Moving Forward for Cybersafe Healthcare

INSIGHTS FROM THE CANADIAN SUMMIT ON HEALTHCARE CYBERSECURITY

Written by: Charles Thompson

HealthCareCAN
Leading. Innovation. Together.

Background

New technologies are penetrating into every facet of health and healthcare; a trend that will only accelerate in the years to come. In the main, this is a very good thing. Increasingly, digital infrastructure is also becoming the backbone of a broad range of everyday health services. More broadly, the newly digitized and networked landscape is turning out to be a core feature of a modern, responsive, and resilient healthcare system.

Yet healthcare's brave new world also poses new and frightening challenges for healthcare leaders, governments, patients, and the public. Lax cybersecurity threatens to undermine the security of the critical infrastructure upon which we all depend and to endanger the safety of the patients and communities we serve. Ultimately, these new technologies, if not properly managed and secured, may prove to be our sector's greatest vulnerability in a moment of crisis.

HealthCare*CAN* recognizes the importance of promoting resilient infrastructure; a project that very much includes shoring up our sector's cybersecurity posture. Our efforts to improve cyber resilience in Canada's healthcare system are one facet of our broader efforts to advance the *National Strategy on Critical Infrastructure*. HealthCare*CAN* undertakes these efforts as the health sector's representative on the National Cross Sector Forum on Critical Infrastructure, (NCSF). The NCSF as a whole, in turn, maintains a comprehensive and collaborative Canadian approach to critical infrastructure by providing a standing mechanism for discussion and information exchange within and between the federal, provincial and territorial governments and the critical infrastructure sectors.

As part of this work, HealthCare*CAN* and our partners became concerned that the conversation around healthcare cybersecurity had stagnated. We determined that it would be necessary to convene key parties from across our sector to invigorate the discussion and galvanize our community around a shared understanding of our risks and a set of key commitments to move forward. The result was the Canadian Summit on Healthcare Cybersecurity, which was hosted by HealthCare*CAN* in Toronto, Ontario on February 22nd 2018.

The Canadian Summit on Healthcare Cybersecurity was made possible through the generous support of Public Safety Canada through the Cybersecurity Cooperation Program. Program guidance for the Summit was provided by the Health Sector Steering Committee on Critical Infrastructure and Cybersecurity, which is jointly co-Chaired by HealthCare*CAN* and the Public Health Agency of Canada. HealthCare*CAN* wishes to express its gratitude to our partners in this effort, without whom this project would not have been possible.

The Summit included participation from leaders in a wide variety of different disciplines, including: healthcare executives, clinical leaders, experts in the relevant domains of law, insurance and academia, government partners, industry associations and technical experts from the world of cybersecurity both in Canada and internationally. A full list of Summit participants is provided in Appendix A.

In advance of the Summit, delegates were provided with an Options Brief entitled *Cybersafe Healthcare: Options for Strengthening Resilience in Canada's Health Sector*. The Brief outlines the current state of cybersecurity in health from both a global perspective and within Canada, introduces the *Declaration of Commitment to Cybersafe Healthcare*, and identifies opportunities for collective action to strengthen sector resilience. The Brief was updated to reflect discussions at the Summit and is included in Appendix B to this report.

This report documents the proceedings of the Canadian Summit on Healthcare Cybersecurity. It also acts as a compilation of key insights arising from and related to the day's discussions. We sincerely hope that healthcare leaders, government partners, stakeholders, and other interested parties will make use of these insights in the months and years to come. Many of the risks to our sectors' are obscure or technical in nature. But in the course of our work, we were struck by how much of the battle must be fought on familiar territory, addressing issues of leadership and culture. All of us have stakes and a role to play in these matters. Our goal in this work is to give our partners the tools to do so.

Introduction

The Canadian Summit on Healthcare Cybersecurity began with introductory remarks from HealthCare*CAN* Board Chair and President and CEO of Eastern Health David Diamond (remarks in Appendix C). These were immediately followed by opening remarks by HealthCare*CAN* President and CEO Paul-Émile Cloutier (Appendix D). The Summit's goals, as articulated by Mr. Cloutier, were threefold:

1. To educate participants on the current threat landscape vis-à-vis healthcare cybersecurity;
2. To launch a declaration highlighting a common understanding of the importance of cybersecurity in Canada's health sector and a shared commitment in principle to advancing the sector's resilience; and
3. To review and flesh-out potential options to promote sector resilience and identify potential additional options that had not previously surfaced.

Mr. Cloutier's remarks were followed by an opening address from Mr. Craig Oldham, Director General for Critical Infrastructure Coordination at Public Safety Canada.

An overview of the day's activities was then provided by Summit facilitator Dr. Jennifer Zelmer, President of Azimuth Health Group. These are also overviewed in the Summit Program (Appendix E), which includes the summit's Agenda and speaker bios.

Panel Discussions and Presentations

Principles for Cybersecurity in Healthcare

The Summit's first event was a panel discussion including experts from outside of Canada's healthcare system. Its goal was to glean insights from outside of our own country and sector in the hopes that these insights might help Canadian healthcare leaders build on lessons learned and avoid the mistakes encountered by others. Having discussed the ramifications of increasing threats being experienced abroad and outside of healthcare, the Summit turned its attention to the more local and specific concerns around cyber resilience in Canada's health sector. Participants in both panels are summarized in the table below.

These discussions were followed by a presentation from Kevin Magee, National Director for Intelligent Cloud Emerging Technologies at Microsoft Canada and a former member of the Board of Directors for the Brant Community Healthcare System. Kevin's presentation addressed the importance of planning for cybersecurity events and increasing proficiency and knowledge at the executive level.

In evaluations given after the Summit, participants indicated that they found these discussions to be of considerable value in their efforts to understand how cybersecurity concerns map to the healthcare landscape and to develop their own plans and strategies for enhancing resilience. The key insights from these presentations have been organized into a set of principles to guide leaders' understanding of healthcare's cybersecurity risk landscape, the threats we face, and the ways we might respond.

PANEL #1 Learning from Others: Global and Cross-Sector Perspectives	**PANEL #2:** Current State of Cybersecurity in Canada's Health Sector
Dan Taylor Director of Security National Health Service Digital	**Ray Boisvert** Provincial Security Advisor Government of Ontario
Cédric Arcos Deputy CEO for Paris Region French Hospital Association	**Jeff Curtis** Chief Privacy Officer Sunnybrook Health Sciences Centre
John Riggi Senior Advisor on Cybersecurity and Risk American Hospital Association	**Jim Patterson** Partner Bennett Jones LLP
Francis Bradley Chief Operating Officer Canadian Electricity Association	**Brendan Seaton** President Information Technology Association of Canada Health

Principle #1: Healthcare cybersecurity is a patient safety issue.

The health sector's cybersecurity risk profile is often understood in terms of the sector's information holdings, with the worst outcome being that precious data is stolen or lost. But our sector's risks extend well beyond disruption or loss of data. Healthcare also faces serious potential risks to patient safety arising from gaps in system security. As healthcare becomes more digitized, more automated, and more connected, the risks of inadequate cybersecurity become more and more intimate. As one example, it is not without the realm of possibility that security loopholes in Internet of Things (IoT)-enabled pacemakers or ventilators could be exploited by malicious actors, with frightening implications. These possibilities place healthcare cybersecurity squarely within the domain of patient safety. Summit participants were therefore emphatic on the point that lax cybersecurity presents a real risk to patient safety.

> *"Whether you want it or not, your business is information management now."*
>
> - Panelist

Principle #2: Healthcare organizations are prime targets

Panelists at the Summit made it clear that the health sector has specific characteristics that make it highly attractive to criminals.

One such characteristic is the healthcare environment itself. Healthcare organizations tend to run on a patchwork of software and systems that need to work well together, but which may not have been specifically built with compatibility in mind. This environment selects against good patch management practices, since patching regularly increases the probability of unexpected consequences to the software or systems that need to be available at all times. Hence, healthcare organizations must balance the technical risk of patch management against the clinical risk to patients that may result. In large healthcare facilities which may run on thousands of connected devices – including PCs, phones and medical devices – patching is not a trivial matter to be accomplished overnight. These vulnerabilities are magnified by security issues introduced by the frequent and often unavoidable use of personal devices in the healthcare setting.

A related issue concerns network segmentation practices in healthcare organizations. Some healthcare organizations' systems are unsegmented, meaning essentially that everything in the network is connected to everything else. This simplifies matters for clinical staff, who by the nature of their work need to be able to access records or systems wherever they are in the organization. But it also means that intrusion grants sweeping access to the intruder. There are ways of designing digital environments to mitigate these risks (e.g. by use of Network Access Control solutions) but they require a very sophisticated knowledge of both the organization's assets and the needs of its staff.

The nature of healthcare data turns health sector data stewards into attractive targets for criminal interests. In particular, healthcare data is:

Vital – Given their potential to improve access to care, quality of health services, and efficiency of the health system, healthcare's reliance on digital solutions is growing. Some health systems depend on digital infrastructure to such degree that its compromise can seriously affect care. For instance, hacking and encryption of medical information for ransom could critically impair the ability of some organizations to deliver care or offer services. This has happened in Canada.

Personal – Medical records include highly sensitive enduring data, including confidential diagnoses, and personal identifiers like names, addresses, and Social Insurance Numbers. These data can be valuable targets for ransom or identity theft.

Profitable – Healthcare organizations hold key information about clinicians and staff, as well as patients. This information can be used inappropriately, for instance to make fraudulent claims for healthcare services or drugs and medical equipment for resale. Like organizations in other industries, healthcare organizations have also been victims of business email compromise resulting in misdirected wire transfers and, even forced Bitcoin mining.

Information Dense – Healthcare data can be put to many purposes depending on the criminal enterprise involved. For example, the espionage potential of healthcare data is high. Valuable intellectual property can also be stolen from healthcare research institutes, either for commercial advantage or for other malevolent purposes.

Because healthcare data combines so many valuable characteristics, healthcare organizations and workers cannot afford to take a lax attitude to cybersecurity. While cybersecurity has not traditionally been a part of our sector's core business, as one panelist put it, "whether you want it or not, your business is information management now".

Principle #3: No one organization or sector can 'go it alone'

Partnerships within and across sectors are critical to developing cyber resilience. As noted, the health sector faces a variety of cybersecurity threats by virtue of its operations and data holdings. But our sector also has dependencies with a much wider range of critical infrastructure sectors (for example the energy and water sectors) that also face threats. These other sectors, in turn, depend on a well-functioning health system.

As things stand, 'going it alone' on cybersecurity is not a tenable option for any sector; threat and strategy sharing across sectors and even across borders is to be encouraged. Partnerships are a key resilience factor since it is critical that owner/operators be in the right flows of information to be able to prepare for, detect, and respond to threats. While these partnerships can be encouraged by governments, they also require a deep commitment from within critical infrastructure sectors themselves.

In this context, threat exercises and other platforms for information sharing are especially important. Canada's energy sector participates in exercises that span the continent and has gained valuable insights from doing so. The health sector should give serious consideration to how it can be a more active partner in Canada's broader critical infrastructure community by participating in similar exercises organized at regional, provincial, or federal levels.

Principle #4: Healthcare needs the leadership and capacity to respond to threats

Much global attention was drawn to the vulnerability of the health sector by the WannaCry attack in May of 2017, which was particularly effective in disrupting care at NHS trusts in the United Kingdom. That attack affected one third of NHS trusts, causing roughly 19.000 hospital appointments to be cancelled. It also affected 603 primary care organizations and 595 general practitioners' practices. While WannaCry did give global prominence to the challenges facing health systems, one panelist warned against giving unwarranted emphasis to that event, noting that focusing on WannaCry to the exclusion of other threats can limit the imagination and impede a full risk assessment.

> *"Don't ever overlook the insider threat, you can trust, but always verify."*
>
> - Ray Boisvert, Provincial Security Advisor for Ontario

Yet the WannaCry incident does underline the fact that partnerships are only helpful if healthcare organizations can be responsive to the information they receive.

The WannaCry incident was both predictable and predicted. The vulnerability that made WannaCry possible was, in fact, detected by NHS Digital several weeks in advance of the May outbreak. Notifications were then sent to NHS trusts with instructions on the nature of the vulnerability and advice on how to mitigate risk.

Uptake of that advice was uneven, however. At the time, a significant number of NHS trusts were running on either unpatched versions of Windows 7 or unsupported versions of Windows XP, both of which were vulnerable to the WannaCry exploit. This in turn was a consequence budgeting and other related decisions made years earlier. Hence, many NHS trusts found that they were not in a position to respond in the time that they had, while others did not assign priority to that response in the lead-up to the incident.

Principle #5: Cyber resilience and response is an enterprise-wide responsibility

Other critical infrastructure sectors (for example, the energy and finance sectors) understand cybersecurity as an enterprise-wide responsibility. The health sector, by contrast, often has a limited perspective on the problem, electing to treat cybersecurity as an IT issue. Under this model, resilience and response are effectively delegated to a Chief Technology Officer, Chief Information Officer, or similar position. This mentality can prevent organizations' boards and executive teams from developing the knowledge and expertise necessary to ensure a robust resilience and response plan that cuts across the organization's activities.

Panelists stressed that treating security as an IT issue belies the fact that insider threat is a major driver of security risks. These threats can be either accidental or intentional. "Don't ever overlook the insider threat", advised Ray Boisvert, Provincial Security Advisor for Ontario, "You can trust, but always verify". Technical solutions alone will not guard against these instances of insider threat; an enterprise wide strategy must tackle the behaviour of users as well as the defense of systems.

Enterprise-wide planning means planning in advance. The worst possible time to develop a strategy is during an attack, when stress is high and information is scarce. As with other threats to critical infrastructure, healthcare organizations should have a plan in place that embraces both prevention and response to cyber-attacks in all their forms.

Preventative measures to improve resilience may include, among others, taking steps to ensure backups are frequent and insulated from outside threats, undertaking education programs and building cybersecurity requirements into equipment procurement in order to encourage resilience and prevent attacks. Beyond these, the plan also needs to include a set of criteria for determining the organization's response to an attack, including who to contact for help, whether and when a ransom should be paid, and how to communicate with staff and stakeholders.

An organization's resilience and response plan should also address the legal consequences of a breach. As Jim Patterson noted, any investigation or response an organization undertakes before engaging legal counsel is not covered by attorney-client privilege. Its disclosure can be forced during a class action suit or other legal action. This makes the case engaging legal counsel as early as possible in the process.

Principle #6: Training is essential and simplicity is key

As cybersecurity needs to be embraced as an enterprise-wide responsibility, it follows that cybersecurity awareness initiatives will need to engage organization leaders and staff with varying levels of technical sophistication. Successfully training leaders and staff at all levels need not necessarily entail higher costs or complexity. In fact, reducing complexity, where appropriate, can be seen as an essential first step in training.

Best practices in digital hygiene are relatively simple. Overly technical language can be a barrier to uptake. As one panelist observed "As soon as you make it technical, you lose the argument." John Riggi, Senior Advisor on Cybersecurity and Risk for the American Hospital Association, noted that in his experience training senior hospital executives in cybersecurity he was "mostly acting as a translator". Kevin Magee, National Director for Intelligent Cloud Emerging Technologies at Microsoft Canada, emphasized the roles that terminology and jargon play in making training and response more complicated than it needs to be: "Calling them 'hackers' even makes these people seem untouchable. I prefer the term 'criminals', which is a concept that Board members can understand and grapple with."

Participants noted that training is important for all staff at all levels since cybersecurity is the responsibility of every department and stakeholder in the organization. Audit and feedback strategies are commonly employed both within and outside healthcare. As much as possible, these should be used to lift staff into better digital hygiene practices, rather than castigating staff for poor behaviour. Fear is a poor motivator. Staff should be provided the opportunity to take part in personable, interactive approaches to learning as routine training sessions are rarely memorable. Training can also be 'game-ified' and thereby made engaging and memorable, such as by providing minor rewards for identifying phishing attacks.

> *"As soon as you make it technical, you lose the argument."*
>
> - John Riggi, Senior Advisor on Cybersecurity and Risk, American Hospital Association

Likewise, the simpler it is to share information about cyber threats and to act on them, the more likely this is to take place. Governments can use both regulations and incentives to encourage reporting and contribute to the sector's collective resilience.

Principle #7: Cybersecurity expertise is in short supply

There is no technical panacea that will meaningfully improve cybersecurity resilience in the absence of staff with appropriate expertise. Like other sectors, healthcare as a whole faces problems attracting the necessary cybersecurity talent, both in Canada and abroad. In the United Kingdom there are three jobs for every qualified applicant in the healthcare cybersecurity ecosystem.

In response to this shortage of talent, the United Kingdom has adopted hub and spoke models wherever possible, organized around centres of excellence which lend their expertise to partners. Participants endorsed this strategy as a promising practice for Canada's health sector. Getting to that point will depend first on identifying regional centres of excellence and second on encouraging strong and reliable partnerships between organizations.

Principle #8: Cybersecurity standards are important, but have been challenging to deploy in healthcare

One commonly endorsed strategy for addressing cybersecurity vulnerabilities in healthcare is the adoption of consistent standards to be employed across the industry. For instance, the United Kingdom mandates that organizations doing business with the government must be certified under a platform entitled Cyber Essentials. This platform allows for self-assessment of cyber resilience based on five key security controls, and compliance is estimated to prevent approximately 80% of common internet attacks. Cyber Essentials has made landfall in Canada through CyberNB, based in New Brunswick, and has been raised as a viable option for healthcare organizations seeking to evaluate their level of risk.

Speakers noted that understanding one's current level of resilience and preparedness is as important as knowing what to do next. Yet this level of certification seems to be very difficult for healthcare organizations to attain. As of February 2018, 200 on-site assessments had been performed on NHS trusts and all failed their assessments. Of these assessments, the average score was 59% (range 23% to 74%) where 100% compliance is required for certification.

This presents challenges at the level of public policy. As one participant put it: "If it costs $X Billion to bring our hospitals up to the Cyber Essentials Standard, we need to ask ourselves whether that investment is making a difference, and we need to have an honest conversation about how we are going to get hospitals to that standard in five years."

> *"Believe it or not, the Canadian vendor community has fully bought into the privacy gospel. What we need now are rules of the road that apply equally."*
>
> – Brendan Seaton, President, ITAC Health

Principle #9: Medical device cybersecurity needs to be managed as a matter of policy

The rising use of internet-enabled medical technologies offers many advantages for patient care, but can also pose a range of issues from a cybersecurity perspective with attendant risks to patient safety. For instance, an implanted medical device cannot simply be replaced on-demand if deemed to be a security threat, either to the individual or to the institution. Building in security requirements from the ground up, sometimes known as 'security by design,' is a best practice in this domain. Brendan Seaton, President of ITAC Health, advises that "Believe it or not, the Canadian vendor community has fully bought into the privacy gospel. What we need now are rules of the road that apply equally."

Governments certainly have a role in the regulation of medical devices, though the extent of that role in Canada is not yet clear. Healthcare organizations can also play a role in threat containment by building cybersecurity requirements into the procurement process. This would help to ensure that only devices meeting a certain standard are used in the healthcare ecosystem and help drive the market towards solutions pre-packaged with adequate cybersecurity provisions. It may also be possible to leverage Digital Health Canada's guidelines for health information technology privacy and security to drive policy at the hospital level.

The Declaration of Commitment to Cybersafe Healthcare

In an effort to develop our sector's cybersecurity resilience going forward, HealthCare*CAN* took the opportunity to introduce a *Declaration of Commitment to Cybersafe Healthcare*. The purpose of the session was first to gain participant feedback, but more importantly to gauge organizations' willingness and ability to commit to and live the spirit of the *Declaration*. The *Declaration* commits its signatories to six tangible actions to increase cybersecurity preparedness and resilience:

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 resilience to cyberattacks;
4. **Advance**: Progressing cybersafety in ways consistent with our mandates, 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**: Publishing by Cybersecurity Awareness Month in October 2018 how we will apply these commitments in our unique context and/or with our community.

Attendees were asked about their level of comfort with the *Declaration* and its feasibility for scale within the health sector. Responses from the group were generally positive, though it was noted that delegates would need time to respond to the *Declaration* on behalf of their organizations.

In the months to follow, the *Declaration* will serve as the cornerstone for a Canadian Coalition for Cybersecurity in Health, which will jointly pursue education, information sharing, and other hallmarks of cyber resilience.

Recognizing that the nascent Coalition should include membership beyond those represented at the Summit, participants were asked which other organizations should be engaged as part of a membership drive to raise awareness and the effectiveness of cyber risk mitigation efforts. Participants highlighted the following organizations or leadership structures:

- The academic community
- Clinical associations and regulatory authorities
- The digital technologies supercluster
- Insurers
- Law enforcement
- Ministries of Health
- Municipal governments delivering health services
- Health care providers and regional authorities
- Patient associations
- Privacy and information commissioners' offices
- Health data custodians outside of provider or government networks
- Procurement and shared services organizations
- Health employee associations and unions
- Relevant government depts. outside the health sector
- Héma-Québec
- Standards organizations
- Stakeholders from the health technologies industry
- Innovation incubators and accelerators

Further Options for Collective Progress

The Options Brief prepared in advance of the Summit identified measures that can be taken at various levels to collectively advance cyber resilience in the health sector, based on the experience of other countries and industries. These measures included:

- **Standards**: Incorporating cybersecurity standards into accreditation and/or audit processes;
- **Expanded Training**: Incentivizing regular cybersecurity training or refreshers by means of academic credits or other incentives;
- **Mandatory Reporting & Response**: Obliging organizations to report cyber risks or attacks and/or to respond to identified risk;
- **Readiness Assessment**: Invest in assessments of current levels of preparedness and response capabilities across the sector, tracking changes over time;
- **Practical Exercises**: Holding joint exercises to test cybersecurity preparedness and response capabilities;
- **Certification**: Expanding cybersecurity certification or regulation for digital health products, internet-connected medical devices and related systems;
- **Moral Commitment**: Committing against paying ransoms in response to cyberattacks in order to lower the sector's attractiveness to criminals – while balancing this commitment against the legal responsibilities of healthcare organizations and providers; and
- **Response Network**: Identifying health organization security leads to engage in regular information sharing and who can be contacted before, during, and after serious cyber attacks.

Above and beyond these, participants were asked to generate their own ideas of for achieving substantial increases in health sector cybersecurity resilience. Top-scoring ideas – those scoring above an average of 3 on a 5 point rating scale by Summit attendees – are identified:

- **Standards**: Establish and commit to consistent standards, accountabilities, and standard operating procedures that cross organizational mandates;
- **Hub and Spoke**: Identify Centres of Excellence to lead on 'what good looks like' and provide guidance to others, including by piloting standards and promoting uptake in the broader community;
- **Cybersafe Culture**: Foster a culture of cybersecurity in healthcare by using systematic approaches to educate on cyber risks and their mitigation;
- **Collaboration**: Involve public and private actors from all 10 Critical Infrastructure sectors in national efforts, including by providing capital to address priority risks;
- **Legislation**: Pass legislation related to information security, similar in concept to the *Health Information and Protection of Privacy Act* in the United States;
- **Simulation**: Simulate a cyber attack to raise awareness of potential impacts and strengthen preparedness within the health organization;
- **Benchmarking**: Establish a baseline for cybersecurity in the health sector and set measurable expectations for organizations to achieve within 24 months;
- **Board Education**: Develop a cross-jurisdictional system for educating healthcare executives on cybersecurity; and
- **Threat Exchange**: Radically expand the health sector's participation in the Canadian Cyber Threat Exchange.

Governments, regulators, device manufacturers, and healthcare organizations should give consideration to all of these options as they consider their own strategies for improving cybersecurity resilience both locally and across the health sector.

Conclusion

This report documents the proceedings of the 2018 Canadian Summit on Healthcare Cybersecurity, and acts as compilation of principles to manage healthcare cybersecurity based on the day's discussions. Our sincere hope is that readers will see value in this report as a record of our sector's strengths and failings and the challenges it will face in the months and years to come.

More than serving to educate participants and the broader audience who will read this report, the Summit was an opportunity for healthcare leaders to plant a stake in the ground by declaring their commitment to progress in healthcare cybersecurity. We welcome readers to judge the strength of our commitment in the success of our next steps. In the immediate future, HealthCare*CAN* will be reaching out to Summit participants and other stakeholders within and beyond the health sector to grow the constituency of the *Declaration of Commitment to Cybersafe Healthcare* By October 2018, signatories to the *Declaration* will have published their own plans to increase cybersecurity preparedness and resilience. This will allow for a further exploration of our sector's readiness position and its opportunities to move forward.

As we build the constituency for change, it also falls to signatories to judge how exactly those changes will map onto our organizations, our sector, and our country. As one speaker at the Summit put it, "What we are facing now is the inevitable, and there is no avoiding the inevitable." All of us have a role to play. This report outlines some of the measures that will warrant the consideration of governments, *Declaration* signatories, and allies in the effort to insulate the health sector against cybersecurity threats. We hope that such actors will give these measures their due consideration as they develop resilience and risk mitigation strategies for cybersafe healthcare.

Useful Tools & Links

Participants highlighted tools and resources currently available to help inform and support cyber threat detection and response. Annotated descriptions of some of these tools are included below:

Canadian Cyber Threat Exchange (CCTX) –CCTX is an independent, not-for-profit organization, launched in 2016 that helps Canadian businesses and consumers detect and mitigate cyber attacks. CCTX acts as a node in which threat information from various industries and sectors can be analyzed, to the benefit of all members. Partners in CCTX provide access to internal data, which CCTX then collects, analyzes, aggregates, and anonymizes for distribution within the network. Any threats detected through this process are identified, and all members are alerted to threats with advice on strategies for mitigation. CCTX's approach is consistent with the National Strategy for Critical Infrastructure and the network was recently joined by key federal departments, including Public Safety Canada and the Canadian Communications Security Establishment.

Cyber Essentials - Cyber Essentials Canada is a platform that allows firms to undertake self-assessment of cyber resilience based on five key security controls: (1) firewalls and gateways, (2) secure configuration, (3) access control, (4) malware protection, and (5) patch management. Compliance with Cyber Essentials standards is estimated to prevent approximately 80% of common internet attacks. Certification with Cyber Essentials is compulsory in the United Kingdom for firms doing business with the government.

Canadian Cyber Incidence Response Centre (CCIRC) - CCIRC is Canada's national coordination centre responsible for reducing the cyber risks faced by Canada's key systems and services and works within Public Safety Canada in partnership with provinces, territories, municipalities, private sector organizations and international counterparts. It also coordinates the national response to any serious cybersecurity incident.

Critical Infrastructure Information Gateway - The Canadian Critical Infrastructure Information Gateway is a collaborative, unclassified workspace for the critical infrastructure community with the aim of facilitating information sharing in support of building a safer, more secure and more resilient Canada. Critical infrastructure owner/operators can gain the benefit of joint expertise as well as rapid access to threat information by joining and participating in the Gateway.

Health Insurance Reciprocal of Canada (HIROC) – HIROC is a non-profit insurance reciprocal serving Canada's healthcare organizations with cost-effective and comprehensive insurance coverage and risk management solutions to help subscribers make better decisions. HIROC has published a guide to cyber risk management in Canadian healthcare organizations that includes advice on how to protect your organization from breaches, threats and vulnerabilities.

Firstreceivers.ca – Firstreceivers.ca is a community of practice that links health professionals with up to date resources and news in response to disasters that affect healthcare critical infrastructure. The community is administered by the Centre for Excellence on Emergency Preparedness, which promotes excellence and standards of care for emergency preparedness and response.

American Hospital Association – AHA has been a leader in improving the United States healthcare system's resilience against cyber threats. Incisive commentary and advice on leadership in healthcare cybersecurity is available in AHA's Cybersecurity and Hospitals Series: Questions Hospital Leaders Should Ask and What Hospital Trustees Need to Know.

CSE's Top 10 Security Actions – The Communications Security Establishment (CSE) publishes a set of 'top 10' security actions based on its analysis of cyber threat trends affecting Internet-connected networks. When implemented as a set, the Top 10 help minimize intrusions and mitigate the effects of an intrusion if one occurs.

HealthCareCAN
Leading. Innovation. Together.

HealthCareCAN
17 York Street, Suite 100
Ottawa, Ontario K1N 5S7

(613) 241-8005
1 (855) 236-0213

www.healthcarecan.ca