HealthCare*CAN*
Leading. Innovation. Together.

Issue Brief

Critical Infrastructure in Canada's Health Sector
Part B – A Focus on Cybersecurity

2018

Use of digital solutions and connectivity is growing rapidly in the health sector and beyond. Essential services increasingly depend on digital systems and these systems are becoming an increasingly significant part of the country's critical infrastructure. Health system critical infrastructure is no exception. In today's digital world, more people are using more systems, devices, and applications in more ways to perform more core health system functions. Large health organizations use hundreds of different clinical and administrative systems, and must maintain interfaces between then. Information sharing between health care providers is also on the rise so as to improve patient safety and the continuity of care. But the more we rely on these digital solutions, the more vulnerable we become if they should fail. At the time of writing, the number, significance, and complexity of cyberattacks is increasing, with important implications for Canada's health sector.

This trend reinforces the rising importance of cybersecurity to the resilience of our critical infrastructure. In the health sector, this includes ensuring that neither the continuity of operations nor the confidentiality of personal health information is compromised due to cyber attacks.

Our Approach

A HealthCare*CAN* 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 oversaw the preparation and updating of this *Issue Brief*. In addition to advice from members of the Steering Committee, key inputs included:

- A rapid review of the literature on critical infrastructure in the health sector, with a focus on cybersecurity;
- Online Surveys: Of HealthCare*CAN* members conducted between November 2016 and February 2017 (24 responses for a response rate of 46%), of HealthCare*CAN* and Canadian College of Health Leaders members conducted between May 17th and 26th, 2017 (227 responses), and of adults living in Canada's provinces conducted between May 19th and 23rd, 2017 (n=1005);
- Key informant interviews with health sector leaders across the country, authorities on critical infrastructure and emergency preparedness; and cyber-security experts; and
- Validation of outcomes with selected interviewees, members of the Steering Committee, and HealthCare*CAN*'s Board of Directors.

Issue

Use of digital solutions and connectivity is growing rapidly in the health sector. Essential services increasingly depend on digital systems and these systems are becoming an increasingly significant part of the country's critical infrastructure. The more we rely on these digital solutions, the more vulnerable we become if they should fail. At the time of writing, the number, significance, and complexity of cyberattacks is increasing, with important implications for Canada's health sector. This trend reinforces the rising importance of cybersecurity to the resilience of our critical infrastructure.

HealthCare*CAN* has prepared this *Issue Brief* for the Health Sector Critical Infrastructure and Cyber Security Steering Committee (under the auspices of the National Strategy for Critical Infrastructure).

Part B of this *Issue Brief* provides an overview of cybersecurity considerations for Canada's health sector, in contrast to Part A, which focuses on Critical Infrastructure more broadly.

By: Jennifer Zelmer, PhD

For more information:

Jonathan Mitchell
Consultant, Policy & Strategy
jmitchell@healthcarecan.ca

"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."[1]

Cybersecurity in the Health Sector

Cyberattacks are frequent in Canada's health sector. (2) 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% of respondents to HealthCare*CAN*'s 2016-17 survey said that they have 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."

Multiple organizations also reported the following types of cyber risks:

- **Malware, spyware, or ransomware:** code with malicious intent (e.g. viruses or worms) that may steal or destroy data;
- **Phishing and cyber fraud:** emails or other communications that, when the instructions in them are followed (e.g. a link is clicked), may provide access to a computer system, activate other malicious functions, or ask for confidential information;
- **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; and/or
- **Human error that affected critical systems**, such as plugging a Voice Over Internet Protocol (VOIP) phone into a jack not wired for the service.

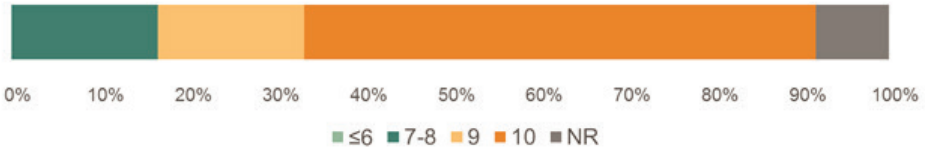
Canadian health organizations are not alone in experiencing cyberattacks, as recent high-profile ransomware attacks that affected health services in the United Kingdom and elsewhere demonstrate. In the United States, more than one health data breach per day was reported to the Department of Health and Human Services or in the media in 2016[2]. 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. Likewise, in the United Kingdom, 27 of 94 NHS Trusts that responded to a recent information request said that "an external hacker encrypted a PC or device or network … and demanded payment in order to decrypt the device."

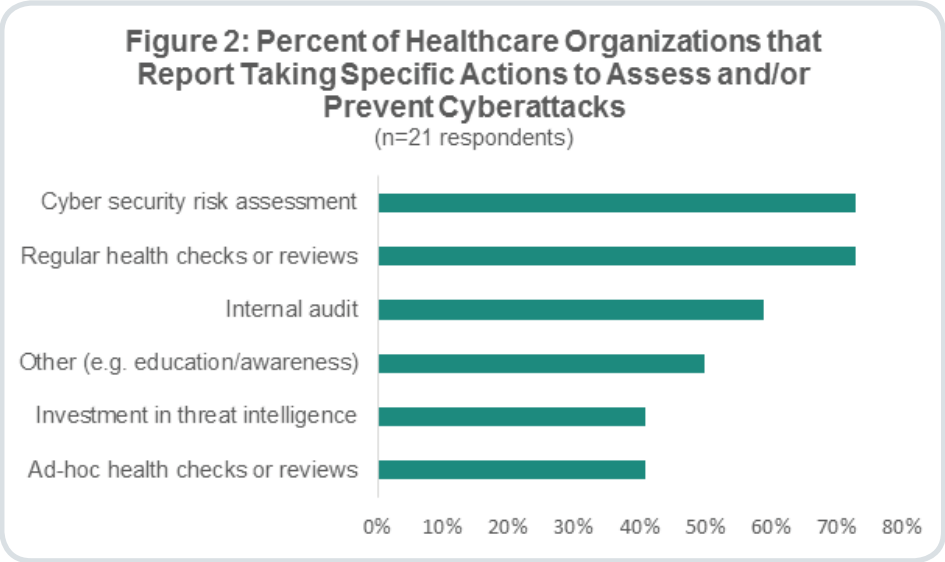
These and other similar events indicate that in addition to random attacks, health organizations can be specifically targeted for a variety of reasons, including:

- Personal information health organizations hold about patients and employees can be valuable and some types of health information have enduring value;
- 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;
- Many health organizations have substantial financial resources and are large employers with significant payroll;
- Health organizations often have a high profile in their communities and may make decisions that individuals or groups disagree with; and
- There is potential for disruption of critical infrastructure and services.

Figure 1: How healthcare leaders rate the importance of cyber security to their organizations

(1=not important at all; 10=extremely important)





In this context, it is perhaps not surprising that many health leaders say that cybersecurity is extremely important to their organizations (see Figure 1)[i]. That said, organizations face many competing priorities and face difficult decisions in allocating resources among them.

Cybersecurity Preparedness

Cybersecurity reflects the interaction of threats, vulnerabilities, how likely an incident is, and its potential impact. In 2017 surveys, more than 8 in 10 health leaders and members of the general public said that they felt that Canada's health sector was somewhat or very vulnerable to cyber attacks.

There are many steps that organizations can take to enhance preparedness and mitigate risk. For example, the National Institute of Science and Technology's Framework for Improving Critical Infrastructure Cybersecurity recommends on-going efforts that enable an organization to:

- **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** 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;
- **Detect** incidents in a timely way by having appropriate mechanisms in place;
- **Respond** quickly to incidents thanks to advance preparations; and
- **Recover** normal operations following an information security incident.

Likewise, Public Safety Canada[3] recommends a focus on raising security awareness, defining roles and responsibilities, developing policies and standards, establishing a cybersecurity plan, and budgeting for cybersecurity. They also highlight four specific safeguards to prevent most cybersecurity problems:

- **Application whitelisting** to allow only identified programs to execute on a given system;
- **Use of modern operating systems and applications**, including a life-cycle approach to migrate to newer versions of systems/programs;
- **Patching operating systems and applications** within two days of a high-risk vulnerability being made public; and
- **Restricting administrative privileges.**

Canadian healthcare organizations report taking a variety of measures to assess and/or prevent cyber attacks (see Figure 2). In addition, just under half (45%) reported that cybersecurity was a standing item on their Board of Directors' agendas.

Evolving Cybersecurity Risks and Responses

In key informant interviews, many health leaders emphasized the evolving risk environment that they face. For example, one 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

i. Based on a survey of HealthcareCAN members conducted between November 2016 and February 2017. There were 24 responses to the survey, a response rate of 46%.

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.'"

Other common themes from the interviews included:

- **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. Some healthcare organizations have already experienced the consequences. 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[4].

"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. Reflecting this perspective, one indicated that "we have a lot to learn from other sectors; I don't think the requirements [of healthcare] are particularly unique."
- **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[5]. 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. In one case, for instance, hackers using a phishing attack accessed hospital payroll files and made three "significant transactions from the payroll accounts." In another, 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[6]. 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 (see Figure 2). 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.
- **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."
- **A number of interviewees called for collaborative efforts** to strengthen the health sector's responsiveness and resilience overall, taking into account the need for specialized expertise and for sector-wide awareness/education. Likewise, there were calls to integrate cybersecurity recovery capabilities with broader business/service continuity planning.
- **Many see general cybersecurity education and preparedness for citizens and health professionals as challenging but key** to the health sector's overall preparedness, particularly as more and more people gain access to health information (e.g. via patient portals). Both inadvertent and deliberate actions by insiders that compromise cybersecurity are seen as important potential risks. Interviewees suggested enhancing communication channels and education to address these risks. For instance, one interviewee indicated that there are "lots of tools and technologies, but that seems to me to be the easy part. Putting in the processes and the awareness and behaviours, and policy procedures is far harder to do and needs at least as much attention. And it's seldom well received."
- **Growth in the Internet of Things**, including increasing connectedness for medical devices, was seen as a rising future point of potential vulnerability for the health sector. Some argued that medical device hijacking will be among the greatest cybersecurity threats that the health sector will face over the next decade. Addressing this challenge requires attention to potential cyber vulnerabilities throughout the medical device lifecycle, including as part of post-market device management[7].
- **We need to share experiences but also to protect security strategies and systems.** There was strong interest in sharing lessons learned, effective strategies, tools, and other resources among health care organizations. At the same time, there was a recognition that detailed information about cybersecurity provisions must be kept confidential. One interviewee noted that it was not clear whether this was permitted under provincial legislation should there be a *Freedom of Information* request.

Facing similar issues, other countries have also seen the need to put in place sector-wide, broad-based responses to cyber threats. For instance, a recent report by the United State's Health Care Industry Cybersecurity Task Force, a group established by the Cybersecurity Act of 2015, provided detailed recommendations to strengthen cybersecurity. Likewise, the disruptions caused by the spring 2017 WannaCry attacks triggered several reviews in the United Kingdom. Results include identifying steps that all health and social care organizations and general practices must take in 2017/18 to implement data security standards. These approaches reflect an understanding parallel to that expressed in a recent report from Australia: "Cyber security is not simply a technology challenge. It is also a cultural challenge and one that extends beyond traditional information security practices."[8]

Cybersecurity at Canadian Blood Services

Like many organizations that depend on digital solutions and networks, Canadian Blood Services[ii] routinely deals with minor cyber events. These events occur almost daily and typically cause minimal disruption due to the organization's foundational cybersecurity controls and processes. But occasional more significant events reinforce the priority that the organization places on cybersecurity.

For example, in late 2015 the organization identified a trend whereby donors were not showing up for their scheduled appointment in a particular geographic area. After reviewing logs of CBS's online appointment management system, it was determined that a series of false appointments had been booked by a software

ii. Canadian Blood Services (CBS) manages the supply of blood, blood products, and stem cells outside of Quebec, as well as a pan-Canadian system for organ donation and transplantation.

application running an automated task. The net impact was a temporary reduction in collections. And in October 2016, CBS' peers at the Australian Red Cross experienced the largest-ever leak of personal data in Australia. (A person scanning for security vulnerabilities found a file containing sensitive donor information that had been placed in an insecure environment by a third party that develops and maintains the service's website. Once identified, the problem was contained and an independent review determined that there was a low risk of future direct misuse of the information.)

Today, cybersecurity is no longer an administrative function led by IT, but an enabler of CBS's corporate strategy:

- Cybersecurity enables agility by allowing CBS to confidently exploit technology to engage with donors and partners;
- Cybersecurity serves as the sentry for the organization's brand as the organization is increasingly becoming identified by its online presence; and
- Cybersecurity enables operations – from the core supply chain to administration of the organization, cybersecurity ensures data and systems are available when needed, and the data in those systems can be relied upon to be accurate and complete.

This renewed perspective establishes cybersecurity as a critical element to core operations and achieving the organization's mandate to meet the needs of Canadian patients.

Building on industry-standard frameworks (e.g. ISO/IEC 27001 and the National Institute for Science and Technology's Framework for Improving Critical Infrastructure Cybersecurity), CBS has developed a cybersecurity framework and strategic plan which places an emphasis on implement capabilities to stay engaged in the face of an ever-changing threat and being prepared to endure a cybersecurity incident. Driven by an assessment of the organization's capabilities and the threat landscape, CBS is moving forward with several key initiatives that will reinforce a security-aware mindset and rigorous cybersecurity processes across the organization, tailor cybersecurity controls based on risk assessments, and ensure a cybersecurity architecture that enables CBS to leverage digital solutions, with confidence, to achieve its corporate objectives.

Looking Ahead: Enhancing Cooperation with a Health Sector Roundtable

Preparation, planning, and communication are essential enablers of critical infrastructure resilience and therefore the effective functioning of the health sector in the face of potential hazards. To support this process, the Public Health Agency of Canada and HealthCare*CAN* established a Steering Committee in 2016 to guide and direct key elements of the development of a pan-Canadian Health Sector Network focused on critical infrastructure issues. The Committee has provided guidance on the development of this *Issue Brief*. Members are also informing the Network's terms of reference and membership, as well as its deliverables and priorities.

Find Out More

- Canada's National Strategy for Critical Infrastructure and Action Plan for Critical Infrastructure (2014-2017)
- The American Hospital Association's Cybersecurity and Hospitals series: Questions Hospital Leaders Should Ask and What Hospital Trustees Need to Know
- 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)
- Advice from the Heathcare Insurance Reciprocal of Canada (HIROC) on cyber risk management, including protecting organizations from breaches, threats, and vulnerabilities
- National Institute for Science and Technology Framework for Improving Critical Infrastructure Cybersecurity
- Report of the Health Care Industry Cybersecurity Task Force (United States)
- 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

Bibliography

1. Public Safety Canada, "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada," 2010. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf. [Accessed 24 January 2017].
2. Protenus, Inc. in Collaboration with DataBreaches.net, "BREACH BAROMETER REPORT: YEAR IN REVIEW 2016 Averaged at Least One Health Data Breach Per Day, Affecting More Than 27M Patient Records," 2017. [Online]. Available: http://www.protenus.com/hubfs/Breach_Barometer/Protenus%20Breach%20Barometer-2016%20Year%20in%20Review-%20final%20version.pdf. [Accessed 27 January 2017].
3. Public Safety Canada, "Fundamentals of Cyber Security for Canada's Critical Infrastructure Community," 2016. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx. [Accessed 17 December 2016].
4. HIROC at https://www.hiroc.com/News-Media/News/2016/Cyber-Risk-Management-Protecting-your-organization.aspx
5. H. Elrefaey, E. Borycki and A. Kushniruk, "Developing a Security Metrics Scorecard for Healthcare Organizations," Healthcare Quarterly, vol. 18, no. 3, pp. 61-68, 2015.
6. HIROC at https://www.hiroc.com/News-Media/News/2016/Cyber-Risk-Management-Protecting-your-organization.aspx
7. Food and Drug Administration, "Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff," 28 December 2016. [Online]. Available: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf. [Accessed 6 March 2017].
8. Enabling Australia's Digital Future: Cybersecurity. Available: https://www.csiro.au/en/Do-business/Futures/Reports/Enabling-Australias-digital-future

HealthCareCAN
Leading. Innovation. Together.

17 York Street, Suite 100, 3rd floor
Ottawa, Ontario K1N 5S7
(613) 241-8005
www.healthcarecan.ca