From public health to cyber hygiene: Cybersecurity and Canada’s healthcare sector

Alex S. Wilner, Harrison Luce, Eva Ouellet, Olivia Williams and Nelson Costa
Carleton University, Ottawa, ON, Canada

Abstract
The COVID-19 pandemic has ushered in a wave of cyberattacks targeting the healthcare sector, including against hospitals, doctors, patients, medical companies, supply chains, universities, research laboratories, and public health organizations at different levels of jurisdiction and across the public and private sectors. Despite these concerns, cybersecurity in Canadian healthcare is significantly understudied. This article uses a series of illustrative examples to highlight the challenges, outcomes, and solutions Canada might consider in addressing healthcare cybersecurity. The article explores the various rationales by which Canadian healthcare may be targeted, unpacks several prominent types of cyberattack used against the healthcare sector, identifies the different malicious actors motivated to conduct such attacks, provides insights derived from three empirical cases of healthcare cyberattack (Boston Children’s Hospital [2014], Anthem [2015], National Health Service [2017]), and concludes with lessons for a Canadian response to healthcare cybersecurity from several international perspectives (e.g., Australia, New Zealand, the UK, Norway, and the Netherlands).

Keywords
Healthcare, COVID-19, cybersecurity, ransomware, Canada, critical infrastructure

As the COVID-19 public health crisis continues to unfold and evolve, the health sector has emerged as an appealing target for cyberattacks; the sector is, by some accounts, at
its most vulnerable. The COVID-19 pandemic has, as Canada’s Communications Security Establishment (CSE) underscored in its November 2020 National Cyber Threat Assessment, ushered in a wave of different types of cyberattacks targeting the healthcare sector, including against hospitals, doctors, patients, medical companies, supply chains, universities, research laboratories, and public health organizations at different levels of jurisdiction and across the public and private sectors. Recent examples illustrate the scope of the challenge. In June 2019 and March 2020, Health Canada warned that certain wireless medical devices, including insulin pumps, pacemakers, and blood glucose monitors, were vulnerable to cyberattack. The vulnerabilities could allow malicious actors to “deadlock the devices.” In other developments, foreign states have hacked medical laboratories and biotech companies in order to steal research. The US accused Chinese state hackers of doing this in May 2020. Weeks later, the US, UK, and Canada issued a joint advisory noting that malicious actors—“almost certainly part of the Russian intelligence services”—were conducting cyberattacks on organizations involved in developing COVID-19 vaccines, “with the intention of stealing information and intellectual property.” Microsoft followed suit with a November 2020 warning that it had detected state-backed hackers from North Korea and Russia targeting vaccine researchers in Canada, France, India, the UK, South Korea, and the US. IBM issued similar warnings regarding a “global phishing campaign” targeting organizations involved in the COVID-19 vaccine “cold chain,” a part of the “vaccine supply chain that ensures the safe preservation of vaccines in temperature-controlled environments.” IBM noted that the “precision targeting of executives and key global organizations” during the phishing campaign had the “hallmarks of nation-state tradecraft.”

Besides crashing medical devices or stealing data, ransomware attacks against healthcare organizations have also spiked in recent months. On 28 October 2020, the US Cybersecurity and Infrastructure Security Agency issued an unprecedented warning

1. David Burke, “Hospitals ‘overwhelmed’ by cyberattacks fuelled by booming black market,” CBC, 2 June 2020.
2. Canadian Centre for Cyber Security, National Cyber Threat Assessment 2020, November 2020.
3. Health Canada, “Certain older Medtronic MiniMed insulin pumps may be vulnerable to cybersecurity risks,” 29 June 2019; Health Canada, “Cybersecurity risks associated with some medical devices with Bluetooth and Low Energy chips,” 11 March 2020.
4. Robert Lemos, “State sponsored cyberattacks target medical research,” DARKReading, 21 August 2019.
5. Federal Bureau of Investigation, “FBI and CISA warn against Chinese targeting of COVID-19 research organizations,” 13 May 2020.
6. National Cyber Security Centre, “Advisory: APT29 targets COVID-19 vaccine development,” 16 July 2020.
7. Gordon Corera, “Coronavirus: North Korea and Russia hackers ‘targeting vaccine,’” BBC, 13 November 2020.
8. Claire Zaboeva and Melissa Frydrych, “IBM uncovers global phishing campaign targeting the COVID-19 vaccine cold chain,” Security Intelligence, 3 December 2020.
to healthcare providers and hospitals “of an increased and imminent cybercrime threat.”\(^9\) Within days, Russian cybercriminals had unleashed a wave of ransomware attacks against several dozen US hospitals; the group purportedly developed a list of 400 such organizations to target.\(^10\) Charles Carmakal, chief technical officer of Mandiant, a cybersecurity firm, called the attacks “the most significant cyber threat that we’ve experienced in the US to date.” Carmakal reserved special judgment for the hackers’ choice of target: “There is a moral line that every person, just as a human being, recognizes exists—when you do something knowing that you are potentially impacting somebody’s life you’ve crossed the line. This group is incredibly brazen, heartless, relentless.”\(^11\) Indeed, outrage like Carmakal’s may have been the intended point. The attacks were, in part, retaliation for US efforts to dismantle the group’s cybercrime infrastructure leading up to the November 2020 US presidential election, in hopes of limiting election meddling.\(^12\) The organization struck back by disrupting US healthcare in the midst of a surge in COVID-19 infections. And finally, in November 2020, Canada’s CSE highlighted several COVID-19 related scams, including one that sent individuals links to fraudulent websites apparently associated with the Canadian Emergency Response Benefit program—a major component of Canada’s pandemic response—and another that impersonated the Public Health Agency of Canada’s Medical Officer of Health. In response to these recent events, the Canadian federal government, through the Canadian Centre for Cyber Security, has issued a flurry of alerts publicizing the nexus between the pandemic and cyber threats, with a focus on public health and healthcare organizations.\(^13\)

Cybersecurity in Canadian healthcare has long been overlooked and understudied, both from a theoretical and practical perspective, though public health responses to the pandemic have begun to pull back the curtain. As Paul Émile Cloutier, CEO of HealthCareCAN, reiterates, “Cybersecurity represents the hidden pandemic beneath the pandemic we are already facing.”\(^14\) Until COVID-19, the stability of the healthcare sector was often treated as a domain separate from standard discussions on national security—despite being listed as one of Canada’s ten critical infrastructures—when in reality, its resilience is fundamental to the security, welfare, and wellbeing of the country.\(^15\) Today, the cybersecurity of the healthcare sector has shifted from a

\(^9\) Cybersecurity & Infrastructure Security Agency, “Alert (AA20-302A): Ransomware activity targeting the healthcare and public health sector,” 28 October 2020.

\(^10\) Nicole Perlroth, “Officials warn of cyberattacks on hospitals as virus cases spike,” *The New York Times*, 28 October 2020.

\(^11\) Lily Hay Newman, “Ransomware hits dozens of hospitals in unprecedented wave,” *WIRED*, 29 October 2020.

\(^12\) Wayne Rash, “Ransomware group targets hospitals at height of pandemic,” *Forbes*, 29 October 2020.

\(^13\) Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2020*; HealthCareCAN, “Cybersecurity in the time of COVID,” 2020.

\(^14\) Dianne Daniel, “Focused on COVID-19, many have let their guard down on cyber-security,” *Canadian Healthcare Technology* 25, no. 4 (2020): 18.

\(^15\) With thanks to an anonymous reviewer for pressing this point.
consideration of personal safety to one of national security. This article explores the nexus between cybersecurity, healthcare, and public policy, applying comparative lessons from international developments to the Canadian context. Informed by high level consultations with Canadian and international public and private sector cybersecurity and healthcare professionals, we use a series of illustrative examples to highlight the challenges, outcomes, and possible solutions Canada might consider in addressing healthcare cybersecurity.16

Our argument unfolds in six sections. First, we establish the Canadian context, providing the foundational background for our research puzzle. Second, we discuss the Canadian healthcare system, exploring the various reasons and rationales by which the sector may be targeted by cyberattacks.17 Third, we unpack several prominent types of cyberattack against the global healthcare sector seen in recent years. Fourth, we link these types of attack to the actors most involved in their planning. Fifth, providing an empirical backdrop for the different types of and motivations for healthcare cyberattacks, we showcase three specific international examples to illustrate possible cyberattacks: a distributed denial of service (DDoS) attack on the Boston Children’s Hospital (BCH) in 2014, a data breach targeting Anthem Inc. in 2015, and a ransomware attack against the National Health Service (NHS) in 2017. Finally, in the conclusion, we analyze several existing international perspectives on healthcare cybersecurity, providing lessons for a Canadian response. In sum, our analysis explores both the cybersecurity challenges Canadian healthcare and its various stakeholders currently face, alongside the opportunities they have for improving their responses and defences.

16. This article is derived from a 2019 project conducted as part of the Capstone in Canadian Security Policy course, taught by Professor Alex Wilner in collaboration with Government of Canada partners at Public Safety Canada. The views contained herein are those of the authors alone. As part of the project, eight informal consultations were conducted between March 2019 and February 2020 with subject matter experts at Boston Children’s Hospital, eHealth Saskatchewan, HelseCert, the New Zealand Ministry of Health, the Department of Systems and Computer Engineering at Carleton University, Philips, and HealthCareCAN, either in person, by videoconference, or through written correspondence. Subject matter experts helped elucidate the general topic on hand; interview data was neither recorded nor attributed.

17. In keeping with the scope and nature of this paper, we adopt the Canadian Government’s definition of both cyberattack—“the unauthorized use, manipulation, interruption or destruction of, or access to, via electronic means, electronic information or the electronic devices or computer systems and networks used to process, transmit or store that information”—and cyber incident—an “unauthorized attempt … to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource.” Public Safety Canada, National Cyber Security Strategy 2018, 35.
Canadian healthcare and cybersecurity

According to cybersecurity expert David Kennedy, “the medical field is one of the worst when it comes to cybersecurity practices.”18 Hospitals typically dedicate less than 3 percent of their budget towards IT, let alone cybersecurity.19 While other critical infrastructures have a significant private sector component, in Canada, healthcare services are largely provided through public funding from the provincial and federal governments. This creates certain trade-offs. As one cybersecurity expert with experience working with US-based hospitals explained, healthcare professionals often cite financial constraints as a main barrier to implementing effective cybersecurity practices: If a hospital has a certain amount of funding and they can either use that to buy new life-saving equipment they have been waiting for, or, alternatively, to upgrade their network security, they will regularly choose the former. This sentiment illustrates one of the major barriers to changing cyber practices in Canada’s health sector; spending caps and gaps persist and cybersecurity is not traditionally viewed as an issue of patient safety or welfare. Other critical infrastructures like the finance and energy sectors may be targeted more often by cyberattacks, but they also have more resources available to them to guard against an evolving threat.

Canada’s regional health disparities also come into play. Healthcare is a provincially and territorially mandated sector, and as a result, health spending varies considerably. Health organizations in certain provinces have more sophisticated hospitals than other regions. As a result, bigger budgets lead to more advanced technologies, which lead to higher investments in cybersecurity. By contrast, health organizations in other regions of Canada continue to struggle to provide care. Cybersecurity risks are seen as an afterthought given these budgetary constraints. While cybersecurity within the healthcare sector is getting more attention—in part because the global pandemic has shone a light on the issue of information security—resources have yet to increase accordingly, let alone equally, across the country.

The mentality and workplace culture within Canada’s healthcare sector is another obstacle to building cyber-resilience. As several Canadian and international cybersecurity and healthcare experts explained to us, the individuals who run healthcare in Canada have a mentality of service and excellence, and of serving their patients and communities. By contrast, however, the very idea of cybersecurity is itself abstract. Canadian healthcare organizations have a hierarchy of concerns, with patient care at the top. Ultimately, healthcare decision-makers may not consider cybersecurity their primary concern; it is an IT problem, not a healthcare problem. In contrast, as another expert reminded us, not every cybersecurity challenge requires an IT solution. Insider threats, for instance, may require an operational, training, and managerial solution. Financial concerns exacerbate this dilemma: every healthcare dollar spent

---

18. Mark Gollom, “LifeLabs cyberattack one of ‘several wake-up calls’ for e-health security and privacy,” CBC/Radio Canada, 19 December 2019.
19. Luis Ayala, “Cybersecurity for hospitals and healthcare facilities,” Apress, 7 September 2016.
on cybersecurity is a dollar taken away from patient needs, potentially creating further resistance against cybersecurity from within healthcare institutions.

Another dilemma is the lack of information-sharing and transparency among and between different healthcare organizations regarding cybersecurity. When a cyberattack occurs, healthcare organizations may address the issue privately, if only to save face with the public, a challenge expanded upon in the case studies. This reflex is understandable, but it is also precisely the opposite response from that which is needed. A cyberattack happening in one place is inevitably happening elsewhere. As such, the timely and efficient sharing of information is crucial for implementing cyber-resilience across the sector and across the country. Public assurance might be best acquired by building robust cybersecurity measures.

The tension between safety and security is another barrier to cyber-resilience in Canadian healthcare. Safety entails ensuring that internet-enabled medical devices are not harmful to patients, while security refers to the vulnerability of internet-enabled devices to hackers. For example, how do we ensure that the device’s update (i.e., security) will not actually make the device more harmful (i.e., safety)? As it stands, healthcare has been largely focused on safety, to the detriment of security. One Canadian university professor cautioned that there currently exists a complacent attitude in Canadian healthcare, wherein basic security requirements are met without giving serious consideration as to whether these measures are enough to keep up with rapidly evolving cybersecurity trends.

Shifting to policy, given that the Canadian health sector is predominantly controlled on a provincial or territorial basis, significant comparisons must be drawn to develop an accurate national assessment of the sector’s overall approach to cybersecurity. Some overarching Canadian frameworks do exist; Canada has a general privacy framework, The Personal Information Protection and Electronic Documents Act, to which only four provincial health privacy laws have been declared substantially similar (Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia).20 Provinces and territories also differ on breach notifications: in the Northwest Territories and Ontario, notification is required in every case where personal health information is accessed, lost, or stolen. However, in New Brunswick, Nova Scotia, Newfoundland and Labrador, Prince Edward Island, the Yukon, and Alberta, notification is only required when the breach poses a reasonable risk of harm to the affected individual. Another unresolved issue is that many cyber breaches go undetected in the first place, and these various acts do not specify or require any standard of cyber detection in the safeguarding of Canadian health information. Even in analyzing cybersecurity within healthcare, Canada’s approach appears disjointed and regionally driven. For illustration, the Northwest Territories’ hazard identification risk assessment process identifies the risk of critical infrastructure failure within healthcare but neglects to

20. Office of the Privacy Commissioner, “PIPEDA in brief,” January 2018.
address cyber vulnerabilities; failure is mostly understood as being driven by environmental causes, inaccessible winter roadways, and remote access.  

Why target healthcare

Canada’s healthcare sector makes an inviting target for cyberattack for four principal reasons. First, as a critical infrastructure that serves as the very backbone for Canadian healthcare provision, the healthcare sector offers would-be hackers with a potentially high-impact and high-visibility target, a key motivator for certain actors who seek to sow public distrust and doubt in Canadian governments. Second, as in many other developed countries, Canada’s medical sector has experienced mass digitization over the past decade. This trend has sped up with COVID-19. Digitization has itself led to an increased reliance on digital systems across the healthcare sector in service provision. In fact, wireless internet-enabled devices have become involved in every step of the healthcare process, from check-in services, to patient evaluations, diagnoses, and treatment services—and, with the recent arrival of Internet-of-Things (IoT) devices, wearable and implementable technologies are being developed to monitor patient health. By some measure, the global market size of IoT healthcare is expected to grow to over $185 billion by 2025; health data will grow in step. At the same time, a significant number of healthcare organizations are still using legacy systems which are outdated and insecure. A compounding factor is the “technological and organizational complexity of the industry, which makes it difficult to implement and maintain tight security controls.” As a result, this creates more vulnerabilities for potential hackers to exploit in order to access healthcare networks. For illustration, Shodan is a publicly available search engine of internet-connected devices. Using open-source intelligence, it lists all unpatched vulnerabilities and exposed ports associated with a particular network. For this reason, it is often referred to as “the world’s most dangerous search engine.” One study looking at exposed devices connected to hospital networks found that nearly 80 percent of the exposed devices in hospitals around the globe could

---

21. Northwest Territories Municipal and Community Affairs, “NWT Hazard Identification Risk Assessment,” Government of Northwest Territories, 2014.
22. Aurore Le Bris and Walid El Asri, “State of cybersecurity & cyber threats in healthcare organizations,” ESSEC Business School, 2016.
23. World Economic Forum, “Understanding systemic cyber risk,” Global Agenda Council on Risk & Resilience, 2016.
24. Aashish Mehra, “IoT in Healthcare Market worth $188.2 billion by 2025,” Markets and Markets, 2020.
25. Ayala, “Cybersecurity for hospitals and healthcare facilities.”
26. Symantec Corporation, “Cyber security and healthcare,” 2018.
27. https://www.shodan.io/ (accessed 20 January 2022); Marya Rosario Fuentes and Numaan Huq, “Securing connected hospitals,” Trend Micro, 2018.
28. Fuentes and Huq, “Securing connected hospitals.”
be traced back to one hospital in Ontario, useful information for gaining entry into healthcare systems.  

Third, the time sensitivity inherent to healthcare provision makes the sector unique from other critical infrastructures. Without quick and accurate access to medical records, patient care can suffer delays, which can lead to lawsuits against doctors and hospitals. Within these constraints, patient safety is prioritized to the detriment of cybersecurity, and as a result, healthcare employees may be willing to cut corners in cyber hygiene and best practices if doing so provides faster care. For illustration, surreptitiously encrypting hospital records in a ransomware attack has repeatedly proven to be a lucrative crime, leading to large ransom payments because hospitals cannot afford to lose access to patient files. Indeed, healthcare providers may be especially prone and inclined to pay a ransom, to their own long-term detriment. As one expert explained, once this behaviour occurs and is repeated, the organization risks developing a reputation as an easy target; they prove themselves willing to pay a ransom to save people’s lives.

Fourth, the value of personal data has increased on the black market, which extends to healthcare data. In fact, in 2018, the price of stolen medical records was estimated to be worth more than ten times that of stolen credit card information. To put this into perspective, in 2018, the Canadian Internet Registration Authority estimated that confidential medical records could be sold for as much as $1,000 on the dark web versus $5 for credit card information. Medical records are in high demand because the detection period—the lag time between theft and awareness of the theft—is significantly longer than in the case of credit card theft; it can take hundreds of days for a healthcare organization to detect a data breach. That means criminals have more time to put the data to use; unlike stolen credit card information, the value derived from stolen healthcare is longer lasting. The healthcare sector is likewise targeted for purposes of industrial espionage due to the high value of its intellectual property and research data, something COVID-19 researchers are finding out today. Stolen research data, including patient data, can be highly profitable, because research trials require a significant financial investment coupled with years of diligent and careful work.

29. Ibid.
30. Le Bris and El Asri, “State of cybersecurity & cyber threats.”
31. Centre for Cyber Security, Denmark, “Threat assessment,” 2018.
32. Lynne Coventry and Dawn Brantley, “Cybersecurity in healthcare,” Maturitas 113 (2018): 48–52; Ayala, “Cybersecurity for hospitals and healthcare facilities.”
33. Azura Stedman, “Healthcare is under attack,” ProQuest LLC, 2018.
34. Canadian Internet Registration Authority, “Fall 2018: Cybersecurity survey,” 2018.
35. Stedman, “Healthcare is under attack”; Canadian Health Information Management Association (CHIMA), “Professional Practice Brief 0045: Cybersecurity,” 2018; Jennifer Zelmer, “Issue Brief: Critical Infrastructure in Canada’s Health Sector,” HealthCareCAN, 2018.
How to target healthcare

The healthcare sector can be targeted by a range of different types of cyberattack. Five stand out: data breaches, data manipulation, DDoS attacks, ransomware, and med-jacking. In the case of data breaches, malicious actors may seek not only biometric and physical health data on individuals, but also other more tailored information such as recent prescriptions or medical interventions. While data breaches are often fuelled by financial motivations, other actors may steal health-related data for purposes of cyber-espionage and blackmail. The Danish Centre for Cyber Security categorizes these types of data breach as very likely. This subclass of data breach incorporates theft of intellectual property and personal health data of prominent officials—useful for extortion—and probes meant to survey the general cyber defence landscape across the sector or country.36

Similar to data breaches, health data manipulation attacks require a malicious actor to gain access to a digital health record, but instead of exfiltrating this data (or, perhaps, in addition to doing so), they change the information on hand, tampering with electronic health records, potentially causing patient mistreatment and misdiagnosis.37 An additional scenario envisions malicious actors erasing a patient’s known allergy or changing their prescription. Importantly, data manipulation could affect a broad range of healthcare organizations, beyond hospitals, medical clinics, and insurance companies. Changing an individual’s prescription might be most easily accomplished by hacking a local pharmacy, whose cybersecurity measures are likely to be even lower than a local hospital.

Alongside these data-related attacks, malicious actors might pursue DDoS attacks. Here the goal is disruption, rather than theft or manipulation of patient information. These attacks overwhelm web servers with unsustainable amounts of internet traffic, slowing or crashing a target’s ability to function properly. Attackers usually flood a server by first taking control of multiple network-connected machines, often by employing malware, which are then used to amplify web traffic.38 Distributed denial of service attacks on the health sector are neither particularly resource-intensive nor challenging to conduct.

Ransomware is a fourth, and increasingly prolific, type of cyberattack targeting healthcare actors: malicious actors infect a computer or network with malware which is used to lock the system until a financial ransom is paid. The data itself is not usually stolen; it is encrypted, depriving legitimate users of the ability to access it until and unless they pay a ransom. Like other forms of extortion, once a ransom is paid, users are—at least in theory—provided with an encryption key that unlocks their data.39 The

36. Centre for Cyber Security, “Threat assessment.”
37. John Carlin et al., “Click here to kill everybody,” C-SPAN, 11 September 2018; Ayala, “Cybersecurity for hospitals and healthcare facilities.”
38. Cloudflare, “What is a distributed denial-of-service attack?”, 2019.
39. Alex Wilner et al., “On the social science of ransomware: Technology, security, and society,” Comparative Strategy 38 no. 4 (2019): 347–370.
malware that encrypts the data is usually delivered through a phishing email (which fools a user into clicking a link embedded with the malware); by brute-force attacks (where automated software cracks logins and passwords); or as a result of simple human error (where individuals fail to follow proper security protocols). Ransomware attacks share some general characteristics with DDoS and data breaches; they can cripple a healthcare provider’s operational ability and generate revenue for malicious actors.  

Medical device jacking, or medjacking, is a fifth type of healthcare cyberattack. In this case, malware is used against the IoT devices embedded across the healthcare ecosystem, from the tools designed to improve patient care or monitor employee productivity, to specific machines, like cardiac pacemakers, diagnostic equipment (e.g., MRIs), monitoring devices, and life support equipment (e.g., defibrillators). The primary concern with medjacking is that it may constitute the most direct threat to a patient’s physical health. The most frequently used hypothetical scenario is one in which malicious actors identify the serial number of an IoT medical device—a pacemaker, or insulin pump—and manipulate the device’s function, threatening the individual’s physical health. These types of attacks have yet to occur, but are theoretically and technically possible, as aforementioned Government of Canada warnings illustrate. Current medical devices are built with an emphasis on safety (e.g., whether or not the pacemaker will work in extreme temperatures), rather than security (i.e., whether or not the pacemaker is easily hackable).

Who targets healthcare

A range of actors working both internationally and domestically might organize and conduct cyberattacks against Canada’s healthcare sector. Violent non-state actors, including extremist or terrorist organizations, might find Canada’s critical infrastructure an attractive target due to its high-profile nature. Canada’s healthcare sector might be targeted to cause public panic and erode confidence in the Canadian government’s ability to secure and protect Canadians. For this class of actor, success would not necessarily be measured in financial gain, but rather in loss of life and civil disruption. For example, the UK’s NHS websites were hacked in 2017 by ISIS-linked militants and defaced with gruesome images of the Syrian civil war, possibly as a way to promote the group’s cause, humiliate the British government, drive recruitment to their organization, and/or spur sympathetic Brits into conducting domestic attacks. These defacements, however, had little practical effect on healthcare services. And yet, while several different terrorist groups have expressed an interest in conducting cyberattacks

40. Chris Sienko, “Ransomware case studies,” Infosec Resources, 2019.
41. Bob Curley, “Hackers can access pacemakers, but don’t panic just yet,” Healthline, 4 April 2019.
42. Casey Babb and Alex Wilner, “Passwords, pistols, and power plants,” International Journal 74, no. 4 (2019): 518–536.
43. Covent and Brantley, “Cybersecurity in healthcare”; Centre for Cyber Security, “Threat assessment.”
on critical infrastructure, only the most sophisticated groups have the ability to do so.\textsuperscript{44} Moreover, these same groups do not lack the means and motivation to get attention, kill and harm people, and embarrass governments using traditional and far less sophisticated physical attacks. In sum, then, while terrorists might be willing to attack Canada’s healthcare sector in cyberspace for a variety of reasons, doing so would require investments more efficiently served conducting other physical attacks.

Second, hacktivists—politically and thematically motivated non-state actors that use cyberattacks to draw attention to a cause—might target Canada’s healthcare sector. Hacktivists differ from terrorists in that their actions are usually non-violent in nature; they target specific people and organizations they deem problematic, but instead of intending widespread harm or destruction, they seek to promote their cause while degrading their opponent’s stature or capability.\textsuperscript{45} This suggests that hacktivists might prefer to conduct DDoS over other types of attack. Then again, hacktivist groups are often highly decentralized, with a wide range of hacking skills that vary from member to member. This makes hacktivist behaviour and motivation difficult to anticipate since any member can act on behalf of the group, a topic discussed in greater detail below.

Third, other nation states might target Canada’s healthcare sector. The concern here is two-fold and includes cyber espionage and cyberattack. The former is very likely; indeed, it has occurred repeatedly with regards to COVID-19 research, as noted in the introduction. Some foreign states possess both the intent and capability to commit cyber espionage with a view of accessing Canadian research data and intellectual property. Even before the pandemic, this type of activity was common: Chinese hackers targeted eighteen healthcare organizations in 2013 and 2014 alone.\textsuperscript{46} Foreign governments might target research data and intellectual property in the healthcare sector in order to gain a comparative advantage in medical research, to strengthen their own healthcare sector, or to simply gather other useful information and intelligence (including sensitive medical information of prominent individuals).\textsuperscript{47} For illustration, consider Deep Panda, a hacker group believed to be associated with the Chinese government. It carried out operations against health care service and insurance providers like Anthem, Empire Blue Cross Blue Shield, and Premera Blue Cross, stealing social security numbers and other sensitive information. Around the same time, related hacking groups targeted the US Office of Personnel Management, stealing information on millions of American federal employees, including financial information, social security numbers, and fingerprints.\textsuperscript{48} Some experts believe that the information stolen from these various

\textsuperscript{44} Centre for Cyber Security, “Threat assessment”; Ayala, “Cybersecurity for hospitals and healthcare facilities”; Her Majesty’s Government, \textit{National Cyber Security Strategy 2016–2021}, 1 November 2016.
\textsuperscript{45} Institute for Critical Infrastructure Technology, “Hacking healthcare IT in 2016,” 2016; Centre for Cyber Security, “Threat assessment.”
\textsuperscript{46} Fuentes and Huq, “Securing connected hospitals.”
\textsuperscript{47} Centre for Cyber Security, “Threat assessment”; Le Bris and El Asri, “State of cybersecurity & cyber threats.”
\textsuperscript{48} Institute for Critical Infrastructure Technology, “Hacking healthcare.”
hacks was purposefully combined and aggregated into a database for future espionage purposes. As for the latter type of state-sponsored cyberattack meant to cause harm, Danish intelligence suggests adversary states target the healthcare sector to identify potential cyber vulnerabilities which could be exploited in the event of a future geopolitical crisis or conflict. And yet, Canada’s healthcare sector may not be as attractive a direct target to adversary states when compared to other critical infrastructure, such as the energy or communications sectors. The healthcare sector is heavily reliant on essential services including energy, water, transportation, and communications technology, suggesting a hierarchy of targets. Healthcare may be at the bottom of the list if it can be intentionally crippled by the cascading effects of attacking other sectors.

Fourth, criminals tend to be active wherever a profit can be made and where the risks of attribution and apprehension are low. As a result, cyber crime is an especially attractive endeavour. Some criminal entities have the intent and capability to target Canada’s healthcare sector. The threat is two-pronged: cyber-enabled crimes and cyber-dependent crimes. Both share a financial motive, but they differ in characteristics: cyber-enabled crimes are facilitated through computers (data theft); cyber-dependent crimes rely on computers as both a vehicle and a target (ransomware). On the former, criminal entities are thought responsible for approximately 48 percent of data breaches targeting the healthcare sector. While certain criminal entities may have limited programming skills and will resort to purchasing hacking tools from the dark web, other organizations are known to have developed and deployed custom malware to target specific victims. For instance, consider the Orangeworm criminal hacker group. Approximately 40 percent of its victims are healthcare sector organizations located in the US, Europe, and Asia. The group is highly selective in its choice of victim and approach, conducting thorough research prior to carrying out their attacks, and deploying custom malware to infiltrate specific X-ray and MRI machines. On the latter—cyber-dependent crimes—ransomware has become the classic exemplar. For illustration, The Dark Overlord criminal group has targeted several international healthcare organizations. Their modus operandi has remained consistent: identify and target a vulnerable healthcare organization, steal or lock its files, and demand a cryptocurrency ransom. If a healthcare organization refuses to pay, the group releases

49. Ibid.  
50. Centre for Cyber Security, “Threat assessment.”  
51. HM Government, National Cyber Security Strategy 2016–2021.  
52. CHIMA, “Professional Practice Brief 0045.”  
53. Institute for Critical Infrastructure Technology, “Hacking healthcare.”  
54. Centre for Cyber Security, “Threat assessment”; Security Response Attack Investigation Team, “New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia,” Symantec Enterprise Blogs, 2018.
stolen files onto the dark web for resale, publicly naming and shaming the targeted organization. Of all the different actors motivated to target Canada’s health sector, criminals of all stripes are the most likely to do so.

Fifth, and finally, current and former healthcare employees or personnel may be responsible for attacks on healthcare. Indeed, by some accounts, approximately 58 percent of cyberattacks affecting the healthcare sector were facilitated by insiders. At its broadest, an insider threat is defined as “the potential for an individual who has or had authorized access to an organization’s assets to use that access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.” The concern includes both individuals with a desire to cause harm (such as disgruntled employees) and others who inadvertently facilitate attacks by falling prey to phishing schemes, or otherwise share their passwords. Focus here will be placed on the former of the two. Traditionally, insider threats are thought to be influenced “by a combination of technical, behavioural, and organizational issues.” Under certain conditions, greed can play a role. As mentioned, selling unauthorized access to confidential records can be a lucrative business; employees with excessive debt may turn to illicit income streams. One survey of both Canadian and American healthcare organizations found that 29 percent of healthcare employees were aware of someone within their organization selling access to confidential patient data. Incredibly, an additional 21 percent of surveyed employees indicated that they would themselves be willing to sell access to patient data to make an extra profit. Doing so may appear as a victimless crime. Under other conditions, personal vendettas come into play; an employee may become so disgruntled with their place of work that they decide to retaliate by embarrassing or harming their employer. Stressful events such as employer sanctions that are perceived as unwarranted, or lack of recognition, can act as precursors to retaliatory behavior. Additionally, as the chief security officer of one Canadian provincial government health organization noted, employees may interpret the loss of a loved one or of a particular patient as the hospital’s or health organization’s fault; exposing a perceived wrongdoing motivates subsequent insider threat behaviour. In this case, the employee may grant third parties unauthorized access to confidential records to prove employer incompetence, a practice an expert noted occurs more often than most casual observers realize. Under a third set of conditions, employees may be blackmailed, coerced, or otherwise convinced to conduct insider attacks on behalf of an external actor, including criminal organizations. Luis Ayala, a technical expert with the US Department of

55. Centre for Cyber Security, “Threat assessment”; “Another healthcare organization attacked by the Dark Overlord,” HIPAA Journal, 26 September 2017; Gautham Thomas, “Defending your data from the Dark Overlord,” Inside Digital Health, 27 February 2018; Stedman, “Healthcare is under attack.”
56. Verizon, “Protected health information data breach report,” white paper, 2018.
57. Carnegie Mellon University, Software Engineering Institute, “Common sense guide to mitigating insider threats, sixth edition, CERT National Insider Threat Center, 2018.
58. Ibid.
59. HealthCareCAN, “Cybersafe healthcare,” Options Brief Summit Report, 2018.
Defense, argues that specific employees—against which the external actor has compromising information—may be purposefully recruited.60

**Insights from past healthcare cyberattacks**

A review of several different high profile, international cyberattacks targeting the healthcare sector over the past half-decade offers insights for Canada in preparing its own sector for a range of emerging challenges. We present three cases that span the different types of attacks, motivations, and perpetrators discussed in this paper, including a DDoS attack launched against the BCH (2014), a data breach targeting Anthem (2015), and a ransomware attack that struck the UK’s NHS (2017).

**Boston Children’s Hospital**

On 20 March 2014, individuals, working under the banner of the hacktivist group Anonymous, began threatening the BCH on Twitter. The attack began in support of #opJustina, a social media campaign centred on fifteen-year-old Justina Pelletier, a patient at the hospital who had been recently declared a ward of the state. Pelletier’s custody case was a contentious and highly publicised one. Her supporters first threatened the hospital in messages demanding she be returned to her parents. Later, contact information and personal details regarding people involved in her case were published online. Eventually, hackers shared information about the hospital’s website, calling for direct attacks against the institution. One Anon, on March 25, posted: “We need more people attacking 184.154.224.18, fire up your VPN & Tor’s Hammer! #OpJustina #Anonymous #Target.” Several weeks later, beginning in late April, the hospital faced a crippling wave of internet traffic, part of a six-day-long DDoS attack organized to disrupt its services. Alongside the DDoS attack, hackers tried to gain entry to the hospital’s network by directly targeting “exposed ports and services,” and by orchestrating a phishing email campaign targeting the hospital’s staff.61

Boston Children’s Hospital took proactive measures, explained one expert, to ensure that the attackers did not gain entry: it shut down all web-facing applications, including email services, effectively eliminating any ports of entry within the firewall and ensuring that employees could not inadvertently click a malicious link. And because part of the threatening behaviour was playing out on social media, the hospital monitored posts to explore whether Anonymous supporters would reveal their next steps. Fortunately, the attack had little effect on patient care, though it did cost the hospital roughly $600,000 USD in repairs to damaged devices and compromised networks. The

60. Ayala, “Cybersecurity for hospitals and healthcare facilities.”
61. Daniel J. Nigrin, “When ‘hacktivists’ target your hospital,” *New England Journal of Medicine* 371, no. 5 (2014): 393–395; ERT Case Studies, “DDoS case study,” Radware, 21 October 2015; Daniel Nigrin, “How Boston Children’s Hospital survived an attack from Anonymous,” Proceedings from HIMSS Annual Conference, 2017; “Episode 14:#OpJustina,” *Darknet Diaries*, 1 March 2018.
hospital also had to completely reorient its cyber strategy. This included a complete security overview of which services were reliant on the internet, as well as educational training for staff on how to spot a malware email and increase overall cybersecurity awareness.

One expert provided a series of lessons derived from the attack on the BCH. First, hospitals are not immune to a range of cyberattacks. Prior to the incident, few cybersecurity analysts had contemplated the prospect of a DDoS attack targeting the healthcare sector; until then, DDoS was primarily thought of as a financial sector concern. This was a failure of imagination: very few healthcare CIOs considered or prepared for a cybersecurity event of this nature or magnitude. These types of attacks were seen as simply beyond the pale: ethically, morally, and socially unacceptable. A similar sense of public revulsion is felt today regarding attacks targeting efforts to combat and defeat COVID-19. Second, hospitals need to be aware of their dependencies: what day-to-day processes depend on a viable network, and what happens if that network is lost? Charting out an institution’s dependency on the internet is critical to its ability to respond to cyberattacks. Hospitals must have mitigation strategies in place to function offline. Electronic health records are a good example of this: during the DDoS attack, the system appeared to be running smoothly on the surface, though below it, certain components—like prescription routing—were not able to function properly offline. The hospital had to strategize new ways to provide patients’ medication without network access. Third, hospitals need a communication contingency plan. As noted, email services were interrupted during the DDoS attack. Coincidentally, however, BCH had recently established a secure texting platform, not out of cybersecurity concerns but rather to provide better services. The platform provided the hospital with an alternative to email. Finally, raising awareness is as important as raising security measures. Health providers may engineer and implement as many cybersecurity measures as they want, but educating staff is just as critical. One approach BCH has adopted since the DDoS attack is to conduct hacking simulation exercises to raise awareness and preparedness.

Anthem

On 27 January 2015, a database administrator at Anthem Inc.—an American health insurance provider—noticed irregular search queries being conducted through their account that they did not themselves initiate. Suspecting that their account may have been compromised, the administrator reported the event. Two days later, Anthem alerted federal authorities, triggering an independent assessment by a third-party investigator. On 4 February, Anthem disclosed the breach to the public. According to investigators, the breach, which was initially assumed to have occurred on 10 December 2014, had in fact taken place on 18 February 2014, nearly a full year
before anybody realized anything was wrong. The vector for the attack was an employee innocently opening a phishing email and downloading a malicious file. In May 2019, the US Department of Justice officially attributed the attack to several Chinese nationals.\footnote{Department of Justice, “Member of sophisticated China-based hacking group indicted for series of computer intrusions,” 2019.}

The breach led to one of the largest data heists in American history: records on over 78 million individuals were compromised.\footnote{Marianne McGee, “A new in-depth analysis of Anthem breach,” BankInfo Security, 2019.} Anthem reported that the information accessed included “names, birthdays, social security numbers, street addresses, email addresses and employment information, including income data.”\footnote{Anthem Inc., “Statement regarding cyber attack against Anthem,” 5 February 2015.} The fallout was swift and severe; a class action lawsuit was eventually settled for $115 million—one of the biggest settlements on record—with an additional $15 million rewarded to plaintiffs for related expenses.\footnote{Rachel Arndt, “Anthem settles data-breach litigation for record $115 million,” Modern Healthcare, 23 June 2017; Department of Health and Human Services, “Anthem pays OCR $16 million in record HIPAA settlement,” 15 October 2018.} With support from the US government, Anthem reviewed its entire system, initiated a company-wide resetting of passwords, created new network admin IDs to replace existing ones, launched a series of cyber awareness campaigns, invested in bolstering its cybersecurity measures by adopting mandatory two-factor authentication, and developed a cybersecurity response plan to help the organization better manage other and related threats.\footnote{McGee, “A new in-depth analysis of Anthem breach.”} A major lesson derived from Anthem’s data breach is that the human perimeter around IT systems is sometimes the weakest link in cybersecurity. In essence, the breach took place because of human error.

**National Health Service**

On 12 May 2017, ransomware known as WannaCry began to infect and spread across computer systems around the globe, encrypting its victims’ files through a vulnerability of Microsoft Windows, and demanding a ransom be paid for their release. Over 200,000 computers in 150 countries, including in Canada, fell victim. Hardest hit was the UK’s NHS; a vast majority of the roughly 230 NHS trusts across England reported disruptions, with thirty-four of them being locked out of their devices and data. With patient data and systems crippled by the ransomware, crucial surgeries and other medical procedures were cancelled and hospitals were placed on diversion status. Some organizations, including Barts Health NHS Trust, were so adversely affected that they...
were unable to provide care; they were forced to divert patients to other hospitals. As the attack unfolded, trusts lost access to email services either because they had been affected by the virus or because email services were shut down as a precautionary measure. As a result, the affected health organizations did not know who to contact nor how to mitigate the attack internally.\textsuperscript{67}

The attack, however, ceased as suddenly as it had started. After a cybersecurity researcher surreptitiously identified and triggered a kill-switch located within the ransomware, WannaCry’s global and institutional spread slowed. By 19 May, the attack was over, and though still reeling, NHS was able to reorganize its efforts towards repairing its information technology systems and bringing services back to full capacity. While no NHS organization paid the ransom, the costs inflicted on the NHS were substantial, with an estimated loss of £5.9 million. Canceled appointments, additional IT support from local NHS bodies and IT consultants, the restoration of data and affected systems, and overtime accrued by national and local NHS staff were all critical.\textsuperscript{68}

Various aspects of the NHS’s information infrastructure ecosystem made it particularly vulnerable to malicious cyberattacks. First, software patches can be difficult to implement effectively when information systems are not themselves upgraded. In the case of WannaCry, a patch released by Microsoft in March 2017 would have protected computer systems from infection; the patch was generally free to users of Windows’ current programs, though users with older versions of software, such as Windows XP, were required to pay for the upgrade. While hospital budgetary considerations might have forced some organizations to deemphasize information system security, more than 90 percent of NHS devices were indeed operating Windows 7, eligible for the free patch. And yet, by the time of the attack in May, the majority of these devices were still unpatched, despite government alerts issued on March 17 and April 28 requesting that users do so. In addition to these oversights, according to NHS Digital, given that WannaCry spread through the internet through the N3 broadband network that connected all NHS sites in England, improved management of firewalls would have better guarded against the ransomware’s spread.\textsuperscript{69} Second, prior attempts to bolster cybersecurity within the NHS were neglected. Reports published by the National Data Guardian and the Care Quality Commission in July 2016 warned the Department of Health of ongoing vulnerabilities within the system and the risk of losing patient

\textsuperscript{67} Tobias Mattei, “Privacy, confidentiality, and security of healthcare information: Lessons from the recent WannaCry cyberattack,” \textit{World Neurosurgery} 104 (2017): 972–974; National Audit Office, “Investigation: WannaCry cyber attack and the NHS,” 2018; UK Parliament, “Cyberattack on the NHS,” House of Commons Committee of Public Accounts, 18 April 2018; John Riggi, “Ransomware attacks on hospitals have changed,” American Hospital Association Center for Health Innovation, May 2020.

\textsuperscript{68} Lily Newman, “How an ‘accidental killswitch’ slowed Friday’s massive ransomware attack,” \textit{WIRED}, 13 May 2017; Saira Ghafur et al., “A retrospective analysis of the WannaCry attack on the NHS,” \textit{Digital Medicine}, 2 October 2019; Shireen Khalil, “WannaCrypt cyber-attack continues to impact NHS trusts,” \textit{Digital Health}, 19 May 2017.

\textsuperscript{69} National Audit Office, “Investigation.”
information and data. The Department of Health did not respond until July 2017, two months after WannaCry’s devastation. Other initiatives put forward by the Department of Health, including migrating away from unsupported Windows XP software—a process which began in 2015—repeatedly failed to meet internal deadlines; all the while, cybersecurity assessments conducted by NHS Digital lacked an enforcement mechanism to ensure compliance. Further, the NHS had no clear guidelines for responding to a nation-wide cyberattack, which made it difficult once WannaCry struck to determine who would lead the response, how communications within NHS and the UK government would function, and which agency—if any—NHS organizations would report specific attacks to.70

In response to WannaCry, the Department of Health, NHS, and other related organizations later identified several tasks needed to bolster the health sector against future cyberattacks. First, a response plan was developed setting out what the NHS should do in the event of a cyberattack that further established clear roles and responsibilities for local and national NHS bodies and the Department of Health. Second, NHS organizations were to ensure the full implementation of CareCERT alerts—emails sent by NHS Digital providing information or requiring further action—including applying software patches and updating anti-virus software. As part of this process, trusts were to individually assess the specific cybersecurity needs of the equipment they possessed: for instance, some devices like MRI scanners purportedly had Windows XP embedded into the machine that required a vendor, rather than the hospital, to trigger the update. Third, an approach to essential communications was established to ensure that the flow of critical information within and beyond NHS could continue in spite of a cyberattack that took some systems offline. And fourth, healthcare organizations, boards, and staff were to ensure the sector took cybersecurity more seriously, linking cybersecurity to frontline services and building greater cyber-resilience that would minimize future disruptions to patient care. Part of this learning process entailed voluntary cybersecurity inspections to ensure best practices were being put to best use.71

Securing Canadian healthcare: Lessons from abroad

The COVID-19 pandemic and the associated social, technological, and economic responses are forcing Canadians to reassess and reinterpret the cybersecurity challenges they face in securing their healthcare sector. While other countries find themselves in a similar immediate situation, many of them have previously addressed cybersecurity in healthcare as a result of local developments, past crises, and previous initiatives. Canada is still catching up, providing it with an opportunity to learn from others’

70. Ibid.
71. IDG Contributing Editor, “The lessons of WannaCry attack,” CSO Online, 28 June 2017; Department of Health & Social Care, “Lessons learned review of the WannaCry ransomware cyber attack,” February 2018.
experience. By way of conclusion, what follows is an overview and analysis of different cybersecurity approaches and models derived from Australia, New Zealand, the UK, Norway, and the Netherlands, providing Canada with examples, highlights, and lessons for better protecting its own healthcare sector. 

First, Australia’s Digital Health Cyber Security Centre was created as part of the Australian Digital Health Agency (the Agency) to help protect digital health technologies, safeguard personal health information, and improve the overall resilience of Australia’s healthcare sector. Because cybersecurity continues to evolve, the organization, in alignment with other federal partners—notably the Australian Cyber Security Centre—plays a key prevention role in developing cyber threat reports that outline emerging challenges, risks, and concerns that are likely to impact the healthcare sector directly. The Centre disseminates threat alerts and associated mitigation strategies to healthcare providers across Australia. It also provides nation-wide cybersecurity training and awareness campaigns to healthcare organizations and their personnel, adding another layer of protection. It provides a range of useful cybersecurity information to healthcare practitioners, from advice on building a culture of cybersecurity excellence, to protecting healthcare consumers and small businesses. The Centre also has a crisis management and leadership function: in the event a major cybersecurity attack successfully targets Australia’s healthcare sector, it would help coordinate the national response alongside other federal partners.72 For Canada, the lesson might entail building a specific federal body or organization—potentially within or alongside CSE’s Canadian Centre for Cyber Security, Public Safety Canada, or the Public Health Agency of Canada—with a mandate to oversee cybersecurity within Canada’s healthcare sector, providing healthcare-specific best practices and advice that resonate across Canada’s provinces and territories. The organization would help level the disparities in Canadian healthcare that currently include inequalities in cyber-preparedness.

Second, the New Zealand Ministry of Health—in its capacity of exercising stewardship across the healthcare sector—created a healthcare cyber response plan specific to the sector. New Zealand’s healthcare system—much like Canada’s—is managed independently by district health boards.73 Traditionally, management extended to IT systems. Following the WannaCry attack, it became clear that this disparate approach to decision-making and information-sharing was less than optimal. As one New Zealand expert explained, if one healthcare organization is experiencing a problem, there is an increased likelihood that others are also experiencing the same

72. Cyber Security Centre, “Cyber security,” Digitalhealth.gov.au, 2019; HealthCareCAN, “Cybersafe healthcare”; Global Digital Health Partnership, “Securing digital health,” white papers, 2019; Australian Digital Health Agency, “Supporting a positive security culture,” 2020; Australian Digital Health Agency, “Supporting a positive security culture,” 2020; Australian Digital Health Agency, “Think before you click-protect your healthcare customers,” 2020; Australian Digital Health Agency, “Information Security Guide for small healthcare businesses,” 2020.

73. Global Digital Health Partnership, “Securing digital health.”
issue, elevating the challenge to the national level and requiring government action. As a result, New Zealand began breaking down its healthcare silos. Its cyber response plan identifies criteria for the activation of a nation-wide and cross-sector response, clarifying issues over leadership and decision-making. New Zealand’s approach was to find a way to standardize incident escalation criteria and centralize strategic decision-making to make it more efficient, while at the same time respecting jurisdictional control over healthcare. In the event that a cyber incident meets the activation criteria, the Ministry of Health is given a mandate to facilitate and support a wider, cross-jurisdiction response. The plan has eliminated the ambiguity that once existed regarding crisis decision-making and emergency leadership. Importantly, it was created with bottom-up input from the sector itself to work with healthcare cultural norms, rather than against them. As a result of this input from the sector, the plan has cultivated support from health providers. Framing cybersecurity within the context of patient harm and trust and confidence—something the healthcare sector cares deeply about—has reduced resistance to cybersecurity planning within the sector. New Zealand’s collaborative approach with healthcare organizations in developing the cyber response plan has been a key part of its success.\(^\text{74}\) The lesson for Canada is that building a pan-Canadian cybersecurity response policy, plan, and strategy—alongside healthcare organizations—in advance of a major cybersecurity incident will go a long way in identifying the parameters of emergency response, management, and leadership that suits the sector’s unique organizational and jurisdictional constraints. Cybersecurity prevention may be the best cure.

Third, various healthcare-specific computer emergency response teams (CERTs) developed in the UK (CareCERT), Norway (HelseCERT), and the Netherlands (ZorgCERT) were created to better prepare healthcare organizations to address cybersecurity concerns and challenges. CareCERT, for instance, was created as part of NHS Digital to provide situational awareness of the emerging cybersecurity landscape, and to carry out preventive assessments by training healthcare sector employees in cyber hygiene, providing guidance to healthcare organizations for improving their cybersecurity capabilities, and assisting in containing and defeating cybersecurity attacks if and when they struck.\(^\text{75}\) For example, as a result of a breakdown in communication among NHS organizations during the WannaCry attacks, CareCERT developed the capacity to deliver updates through SMS alerts to affected organizations.\(^\text{76}\) HelseCERT was likewise created because Norway understood that different critical infrastructures, including healthcare, needed dedicated and tailored resources, something that could not be assured by only one general CERT whose resources were shared across all critical sectors. As noted by an expert, the constant development and improvement of HelseCERT is a key deliverable according to the Norwegian Health Network’s mandate, and is publicly funded through Norway’s national budget; all government-run

\(^\text{74}\) Ibid.

\(^\text{75}\) Jon Hoeksma, “NHS Digital to roll out new CareCERT cyber security services,” Digital Health, 2016.

\(^\text{76}\) NHS Digital, “CareCERT uses SMS alerts to boost NHS communications for cyber incidents,” 2017.
healthcare providers participate in the program, in addition to some private sector organizations, such as healthcare software developers. HelseCERT provides prevention services, including vulnerability overviews, white hat hacking exercises, and threat advisories, and provides advice and recommendations on how detected vulnerabilities can be mitigated. It also assists in event-response by coordinating efforts and facilitating information-sharing. Like its European counterparts, Zorg-CERT provides services for all healthcare providers in the Netherlands, including prevention and detection services, information-sharing, and incident response. It functions, however, as a non-profit organization, acquiring its funding partially from public funds and participating healthcare providers. The lesson for Canada is that healthcare, as a critical infrastructure, needs dedicated and nuanced cybersecurity attention, expertise, and support tailored to the specifics of the sector. Good cyber health flows from understanding the disease.

Taken as a whole, our exploration and analysis of Canadian healthcare cybersecurity suggests the discourse has begun shifting from public health and personal safety to national security. This shift in focus predates, but was accelerated by, the COVID-19 pandemic. Two avenues for further research present themselves. From an academic perspective, a more nuanced understanding is needed of critical infrastructure protection, both in theory and empirically. On the former, scholarship should continue broadening the traditional scope of critical infrastructure studies from the physical to cyber domains, and better incorporate state, sub-state, and societal perspectives into its analysis. On the latter, among and between the disparate infrastructure categories listed in Canada, empirical lessons in cyber and physical security from one might be better applied to another, building towards a general consensus of shared and transferable observations across all critical infrastructures. Similar analysis might probe commonalities among and between different countries, building towards an international consensus. From a policy perspective, these theoretical and empirical lessons might be better woven into practical responses, both in Canada and abroad, that help guide the development of functional and equitable cybersecurity systems that bridge the divide between federal, provincial, and local governments, and private, non-profit, and societal stakeholders.

**Declaration of conflicting interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

77. Global Digital Health Partnership, “Securing digital health”; Z-CERT, “Services,” Computer Response Team for Healthcare, n.d.

78. Babb and Wilner, “Passwords, pistols, and power plants,” 2019.
Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

Alex S. Wilner  ➥ https://orcid.org/0000-0003-2087-252X
Nelson Costa  ➥ https://orcid.org/0000-0002-3987-7913

Author Biographies

Dr. Alex S. Wilner is an associate professor at the Norman Paterson School of International Affairs (NPSIA), Carleton University, Canada.

Harrison Luce is a graduate of the Norman Paterson School of International Affairs’ MA program. He was part of the 2019 Capstone cluster that helped produce the article.

Eva Ouellet is a graduate of the Norman Paterson School of International Affairs’ MA program. She was part of the 2019 Capstone cluster that helped produce the article.

Olivia Williams is a graduate of the Norman Paterson School of International Affairs’ MA program. She was part of the 2019 Capstone cluster that helped produce the article.

Nelson Costa is a graduate of the Norman Paterson School of International Affairs’ MA program. He was part of the 2019 Capstone cluster that helped produce the article.