HealthCareCAN
Leading. Innovation. Together.

SoinsSantéCAN
Leadership. Innovation. Collaboration.

COVID-19 AND CYBERSECURITY

Cyber criminals not deterred by lockdowns

OVERVIEW

The COVID-19 pandemic has led to a welcome increase in virtual care across Canada, with the unfortunate side effect being the healthcare sector is now even more vulnerable to cybersecurity threats. Recently, UK, US and Canadian cybersecurity intelligence services identified Russian intelligence services as responsible for targeting organizations conducting vaccine research. All national cybersecurity agencies are continuing to ring the alarm that pandemic related intelligence is a high priority target. HealthCare*CAN* has examined the implications for our members to provide a roadmap that can mitigate this emerging risk and identify crucial next steps.

PANDEMIC HAS HEIGHTENED CYBERSECURITY RISKS

The COVID-19 pandemic changed the world as we know it. The pandemic resulted in a massive expansion of virtual primary care Canada-wide[1] and more than half of patient visits with health care providers shifted to virtual care[2]. The Canadian Medical Association recently released a poll that showed of the 1,800 Canadians interviewed, 91% stated there were very satisfied with virtual care services and 42% would prefer to continue using them[3] after the pandemic crisis has passed.

HealthCare*CAN* conducted a poll of our members in April 2020 about their immediate needs regarding virtual care during COVID-19 and their responses stressed the importance of increasing support structures. They identified many gaps and some of their main suggestions were:

- Integration with EMRs;
- Better sharing across platforms and regional databases;
- Increasing investment in infrastructure;
- Expanding resources to rural and remote communities.

As our healthcare system continues to increase virtual care services, healthcare organizations must improve their cybersecurity capabilities. It is also vitally important that the healthcare sector realize that cybersecurity is not simply an IT issue. A breach of healthcare facilities can impact the integrity, confidentiality, and availability of vital information (e.g. patient records, appointments, doctor call schedules, procedure room bookings, etc.), which makes securing critical infrastructure a pressing business issue.

Healthcare providers have access to enormous amounts of sensitive data that are attractive to malicious actors. Some of the most common cyber attacks involve:

- **Hacking:** A term that generally describes a third-party's attempt to compromise digital devices and can encompass using any of the tactics described below.
- **Phishing and spear phishing:** An attempt to gain personal data, banking information, and other sensitive information by mimicking or spoofing, a specific, usually well-known brand. They may then use the information to commit fraudulent acts. Spear phishing is highly targeted towards a specific individual and often the corrupt email appears to be from a trusted source and includes personalized information.
- **Ransomware:** A type of malware (harmful software, viruses, worms, etc.) that denies a user's access to a system or data until a sum of money is paid.
- **Denial-of-service (DoS) or a Distributed Denial of Service attack (DDoS):** Any activity that makes a service unavailable for use by legitimate users (e.g. scheduling appointments) or that delays system operations and functions. While a DoS attack uses one device to mount the attack, a DDoS attack uses multiple devices to attack a target e.g. crashing a website by overwhelming it with excessive traffic from multiple devices.
- **Password Spraying:** attempts to gain unauthorized access to a large number of accounts by trying a few commonly used passwords.

[1] Telemedicine and virtual care guidelines (and other clinical resources for COVID-19). Retrieved from: http://www.royalcollege.ca/rcsite/documents/about/covid-19-resources-telemedicine-virtual-care-e
[2] Rapid Response to COVID-19. Retrieved from: https://infoway-inforoute.ca/en/solutions/rapid-response-to-covid-19
[3] Virtual care is real care: National poll shows Canadians are overwhelmingly satisfied with virtual health care. Retrieved from: https://www.cma.ca/news/virtual-care-real-care-national-poll-shows-canadians-are-overwhelmingly-satisfied-virtual

- **Exploiting critical vulnerabilities:** Configuration errors and unpatched software being used on infrastructure. This is of particular concern in the COVID-19 era as organizations rapidly scale up virtual and remote operations.[4]

HEALTHCARE*CAN* CHAMPIONS CYBERSECURITY RESILIENCE

HealthCare*CAN* recognizes the importance of promoting resilient critical infrastructure and cybersecurity. The pandemic has caused a sudden increase in people working remotely without their organization's IT security net (e.g. infrastructure, firewalls, policies, etc.), making the potential of cybersecurity breaches even more likely. The healthcare sector has the added challenges of using legacy technology, lack of funding and resources, and lack of guidance and support from both government and industry. We are involved with several organizations to stay aware of the current situation and mitigate risk for our members.

In October 2019, along with our member Eastern Health in Newfoundland and Labrador, and our partner the **Canada-Israel Industrial Research and Development Foundation (CIIRDF)**, we co-hosted the Canada-Israel Exchange on Cybersecurity in Health in St. John's. The Exchange was created as a tool to mitigate cybersecurity gaps by developing collaboration between Israeli technical experts, Canadian innovation partners (e.g. Telus, Becton, Dickinson and Company (commonly known as BD) or GE Health), health system leaders, and provincial/territorial governments. The agenda for the event centred on two goals:

- Raising awareness on the various cyber security domains and how they map onto healthcare; and,
- Connecting local needs to the expertise of Canadian and Israeli firms to encourage partnerships that meet those needs.

The Exchange shed light on many of our cybersecurity vulnerabilities and some experts estimated that while the optimal investment in cyber security is between 9 – 14% of the overall IT budget, actual investment averages closer to 6%. Experts also shared that globally, the growth in the number and costs of cyber attacks is large and growing. Across industries, healthcare is consistently in first, second, or third place in terms of volume of attacks. The costs of attacks in aggregate grows by double digits every year but the security budget has tended to remain the same.[5]

We are the health sector's representative on the **National Cross Sector Forum on Critical Infrastructure (NCSF).** As a part of the NCSF, we work to maintain 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.

We also work closely with the **Canadian Centre for Cyber Security (CCCS)** to stay abreast of the current cybersecurity threats and attend a weekly health sector COVID-19 call with pan-Canadian health organizations. CCCS warns that network penetration attempts (phishing, hacking, password spraying etc.) have increased. They also warn that criminals may take advantage of increased pressure on Canadian health organizations in response to the pandemic to extract ransom payments or hide other compromises. In a testament to how quickly cyber criminals take advantage of a quickly moving situation, as the Canadian federal government announced the introduction of a contact tracing app, CCCS almost immediately identified a ransomware "CryCrypter", masquerading as the purported app.

[4]Cyber threats to Canadian health organizations. Retrieved from: https://cyber.gc.ca/en/alerts/cyber-threats-canadian-health-organizations

[5] Data gathered from an expert at the Canada-Israel Exchange for Cybersecurity in Health

In May 2020, CCCS highlighted intelligence received from the Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) about continued efforts of advanced persistent threat (APT) groups to target organizations involved in the response to COVID-19. The CCCS has assessed that sophisticated threat actors may attempt to steal the intellectual property of organizations engaged in research and development related to COVID-19, or sensitive data related to Canada's response to COVID-19. Targets have included vaccine and medicine research and development by pharmaceutical bodies and gathering bulk personal information from healthcare bodies. In a recent stunning development, the group APT29 has been linked to Russian intelligence agencies and was previously responsible for hacking political parties in the US and Norway. They are using a variety of tactics such as spear-phishing and exploiting software flaws but are highly adaptable, making cybersecurity vigilance all the more important[6].

OUR GOALS

HealthCare*CAN* advocates for improved awareness and attention to cybersecurity gaps in healthcare, both among our membership and through our strong working relationships with Public Safety Canada, Health Canada, and the Public Health Agency of Canada. We also strive to provide information and share best practices on enhancing cybersecurity in health. To improve the protection of sensitive and private information and provide essential services unencumbered of cyber attacks, we urgently require:

1. **Greater attention towards cyber security in the healthcare sector.** The sensitive nature of healthcare information and the escalation of cyber attacks makes this a critically important arena that is being largely ignored. The threat landscape and its impact on the functioning of healthcare services needs to be clearly and urgently communicated.
2. **Increase in resources for capacity building.** Healthcare organizations need greater investment from the federal government to assist in risk assessment, creation of a centralized security operations center (SOC), provide training to employees, improve cybersecurity resilience, and employ better cyber-defence practices.
3. **Developing national standards for cybersecurity in healthcare organizations.** We have continued to strongly advocate for developing national standards for cybersecurity in healthcare organizations. These efforts have become even more critical with the increase in virtual care and people working remotely.

ROADMAP FOR OUR MEMBERS

HealthCare*CAN* continues to closely monitor this rapidly evolving threat to our sector and has identified key questions for healthcare organizations to use as a starting point when initiating conversations around cybersecurity with senior management teams:

1. Is there an active and effective dialogue within your organization among the Board of Directors, leadership, and the cybersecurity team about where the value is created in the organization, where the critical assets are, and what is their vulnerability to key threats?
2. With the expansion of virtual care, are you considering cybersecurity with a true enterprise-wide lens?
3. In your organization, is protecting critical information seen as an IT issue rather than good business practice?

[6] CSE Statement on Threat Activity Targeting COVID-19 Vaccine Development – Thursday, July 16, 2020. Retrieved from: https://cse-cst.gc.ca/en/media/2020-07-16

4. Are you looking at new ways of investing in cybersecurity to help mitigate risk?
5. Are you considering how you can bring the need for increased funding for cybersecurity to the attention of provincial and territorial governments?
6. How can HealthCare*CAN* help your organization address your cybersecurity needs from a policy and/or advocacy perspective?

FOR FURTHER INFORMATION

HealthCare*CAN* will keep members apprised of developments as they occur. If you have questions, feedback or are interested in discussing specific cybersecurity concerns, we would be pleased to hear from you.

Siri Chunduri
Policy and Research Analyst
schunduri@healthcarecan.ca

Jonathan Mitchell
Vice President – Research and Policy
jmitchell@healthcarecan.ca