




5/5/2023

Cyber Threat Intelligence in Canada



Scott Davenport -scottdavenport80@gmail.com,
David Macintyre -davidmacintyre01@gmail.com,
Jace Stelman -jstelman27@outlook.com
NORMAN PATERSON SCHOOL OF INTERNATIONAL AFFAIRS (NPSIA),
CARLETON UNIVERISTY

Contents

Executive Summary ii

Introduction 1

Cyber Threat Intelligence Overview and Definitions 2

Literature Review 4

Methodology 6

Analysis of Canadian Sectors 7

 Healthcare 7

 Agriculture 10

 Finance 14

 Higher Education 18

Broad Gaps and Recommendations 21

 Technical Deficiencies 21

 Legal Deficiencies 23

 Organizational Deficiencies 24

 Lack of Transparency 25

Conclusion 26

Bios 29

Bibliography 29

Appendices 37

Executive Summary

This study aims to identify gaps in the Canadian Cyber Threat Intelligence (CTI) sphere and provide possible solutions by cross-examining case studies against cyber security and intelligence frameworks. The selected case studies represent sectors – health care, agriculture, finance, and higher education – with varying vulnerability, targetability, and criticality. The study analyzed the overlooked issues in CTI in each sector to identify overarching gaps that exist across Canada. The gaps identified are legal, technical, organizational, and information sharing. Each case study illustrates at least one of each gap with specific examples in which those gaps were exploited and resulted in a successful cyber breach from a threat actor.

The first case study examined the cyber security of the Canadian healthcare sector. It was discovered that the healthcare sector is a highly vulnerable target due to the critical nature of its services and the valuable sensitive information it houses. The use of new technologies at every level of the organization has presented new vulnerabilities. The poor cyber security practices, lack of cyber awareness among staff, and outdated software has also added to the sector's vulnerability to cyber attacks. The fragmented nature of the healthcare system and it being largely run by the public sector create a culture that does not prioritize cyber security.

The second case study examined the Canadian agriculture sector. The vulnerabilities that exist in this sector are due to a lack of cyber security defenses, awareness, and standards. Recent cyber events have exposed gaps in technological deficiencies and a lack of transparency, with the same threat actor being able to target major organizations in the sector with the same type of attack within days of each other. The agriculture sector represents an embryonic sector in cyber security with little protective measures and an ignorance to their growing dependence on cyber systems. As the sector continues to digitize and innovate out its manual back-up systems, its dependency on IT systems coupled with a lack of defenses makes it vulnerable to attacks that could have disastrous consequences, given the sector's critical importance to Canada's well-being.

The third case study examined the Canadian finance sector. It is one of the most protected sectors in the country. Yet despite its robust protective measures it still has sizeable gaps, including a notoriously slow timeframe for detecting and containing cyber intrusions. While it is the most protected sector, it is also the most targeted by threat actors due to the financial and highly sensitive information it stores. Three successful cyber attacks are discussed to illustrate the timeliness and importance of CTI and to inform on the current gaps that exist in the Canadian financial sector.

The final case study examined the Canadian education sector, specifically its Higher Education Institutions (HEIs). Like other sectors, it has experienced an increasing number of cyberattacks. The decentralized organizations, coupled with the high volume of sensitive data stored make them an ideal target for threat actors. Despite the upward trend in cyberattacks, there is still a legal confusion on how to handle cyber security

incidents within the education sector, as federal legislation does not apply to the education sector, except in a few provinces.

Out of the case studies, four gaps emerged from their analysis: legal gaps, organizational gaps, transparency gaps, and technical gaps. The research identified gaps in Canadian legislation around cyber security. Current laws, such as PIPEDA, only apply to personal information collected through commercial activity and have minimal punitive damages for non-compliance. Bill C-27, which is currently proposed legislation, would result in the mandated organization the ability to impose higher fines. Despite the new proposed legislation, Canadian laws still need to be updated to incentivize increased investment in CTI.

Organization gaps in cyber security is caused by the tension between standard business structures and the increasing sophistication of cyber threats. To address this gap, CTI needs to be plugged in at every level of the organization while increasing the basic cyber hygiene of each employee, changing the culture to a proactive rather than reactive approach to CTI, and making management aware of the cyber landscape to better inform the executive responsible for strategic decision making.

The lack of transparency is another cyber security gap. While the public sector is better positioned for intelligence gathering and dissemination, the private sector lacks the redundancies and manpower to replicate such a system. Therefore, to address the lack of intelligence being gathered and shared to make organizations more cyber resilient, third-party associations should be created and leveraged to allow for intelligence sharing while maintaining anonymity and competitive advantage.

The final gap identified are technical abilities. While all sectors have increased their reliance on cyber systems, many sectors still are outdated in their protective measures, with some completely and ignorantly unprotected. Most of the literature discusses the tactics, techniques, and practices (TTPs) of cyber security however the analysis of each sector points to a lack of education and awareness on how dependent yet unprotected much of the country's sectors are.

In all four of these gaps, cyber threat intelligence can be leveraged to help fill these gaps and make Canada's public and private organizations more cyber resilient to mitigate the increasing threat of cyber attacks.

Cyber threat intelligence can be used to address technical deficiencies in several ways. To address issues regarding networks, it can be used to create policies regarding what devices may connect to networks and maintaining separate rather than merged networks. Policies concerning third party contractors and vendors can help ensure they have appropriate cyber security standards to limit additional vulnerabilities. They can also be used to certify high cyber security standards in publicly accessible spaces for organizations who use public facing points.

Government regulations and policies can help promote CTI and address the legal deficiencies that exist in Canada. Legislative reform such as bill C-27 will help impose

larger legal penalties for organizations with lax cyber security practices. These can help incentivize companies to increase investment in CTI as proactive mitigation.

To address the organizational deficiencies, organizations can build their cyber security by operationalizing CTI in many ways. First, they must change their perspective of investing in cyber security, viewing it as a necessary protection in the short run to avoid potentially catastrophic losses in the long run. They can educate their entire workforce through administering basic cyber hygiene training. They can have their IT teams approach CTI proactively rather than reactively and provide them with intelligence training to help identify future threats. Finally, they can require middle management to be constantly aware of the cyber landscape of their organization to keep cyber threat intelligence on the minds of managers and executives.

To address the final gap in this report, the lack of transparency in CTI, information sharing can be promoted, both horizontally to government bodies and vertically to other organizations within the sector. A recommendation to facilitate such information sharing is to leverage pre-existing business associations to disseminate key intelligence to all relevant parties. Such information sharing practices can help build cyber security in the sector to help protect not only individual organizations but Canada as a whole.¹

¹ This report was completed as part of the "Capstone in Canadian Security Policy," hosted by Prof Alex Wilner, at the Norman Paterson School of International Affairs, Carleton University, in partnership with Accenture.

We would like to thank Maryam Jafari Lafti and Victor Munro for their support throughout this process and we are greatly appreciative of their efforts in ensuring that we had the guidance necessary to complete this report.

Introduction

The practice of collecting and analyzing information to predict threats seems to be intrinsic to the human experience. This process, broadly referred to as intelligence, was folded into military domains at its most rudimentary level in the aftermath of the Napoleonic wars and has existed in its modern form since the end of the second world war.² However, we are living in unprecedented times where threats lurk around every corner, and the state is no longer the sole key victim of nefarious action by other states or criminal actors. Technology and, more specifically, the proliferation of cyberattacks have put everyone on the frontline.

Cyberthreats are becoming ubiquitous, as our society becomes ever more technologically dependent. In 2021, there were over 70,000 reported crimes in Canada.³ Despite this, the infrastructure to appropriately respond to cyber-attacks is still nascent. While states retain a variety of intelligence approaches for responding to cyber threats, other facets of society are still particularly vulnerable. Businesses and individuals lack the same knowledge and know how to adequately address cyber security. While the question of the individual is still immensely elusive, there is progress regarding the response of business. One evolving practice is the incorporation of Cyber threat intelligence (CTI) as a means to proactively address cyber threats.

Cyber threat intelligence is the use of intelligence work to augment cyber security. CTI can be used to identify threats, threat actors, security vulnerabilities and any other information that might help an organization protect itself. CTI also involves an important educational component which seeks to make organizations more resilient through raising awareness and knowledge of cyber threats and proper cyber security practices.

As will be addressed later in this report, CTI has generally been hyper-focused on the technological components of the process. We seek to provide a greater understanding of how to operationalize CTI, specifically emphasizing its implementation beyond the technical level. Focusing on salient Canadian sectors, we identify weak points in current CTI practices. To this end, our report covers an overview of cyber threat intelligence, where key definitions are laid out. Subsequently, we conduct a review of the academic literature on CTI, which is still in its infancy, in order to provide a thorough understanding of the major debates surrounding this process. The next section will describe this report's methodology, where we focus on case studies on the state of cyber security in several Canadian sectors, including healthcare, agriculture, finance and higher education. These sectors each display variation in criticality, targetability and vulnerability. Each case study

² Mark Phythian, *Understanding the Intelligence Cycle* (London, UNITED KINGDOM: Taylor & Francis Group, 2013), 9-13. <http://ebookcentral.proquest.com/lib/oculcarleton-ebooks/detail.action?docID=1209543>

³ "Police-Reported Cybercrime, Number of Incidents and Rate per 100,000 Population, Canada, Provinces, Territories, Census Metropolitan Areas and Canadian Forces Military Police," Statistics Canada, August 2, 2022, <https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510000201>.

highlights broad gaps in Canadian cyber security and CTI. These four case studies show that CTI in Canadian business suffers from technical, legal and organizational deficiencies as well as a lack of transparency. For each of these broad gaps we provide a series of recommendations with the objective of improving the operationalization of the cyber threat intelligence in Canadian businesses.

Cyber Threat Intelligence Overview and Definitions

Cyber Threat Intelligence is a new field. Different experts with various backgrounds (business, IT, intelligence services, law enforcement, etc.) have a range of views as to how to define and approach the subject. Accordingly, no one set definition exists. Some experts use traditional definitions of “intelligence”, seeing CTI akin to traditional intelligence gathering.⁴ For the purposes of this report, we have decided to utilize a definition that is specific to CTI, and which emphasizes the cyber threat element of intelligence. Some definitions are general while others are more technical or specific in their approach.

Technical definitions include the application of the intelligence cycle or other specific tools. Other definitions specify types of threats or vulnerabilities about which CTI should seek to gain knowledge. An appropriate definition for the purposes of this report will facilitate a broad approach to examining CTI. Technical definitions narrow the scope of study, limiting the issues and solutions we can analyze. As such we have elected to take on a broader definition. This inclusive approach to CTI, gives more flexibility in identifying and mitigating cyber threats.

Accordingly, we’ve decided to use the definition provided by Shin and Lowery in, “A review and theoretical explanation of the cyberthreat-Intelligence (CTI) capability”. They define cyber threat intelligence as:

“CTI represents actionable threat information tailored to a specific organization that requires careful attention and prevention. CTI consists of activities designed to recover threat information germane to a specific organization to engineer more precise defense strategies. This information includes threat types, sources, actors, technologies, and attack vectors.”⁵

This definition will maintain an emphasis on Cyber Threat Intelligence while offering flexibility to analyze technical and organizational challenges while offering

⁴ Kris Oosthoek and Christian Doerr, “Cyber Threat Intelligence: A Product Without a Process?,” *International Journal of Intelligence and Counterintelligence* 34, no. 2 (2021): 305, <https://doi.org/10.1080/08850607.2020.1780062>.

⁵ Bongsik Shin and Paul Benjamin Lowry, “A Review and Theoretical Explanation of the ‘Cyberthreat-Intelligence (CTI) Capability’ That Needs to Be Fostered in Information Security Practitioners and How This Can Be Accomplished,” *Computers & Security* 92 (2020), 1, <https://doi.org/10.1016/j.cose.2020.101761>.

technical and organizational solutions. It emphasizes actionable intelligence that is specific to an organization which provides useful guidelines for our goal of operationalizing CTI.

Other key concepts relevant to the discussion of CTI include tactical technical procedures (TTPs), indicators of compromise (IoCs) and the intelligence cycle. Each refers to the foundational elements of a functioning CTI process. TTPs refer to:

“The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.”⁶

TTPs are used for counterintelligence purposes. They are used to develop a profile of threat actors and to link them to cyber attacks.⁷

Indicators of compromise (IoCs) are evidence that a system or network has been breached. In digital forensics, they are used to detect and identify malicious actors and their activity. Common IoCs include unusual and unexplained traffic, unknown applications, strange IP addresses or domain names, and unusual activity from privileged and administrator accounts.⁸

The Intelligence Cycle is an intelligence framework used to develop intelligence. The steps of the cycle are direction, planning, collection, analysis, dissemination, and feedback.⁹ This popular model is utilized by the Government of Canada and its allies. Many variations of this model exist, however it is typically conceptualized to function as a linear series of events, while in reality several of these steps operate simultaneously.¹⁰

The final concepts to be defined within the context of Cyber Threat Intelligence are the levels of governance at which it operates. These are the strategic, operational, and tactical levels. The strategic level of CTI is the broadest level of analysis focusing on types of threat, threat actor profiles and organization criticality and vulnerability.¹¹ The operational level informs daily decision making and involves trend analysis, cyber attack

⁶ What Are Tactics, Techniques, and Procedures (TTPs)?, Feroot Education Center, n.d., <https://www.feroot.com/education-center/what-are-tactics-techniques-and-procedures-ttps/>.

⁷ Ibid.

⁸ “Indicators of Compromise (IoC) Security,” CrowdStrike - Cyber security 101, October 5, 2022, <https://www.crowdstrike.com/cyber-security-101/indicators-of-compromise/>.

⁹ Canadian Security Intelligence Service, “The Intelligence Cycle,” Government of Canada, May 20, 2020, <https://www.canada.ca/en/security-intelligence-service/corporate/publications/2019-public-report/the-intelligence-cycle.html>.

¹⁰ Phillip H.J. Davies, “The Intelligence Cycle Is Dead, Long Live the Intelligence Cycle: Rethinking Intelligence Fundamentals for a New Intelligence Doctrine,” *Brunel Centre for Intelligence and Security Studies*, 2013, 21, <https://bura.brunel.ac.uk/handle/2438/11901>.

¹¹ Bob Gourley, “Security Intelligence at the Strategic, Operational and Tactical Levels,” *Security Intelligence*, March 19, 2018, <https://securityintelligence.com/security-intelligence-at-the-strategic-operational-and-tactical-levels/>.

techniques, indications of a pending attack, and information of malware.¹² The tactical level is the narrowest in scope and the most time sensitive.¹³ It focuses on activity within an organization's system or on evidence that an attack is imminent.¹⁴ Tactical cyber intelligence involves information on what systems have been compromised and how they've been compromised.¹⁵

Literature Review

The academic landscape addressing Cyber Threat Intelligence is in its nascent stages. As such, much of what is discussed addresses technical aspects of CTI that are typically confined to the tactical stage of this process. These works generally focus on narrowing in on the most efficient indicators of compromise or technical system that will facilitate or produce quality intelligence.¹⁶ As Pythian points out, technology moves far too quickly for traditional intelligence mechanisms to provide actionable information to the relevant decision-makers.¹⁷ Beyond this, there are emerging discussions that have yet to garner the same degree of attention as the technical factors.

The first point of departure is whether the focus on technical capabilities in CTI is really the most efficient way to orient the process. From here we can assess other interesting insights in the literature that tackle the wider concept of CTI. We have divided the debates into three categories.

The first is the deficiency in understanding for businesses when implementing CTI. Zibak et al. identify a weakness in CTI today as the general lack of resources and knowledge to independently collect, process, and exchange threat intelligence.¹⁸ Businesses are not implementing CTI into their organizational structures in a way that would maximize the efficiency of existing frameworks. Often businesses remain in a state of unawareness. As Schlette et al. and the SANS 2022 survey point out, businesses often have no efficient mechanism or metric to understand if their CTI efforts have been effective.¹⁹ Somewhat problematically, such a lack of clear indicators of effectiveness brings into question the utility of the endeavor itself.

¹² Gourley, "Security Intelligence at the Strategic, Operational and Tactical Levels"

¹³ Ibid.

¹⁴ Ibid.

¹⁵ Ibid.

¹⁶ Paris Koloveas et al., "InTIME: A Machine Learning-Based Framework for Gathering and Leveraging Web Data to Cyber-Threat Intelligence," *Electronics (Basel)* 10, no. 7 (2021): 1–34, <https://doi.org/10.3390/electronics10070818>.

¹⁷ Pythian, *Understanding the Intelligence Cycle*, 17.

¹⁸ Adam Zibak, Clemens Sauerwein, and Andrew Simpson, "A Success Model for Cyber Threat Intelligence Management Platforms," *Computers & Security* 111 (December 1, 2021): 2, <https://doi.org/10.1016/j.cose.2021.102466>.

¹⁹ Daniel Schlette et al., "Measuring and Visualizing Cyber Threat Intelligence Quality," *International Journal of Information Security* 20, no. 1 (2021): 21–38, <https://doi.org/10.1007/s10207-020-00490-y>.

The second deficiency is businesses' inconsistency with how and to what degree they operationalize CTI. CTI is ultimately a proactive cyber security measure, yet several authors illuminate that businesses only address cyber security insofar as the law requires it.²⁰ This allows for investment in CTI to be overlooked in pursuit of preserving profits. This minimum legal threshold is often below where one needs to be for a state of relative security. Laws are often too slow to adapt to the evergreening nature of the cyber landscape.

Another way business attitudes hinder CTI operationalization is a hyper-focus on the tactical level. Oosthoek and Doerr are critical of CTI in its current state, claiming it lacks a true process to develop intelligence.²¹ They argue that the current CTI landscape is overly focused on the technology portion of cyber defense. Ultimately, CTI requires a process "informed by intelligence analysis, methodology, and analytical tradecraft."²² Thus, the elusive nature of CTI effectiveness may lie in weaknesses at the operational and strategic level.

The third deficiency is the detailed methods to implement CTI. Kotsias et al., Koloveas et al., and Riesco et al. offer different concrete processes to increase CTI effectiveness. The latter two direct their efforts on technical innovations or practices to increase CTI efficiency.²³ Uniquely, Kotsias et al. attempt to build a framework that goes beyond technical application and focuses on broader organizational integration. They advocate that since intelligence is a military process, companies must adopt a military approach to practice successful CTI. More tangibly, they describe a two-phase approach for widespread CTI adoption: phase 1 integrates CTI it with a business's IT unit; phase 2 provides CTI "as-a-service" to business units and executives.²⁴

While the crux of the issue seems to always route back to organizational deficiencies, Shin and Lowry derive a model that is meant to enhance the intelligence

Rebekah Brown and Pasquale Stirparo, "SANS 2022 Cyber Threat Intelligence Survey" (SANS, February 2022).

²⁰ James Kotsias, Atif Ahmad, and Rens Scheepers, "Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organisation," *European Journal of Information Systems* ahead-of-print, no. ahead-of-print (2022): 2. <https://doi.org/10.1080/0960085X.2022.2088414>

²¹ Oosthoek and Doerr, "Cyber Threat Intelligence: A Product Without a Process?" 300–315.

²² *Ibid.* 302

²³ R. Riesco, X. Larriva-Novo, and V. A. Villagra, "Cyber security Threat Intelligence Knowledge Exchange Based on Blockchain: Proposal of a New Incentive Model Based on Blockchain and Smart Contracts to Foster the Cyber Threat and Risk Intelligence Exchange of Information," *Telecommunication Systems* 73, no. 2 (2020): 259–88, <https://doi.org/10.1007/s11235-019-00613-4>.

Koloveas et al., "InTIME."

²⁴ Kotsias, Ahmad, and Scheepers, "Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organisation." 5-11.

abilities of individual practitioners which would then disperse into positive benefits for the entire firm.²⁵

The point of consensus we can glean from the literature is that the operationalization of CTI is not only complex but is also at odds with commercial structures and will require significant change in priority, attitude, and culture before Cyber Threat Intelligence is implemented both broadly and efficiently.

Methodology

The purpose of this study is to identify key issues that have been overlooked in the Canadian Cyber Intelligence Context and offer possible solutions to these issues. The approach taken will focus on cross examining case studies against cyber security and cyber intelligence frameworks. These case studies will be used to analyze cyber security practices and threats in different sectors. This analysis will be supplemented by academic research to identify potential issues that may not be identified through the case studies.

Case studies have been used because they act as a representative sample allowing us to efficiently study each sector in greater depth. Case studies also present the benefits of being able to investigate the application of CTI, in a real-world setting, which will provide specificity and contextualization necessary for operationalization. It also allows for a mixture of quantitative and qualitative data and analysis.²⁶

Case studies were selected based on a mixture of three variables: criticality (impact of attack), vulnerability (frequency of attack), and targetability (difficulty of attack). To justify these variables, we drew on a variety of sources including statistics from the government of Canada and other academic sources. For the purpose of this report, a sector is the unit of analysis. The sectors examined are health care, finance, agriculture, and higher education. Within each sector, several examples of successful cyber attacks have been provided. These are used to gain a greater understanding of the sector, identify gaps within CTI, and to inform on how CTI can be leveraged to better operationalize it in each sector. Our analysis will provide a greater understanding of whether issues are universal or if the gaps are unique to individual sectors.

Our report has the following limitations. Firstly, we acknowledge that the selection of each sector may indicate a selection bias. However, together each sector represents a diverse distribution across the selected variables. Secondly, there was a general lack of information regarding how CTI is conducted within particular organizations, if at all.

²⁵ Shin and Lowry, "A Review and Theoretical Explanation of the 'Cyberthreat-Intelligence (CTI) Capability' That Needs to Be Fostered in Information Security Practitioners and How This Can Be Accomplished"

²⁶ Jennifer Rowley, "Using Case Studies in Research," *Management Research News* 25, no. 1 (January 1, 2002): 16–27, <https://doi.org/10.1108/01409170210782990>.

However, we have been able to approximate the success of CTI based on examining and analyzing the impact of cyber instances in each case.

Analysis of Canadian Sectors

Healthcare

In November of 2019, LifeLabs, a medical testing company in B.C., experienced a data breach where over 15 million patient files were stolen.²⁷ Affected individuals filed lawsuits as their personal and medical information was stolen. The investigation determined that LifeLabs had inadequate cyber security measures making them negligent with plaintiffs asking for \$1.1 Billion in compensation.²⁸

In November of 2021, Eastern Health the organization that runs Newfoundland Hospitals, experienced a significant cyber attack. Over 58,000 patients were impacted by the data breach where information going back to 1996 was stolen.²⁹ Information leaked includes medical information, medical care plan numbers and administrative information, social insurance numbers and financial information.³⁰ A review by an Israeli cyber security firm concluded that Eastern Health had numerous cyber security concerns and vulnerabilities emphasizing the lack of cyber security awareness amongst staff.³¹

Cyber security concerns in the health care sector have been gaining increased attention in recent years. The health care sector - hospitals, clinics, research labs, pharmaceutical clinics and the machinery and products produced by these organizations - tend to be extremely vulnerable to cyber attacks and have some of the worst cyber security practices of any major industrial sector.³² This is particularly concerning given the high degree of criticality embedded in this field.

²⁷ Jessica Davis, "Inadequate Security, Policies Led to LifeLabs Data Breach of 15M Patients," Health IT Security, July 1, 2020, <https://healthitsecurity.com/news/inadequate-security-policies-led-to-lifelabs-data-breach-of-15m-patients>.

²⁸ Ibid.

²⁹ Darrel Roberts, "Number of People Hit by Privacy Breach in 2021 Cyberattack Now up to 58,000: Eastern Health," CBC, December 12, 2022, <https://www.cbc.ca/news/canada/newfoundland-labrador/cyberattack-update-eastern-health-1.6678660>.

³⁰ Ibid.

³¹ Rob Antle, Patrick Butler, and Peter Cowan, "Long before N.L. Cyberattack, Report Flagged Flaws in System," CBC, May 12, 2022, <https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cyber-security-eastern-health-report-1.6447807>.

³² Mark Gollom, "LifeLabs Cyberattack One of 'Several Wake-up Calls' for e-Health Security and Privacy," CBC, December 19, 2019, <https://www.cbc.ca/news/science/lifelabs-data-breach-security-ehealth-1.5400817>.

Healthcare is one of Canada's critical infrastructure sectors.³³ It also carries a high degree of risk because of the extensive amount of personal information (including financial and medical) these organizations carry. Most importantly healthcare services are responsible for the preservation of lives and the disruption of these services can lead to death and bodily harm.

Healthcare is a field that touches every Canadian. Disruptions to the healthcare sector are therefore high visible, making them an ideal target for threat actors who want to draw attention or cause a maximum amount of harm.³⁴

Healthcare services are often time sensitive.³⁵ Organizations often have little time to react to cyber threats and may not be able to make consultations before responding to a threat actor's demands. They are therefore more susceptible to caving to attackers demands quickly, with little negotiation or attempts to dislodge the attackers. Healthcare organizations pay ransoms 60% of the time compared to an average of 46% in other sectors.³⁶

Threat actors target the healthcare sector because of the use of new technology. IT systems, specifically internet connected devices, are increasingly used.³⁷ Each new network connected device presents the potential for new vulnerabilities that can be exploited. More network connected devices also mean that more data is stored online, increasing the risk for potential data breaches.³⁸

Healthcare organizations hold enormous amounts of valuable data. This includes but is not limited to biographical information, health information, personal financial information, corporate financial information and intellectual property. The Canadian Internet Regulation Authority has estimated that the value of an individual's private health information can be worth 200 times (\$1000) the amount of a stolen credit card (\$5).³⁹ Healthcare data can be extremely valuable due to slow response times by health care organizations, prolonging its utility to criminals.⁴⁰ This data can also be extremely valuable

³³ "National Strategy for Critical Infrastructure" (Public Safety Canada, 2019), 4, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx>.

³⁴ Alex Wilner et al., "From Public Health to Cyber: Cyber security and Canada's Healthcare Sector," *International Journal* 76 (4) (2021), 528.

³⁵ Ibid. 528.

³⁶ Micheal Marvin, "Why Is the Healthcare Industry the Most Likely To Pay Cybercriminals for Ransomware Attacks?," Portnox, September 19, 2022,

³⁷ Aurore Le Bris and Walid El Asri, "State of Cyber security & Threats in Healthcare Organizations: Cyber security Strategy for Managers," *ESSEC Business School*, 2017, 3.

³⁸ Canadian Centre for Cyber Security, "Cyber Security for Connected Medical Devices (ITSAP.00.132)," Government of Canada, November 5, 2021, <https://www.cyber.gc.ca/en/guidance/cyber-security-connected-medical-devices-itsap00132>.

³⁹ Arapi Kreshnik, "The Healthcare Industry: Evolving Cyber Threats and Risks.," *Master's Thesis - Utica College*, May 2018, 12.

⁴⁰ Wilner et al., "From Public Health to Cyber Hygiene: Cyber security and Canada's Healthcare Sector," 528.

to health research labs or pharmaceutical companies because it can be extremely expensive, difficult, and time consuming to acquire legally.⁴¹

Finally, targeting the healthcare sector can directly lead to injury or death. White hat hackers have demonstrated that medical devices can be targeted to harm or kill people. Pacemakers and defibrillators can be hacked to stop an individual's heart.⁴² Although there are no documented cases of assassination using healthcare devices, experiments have demonstrated that this is possible and that sophisticated actors do potentially have the means to carry out this form of attack.⁴³

Cyber threat actors can be loosely broken into three categories: State sponsored actors, extremists/hacktivists and cyber criminals. Each of these profiles tends to have different objectives for attacking the healthcare sector.

Extremists, terrorists, and hacktivists generally want to cause disruption to make a political statement and draw attention to an issue.⁴⁴ Cybercriminals are motivated by profit and will tend to focus on ransomware or data breaches.⁴⁵ State-backed actors will focus on either establishing a presence or stealing intellectual property.⁴⁶ State-backed actors will establish a foreign presence so that they can develop a threatening posture, the threat being that in the event of conflict, they could use their presence to quickly disrupt healthcare services.⁴⁷ State-back actors also cause data breaches but for different reasons than cyber criminals. They may steal data to benefit their own health services.⁴⁸ A prime example of this was how Chinese hackers targeted healthcare organizations so they could steal COVID-19 vaccine information to further the development of their own vaccine technology.⁴⁹

⁴¹ Ibid.529.

⁴²Lily Hay Newman, "A New Pacemaker Hack Puts Malware Directly on the Device," Wired Magazine, August 9, 2018, <https://www.wired.com/story/pacemaker-hack-malware-black-hat/>.

⁴³ Thomson Reuters, "Pacemakers, Defibrillators Are Potentially Hackable | CBC News," CBC, February 21, 2018, <https://www.cbc.ca/news/health/pacemakers-hack-1.4545001>

⁴⁴ Wilner et al., "From Public Health to Cyber Hygiene: Cyber security and Canada's Healthcare Sector," 529.

⁴⁵ Menaka Muthuppalaniappan and Kerrie Stevenson, "Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health.," *International Journal for Quality Healthcare* 33, no. 1 (2021), 3.

⁴⁶ "People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices," Cyber security and Infrastructure Security Agency, June 10, 2022, <https://www.cisa.gov/news-events/cyber-security-advisories/aa22-158a>.

⁴⁷ Wilner et al., "From Public Health to Cyber Hygiene: Cyber security and Canada's Healthcare Sector," 529.

⁴⁸ Le Bris and El Asri, "State of Cyber security & Cyber Threats in Healthcare Organizations. Applied Cyber security Strategy for Managers" 5.

⁴⁹ Robert Lemos, "State-Sponsored Cyberattacks Target Medical Research," Dark Reading, August 21, 2019, <https://www.darkreading.com/threat-intelligence/state-sponsored-cyberattacks-target-medical-research>.

Another key group is disgruntled employees. Fifty eight percent of cyber attacks in the healthcare sector are facilitated by employees.⁵⁰ Furthermore, in one survey, 29% of healthcare employees reported being aware of someone in their organization who sold confidential information and 21% reported that they were willing to sell confidential information themselves given the opportunity.⁵¹

The healthcare industry suffers from a myriad of organizational and technical challenges. At the macro-level the Canadian healthcare system suffers from being a fractured system. The healthcare sector therefore does a poor job helping and learning from one another leading to healthcare organizations responding to issues on an individual level and not as an ecosystem.⁵²

At the micro-level a key challenge is the cyber security awareness of healthcare workers. They see cyber security as an issue for the IT department and therefore lack cyber security knowledge or best practices. A deficiency of cyber security knowledge and training leads to poor cyber hygiene which needlessly increases vulnerabilities and risks.

Healthcare organizations suffer from technical challenges as well. Healthcare organizations often have antiquated software with relatively high amounts of vulnerabilities.⁵³ Even when new software packages are installed, it tends to interfere with existing software creating software vulnerabilities. Finally, healthcare is a tech dependent sector. More and more network connected devices are used and each of these brings potential vulnerabilities and an increased risk level.

Agriculture

In November 2022, Sobeys's grocery chain's parent company, Empire, experienced a cyber incident that is estimated to have cost \$32 million, minus any recoveries they can receive through cyber insurance.⁵⁴ Ransomware was installed, preventing their pharmacy

⁵⁰ Suzanne Widup et al., "2018 Verizon Data Breach Investigations Report" (Verizon, April 2018), 4, https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report

⁵¹ "Cybersafe Healthcare: Options for Strengthening in Canada's Sector" (HealthCareCAN, 2018), 19, <https://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/Cyber%20Security/Options%20Brief%20Summit%20Report.pdf>.

⁵² Mike Colias, "Cyber Security: Health Care Learns to Share Scares and Solutions," *Hospitals and Healthcare Networks* 78, no. 5 (n.d.): 2004, 62.

⁵³ Yussuf Ahmed, Syed Naqvi, and Mark Josephs, "Cyber security Metrics for Enhanced Protection of Healthcare IT Systems," in *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)* (2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway: IEEE, 2019), 2. <https://doi.org/10.1109/ISMICT.2019.8744003>.

⁵⁴ Paul Withers, "Sobeys Cyberattack Cost Grocery Store Operator \$25 Million | CBC News," CBC, December 15, 2022, <https://www.cbc.ca/news/canada/nova-scotia/sobeys-cyber-attack-25-million-1.6686838>

services from operating for four days and halting other operations for roughly a week.⁵⁵ The \$39.1 million direct costs reported so far are attributed to legal and professional fees, IT system restoration and spoiled inventory.⁵⁶ Empire experienced indirect costs associated with sales declines and reduced operations, estimated to total \$15 million. The attack has inspired the company to further invest in cyber security over the next few years.⁵⁷

In the same month of Empire's cyber incident, Maple Leaf Farms, a pork and poultry packing company experienced their own attack which led to a system-wide outage.⁵⁸ The total estimated cost of the incident is \$23 million from similar expenditures as Empire such as professional fees, system restoration costs, lost sales, and spoiled inventory.⁵⁹ It too had cyber insurance which will mitigate some of the costs. Initiating their business continuity plan enabled Maple Leaf to continue operations manually (with paper-and-pencil) within 48 hours of the incident being discovered⁶⁰ – a contingency plan that most critical infrastructure (CI) sectors might be unable to rely on.

Both examples illustrate some of the gaps that currently exist in the Canadian agriculture sector – which includes farms, forestry, fishing, and hunting as well as meat processing and packaging plants and food distribution services according to the North American Industry Classification System (NAICS) codes.⁶¹ In the realm of cyber security, Canada's agriculture sector represents an embryonic sector in its cyber security defences, awareness, and standards (awk). Researchers such as University of Guelph's Dr. Ali Dehghantanha have labelled it a "soft underbelly" having minimal to no cyber security protection.⁶² According to a Statistics Canada analysis in 2021, the agricultural sector was one of the most vulnerable sectors due to their lack of security preparedness. They were the fourth least protected sector against malware, including viruses, spyware, ransomware, etc. As seen in Figure 1, only 65% of enterprises in the sector have anti-malware protection. They were the third highest sector for having no cyber security measures in place, with 12.2% of businesses in the sector being completely

⁵⁵ Robertson, Susan Krashinsky. "Empire Says Cost of Sobeys Cyber security Breach Higher than Initial Estimates." The Globe and Mail, March 16, 2023. <https://www.theglobeandmail.com/business/article-sobeys-empire-earnings-q3-cyberbreach/>.

⁵⁶ Krashinsky Robertson, "Empire Says Cost of Sobeys Cybersecurity Breach Higher than Initial Estimates."

⁵⁷ *ibid.*

⁵⁸ Adriano, Lyle. "Maple Leaf Foods Confirms Cyberattack, Will Not Pay Ransomware Gang." *www.insurancebusinessmag.com*, December 1, 2022.

<https://www.insurancebusinessmag.com/ca/news/cyber/maple-leaf-foods-confirms-cyberattack-will-not-pay-ransomware-gang-429218.aspx>.

⁵⁹ Roy Graber, "Cyberattack Cost Maple Leaf Foods at Least CA\$23 Million | WATTPoultry.," March 9, 2023, <https://www.wattagnet.com/articles/46910-cyberattack-cost-maple-leaf-foods-at-least-ca23-million>.

⁶⁰ *Ibid.*

⁶¹ Codes 113 and 11531.. "North American Industry Classification System (NAICS) Canada 2017 Version 3.0." Statistics Canada. 2018. *Www23.Statcan.gc.ca*.

<https://www23.statcan.gc.ca/imdb/p3VD.pl?Function=getVD&TVD=1181553>.

⁶² Ali Dehghantanha, "Cyber-Attacks a Growing Threat to Farm, Food Security, Warn U of G Researchers," U of G News, August 17, 2022, <https://news.uoguelph.ca/2022/08/cyber-attacks-a-growing-threat-to-farm-food-security-warn-u-of-g-researchers/>

unprotected.⁶³ This has been attributed to slim profit margins that many businesses, like farmers, in the sector work with, making investing in cyber security a luxury.⁶⁴ Many are also uneducated or unaware of their dependency on data, as many claim they can go back to pen and paper at a moment's notice, as was the case with Maple Leaf Farms.⁶⁵ However, with the agriculture sector becoming increasingly digitized, the sector's dependency on data coupled with its lack of defences is making it increasingly vulnerable.⁶⁶ And with threat actors targeting businesses during critical times, like planting and harvesting seasons, a growing number of attacks are leading to ransoms being paid.⁶⁷

The agriculture sector is critical to Canada's well being and economy. It is considered one of Canada's ten critical infrastructures⁶⁸, generating 6.8% of Canada's GDP and employing 1 in 9 Canadians nationally.⁶⁹ Cyber attacks in the agriculture sector have increased in the past few years and are projected to keep on increasing over the coming decade.⁷⁰ So far, the industry has been left relatively unscathed compared with other sectors, like the financial sector (Figure 2), with malicious cyber incidents, privacy and lost data incidents and IT implementing and processing errors making up only 4.1%, 1%, and 0.5%, respectively, of total incidents across all sectors.⁷¹ However, advocates in agriculture are increasingly warning of the catastrophic implications that the sector will face if they remain under and unprotected.⁷²

⁶³ "Cyber Security Measures Enterprises Have in Place by Industry and Size of Enterprise," Statistics Canada. October 18, 2022, <https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2210000101>

⁶⁴ John Cox, "Agriculture Industry on Alert After String of Cyber Attacks," GovTech, June 13, 2022, <https://www.govtech.com/security/agriculture-industry-on-alert-after-string-of-cyber-attacks>

⁶⁵ Graber, "Cyberattack Cost Maple Leaf Foods at Least CA\$23 Million | WATTPoultry."

⁶⁶ Cox, "Agriculture Industry on Alert After String of Cyber Attacks"
Robert Arnason, "Ag Sector Warned of Cyberattack Vulnerability," The Western Producer (blog), August 25, 2022, <https://www.producer.com/news/ag-sector-warned-of-cyberattack-vulnerability/>

⁶⁷ Ibid.

⁶⁸ "Critical Infrastructure Partners," Public Safety Canada. December 21, 2018. <https://www.publicsafety.gc.ca/cnt/ntnl-scrtr/crtcl-nfrstrctr/crtcl-nfrstrtr-prtnrs-en.aspx>.

⁶⁹ Agriculture and Agri-Food Canada, "Overview of Canada's Agriculture and Agri-Food Sector," November 5, 2021, <https://agriculture.canada.ca/en/sector/overview>

⁷⁰ Simon Harvey, "Canada's Maple Leaf Foods Hit by Cyberattack," Just Food (blog), November 7, 2022, <https://www.just-food.com/news/canadas-maple-leaf-foods-hit-by-cyberattack/>

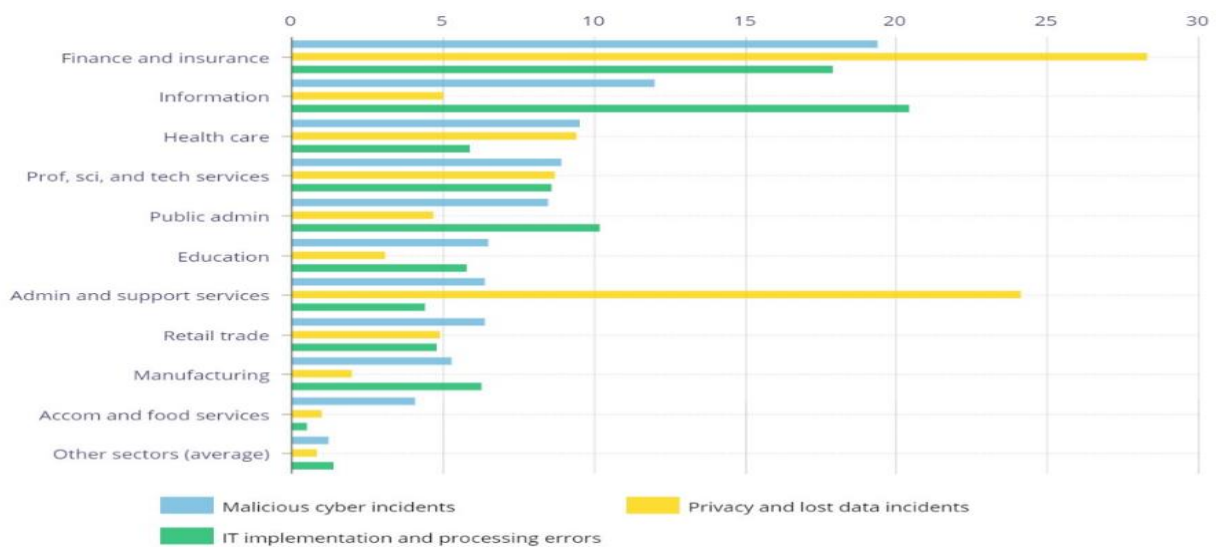
⁷¹ Nikil Chande and Dennis Yanchus, "The Cyber Incident Landscape" (Bank of Canada, December 13, 2019), <https://doi.org/10.34989/san-2019-32>

⁷² Arnason, "Ag Sector Warned of Cyberattack Vulnerability"
James Tyrrell, "Security Agencies Warn of Cyber Attacks against Agriculture," TechHQ, August 17, 2022, <https://techhq.com/2022/08/security-warning-cyber-attacks-against-agriculture/>

Figure 1 Cyber Security Measures Enterprises Have in Place by Industry and Size of Enterprise

North American Industry Classification System (NAICS)	Agriculture, forestry, fishing and hunting	Finance and insurance	Educational services	Health care and social assistance
Cyber security measures	2021	2021	2021	2021
Mobile security	30%	74%	42%	37%
Anti-malware software to protect against viruses, spyware, ransomware, et cetera	65%	94%	76%	76%
Web security	24%	80%	65%	45%
Email security	53%	94%	82%	71%
Network security	43%	91%	65%	66%
Data protection and control	17%	76%	41%	40%
Point-Of-Sale (POS) security	6%	30%	29%	20%
Software and application security	11%	68%	31%	22%
Hardware and asset management	12%	71%	35%	30%
Identity and access management	24%	79%	53%	44%
Physical access controls	12%	62%	29%	31%
Business does not have any cyber security measures in place	12%	1%	1%	5%
Business does not know	11%	1%	9%	7%

Figure 2 Percentage of Total Incidents



The major gaps in the agriculture sector as illustrated by the previous examples, fall under four major categories: technological deficiencies, organizational gaps, legal gaps, and a lack of transparency. The technological deficiencies are clear, with less than two-thirds of enterprises having malware protection and 12% of enterprises having no protections at all.⁷³ With the recent digitization of the industry, there appears to be a lack of understanding of their reliance on cyber infrastructure leading to a lack of investment and an ignorant self-reliance on analogue methods, believing that they can resort to “pen-and-paper” if need be. This may be the case in some instances, but with increasing sophistication and innovation, analogue solutions will likely be phased out soon enough. This cyber illiteracy can also be categorized into an organizational gap, with a lack of education on the importance of cyber security and obstacles to investment because of slim profit margins. With legal gaps, there are little to no mandatory regulatory requirements for cyber security in the industry, however there are current initiatives that are trying to build a more resilient agriculture sector. For instance, the Community Safety Knowledge Alliance (CSKA) is working with Public Safety Canada to enhance the cyber security of the entire sector by 2024.⁷⁴ Government regulations and organizational standards can help raise a baseline security level for the industry. The black basta group ransomware attack that targeted and successfully breached two organizations in the agriculture sector (Empire and Maple Leaf Foods) points to another gap around a lack of transparency. The two attacks occurred within a week of each other; had there been some system in place that encouraged and enabled horizontal information sharing within the ag sector, perhaps the second attack could have been avoided.

Finance

In terms of cyber security, Canada’s financial sector – which includes banks, securities and other financial investment activities, insurance carriers and funds – is one of Canada’s most well-protected and highly targeted critical infrastructure sectors. Yet despite its robust cyber defences, threat actors continue to successfully compromise its IT systems, causing major, publicly-known breaches, leading not only to economic and reputational damages but also threatening customers with the loss, theft, and potential exploitation of personal data. Like any other organization in our increasingly digitized world, reliance on IT systems has made cyber security critical to all areas of financial organizations. It has also created new vulnerabilities both internally and externally that may be overlooked. CTI can help identify and address the gaps in the financial sector’s cyber defenses to help make it more protected and resilient to cyber threats.

Three successful cyber attacks against Canadian financial institutions – a major bank, an insurance carrier, and a country-wide credit union – will help provide context to

⁷³ Statistics Canada, “Cyber Security Measures Enterprises Have in Place by Industry and Size of Enterprise”

⁷⁴ Community Safety Knowledge Alliance. n.d. “Strengthening the Cyber Security Capacity of Canada’s Agricultural Sector – CSKA.” CSKA. <https://cskacanada.ca/projects/strengthening-the-cyber-security-capacity-of-canadas-agricultural-sector/>.

the relevancy and importance of CTI, further informing gaps currently existing within the financial sector.

The first is the 17 month long breach of BMO's online banking software that occurred in 2017-2018 that resulted in unauthorized third parties obtaining sensitive data from 113,154 accounts and the eventual unauthorized disclosure of personal data of 3,190 of its customers.⁷⁵ The two attacks were a result of BMO's inadequate security testing, vulnerability management, and oversight monitoring.⁷⁶ This incident illustrates a number of gaps that exist in the CTI of the financial sector including the slow detection and containment of data breaches and a reactionary approach to cyber security.

The next was a successful ransomware attack against an unnamed Canadian insurance firm in the fall of 2019. The threat actors were able to successfully infiltrate and bypass the firm's firewalls and infect 1,000 of their computers.⁷⁷ The firm paid the threat actors \$950,000 US to decrypt their computers with funds from previously purchased cyber insurance. Despite the sizeable breach, the economic loss, and the potentially damaging unauthorized access of customers' sensitive data, the incident only became public because the reinsurer used to pay the ransom filed legal actions against the threat actors to recuperate the ransom.⁷⁸ This incident illustrates two other gaps in the financial sector: insufficient defenses and the non-disclosure of cyber incidents.

The third and most recent incident occurred in June of 2022 when several credit unions in Manitoba and across Canada experienced a "cyber security incident."⁷⁹ The credit union used a third-party digital technology company to service their cyber security systems. When they became aware of the unauthorized access, they initiated their incident response plan and secured their digital networks and systems. The firm confirmed that there was no unauthorized access or compromise of personal data, however services were impacted during the investigation.⁸⁰

The Canadian financial sector is one of Canada's most well protected sectors, with between 89.8% and 97.5% of enterprises being equipped with anti-malware software to protect against viruses, spyware, ransomware, etc.⁸¹ However, as seen in the example

⁷⁵ Office of the Privacy Commissioner of Canada. 2021. "PIPEDA Findings #2021-003: Security Deficiencies at BMO Lead to Large-Scale Breach." [Www.priv.gc.ca](https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-003/). December 9, 2021.

⁷⁶ Ibid.

⁷⁷ Thomas Daigle, "Hackers Were Paid Ransom after Attack on Canadian Insurance Firm, Court Documents Reveal," CBC, January 30, 2020, <https://www.cbc.ca/news/science/unnamed-insurance-company-cyberattack-1.5445326>

⁷⁸ Ibid.

⁷⁹ Vera-Lynn Kubinec, "Credit Unions across Canada Targeted in Cyber security Incident, but No Evidence Data Compromised: Tech Company | CBC News," CBC, June 15, 2022, <https://www.cbc.ca/news/canada/manitoba/credit-unions-cyber-security-incident-1.6488872>

⁸⁰ Ibid.

⁸¹ Statistics Canada, "Cyber Security Measures Enterprises Have in Place by Industry and Size of Enterprise"

of the unnamed insurance firm, these protective measures are not impenetrable. Although the financial sector may appear to be adequately protected against cyber attacks, it is also notoriously slow at detecting and containing data breaches. According to a 2021 Data Risk Report by Veronis, it can take as many as 233 days to detect and contain a breach.⁸² This was exemplified by the example of BMO. According to a PIPEDA report of findings from the Office of the Privacy Commissioner of Canada, BMO was not aware of the unauthorized breach and exfiltration of the personal data until it received a ransom email in May 2018, 7-11 months after the original attack took place.⁸³ BMO only took action to review its systems and assess the risk to its customer's personal information after they received proof that personal information was stolen.⁸⁴ This slow awareness and responsiveness of financial organizations is likely due in part to the "low and slow" approach taken by malicious actors to stay undetected for as long as possible to maximize how much data and money they would be able to exfiltrate and secure.⁸⁵

The housing of financial resources and highly sensitive data makes the financial sector one of the most targeted sectors in Canada.⁸⁶ In 2021, there were 2,527 reported cyber incidents worldwide, more than triple the amount from the previous year.⁸⁷ With their efforts to digitize their data and automate their systems, the financial sector has created new vulnerabilities.⁸⁸ According to research from the Bank of Canada, of the total cyber incidents in the critical infrastructure sectors, the financial sector is the most targeted. It makes up 28% of all privacy and lost data incidents,⁸⁹ 19% of malicious incidents⁹⁰ and 18% of IT implementing and processing errors.⁹¹ Financial institutions typically face two types of attacks from malicious actors: conventional attacks that try to steal financial and data resources from organizations and ransomware attacks to seize control of an organization's systems until a ransom is paid.⁹² Of the three types of incidents, IT implementation and processing errors pose a significantly bigger financial threat to organizations. Figure 3 shows the median losses by cyber incident types, both

⁸² Mike Cline, "The Top 5 Industries Most Vulnerable to Cyber Attacks," ProcessBolt, September 26, 2022, <https://processbolt.com/top-5-industries-most-vulnerable>

⁸³ Office of the Privacy Commissioner of Canada, "PIPEDA Findings #2021-003: Security Deficiencies at BMO Lead to Large-Scale Breach,"

⁸⁴ Ibid.

⁸⁵ Chande and Yanchus, "The Cyber Incident Landscape," December 13, 2019

⁸⁶ Jen Miller-Osborn, "3 Reasons Cyberattacks Target Financial Services and How to Fight Back," Palo Alto Networks Blog (blog), August 31, 2021, <https://www.paloaltonetworks.com/blog/2021/08/financial-services-cyberattacks/>

⁸⁷ Ani Petrosyan, "Cyber Incidents in Financial Industry Worldwide 2021," Statista, accessed April 25, 2023, <https://www.statista.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide/>

⁸⁸ Miller-Osborn, "3 Reasons Cyberattacks Target Financial Services and How to Fight Back"

⁸⁹ Chande and Yanchus define privacy and lost data incidents as "where the firm has inadvertently misused or lost information."

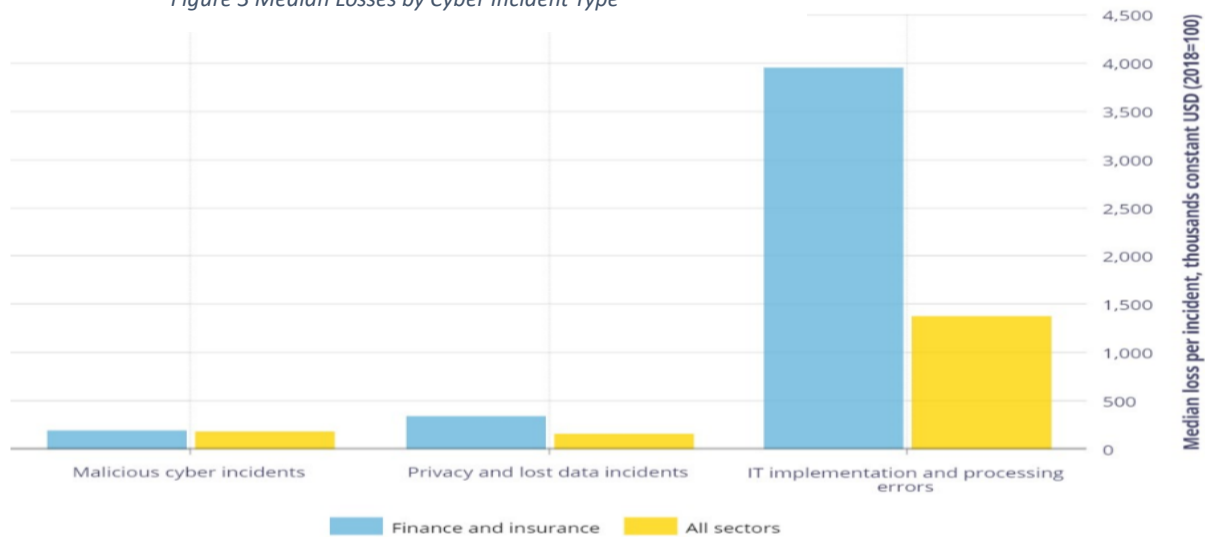
⁹⁰ Chande and Yanchus define malicious incidents as "cyber attacks—where the threat actor is intending to do harm (e.g., ransomware attacks, hacking incidents or data theft by employees)"

⁹¹ Chande and Yanchus define processing errors as "where the incident occurs while firms are maintaining, upgrading or replacing IT hardware or software assets."

⁹² Toni Ahnert et al., "Cyber Security and Ransomware in Financial Markets" (Bank of Canada, July 14, 2022), <https://doi.org/10.34989/swp-2022-32>.

in the finance and insurance sector and among all sectors. It demonstrates that IT implementation and processing errors are more than eight times more financially damaging than either malicious cyber incidents or privacy and lost data incidents. The other reason it is such a major target is because of the sensitive information they house. The wide range of personal information that financial organizations have access to – such as financial account numbers, social insurance numbers, and/or credit or debit card numbers – can be sold on black markets, used to perpetrate identity theft, or disclosed on public sites as was the case in the BMO example.

Figure 3 Median Losses by Cyber Incident Type



In analyzing the financial sector, there are several CTI gaps, namely IT challenges and a lack of transparency. The BMO example illustrates the deficiency in IT. Although the financial sector may appear to be sufficiently safe with malware-protecting software, IT implementing errors can cause major cyber incidents that are damaging. With customer-applications increasingly being implemented by financial institutions, expanding the users able to regularly access their IT systems, the need for proper testing and ongoing oversight monitoring is essential. The BMO and unnamed insurance firm examples also illustrate the sector’s lack of transparency. Financial institutions typically avoid disclosing cyber incidents for fear of reputational harm and notifying threat actors of their vulnerability; only 10-20% of firms who face a successful ransomware attack disclose it publicly.⁹³ This can cause significant harm to customers, vendors, and business partners in terms of their sensitive data. When firms choose to delay or avoid disclosing when a successful cyber incident occurs, those whose data has been potentially stolen remain unaware, making them vulnerable to identity theft or other personal data related harms.⁹⁴ These gaps can be addressed using CTI to make the financial sector more resilient to cyber threat incidents.

⁹³ Daigle, “Hackers Were Paid Ransom after Attack on Canadian Insurance Firm, Court Documents Reveal”

⁹⁴ Ibid.

Higher Education

Cyber incidents are becoming an increasingly salient issue for Higher Education Institutions (HEIs). In 2016, the University of Calgary suffered a ransomware attack. As a result of the attack, UofC files were encrypted, and faculty and staff were unable to access their email systems.⁹⁵ Beyond the halting of operations within the university, the UofC's administration decided to pay out a demanded ransom of \$20,000 to regain access to their systems.⁹⁶ Despite the payment, the university acknowledged that this does not necessarily mean the issues would be solved. Fortunately, the decryption keys worked, and operations were restored. The reasons cited by the university for paying the ransom were that they did not want impediments to their vital work.⁹⁷ While UofC paid only \$20,000 in ransom, the demands put forth by malicious threat actors have been on the rise. This can partially be attributed to more clandestine ways of acquiring funds like the proliferation of cryptocurrencies.⁹⁸

In 2021, there was an attack on a Simon Fraser University server. The ransomware attack led to a data breach of the personal information of 200,000 people.⁹⁹ Although the attack did not contain highly sensitive information like Social Insurance Numbers or financial information, this was the second data breach suffered by the university in a 2-year time frame. The year prior SFU paid to decrypt files from a ransomware attack that affected over 250,000 individuals.¹⁰⁰ The impacted personal information by this breach included Student and employee IDs, first and last names, dates of birth, courses, and encrypted passwords.¹⁰¹ SFU reported both breaches to the Office of the Information and Privacy Commissioner of British Columbia.¹⁰²

These are two examples of an emerging trend in Canada and globally. According to Statistics Canada, 64% of large educational services organizations have been impacted by a cyber security incident. Educational services were impacted on average of

⁹⁵ "University of Calgary Paid \$20K Ransom to Cyberattackers to Unlock Computer Systems | CBC News," CBC, June 7, 2016, <https://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979>

⁹⁶ Ibid.

⁹⁷ "University of Calgary Pays \$20K Ransom after Cyberattack | CTV News," <https://www.ctvnews.ca/sci-tech/university-of-calgary-pays-20k-ransom-after-cyberattack-1.2935525>.

⁹⁸ "TELUS Canadian Ransomware Study 2022," TELUS, accessed February 8, 2023: 14 https://assets.ctfassets.net/1vipdfivgfy/6KFtVdoPfg3apLZr3NuWLL/e16da7dfa1a259afa2da50dac5177780/TELUS_Canadian_Ransomware_Study_2022_2.pdf.

⁹⁹ "Simon Fraser University Says Server Breach Exposed 'personally Identifiable' Information | CBC News," CBC, February 17, 2021, <https://www.cbc.ca/news/canada/british-columbia/sfu-cyberattack-exposes-info-200-000-1.5916153>

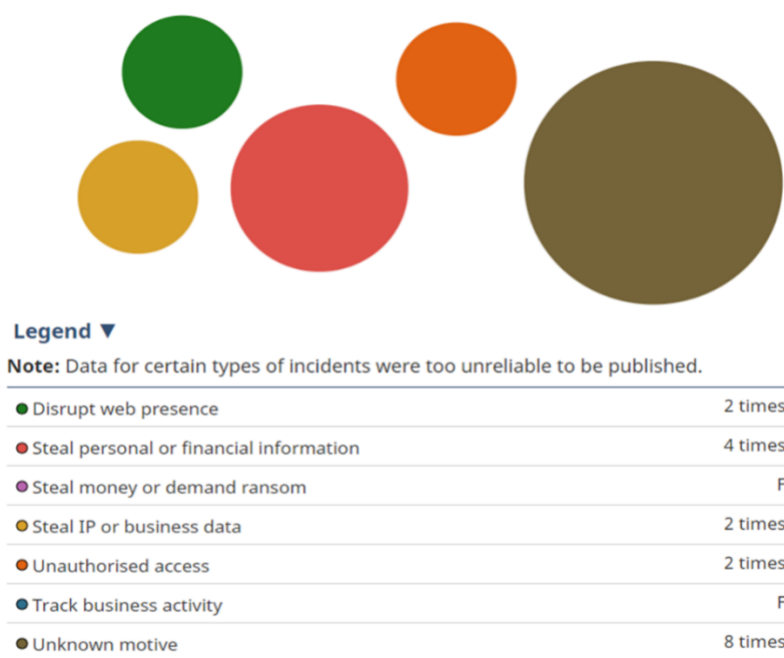
¹⁰⁰ Alex Migdal, "SFU Ransomware Attack Exposed Data from 250,000 Accounts, Documents Show | CBC News," <https://www.cbc.ca/news/canada/british-columbia/sfu-ransomware-attack-1.5732027>.

¹⁰¹ "Cyberattack and Exposure of Personally Identifiable Information," Simon Fraser University, <https://www.sfu.ca/information-systems/announcements-alerts/security-alerts/cyberattack-and-exposure-of-personally-identifiable-information.html>.

¹⁰² Ibid.

four times per year for the purpose of stealing personal or financial information.¹⁰³ Another type of harm experienced was disruptions to services or functioning with organizations in 46% of attack occurrences, as seen in Figure 4.¹⁰⁴

Figure 4 Types of Cyber Security Incidents that Impacted Educational Services



Source: Statistics Canada, tables 22-10-0076-01 and 22-10-0079-01.

This is undoubtedly exacerbated by the increased technological complexity that has entered higher education since the start of the COVID-19 pandemic. This illuminates part of why the education sector is a growing target. The data that universities hold can be extremely valuable for a variety of reasons. Unlike the financial sector, monetary gain is not the only motivating factor that can increase an HEI's targetability. While they do hold financial information, they also control information relating to staffing, enrolment, and personal health information which often includes sensitive personal identifying information.¹⁰⁵ There is a myriad of information collected and controlled by these institutions concerning the population of the organization. At a broader level, these institutions conduct research that can be valuable intellectual property. This research can

¹⁰³ "Cyber Security and Cybercrime in Canada, 2017," Statistics Canada. October 15, 2018, <https://www150.statcan.gc.ca/n1/pub/71-607-x/71-607-x2018007-eng.htm>.

¹⁰⁴ Ibid.

¹⁰⁵ Noran Shafik Fouad, "Securing Higher Education against Cyberthreats: From an Institutional Risk to a National Policy Challenge," *Journal of Cyber Policy* 6, no. 2 (May 4, 2021): 143-144. <https://doi.org/10.1080/23738871.2021.1973526>.

be highly impactful for the global markets or even strategically valuable for the security and development of nation states.¹⁰⁶

The sheer quantity of data in HEIs makes them enticing targets, but threat actors have the added benefit that their IT systems are often decentralized. This decentralization is a consequence of the higher education structure where separate faculties and departments might have vastly different technological needs. Unfortunately, this creates a rich environment for abuse by malicious actors as “this kind of piecemeal setup creates apparent security vulnerabilities that attackers can exploit.”¹⁰⁷ Also, HEIs are becoming a more lucrative target even if data is not exfiltrated. Where UofC paid \$20,000, other institutions have suffered much greater costs of extortion.¹⁰⁸ The average cost associated to data breaches in HEIs are approximately \$3.86 million.¹⁰⁹ While in some instances this can be attributed to higher ransoms being paid, there is also the additional operational cost associated with securing a system during and after an attack.

The most common methods of attack in higher education are ransomware and phishing attacks. While this is not so different from the general cyber threat trends, HEIs have structural components that leave them more exposed. Ransomware attacks involve encryption and at times exfiltrating information. The data stolen can then be sold and the promised de-encrypting of critical data is used to extort funds from the target institutions. As already mentioned, the volume, variety and sensitivity of data in HEIs make ransomware attacks harmful and can halt operations. These institutions are also highly susceptible to phishing campaigns. University campuses are often “bring your own device” centred, which opens the avenues for attack. Everyone within the HEI, including students, professors, alumni, and other staff are all points of infiltration via email phishing campaigns. It is difficult for the organizations to manage the behaviour and devices of these diverse points of attack. In response to these threats, Canadian HEIs have increased their technical cyber capabilities but it is unclear if this is sufficient to meet the threat.

Another exacerbating factor is the legal confusion in this sector. While Canadian federal legislation does require mandatory breach reporting, under its Data Protection Legislation (PIPEDA), the scope is limited. Only organizations that are in control of personal information that was collected over the course of commercial activity are subject to the act.¹¹⁰ This means that the law does not cover all organizations in Canada.

¹⁰⁶ Fouad, “Securing Higher Education against Cyberthreats”. 142

¹⁰⁷ Eric C. K. Cheng and Tianchong Wang, “Institutional Strategies for Cyber security in Higher Education Institutions,” *Information* 13, no. 4 (April 12, 2022): 2, <https://doi.org/10.3390/info13040192>.

¹⁰⁸ Fouad, “Securing Higher Education against Cyberthreats” 141.

¹⁰⁹ “Cost of a Data Breach Report 2022,” IBM. February 20, 2023, <https://www.ibm.com/resources/cost-data-breach-report-2022>.

¹¹⁰ Office of the Privacy Commissioner of Canada, “What You Need to Know about Mandatory Reporting of Breaches of Security Safeguards,” October 29, 2018, https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/.

Office of the Privacy Commissioner of Canada, “The Application of PIPEDA to Municipalities, Universities, Schools, and Hospitals,” December 16, 2015, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_25/.

Education is generally under the purview of the provinces. PIPEDA does not apply to the education sector. Only Alberta, Quebec and British Columbia have substantially similar legislation with mandatory breach reporting¹¹¹ that can hold these institutions to an elevated standard.

In both the examples for this sector, the universities fell under the jurisdiction of provinces with substantially similar legislation to federal data protection legislation and require breach reporting. However, in provinces that lack this legislative framework, many attacks can fly under the radar. Unfortunately, education is one of the most prevalent sectors where ransomware attacks go underreported.¹¹²

As these institutions become more aware of their targetability, they need to focus on pre-emptively dealing with threats and responding appropriately when threat actors succeed. This requires technical capabilities, developing a minimum standard of preparedness and response plans, potentially set out by the government and increased information sharing.

Broad Gaps and Recommendations

Over the course of this research, we have identified several broad gaps that should be addressed to not only allow for more efficient operationalization of the intelligence process but also strengthen cyber security in Canada. These gaps include deficiencies in technical capabilities, Canadian cyber security legislation, business organizational structures, and a lack of transparency. We will address these gaps through several recommendations that will benefit the operationalization of CTI.

Technical Deficiencies

Healthcare, finance, agriculture, and higher education all suffer from a range of technical deficiencies. Our research has found that there are large disparities in the quality of cyber security between sectors, with healthcare and agriculture having the weakest cyber security while finance and higher education have better protection.

The most glaring gap in the case studies was the lack of cyber security precautions in healthcare and agriculture. Many systems used in these fields do not have any anti-virus or cyber security software.¹¹³ This stems from work cultures that are unaware of

¹¹¹ Office of the Privacy Commissioner of Canada, "Provincial Laws That May Apply Instead of PIPEDA," May 29, 2017, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/.

¹¹² "TELUS Canadian Ransomware Study 2022,"

¹¹³ Statistics Canada, "Cyber Security Measures Enterprises Have in Place by Industry and Size of Enterprise"

cyber threats, leading to a serious lack of investment.¹¹⁴ Poor cyber hygiene exacerbates issues caused by the lack of cyber security. Some examples include not updating software, re-using passwords, and having unrestricted access.

All four case studies are experiencing trends of increasing connectivity – the use of more network-connected devices and more networks being connected. This is raising the potential criticality of a cyber attack and therefore proper precautions must be taken. Interconnected devices make it possible for threat actors to move laterally through systems, expanding their potential impact and access to sensitive information. Organizations should be strict regarding what devices may connect to their networks and what sort of activity is allowed to occur on work networks. Personal networks and business networks should be kept separate and used for different purposes. This is exemplified by the agricultural sector; family farms should consider keeping the farmwork and the farmhouse networks separate. Organizations should also be wary of merging networks. For instance, large organizations such as universities may want to consider maintaining numerous networks across their campuses. One network might open to all students and staff, while more sensitive work could be isolated on smaller more restrictive secondary networks.

Connectivity issues also occur with partner organizations and contractors, as these third parties are an important vector of cyber attacks.¹¹⁵ Many organizations within our case studies work with external partners. These connections can be digital or through physical access. If they can access or use organizations' networks or systems, it's key that these partners and contractors maintain appropriate cyber security standards.

The final major IT challenge we identified was the growing amount of public facing points that could be targeted for cyber attacks. Healthcare, higher education and finance all have points of access open to the public. Whether it's an online bank account, a university portal or an online healthcare profile, these public facing surfaces provide potential breach points. Physical access points are also a potential attack vector for cyber attacks. School computers, unsupervised hospital areas and bank offices present physical access points where a threat actor could enter a system. Maintaining high cyber security standards in these publicly accessible spaces will be key and cyber security investments should emphasize these areas. Ultimately, technical capabilities may struggle to keep up with the innovation of the threat actors but continued improvements in this area are vital to successful CTI operations, so that attacks can be prevented and data more securely managed by practitioners.

¹¹⁴ Kamoun Faouzi and Mathew Nicho, "Human and Organizational Factors of Healthcare Data Breaches: The Swiss Cheese Model of Data Breach Causation And Prevention," *International Journal of Healthcare Information Systems and Informatics* 9, no. 1 (2014): 6.

¹¹⁵ Ibid. 6.

Legal Deficiencies

The Canadian legal regime is currently inadequate to ensure that businesses respond to cyber security threats in an effective and efficient manner. The financial sector which is generally federally regulated is one of the few sectors in Canada that has a decent legal regime behind it to ensure appropriate action. This is due to the multiple regulatory obligations within the sector.¹¹⁶ Currently, at the federal level, the only major legislation that incentivizes an appropriate reaction to cyber incidents from businesses, is PIPEDA. While the act promotes good cyber security posture to ensure that personal information is protected, the act has several blind spots.¹¹⁷ The act only applies to personal information collected through the course of commercial activity. This means that only personal information is subjected to the regulatory requirements under the law and that not all organizations collecting personal information could be subject to it. Notably, hospital, educational institutions and even not-for profits are not covered by the act.¹¹⁸ As discussed in “Higher Education” there is also only similar privacy legislation in Alberta, Quebec, and British Columbia. The variety of laws and limited net casted over what is protected, leaves room for many incidents to fall through the cracks. The Office of the Privacy Commissioner, which ensures compliance with the act, can make non-binding recommendations, and has the power to levy finds over companies that are in contravention of the act up to \$100,000.¹¹⁹

This upper limit however is considered a low penalty for larger organizations that often hold large quantities of Data. A proposed bill- C-27 will give a Personal Information and Data Protection Tribunal the power to “impose fines of up to 3% of an organization’s gross global revenue or \$10 million, whichever is higher. For more egregious offences, the Tribunal can issue fines of up to 5% of an organisation’s gross global revenue or \$25 million, whichever is higher.”¹²⁰

As it stands today Canadian law needs to be updated to ensure that companies are adhering to higher standards of cyber security. This will incentivize increased investment in CTI as proactive mitigation will become a cheaper alternative to reactive cyber security.

¹¹⁶ Mitch Kocerginski, Lyndsay A. Wasser, and Carol Lyons, “Cyber security – The Legal Landscape in Canada,” McMillan LLP, October 25, 2017, <https://mcmillan.ca/insights/publications/cyber-security-the-legal-landscape-in-canada/>.

¹¹⁷ “International Comparative Legal Guides,” Text, International Comparative Legal Guides International Business Reports (Global Legal Group), United Kingdom, <https://iclg.com/practice-areas/cyber-security-laws-and-regulations/canada>.

¹¹⁸ Office of the Privacy Commissioner of Canada, “The Application of PIPEDA to Municipalities, Universities, Schools, and Hospitals.”
Office of the Privacy Commissioner of Canada, “How PIPEDA Applies to Charitable and Non-Profit Organizations,” April 1, 2004, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_19/.

¹¹⁹ “International Comparative Legal Guides.”

¹²⁰ Ibid.

Organizational Deficiencies

The organizational gap is informed by the natural tension formed between the cost-averse nature of business and the expense of security capabilities required to protect against highly sophisticated threats. Military grade capabilities can be deployed in the cyber domain with ease and with little tangible consequence. Companies lack the situational awareness to deploy their cyber capabilities effectively.¹²¹ Businesses focus on risk management; they balance the cost of security and productivity. Therefore, investing in cyber security supplemented by an accurate and constant stream of information only becomes a necessity once the damage has been inflicted.

States develop grand strategies as a means to ensuring their success which for these entities, at its most basic level, is continued existence. According to Edward Luttwak, a renowned academic in the field of strategic studies, states can either operate as if they were at peace or at war.¹²² In peacetime, efficiency is favoured while in war, redundancy becomes the most secure method. It is often the least efficient and expected path that produces the greatest effects while under threat. Given that states are constantly under threat, they must always maintain a state of redundancy. This built-in redundancy casts a wider net of security. However, this choice is bizarre at face value as the method for success is paradoxical in that the state must choose the perceived worse option to succeed.¹²³

Businesses face a similar problem with the proliferation of cyberattacks. They must continue to pursue growth and profits while also having to address constant threats. CTI can be a vital component in bridging the void that stands between effective business operations and security. As it stands companies operate CTI via vendor-produced software or by folding it into IT operations. These methods are reactive and cost-effective. For businesses to combat the ever-looming costs of cyber attacks they must engage in the task of expanding CTI operations even if it appears inefficient in the short run. Businesses cannot operate at the same level of redundancy that states do, they must shift their organizational structure to create as many nodes as possible within their organization that increase the efficiency of the CTI endeavour to create an internal approximate for that strategic redundancy.

One way of conceptualizing this is by imbedding existing business organizational structures into the CTI process.¹²⁴ In line with Kotsias et al.'s conception of business integrated CTI, by having the average employees receive basic cyber hygiene training,

¹²¹ Kotsias, Ahmad, and Scheepers, "Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organisation." 2.

¹²² Edward Luttwak, *Strategy: The Logic of War and Peace*, Rev. and enl. ed. (Cambridge, Mass: Belknap Press of Harvard University Press, 2001) 1-15.

¹²³ Ibid.

¹²⁴ Kotsias, Ahmad, and Scheepers, "Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organisation." 9-11.

they become more capable at identifying and reporting issues. By having IT teams look at CTI as a proactive endeavor and receive intelligence training they would be empowered to help identify future threats. By requiring business managers be aware of the cyber landscape they can act as intermediaries able to explain the business costs of inaction to C-suite executives. C-suite executives tapped into the pulse of the cyber landscape could provide a more holistic picture of the real threats facing the company and allow for more adept preventive measures.

Lack of Transparency

The next major gap is the lack of information sharing. The intelligence community at the nation-state level has significant horizontal intra and inter organization intelligence sharing. In the United States there are over 18 intelligence agencies.¹²⁵ State alliances like the 5-eyes (define) cast a wide net of intelligence operations. The same cannot be said for the business sector. States concerned with power and survival are willing to support one another to ensure their continued existence. A similar dynamic of competition exists in the business world, yet mutual benefit seems to be under-emphasized when compared to competitive advantage. A company in the banking sector must report data breaches vertically to the government but they do not need to share with similar organizations facing the same threats. Businesses must start operating in tandem to ensure cyber protection which includes keeping sector participants up to date of relevant threats. As mentioned in the agriculture case study, the black basta group attacks on Empire and Maple Leaf Farms occurring in just a few days of one another highlights similar and repeatable targetability.

Few organizations exist within Canada to help facilitate CTI sharing. The Canadian Centre for Cyber Security (CCCS) exists to provide “expert advice, guidance, services and support on cyber security for government, critical infrastructure owners and operations, the private sector and the Canadian public”.¹²⁶ The Canadian Cyber Threat Exchange’s (CCTX) mission “enables members to collaborate on reducing financial, operational, and reputational risk through access to timely, relevant, and actionable cyber threat information.”¹²⁷ They strive to accomplish this mission through leveraging their data exchange (a forum to “gather, enrich, analyze and share cyber threat information” among its members) and Collaboration Centre (a forum for cyber professionals to collaborate on current problems).¹²⁸ Both these organizations are like a fusion centre which is a commonly discussed solution for operationalizing cyber threat intelligence within

¹²⁵ “Members of the Intelligence Community,” Office of the Director of Intelligence, n.d., <https://www.dni.gov/index.php/what-we-do/members-of-the-ic>.

¹²⁶ “About the Cyber Centre,” Canadian Centre for Cyber Security, May 5, 2022, <https://www.cyber.gc.ca/en/about-cyber-centre>

¹²⁷ “ABOUT CCTX,” Canadian Cyber Threat Exchange – CCTX – Informing Canadian Business. <https://cctx.ca/about-cctx/>

¹²⁸ Ibid.

government. Fusion centres are publicly owned organizations dedicated to information sharing used by public and private sector partners.¹²⁹

An alternative to fusion centres that can operationalize CTI could be to leverage pre-existing business associations to disseminate key intelligence to all relevant parties. Such industry-wide association dedicated to sharing CTI could act as a liaison between organizations for the purpose of sharing CTI. When an event occurs, organizations would report to the association which then would analyze the data, convert it to useful information and actionable intelligence and then disseminate it to other organizations within the sector. The value of such an arrangement would be to enable businesses to maintain anonymity when a cyber event takes place while helping to secure and build resilience in the sector. It would require non-disclosure agreements and/or other contractual agreements to protect privacy and anonymity. Such an arrangement would also require a major shift in organizational thinking as there may exist some organizations that, when hit with a successful cyber attack, would rather their competitors face a similar event than help build resilience among the industry.

Conclusion

Cyber Threat Intelligence is a field in Academia that has a lot of growth potential. Our analysis of the case studies has found actionable information that can be used to inform cyber security best practices.

Despite being critical infrastructure, holding enormous amounts of sensitive data and having enormous potential bodily harm, healthcare is grievously under protected. Poor cyber hygiene, lack of security training, outdated software, and the use of new, unsecure technology all contribute to healthcare's vulnerability.

Agriculture also suffers from inadequate security. Agriculture plays a key role in the Canadian economy making cyber threats high risk. Currently agriculture has little cyber security protections and a lack of transparency that allows threat actors to repeat preventable attacks. Digitization and an increased tech dependency make manual backups an increasingly unreliable contingency raising the potential impact of a successful cyber attack.

The finance sector is one of the best defended sectors in the country but still faces significant challenges, noticeably a notoriously slow reaction time for detecting and responding to cyber intrusions. The financial sector is also one of the most targeted sectors with threat actors aiming to steal money and sensitive information. The financial

¹²⁹ "Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers," Bureau of Justice Assistance, n.d., <https://bja.ojp.gov/library/publications/cyber-integration-fusion-centers-appendix-baseline-capabilities-state-and->

sector would benefit from improved ways to share and analyze data in a confidential and efficient manner, allowing them to better respond to cyber intrusions.

The last case study, Higher Education faced challenges driven by the large, decentralized nature of their institutions. The decentralized nature has led to poor cyber security standards which allow threat actors to enter systems and then travel laterally, allowing them to install ransomware or steal data. Higher Education Institutions also face challenges around complex legal questions surrounding gaps in legislation and questions around jurisdiction.

Analysis of these sectors has led us to identify technical, legal and organization deficiencies as well as issues driven by a lack of transparency. Technical deficiencies include lack of security software, inadequate segmentation of networks and poor cyber hygiene practices. Legal deficiencies center around broad gaps in legislation. Current legislation doesn't apply to every sector and financial penalties aren't sufficient to incentivize large organizations to make change. Organizational gaps are largely driven by business incentives and industry cultures. Tensions exist between the business' bottom line focus and the expense of ensuring adequate security practices. Many sectors also have cultures that don't value cyber security awareness of knowledge. Finally, lack of transparency enables threat actors to repeat attacks which would otherwise be preventable.

Cyber Threat Intelligence can be used as a framework to address and mitigate these gaps. CTI focuses on building knowledge and awareness so that organizations can take a more proactive cyber security approach. Noticeably, this would allow an organization that embraces CTI to use its employees as security actors, preventing and detecting cyber threats in a decentralized manner.

We present several salient recommendations (summarized in Figure 5). Technical recommendations would focus on ensuring continued progress in implementing and improving base security standards, ensuring appropriate use of networks, securing public-facing points, and ensuring adequate security for partner organizations and contractors. Legal recommendations would entail expanding legislation so that all sectors are required to have appropriate cyber security protection and expanding the government's ability to penalize negligent actors. Organizational recommendations would center around making a business case for why expenditures on security are worth the cost. Businesses could fold CTI capabilities into risk management or business intelligence operations. Finally, the lack of transparency should be addressed by developing better ways of sharing intelligence. This could focus on better utilizing institutions like the Center for Cyber Security and the Cyber Threat Exchange or it could focus on using existing business networks.

Figure 5 Recommendations Summary Table

GAPS	RECOMMENDATIONS
Legal Deficiencies	Update Canadian laws to incentivize higher cyber security standard
Organizational Deficiencies	Imbed CTI at all levels of business through: <ul style="list-style-type: none"> • Basic cyber hygiene training for all • IT teams with intelligence training • Cyber landscape understanding for management
Lack of Transparency	Leverage existing cyber security organizations Leverage pre-existing business associations to disseminate key intelligence and best practices Use intelligence sharing to build resilience in sectors
IT Challenges	Continued advancement and implementation to cyber security solutions

CTI helps address the expanding cyber threats that Canada faces. Information brings us close to equalizing the disparity between attacker and target and this process is critical to continued resilience in cyber security. Ultimately, this process can assist in preventing, mitigating, and educating about cyber threats. Further advancement in this field will prove vital to meeting the cyber challenges of tomorrow, and to this end, industry, government, and academia of important roles to play in order to ensure its success.

Authors' Biography

Scott Davenport completed his undergraduate degree in Business Management at Ryerson University and his master's degree in Infrastructure Protection and International Security at Carleton University. He has worked for the Church of Jesus Christ of Latter-Day Saints as a religious educator and program coordinator for nearly ten years. He is interested in applying his education and professional skills as a consultant. He and his wife live in Cantley, Quebec with their three children.

Jace Stelman completed his undergraduate degree in International Development at McGill University and his master's degree in International Affairs at the Norman Paterson School of International Affairs. He has worked in several roles both as student and employee with the Government of Canada.

David completed an undergraduate degree in History and Political Science at Carleton University. He is now a second-year master's student in International Affairs at the Norman Paterson School of International Affairs. He is currently a co-op student with Public Safety Canada.

Bibliography

"About the Cyber Centre." Canadian Centre for Cyber Security, May 5, 2022.

<https://www.cyber.gc.ca/en/about-cyber-centre>.

"Cost of a Data Breach Report 2022," February 20, 2023.

<https://www.ibm.com/resources/cost-data-breach-report-2022>.

"Critical Infrastructure Partners," Public Safety Canada. December 21, 2018.

<https://www.publicsafety.gc.ca/cnt/ntnl-scrtr/crtcl-nfrstrctr/crtcl-nfrstrtr-prtnrs-en.aspx>.

"Cyber Security and Cybercrime in Canada, 2017," Statistics Canada. October 15, 2018. <https://www150.statcan.gc.ca/n1/pub/71-607-x/71-607-x2018007-eng.htm>.

"Cyber Security Measures Enterprises Have in Place by Industry and Size of Enterprise," Statistics Canada. October 18, 2022.

<https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2210000101>.

"Cyberattack and Exposure of Personally Identifiable Information." Simon Fraser University. <https://www.sfu.ca/information-systems/announcements-alerts/security-alerts/cyberattack-and-exposure-of-personally-identifiable-information.html>.

"Cybersafe Healthcare: Options for Strengthening Cyber security in Canada's Health Sector." HealthCareCAN, 2018. <https://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/Cyber%20Security/Options%20Brief%20Summit%20Report.pdf>.

"How PIPEDA Applies to Charitable and Non-Profit Organizations," Office of the Privacy Commissioner of Canada. April 1, 2004. <https://www.priv.gc.ca/en/privacy->

[topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ro p/02 05 d 19/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ro p/02 05 d 19/).

“Members of the Intelligence Community,” Office of the Director of Intelligence, n.d., <https://www.dni.gov/index.php/what-we-do/members-of-the-ic>.

“National Strategy for Critical Infrastructure.” Public Safety Canada, 2019. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx>.

“North American Industry Classification System (NAICS) Canada 2017 Version 3.0,” Statistics Canada. August 17, 2018. <https://www23.statcan.gc.ca/imdb/p3VD.pl?Function=getVD&TVD=1181553>.

“Overview of Canada’s Agriculture and Agri-Food Sector,” Agriculture and Agri-Food Canada. November 5, 2021. <https://agriculture.canada.ca/en/sector/overview>.

“PIPEDA Findings #2021-003: Security Deficiencies at BMO Lead to Large-Scale Breach,” Office of the Privacy Commissioner of Canada. December 9, 2021. <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-003/>.

“Police-Reported Cybercrime, Number of Incidents and Rate per 100,000 Population, Canada, Provinces, Territories, Census Metropolitan Areas and Canadian Forces Military Police,” Statistics Canada. August 2, 2022. <https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510000201>.

“Provincial Laws That May Apply Instead of PIPEDA,” Office of the Privacy Commissioner of Canada. May 29, 2017. <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ro p/prov-pipeda/>.

“Simon Fraser University Says Server Breach Exposed ‘personally Identifiable’ Information | CBC News.” CBC, February 17, 2021. <https://www.cbc.ca/news/canada/british-columbia/sfu-cyberattack-exposes-info-200-000-1.5916153>.

“Strengthening the Cyber Security Capacity of Canada’s Agricultural Sector – CSA.” <https://cskacanada.ca/projects/strengthening-the-cyber-security-capacity-of-canadas-agricultural-sector/>.

“TELUS Canadian Ransomware Study 2022,” TELUS. accessed February 8, 2023: 14 https://assets.ctfassets.net/1viphdfvqfy/6KFtVdoPfg3apLZr3NuWLL/e16da7dfa1a259afa2da50dac5177780/TELUS_Canadian_Ransomware_Study_2022_2.pdf.

“The Application of PIPEDA to Municipalities, Universities, Schools, and Hospitals,” Office of the Privacy Commissioner of Canada. December 16, 2015.

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_25/.

“University of Calgary Paid \$20K Ransom to Cyberattackers to Unlock Computer Systems | CBC News.” CBC, June 7, 2016.

<https://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979>.

“University of Calgary Pays \$20K Ransom after Cyberattack | CTV News.”

<https://www.ctvnews.ca/sci-tech/university-of-calgary-pays-20k-ransom-after-cyberattack-1.2935525>.

“What You Need to Know about Mandatory Reporting of Breaches of Security Safeguards,” Office of the Privacy Commissioner of Canada. October 29, 2018.

https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/qd_pb_201810/.

Adriano, Lyle. “Maple Leaf Foods Confirms Cyberattack, Will Not Pay Ransomware Gang.” <https://www.insurancebusinessmag.com/ca/news/cyber/maple-leaf-foods-confirms-cyberattack-will-not-pay-ransomware-gang-429218.aspx>.

Ahmed, Yussuf, Syed Naqvi, and Mark Josephs. “Cyber security Metrics for Enhanced Protection of Healthcare IT Systems.” In 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), 1–9. Oslo, Norway: IEEE, 2019. <https://doi.org/10.1109/ISMICT.2019.8744003>.

Ahnert, Toni, Michael Brolley, David Cimon, and Ryan Riordan. “Cyber Security and Ransomware in Financial Markets.” Bank of Canada, July 14, 2022.

<https://doi.org/10.34989/swp-2022-32>.

Antle, Rob, Patrick Butler, and Peter Cowan. “Long before N.L. Cyberattack, Report Flagged Flaws in System.” CBC, May 12, 2022.

<https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cyber-security-eastern-health-report-1.6447807>.

Arnason, Robert. “Ag Sector Warned of Cyberattack Vulnerability.” The Western Producer (blog), August 25, 2022. <https://www.producer.com/news/ag-sector-warned-of-cyberattack-vulnerability/>.

Brown, Rebekah, and Pasquale Stirparo. “SANS 2022 Cyber Threat Intelligence Survey.” SANS, February 2022.

Bureau of Justice Assistance. “Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers,” n.d.

<https://bj.a.ojp.gov/library/publications/cyber-integration-fusion-centers-appendix-baseline-capabilities-state-and>.

- Canadian Centre for Cyber Security. "Cyber Security for Connected Medical Devices (ITSAP.00.132)." Government of Canada, November 5, 2021. <https://www.cyber.gc.ca/en/guidance/cyber-security-connected-medical-devices-itsap00132>.
- Canadian Cyber Threat Exchange – CCTX – Informing Canadian Business. "ABOUT CCTX." <https://cctx.ca/about-cctx/>.
- Canadian Security Intelligence Service. "The Intelligence Cycle." Government of Canada, May 20, 2020. <https://www.canada.ca/en/security-intelligence-service/corporate/publications/2019-public-report/the-intelligence-cycle.html>.
- Chande, Nikil, and Dennis Yanchus. "The Cyber Incident Landscape." Bank of Canada, December 13, 2019. <https://doi.org/10.34989/san-2019-32>.
- Cheng, Eric C. K., and Tianchong Wang. "Institutional Strategies for Cyber security in Higher Education Institutions." Information 13, no. 4 (April 12, 2022): 192. <https://doi.org/10.3390/info13040192>.
- Cline, Mike. "The Top 5 Industries Most Vulnerable to Cyber Attacks." ProcessBolt, September 26, 2022. <https://processbolt.com/top-5-industries-most-vulnerable>.
- Colias, Mike. "Cyber Security: Health Care Learns to Share Scares and Solutions." Hospitals and Healthcare Networks 78, no. 5 (n.d.): 2004.
- Cox, John. "Agriculture Industry on Alert After String of Cyber Attacks." GovTech, June 13, 2022. <https://www.govtech.com/security/agriculture-industry-on-alert-after-string-of-cyber-attacks>.
- Crowdstrike - Cyber security 101. "Indicators of Compromise (IoC) Security," October 5, 2022. <https://www.crowdstrike.com/cyber-security-101/indicators-of-compromise/>.
- Cyber security and Infrastructure Security Agency. "People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices," June 10, 2022. <https://www.cisa.gov/news-events/cyber-security-advisories/aa22-158a>.
- Daigle, Thomas. "Hackers Were Paid Ransom after Attack on Canadian Insurance Firm, Court Documents Reveal." CBC, January 30, 2020. <https://www.cbc.ca/news/science/unnamed-insurance-company-cyberattack-1.5445326>.
- Davies, Phillip H.J. "The Intelligence Cycle Is Dead, Long Live the Intelligence Cycle: Rethinking Intelligence Fundamentals for a New Intelligence Doctrine." Brunel Centre for Intelligence and Security Studies, 2013. <https://bura.brunel.ac.uk/handle/2438/11901>.
- Davis, Jessica. "Inadequate Security, Policies Led to LifeLabs Data Breach of 15M Patients." Health IT Security, July 1, 2020.

<https://healthitsecurity.com/news/inadequate-security-policies-led-to-lifelabs-data-breach-of-15m-patients>.

Dehghantanha, Ali. "Cyber-Attacks a Growing Threat to Farm, Food Security, Warn U of G Researchers." U of G News, August 17, 2022.

<https://news.uoguelph.ca/2022/08/cyber-attacks-a-growing-threat-to-farm-food-security-warn-u-of-g-researchers/>.

Faouzi, Kamoun, and Mathew Nicho. "Human and Organizational Factors of Healthcare Data Breaches: The Swiss Cheese Model of Data Breach Causation And Prevention." International Journal of Healthcare Information Systems and Informatics 9, no. 1 (2014).

Feroot Education Center. "What Are Tactics, Techniques, and Procedures (TTPs)?" n.d. <https://www.feroot.com/education-center/what-are-tactics-techniques-and-procedures-ttps/>.

Fouad, Noran Shafik. "Securing Higher Education against Cyberthreats: From an Institutional Risk to a National Policy Challenge." Journal of Cyber Policy 6, no. 2 (May 4, 2021): 137–54. <https://doi.org/10.1080/23738871.2021.1973526>.

Gollom, Mark. "LifeLabs Cyberattack One of 'Several Wake-up Calls' for e-Health Security and Privacy." CBC, December 19, 2019. <https://www.cbc.ca/news/science/lifelabs-data-breech-security-ehealth-1.5400817>.

Gourley, Bob. "Security Intelligence at the Strategic, Operational and Tactical Levels." Security Intelligence, March 19, 2018. <https://securityintelligence.com/security-intelligence-at-the-strategic-operational-and-tactical-levels/>.

Graber, Roy. "Cyberattack Cost Maple Leaf Foods at Least CA\$23 Million | WATTPoultry." March 9, 2023. <https://www.wattagnet.com/articles/46910-cyberattack-cost-maple-leaf-foods-at-least-ca23-million>.

Harvey, Simon. "Canada's Maple Leaf Foods Hit by Cyberattack." Just Food (blog), November 7, 2022. <https://www.just-food.com/news/canadas-maple-leaf-foods-hit-by-cyberattack/>.

International Comparative Legal Guides International Business Reports. "International Comparative Legal Guides." Text. Global Legal Group. United Kingdom. <https://iclg.com/practice-areas/cyber-security-laws-and-regulations/canada>.

Kocerginski, Mitch, Lyndsay A. Wasser, and Carol Lyons. "Cyber security – The Legal Landscape in Canada." McMillan LLP, October 25, 2017. <https://mcmillan.ca/insights/publications/cyber-security-the-legal-landscape-in-canada/>.

- Koloveas, Paris, Thanasis Chantzios, Sofia Alevizopoulou, Spiros Skiadopoulos, and Christos Tryfonopoulos. "InTIME: A Machine Learning-Based Framework for Gathering and Leveraging Web Data to Cyber-Threat Intelligence." *Electronics (Basel)* 10, no. 7 (2021): 1–34. <https://doi.org/10.3390/electronics10070818>.
- Kotsias, James, Atif Ahmad, and Rens Scheepers. "Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organisation." *European Journal of Information Systems* ahead-of-print, no. ahead-of-print (2022): 1–17. <https://doi.org/10.1080/0960085X.2022.2088414>.
- Krashinsky Robertson, Susan. "Empire Says Cost of Sobeys Cyber security Breach Higher than Initial Estimates." *The Globe and Mail*, March 16, 2023. <https://www.theglobeandmail.com/business/article-sobeys-empire-earnings-q3-cyberbreach/>.
- Kreshnik, Arapi. "The Healthcare Industry: Evolving Cyber Threats and Risks." Master's Thesis - Utica College, May 2018.
- Kubinec, Vera-Lynn. "Credit Unions across Canada Targeted in Cyber security Incident, but No Evidence Data Compromised: Tech Company | CBC News." *CBC*, June 15, 2022. <https://www.cbc.ca/news/canada/manitoba/credit-unions-cyber-security-incident-1.6488872>.
- Le Bris, Aurore, and Walid El Asri. "State of Cyber security & Cyber Threats in Healthcare Organizations. Applied Cyber security Strategy for Managers." ESSEC Business School, 2017.
- Lemos, Robert. "State-Sponsored Cyberattacks Target Medical Research." *Dark Reading*, August 21, 2019. <https://www.darkreading.com/threat-intelligence/state-sponsored-cyberattacks-target-medical-research>.
- Luttwak, Edward. *Strategy: The Logic of War and Peace*. Rev. and enl. Ed. Cambridge, Mass: Belknap Press of Harvard University Press, 2001.
- Marvin, Micheal. "Why Is the Healthcare Industry the Most Likely To Pay Cybercriminals for Ransomware Attacks?" *Portnox*, September 19, 2022. <https://www.portnox.com/blog/healthcare-pay-ransomware-attacks/#:~:text=Perhaps%20more%20alarming%2C%20healthcare%20organizations,%2Dsector%20average%20of%2046%25>.
- Migdal, Alex. "SFU Ransomware Attack Exposed Data from 250,000 Accounts, Documents Show | CBC News." <https://www.cbc.ca/news/canada/british-columbia/sfu-ransomware-attack-1.5732027>.
- Miller-Osborn, Jen. "3 Reasons Cyberattacks Target Financial Services and How to Fight Back." *Palo Alto Networks Blog (blog)*, August 31, 2021. <https://www.paloaltonetworks.com/blog/2021/08/financial-services-cyberattacks/>.

- Muthuppalaniappan, Menaka, and Kerrie Stevenson. "Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health." *International Journal for Quality Healthcare* 33, no. 1 (2021).
- Newman, Lily Hay. "A New Pacemaker Hack Puts Malware Directly on the Device." *Wired Magazine*, August 9, 2018. <https://www.wired.com/story/pacemaker-hack-malware-black-hat/>.
- Oosthoek, Kris, and Christian Doerr. "Cyber Threat Intelligence: A Product Without a Process?" *International Journal of Intelligence and Counterintelligence* 34, no. 2 (2021): 300–315. <https://doi.org/10.1080/08850607.2020.1780062>.
- Petrosyan, Ani. "Cyber Incidents in Financial Industry Worldwide 2021." Statista. <https://www.statista.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide/>.
- Phythian, Mark. *Understanding the Intelligence Cycle*. London, UNITED KINGDOM: Taylor & Francis Group, 2013. <http://ebookcentral.proquest.com/lib/oculcarleton-ebooks/detail.action?docID=1209543>.
- Reuters, Thomson. "Pacemakers, Defibrillators Are Potentially Hackable | CBC News." CBC, February 21, 2018. <https://www.cbc.ca/news/health/pacemakers-hack-1.4545001>.
- Riesco, R., X. Larriva-Novo, and V. A. Villagra. "Cyber security Threat Intelligence Knowledge Exchange Based on Blockchain: Proposal of a New Incentive Model Based on Blockchain and Smart Contracts to Foster the Cyber Threat and Risk Intelligence Exchange of Information." *Telecommunication Systems* 73, no. 2 (2020): 259–88. <https://doi.org/10.1007/s11235-019-00613-4>.
- Roberts, Darrel. "Number of People Hit by Privacy Breach in 2021 Cyberattack Now up to 58,000: Eastern Health." CBC, December 12, 2022. <https://www.cbc.ca/news/canada/newfoundland-labrador/cyberattack-update-eastern-health-1.6678660>.
- Rowley, Jennifer. "Using Case Studies in Research." *Management Research News* 25, no. 1 (January 1, 2002): 16–27. <https://doi.org/10.1108/01409170210782990>.
- Schlette, Daniel, Fabian Böhm, Marco Caselli, and Günther Pernul. "Measuring and Visualizing Cyber Threat Intelligence Quality." *International Journal of Information Security* 20, no. 1 (2021): 21–38. <https://doi.org/10.1007/s10207-020-00490-y>.
- Shin, Bongsik, and Paul Benjamin Lowry. "A Review and Theoretical Explanation of the 'Cyberthreat-Intelligence (CTI) Capability' That Needs to Be Fostered in Information Security Practitioners and How This Can Be Accomplished." *Computers & Security* 92 (2020). <https://doi.org/10.1016/j.cose.2020.101761>.

- Tyrrell, James. "Security Agencies Warn of Cyber Attacks against Agriculture." TechHQ, August 17, 2022. <https://techhq.com/2022/08/security-warning-cyber-attacks-against-agriculture/>.
- Widup, Suzanne, Marc Spittler, David Hylender, and Gabriel Basset. "2018 Verizon Data Breach Investigations Report." Verizon, April 2018. https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report.
- Wilner, Alex, Harrison Luce, Eve Ouellet, Olivia Williams, and Nelson Costa. "From Public Health to Cyber Hygiene: Cyber security and Canada's Healthcare Sector." International Journal 76 (4) (2021).
- Withers, Paul. "Sobeys Cyberattack Cost Grocery Store Operator \$25 Million | CBC News." CBC, December 15, 2022. <https://www.cbc.ca/news/canada/nova-scotia/sobeys-cyber-attack-25-million-1.6686838>.
- Zibak, Adam, Clemens Sauerwein, and Andrew Simpson. "A Success Model for Cyber Threat Intelligence Management Platforms." Computers & Security 111 (December 1, 2021): 1–42. <https://doi.org/10.1016/j.cose.2021.102466>.

Appendices

North American Industry Classification System (NAICS)	Agriculture, forestry, fishing and hunting	Finance and insurance	Educational services	Health care and social assistance
Cyber security measures	2021	2021	2021	2021
Mobile security	30%	74%	42%	37%
Anti-malware software to protect against viruses, spyware, ransomware, et cetera	65%	94%	76%	76%
Web security	24%	80%	65%	45%
Email security	53%	94%	82%	71%
Network security	43%	91%	65%	66%
Data protection and control	17%	76%	41%	40%
Point-Of-Sale (POS) security	6%	30%	29%	20%
Software and application security	11%	68%	31%	22%
Hardware and asset management	12%	71%	35%	30%
Identity and access management	24%	79%	53%	44%
Physical access controls	12%	62%	29%	31%
Business does not have any cyber security measures in place	12%	1%	1%	5%
Business does not know	11%	1%	9%	7%

Figure 1: Cyber Security Measures Enterprises Have in Place by Industry and Size of Enterprise

Statistics Canada. Table 22-10-0001-01 Cyber security measures enterprises have in place by industry and size of enterprise, <https://doi.org/10.25318/2210000101-eng>

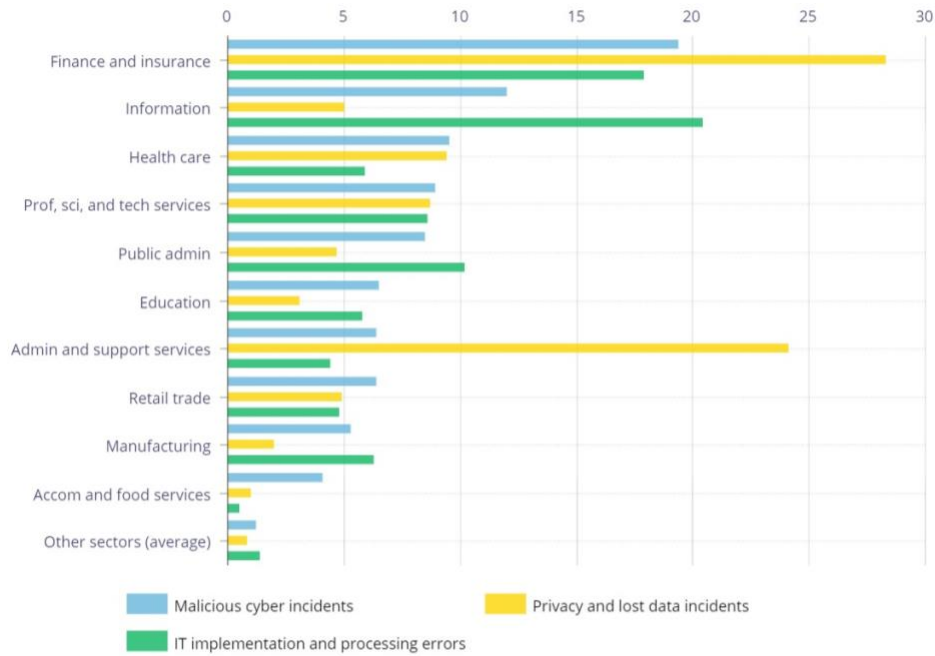


Figure 2: Percentage of Total Incidents

Chande, Nikil, and Dennis Yanchus. 2019. "The Cyber Incident Landscape." [Www.bankofcanada.ca](https://www.bankofcanada.ca/2019/12/staff-analytical-note-2019-32/). December 13, 2019. <https://www.bankofcanada.ca/2019/12/staff-analytical-note-2019-32/>.

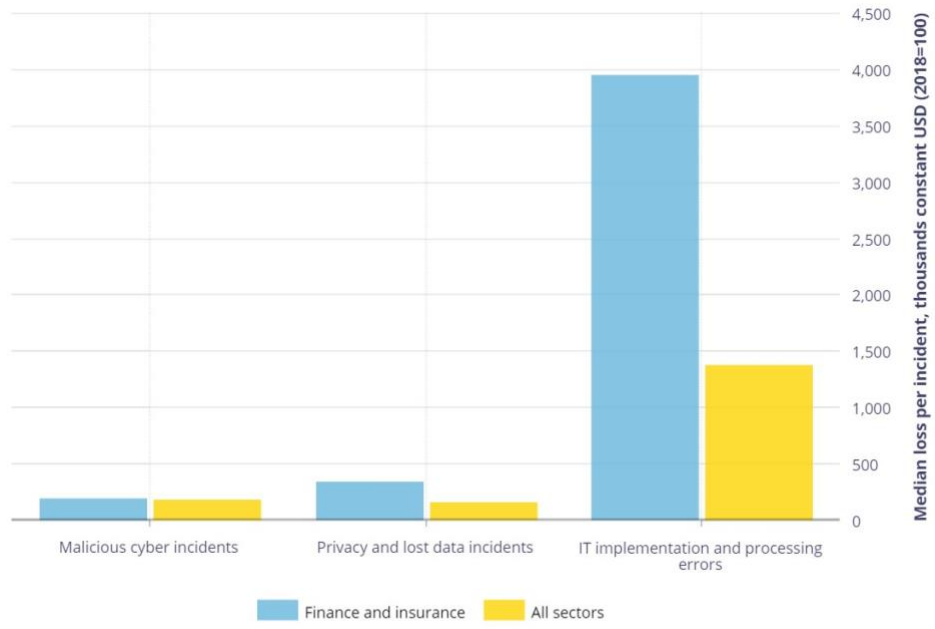


Figure 3: Median Losses by Cyber Incident Type

Chande, Nikil, and Dennis Yanchus. 2019. "The Cyber Incident Landscape." [Www.bankofcanada.ca](https://www.bankofcanada.ca/2019/12/staff-analytical-note-2019-32/). December 13, 2019. <https://www.bankofcanada.ca/2019/12/staff-analytical-note-2019-32/>.

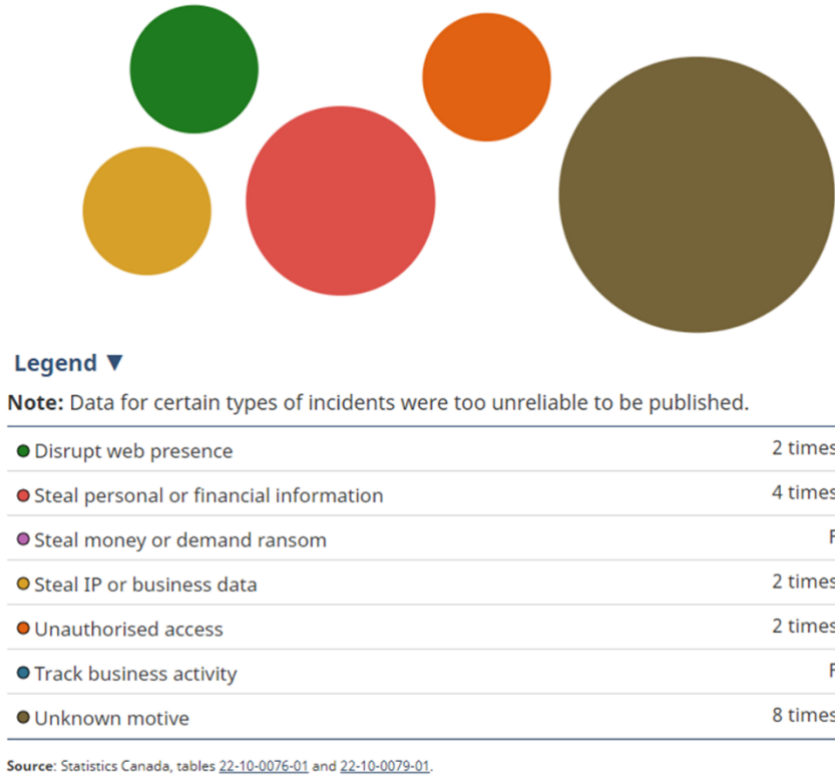


Figure 4: Types of Cyber Security Incidents that Impacted Educational Services, 2017

Statistics Canada. Table 22-10-0076-01 and 22-10-0079-01. Types of Cyber Security Incidents that Impacted Educational Services, <https://www150.statcan.gc.ca/n1/pub/71-607-x/71-607-x2018007-eng.htm>

GAPS	RECOMMENDATIONS
Legal Deficiencies	Update Canadian laws to incentivize higher cyber security standard
Organizational Deficiencies	Imbed CTI at all levels of business through: <ul style="list-style-type: none"> • Basic cyber hygiene training for all • IT teams with intelligence training • Cyber landscape understanding for management
Lack of Transparency	Leverage existing cyber security organizations Leverage pre-existing business associations to disseminate key intelligence and best practices Use intelligence sharing to build resilience in sectors
IT Challenges	Continued advancement and implementation to cyber security solutions

Figure 5: Recommendations Summary Table