants with whom we spoke stated:

"More people are using more systems in a more sophisticated way in more places on more different devices. The threat is evolving. The attacks are fast-growing."

The importance of a strategic, long-term approach based on a sound understanding of risks and opportunities emerged clearly from these discussions.

In considering serious cyber events, the focus may need to be on business continuity and disaster recovery. At the same time, as one Chief Information Officer we spoke with said, on a day-to-day basis,

"We need to balance good access to information and security, not become the department of saying 'no'."

Key themes from key informant interviews are summarized on the following slide. For details, see the Appendix.

COMMON THEMES FROM KEY INFORMANT INTERVIEWS

Use of information and communication technology, including connected medical devices, is growing rapidly in the health sector

Cybersecurity is on the radar for most but not all organizations

Baseline levels of security awareness and assessment are important

Many organizations report experiencing cyberattacks of various types on a regular basis, most of which are detected and prevented

The degree of preparedness varies widely across the health sector and there are limited standard requirements in place

Resourcing cybersecurity initiatives is a challenge

Cybersecurity is not a core competency for most health care providers and organizations

"Critically for us, our biggest vulnerabilities are not in the hardware but in the applications. A lot of the critical applications that we run are basically either obsolete or very close to obsolete."

02

CYBER RESILIENCE

PUBLIC SAFETY CANADA RECOMMENDATIONS & LIST OF 4 SAFEGUARDS THAT PREVENT MOST CYBER PROBLEMS

Focus on raising security awareness, defining roles and responsibilities, developing policies and standards, establishing a cybersecurity plan, and budgeting for cybersecurity. *(LINK)*

Application whitelisting to allow only identified programs to execute on a given system

01

Use of modern operating systems and applications, including a life-cycle approach to migrate to newer versions of systems/programs

02

Patching operating systems and applications within two days of a high-risk vulnerability being made public

03

Restricting administrative privileges

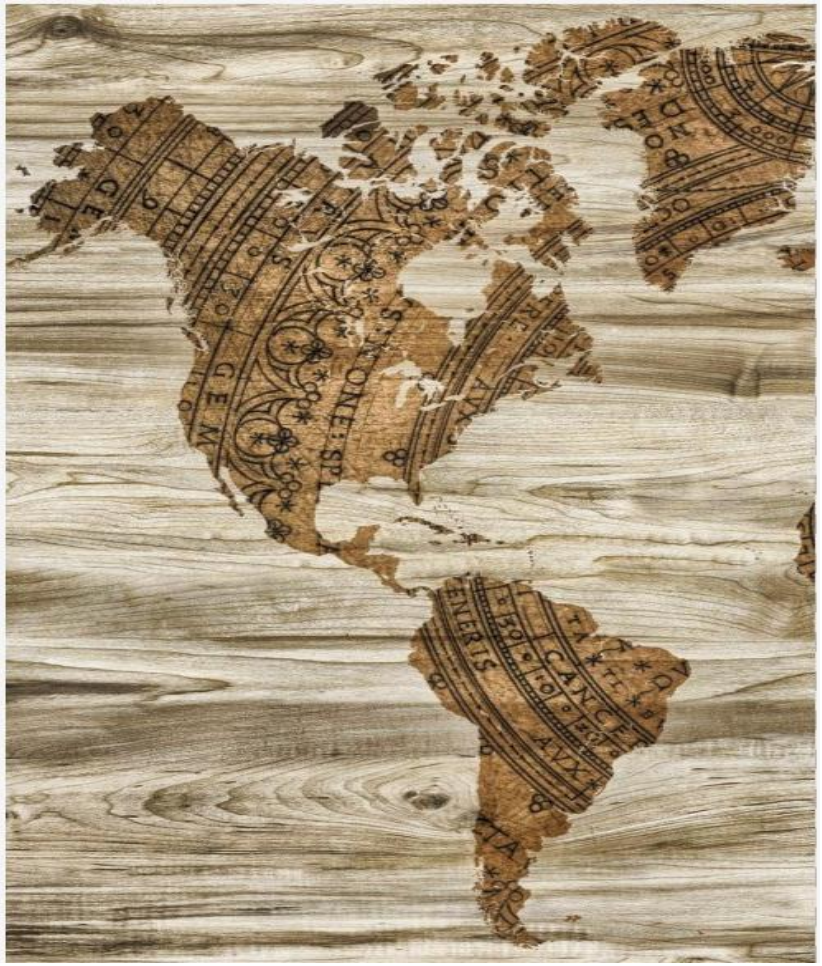
04

MAPPING OUR ASSETS: THE PROCESS

Strengthening the cyber-resilience of Canada's health sector will require a collective effort by many organizations and groups.

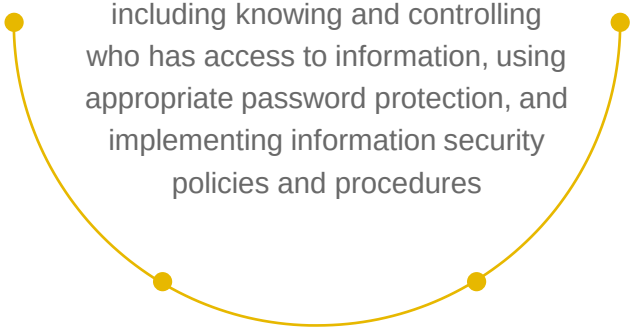
A number have already begun to move ahead. In 2017, *HealthcareCAN* asked more than 25 national and international organizations about their cybersecurity programs and activities. This effort built on earlier surveys of *HealthcareCAN* members across the country.

The results were organized into an asset map using the National Institute of Science and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*.



NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY'S FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

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, efforts are required along the continuum from identification of capabilities and risks to recovery. (LINK)



Identify

Identify capabilities and risks, including knowing and controlling who has access to information, using appropriate password protection, and implementing information security policies and procedures

Protect

Protect or contain the impact of a potential cybersecurity incident by limiting access to data and information, using and updating appropriate technical measures, encrypting sensitive information, educating staff, and similar safeguards

Recover

Recover normal operations following an information security incident

Detect

Detect incidents in a timely way by having appropriate mechanisms in place

Respond

Respond quickly to incidents thanks to advance preparations

MAPPING OUR ASSETS: THE RESULTS

Based on information obtained in the fall of 2017 from more than 25 national and international organizations regarding current or planned cybersecurity activities or programs. Results suggest wide but not necessarily deep engagement.

- **Varying focus:** Some organizations have comprehensive cybersecurity programs or initiatives. Others reported no activities currently underway.

- **Protecting pan-Canadian assets:** Both Canadian Blood Services and CIHI are using ISO/IEC 27001 standards as the basis for comprehensive information security management system. Similarly CPAC has established a privacy and security framework, as well as a risk-based audit plan and program. More…

- **Tracking:** HealthcareCAN has undertaken surveys that explore the attitudes, experiences, and initiatives of health care organizations and the general public.

- **Awareness/Education:** Several organizations – such as HealthcareCAN, ITAC Health, Infoway, Digital Health Canada, CIHR ,Public Safety Canada, and others – have launched initiatives and developed resources to increase awareness of the importance of cybersafety and how to foster it

- **Insurance:** Organizations such as HIROC and CMPA offer cyber coverage, as well as information about cyber incident prevention and post-incident risk management strategies.

- **Standards/Guidelines:** Health Canada establishing new digital health review division within Therapeutic Products Directorate's Medical Devices Bureau as of April 2018. Security requirements are an element of Infoway's certification requirements for digital health solutions.

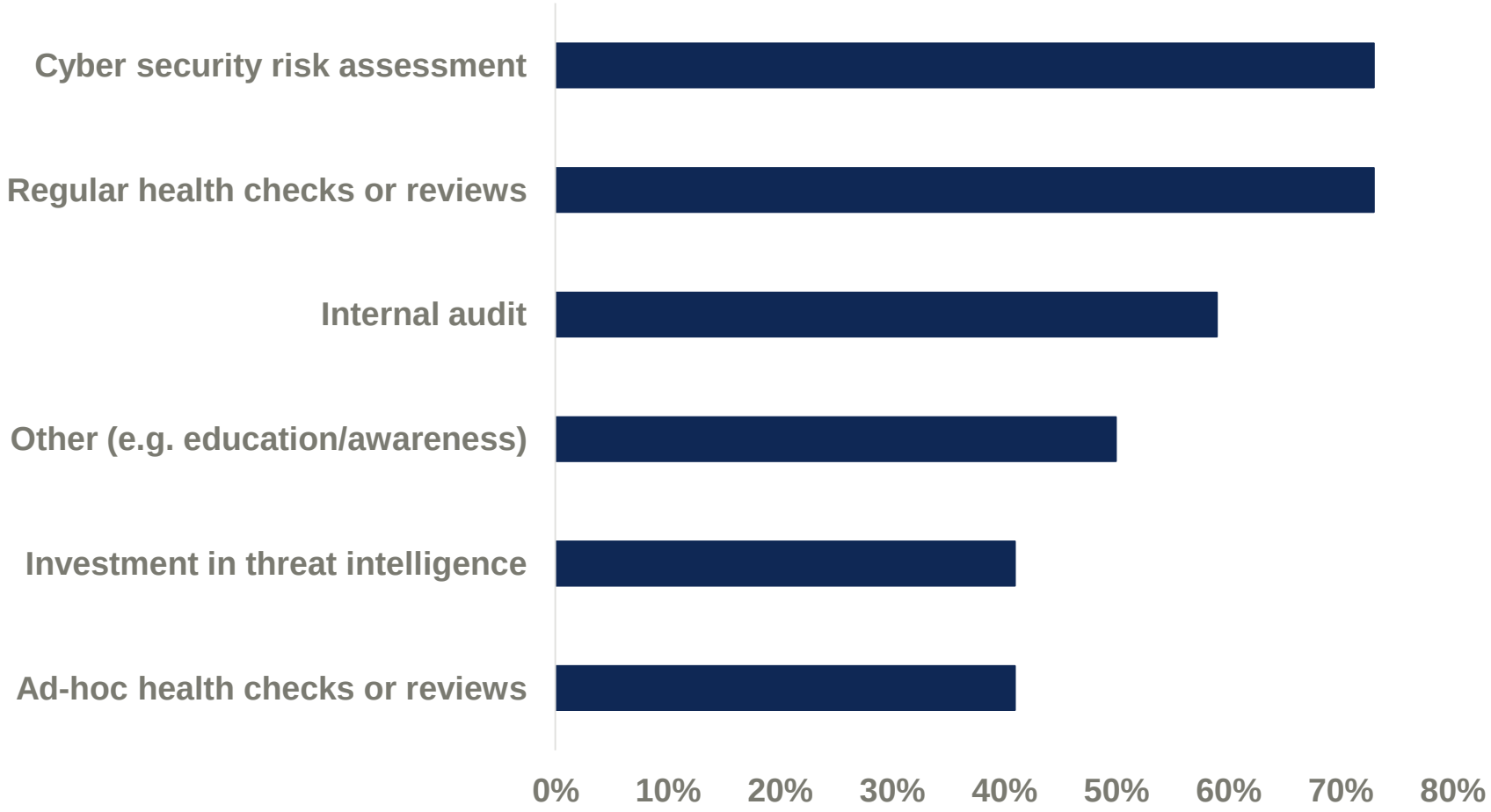
- **Convening/Sharing:** The Healthcare Critical Infrastructure and Cyber Security Steering Committee co-chaired by HealthcareCAN and PHAC provides a pan-Canadian focal point.

- **Cross-Sector Engagement:** Public Safety Canada leads pan-Canadian cross-sector efforts to strengthen cybersecurity. This includes the National Strategy for Critical Infrastructure, cyber-specific functional exercises, the cyber incident response centre, and the regional resilience assessment program.

These multi-jurisdictional activities are in addition to a range of strategies of varying scale put in place by specific organizations, regions, and jurisdictions.

% CANADIAN HEALTHCARE ORGANIZATIONS THAT REPORT TAKING SPECIFIC ACTIONS TO PREVENT CYBER ATTACKS

2016-17 Survey of HealthcareCAN Members (n=21 respondents)

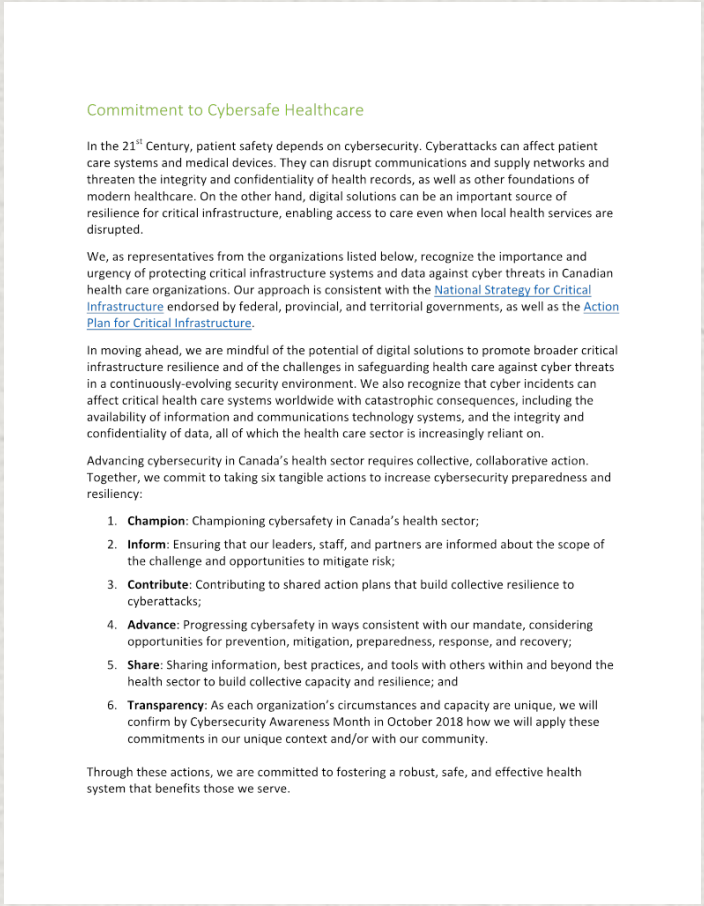


03

WE COMMIT

> *We 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 the Action Plan for Critical Infrastructure.*

– Declaration of Commitment to Cybersafe Healthcare



Commitment to Cybersafe Healthcare

In the 21st Century, patient safety depends on cybersecurity. Cyberattacks can affect patient care systems and medical devices. They can disrupt communications and supply networks and threaten the integrity and confidentiality of health records, as well as other foundations of modern healthcare. On the other hand, digital solutions can be an important source of resilience for critical infrastructure, enabling access to care even when local health services are disrupted.

We, as representatives from the organizations listed below, 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 the Action Plan for Critical Infrastructure.

In moving ahead, we are mindful of the potential of digital solutions to promote broader critical infrastructure resilience and of the challenges in safeguarding health care against cyber threats in a continuously-evolving security environment. We also recognize that cyber incidents can affect critical health care systems worldwide with catastrophic consequences, including the availability of information and communications technology systems, and the integrity and confidentiality of data, all of which the health care sector is increasingly reliant on.

Advancing cybersecurity in Canada's health sector requires collective, collaborative action. Together, we commit to taking six tangible actions to increase cybersecurity preparedness and resiliency:

1. **Champion**: Championing cybersafety in Canada's health sector;
2. **Inform**: Ensuring that our 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.

Through these actions, we are committed to fostering a robust, safe, and effective health system that benefits those we serve.

CANADIAN HEALTH ORGANIZATIONS DECLARE SHARED COMMITMENT TO CYBERSAFETY

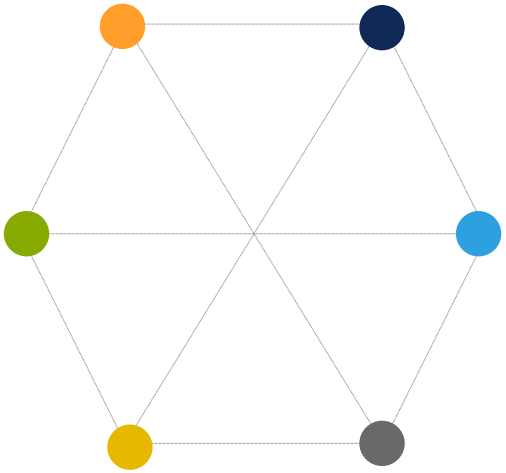
In the 21st Century, patient safety depends on cybersecurity.

Cyber attacks can affect patient care systems and medical devices. They can disrupt communications and supply networks and threaten the integrity and confidentiality of health records, as well as other foundations of modern healthcare. On the other hand, digital solutions can be an important source of resilience for critical infrastructure, enabling access to care even when local health services are disrupted.

Advancing cybersecurity in Canada's health sector requires collective, collaborative action.

In moving ahead, we are mindful of the potential of digital solutions to promote broader critical infrastructure resilience and of the challenges in safeguarding health care against cyber threats in a continuously-evolving security environment.

We also recognize that cyber incidents can affect critical health care systems worldwide with catastrophic consequences, including the availability of information and communications technology systems, and the integrity and confidentiality of data, all of which the health care sector is increasingly reliant on.



Through these actions, we are committed to fostering a robust, safe, and effective health system that benefits those we serve.

OUR COMMITMENTS FOR CYBERSAFE HEALTHCARE

Together, we commit to taking six tangible actions to increase cybersecurity preparedness and resiliency in Canada's health sector

Champion

Championing cybersafety in Canada's health sector

Contribute

Contributing to shared action plans that build collective resilience to cyber attacks

Share

Sharing information, best practices, and tools with others within and beyond the health sector to build collective capacity and resilience

Inform

Ensuring that our leaders, staff, and partners are informed about the scope of the challenge and opportunities to mitigate risk

Advance

Progressing cybersafety in ways consistent with our mandate, considering opportunities for prevention, mitigation, preparedness, response, and recovery

Transparency

As each organization's circumstances and capacity are unique, we will confirm how we will apply these commitments in our unique context and/or with our community by Cybersecurity Awareness Month in October 2018

MOMENTUM TOWARDS ENDORSEMENT FROM FEBRUARY 2018 CYBERSECURITY SUMMIT

Cybersecurity Summit held in Toronto on February 22, 2018. Canadian health and security leaders in attendance, as well as international experts.

85%

Said that it is likely or very likely that their organization would join the coalition for cybersecurity in health by April 22, 2018

SUMMIT ATTENDEES SUGGESTED OTHERS WHO MIGHT BE APPROACHED REGARDING SIGNING THE DECLARATION

Examples of those suggested include the types of individuals/organizations listed below. In many cases, representatives of some of these types of organizations were present, but the suggestion was to engage their counterparts in other similar organizations.

Academics and academic leaders

Clinical associations and regulatory authorities

Digital technology supercluster

Experts in relevant fields (e.g. human factors, change management, implementation science, psychology/sociology, white hat hackers)

Health care providers and regional authorities (broad section of leaders, not just those responsible for IT)

Health data custodians who are not health care providers or government

Health employee associations and unions

HEMA Quebec

Incubators and accelerators

Industry (digital health and medical technology)

Institute of Corporate Directors

Insurers

Law enforcement

Ministries of health

Municipal governments delivering health services

Patient associations

Privacy and information commissioners' offices

Procurement and shared services organizations

Relevant governmental officials/leaders outside health departments

Standards organizations

04

MOVING FURTHER

OPPORTUNITIES FOR COLLECTIVE ACTION TO STRENGTHEN RESILIENCE

Building on the experiences of other sectors and other countries, there are a range of options that could be taken to collectively advance cyber resilience in the health sector. Examples based on the experiences of other countries and industries are shown below.

Incorporate cybersecurity standards into accreditation and/or audit processes

Require regular cybersecurity training/refreshers as a condition of access to electronic health records

Oblige organizations to report cyber risks/attacks and/or response to identified risks

Invest in an assessment of current levels of preparedness and response capabilities across the sector, as well as tracking changes over time

Hold joint exercises to test cybersecurity preparedness and response capabilities

Expand cybersecurity certification/regulation for digital health, connected medical devices, and/or other systems

Commit to avoid paying ransoms in response to cyberattacks

Pre-identify security leads who can be contacted in the case of serious cyber attacks

BEYOND THE DECLARATION: TOP RATED IDEAS FOR MOVING AHEAD FROM THE CYBERSECURITY SUMMIT (1)

*Attendees generated dozens of ideas for achieving substantial advances in health sector cybersecurity over the medium to long-term. Top rated ideas are shown below.**

Top 5

- Establish/commit to consistent standards, accountabilities, and standard operating procedures that cross organizational mandates
- Centre(s) of Excellence to lead on 'what good looks like'; distill, share and generate threat intelligence, guidance, tools, and lessons learned; and promote piloting of standards with test groups and shared learning
- Foster a culture of cyber-security via systematic approaches to educate health sector and users about cyber risks and their mitigation, including sharing information about resources available now to strengthen resilience
- Public/private collaboration at a national level, with mandate based on 2016 Public Safety Canada strategy, provision of capital to address priority risks, and involvement of all 10 critical infrastructure sectors (not just health)
- Legislation related to information security (like US *HITrust Act*)

** Includes ideas rated above an average of 3 on a five-point rating scale by Summit attendees.*

BEYOND THE DECLARATION: TOP RATED IDEAS FOR MOVING AHEAD FROM THE CYBERSECURITY SUMMIT (2)

Attendees generated dozens of ideas for achieving substantial advances in health sector cybersecurity over the medium to long-term. Top rated ideas are shown below

Next 4

- Simulate a cyber-attack to raise awareness of potential impacts and strengthen preparedness
- Establish a baseline for cyber security in the health sector and set measurable expectations for organizations to achieve within 24 months
- Universal cyber-security education for health sector boards
- Radically expand the health sector's participation in the Canadian Cyber Threat Exchange (CCTX)

** Includes ideas rated above an average of 3 on a five-point rating scale by Summit attendees.*

GETTING STARTED: AVAILABLE RESOURCES

Canada's National Strategy for Critical Infrastructure and Action Plan for Critical Infrastructure (2014-2017)

Canadian Cyber Threat Exchange

Public Safety Canada's Get Cyber Safe Guide for Small and Medium Businesses

Public Safety Canada's Cybersecurity Bulletins and Best Practices

Healthcare Sector Cybersecurity Framework Implementation Guide (2016) developed in the United States by HITRUST, the Healthcare and Public Health (HPH) Sector Coordinating Council (SCC) and the Government Coordinating Council (GCC)

National Institute for Science and Technology Framework for Improving Critical Infrastructure Cybersecurity

Advice from the Heathcare Insurance Reciprocal of Canada (HIROC) on cyber risk management, including protecting organizations from breaches, threats, and vulnerabilities

Report of the Health Care Industry Cybersecurity Task Force (United States)

The American Hospital Association's Cybersecurity and Hospitals series: Questions Hospital Leaders Should Ask and What Hospital Trustees Need to Know

Department of Health (England)'s Your Data: Better Security, Better Choice, Better Care response to reviews undertaken following the WannaCry cyber attack in May 2017

RECOGNITION AND DISCLAIMER

This report was prepared by Jennifer Zelmer, PhD (President, Azimuth Health Group, Twitter: @jenzelmer) for HealthcareCAN. The author thanks key informants, Summit participants, and the Steering Group for their insights on cybersecurity in the health sector, as well as HealthcareCAN staff for their helpful comments and suggestions.

HealthCareCAN is the national voice of healthcare organizations and hospitals across Canada, Our goal is to improve the health of Canadians through an evidence-based and innovative healthcare system.

© HealthcareCAN, 2018

17 York Street, Suite 100
Ottawa, Ontario
Canada

05

APPENDIX

COMMON THEMES FROM KEY INFORMANT INTERVIEWS (1)

Use of information and communication technology is growing rapidly in the health sector. Interviewees reported that they were more concerned about application vulnerabilities than hardware because some core solutions are obsolete, out of support, or close thereto. For example, one said,

"Critically for us, our biggest vulnerabilities are not in the hardware but in the applications. A lot of the critical applications that we run are basically either obsolete or very close to obsolete."

While some jurisdictions have embarked on – or are planning – widespread upgrading, this is not the case everywhere. Switching to manual backup processes (where that is the contingency plan) tends to be cumbersome and unsustainable. At the same time, increased use of digital solutions offers potential resilience through data sharing and opportunities to use virtual care to continue to provide services when local physical services are disrupted.

Cybersecurity is on the radar for most but not all organizations. There is a general recognition that we cannot prevent all attacks, but we must reduce the risk of impact, including detecting them and recovering from them as soon as possible. Leadership is key. Larger and more connected organizations are more likely to have sophisticated cybersecurity plans and mechanisms in place. Several interviewees noted that Board members often come from other sectors where cybersecurity is an important issue and have been helpful in elevating its profile in the health sector.

COMMON THEMES FROM KEY INFORMANT INTERVIEWS (2)

Baseline levels of security awareness and assessment are important. Many interviewees emphasized the importance of an improved understanding of the evolving threats, risks, preparedness, and resilience factors.

A variety of tools and services to support a structured assessment process exist, such as Public Safety Canada's Regional Resilience Assessment Program, private sector assessment frameworks, and a security scorecard for healthcare organizations. Nevertheless, the degree to which such assessments have been undertaken, shared with relevant stakeholders, and acted upon varies considerably.

Many organizations report experiencing cyberattacks of various types on a regular basis, most of which are detected and prevented. Both health and financial systems are potential targets. Several insider breaches of health record systems have been well-publicized. Canadian hospitals have also been victims of other types of cyberattacks. While less common, some interviewees also commented on the potential impact of widespread interruptions to internet and data services, which might arise through natural disasters and other similar scenarios.

The degree of preparedness varies widely across the health sector and there are limited standard requirements in place. Almost all organizations have some basic precautions in place (e.g. firewalls).

There is increasing recognition that while these security layers are important, it is insufficient to 'build a higher wall' around our information assets and systems. Some organizations are investing in broader, more integrated strategies, including organization-wide education/awareness, proactive horizon scanning, risk assessment, advanced threat detection and other technology solutions, layered security approaches and redundancy for critical systems and/or networks, spot checks and response testing, post-failure recovery/resilience plans, and capacity development. Smaller organizations, such as individual clinics, may be more vulnerable, but their distributed nature may also offer advantages in terms of resilience. Given the changing risk environment, interviewees consistently expressed a desire to enhance preparedness.

SlideShare™ is a trademark of LinkedIn Corporation. All rights reserved.

COMMON THEMES FROM KEY INFORMANT INTERVIEWS (3)

Resourcing cybersecurity initiatives is a challenge because organizations have many competing priorities with direct impact on health services for patients/ communities and there is often a lack of understanding of the potential impact of information technology failures on health and life safety in a connected digital world. In at least one province, interviewees were concerned that capital investments (whether in cybersecurity or otherwise) can also have perverse effects on government funding because of the structure of current funding models.

Cybersecurity is not a core competency for most health care providers and organizations. Many interviewees recommended leveraging broader expertise (e.g. regarding cyber risk assessment and testing) and solutions (e.g. well-designed cloud solutions) that could enhance preparedness and mitigate risk, including shared services and outsourcing models. For instance, one argued that:

"[What] you want to stay away from is: don't think you need to build all these information systems yourself. You need to integrate the solutions that exist and leverage within the marketplace."