Centre for International Governance Innovation

Digital Policy Hub

Digital Policy Hub – Working Paper

Improving Canadian Digital Defences: A National Security Priority

Ryan Westman

Winter 2024 cohort

About the Hub

The Digital Policy Hub at CIGI is a collaborative space for emerging scholars and innovative thinkers from the social, natural and applied sciences. It provides opportunities for undergraduate and graduate students and post-doctoral and visiting fellows to share and develop research on the rapid evolution and governance of transformative technologies. The Hub is founded on transdisciplinary approaches that seek to increase understanding of the socio-economic and technological impacts of digitalization and improve the quality and relevance of related research. Core research areas include data, economy and society; artificial intelligence; outer space; digitalization, security and democracy; and the environment and natural resources.

The Digital Policy Hub working papers are the product of research related to the Hub's identified themes prepared by participants during their fellowship.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

Partners

Thank you to Mitacs for its partnership and support of Digital Policy Hub fellows through the Accelerate program. We would also like to acknowledge the many universities, governments and private sector partners for their involvement allowing CIGI to offer this holistic research environment.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Key Points

- North American organizations are vulnerable to cyberattacks, such as ransomware. The data in this working paper is compiled from eSentire, a Canada-based global cybersecurity firm with clients in 35 industries, 71 subindustries and 85 countries. The data has been cleaned to reflect cyberattacks eSentire detected and responded to in North America from January to December 2023.
- Cybercriminals and state-sponsored threat actors have impacted Canadian organizations. Most recently, cyberattacks have affected Canadian businesses and organizations such as Sobeys, Suncor, Sick Children's Hospital (SickKids), Global Affairs Canada (GAC) and the Royal Canadian Mounted Police (RCMP).
- In 2021, there were a reported 235 ransomware attacks against Canadian industry; those attacks cost $6.35 million on average.
- This working paper uses open-source reporting from organizations that experienced cyberattacks, government agency reporting and quantitative analysis using eSentire's internal data set on cyberattacks detected and responded to in customer environments in North America. This data set demonstrates the value of managed detection and response (MDR) firms and how they have helped to reduce the cost of cyberattacks to North American organizations by preventing attacks before they have serious financial consequences.
- The findings of this research are applicable to policy makers crafting legislation for better controls to minimize the impact of cyberattacks against Canadian industry: specifically, in creating cybersecurity programs and reporting cybersecurity incidents. This research will be directly applicable for Bill C-26, "An Act respecting cyber security."

Introduction

There is a strong push to use public funds to enhance the competitive advantage of domestic Canadian cybersecurity businesses while simultaneously decreasing the cyber risk that all Canadian businesses face. Reducing the risk of cyberattacks to Canadian businesses is a function of several variables, some of which the Government of Canada can influence and control and others that it cannot. These variables include the external cyberthreat environment, cyber operations (active and defensive), information sharing and domestic investment.

This paper advances two arguments in consideration of these four variables. Given the external cyberthreat environment, risks to Canadian businesses can be reduced by domestic investment and the use of Canadian MDR providers, as well as through skills development of the Canadian cybersecurity labour pool. Additional security benefits, such as reducing the risk of cyberattacks impacting Canadian businesses financially, will accrue to Canadian firms if the Government of Canada fosters a collaborative approach of sharing threat intelligence between MDR firms and a government-sponsored defence community by the government. This defence community should be modelled after the United States' Joint Cyber Defense Collaborative (JCDC), an information-sharing group that would disseminate threat intelligence quickly and broadly and facilitate more effective active and

defensive cyber operations by the Communications Security Establishment (CSE) and the newly announced Canadian Armed Forces (CAF) Cyber Command.

This research can support policy makers looking for ideas to enhance Bill C-26, "An Act respecting cyber security," amending the Telecommunications Act and making consequential amendments to other acts, specifically as it pertains to establishing a cybersecurity program and the reporting of cybersecurity incidents.

The Threat Landscape

How susceptible is Canada to cyberattacks, including highly disruptive and damaging ransomware? Recent and historical examples paint a troubling picture (Westman 2023).

For decades, cybersecurity has been a challenge for Canadian businesses, with some being destroyed by cyberattacks that resulted in data breaches, as was arguably the case with Nortel Networks (Naraine 2012; Braga 2013; Pearson 2020). A University of Ottawa study reviewing Nortel's demise only took into account employees' opinions and did not address any instances of what would have been viewed as corporate espionage (Payton 2012). The evidence of that espionage was so damning that the Department of National Defence reconsidered moving into Nortel's old office because the building was filled with eavesdropping devices (CTVNews.ca Staff 2013; Blackwell 2020). At the same time Nortel was allegedly being targeted, Chinese cyberthreat actors were also busy targeting Canadian law firms, financial institutions and public relations agencies in an effort to gain competitive intelligence on PotashCorp during an attempted hostile takeover (Berkow 2011; Gray 2011). And at roughly the same time as the Nortel and PotashCorp-related hacks, Chinese state-sponsored hackers were busy targeting Canada's Immigration and Refugee Board (Freeze 2014a, 2014b).

Regardless of the reason for Nortel's ultimate demise, there are clear indications that parts of the firm's intellectual property ended up being exfiltrated through its information technology (IT) environment and then used to build a foreign tech giant (Dougherty 2020). This technology acquisition strategy continues to be practised by China today, both through human intelligence operations and through cyberattacks (US Department of Justice 2024b; Cybersecurity & Infrastructure Security Agency [CISA] 2024). Part of the reason the attack on Nortel may have been overlooked is that cybersecurity was still viewed at the time as a non-issue by most businesses: something done by teenagers in their parents' basements, not state intelligence agencies looking to acquire competitive advantages (Calof 2014). At its height, the now defunct Canadian tech company employed 90,000 people and had a market value of $367 billion (about $250 billion at the time), accounting for more than 35 percent of Canada's benchmark stock market index, the Toronto Stock Exchange 300 (Cooper 2020).[1]

Canadian grocer Sobeys was hit with ransomware in November 2022; based on publicly available reporting, the incident impacted Sobeys' business network, including its ability to fill prescriptions and process credit card payments, resulting in a bill of $32 million to recover from the attack (Krashinsky Robertson 2023). The following month, SickKids in Toronto was hit with LockBit ransomware, which impacted several network systems,

1 All dollar figures are in Canadian dollars unless otherwise noted.

resulting in it calling a code grey — a system failure that lasted for weeks while the hospital recovered; the cost of this attack has not yet been disclosed (Mosleh 2023). In the summer of 2023, Suncor confirmed that a cyberattack caused widespread outages that impacted its ability to sell gas, costing the company millions (Stephenson 2023). More recently, in February 2024, Canada's Trans-Northern Pipelines was impacted by the ALPHV/BlackCat ransomware, which exfiltrated data from the oil distributor's environment; the financial impacts have yet to be shared publicly (Solomon 2024).

These cyber incidents are not exclusive to the private sector; government agencies across the country at the federal, provincial and municipal levels have also struggled to protect their IT environments and infrastructure (Rudolph 2022; Riches 2024). In the summer of 2020, for instance, the Royal Military College of Canada was hit with Dopplepaymer ransomware, a ransomware group with links to Russia-based "Evil Corp." The attack resulted in the disclosure of Canadian military officers' and soldiers' personal information (US Department of the Treasury 2019; Freeze 2020; Solomon 2020). More recently, GAC sustained a series of breaches through 2022, 2023 and 2024; these breaches potentially impacted internal and highly classified data (McKenna and Ling 2024; Moss 2023; Riches 2024). The Royal Canadian Mounted Police (RCMP) also experienced a cyber incident following a high-profile operation targeting the ransomware group LockBit (Arghire 2024; Vx Underground 2024).

The Government of Canada's Response

To address this evolving threat, the Government of Canada updated the Communications Security Establishment (CSE) Act in June 2019.[2] The updated powers provided the Communications Security Establishment with the ability to conduct "active cyber operations," or, in simpler terms, cyberattacks: "The active cyber operations aspect of the Establishment's mandate is to carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security."[3]

It also provided "defensive operations" to the Government of Canada with the caveat of being able to provide support if the minister of defence decided to designate an organization within the scope of the mandate:

> 18 The defensive cyber operations aspect of the Establishment's mandate is to carry out activities on or through the global information infrastructure to help protect
>
> (a) federal institutions' electronic information and information infrastructures; and

2 *Communications Security Establishment Act*, SC 2019, c 13, s 76, online: <https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html>.

3 *Ibid*, s 19.

> (b) electronic information and information infrastructures designated under subsection 21(1) as being of importance to the Government of Canada.[4]
>
> 21(1) The Minister may, by order, designate any electronic information, any information infrastructures or any class of electronic information or information infrastructures as electronic information or information infrastructures — as the case may be — of importance to the Government of Canada.[5]

This legislation provided the Government of Canada with options to engage in cyberattacks against hybrid threat activity and hostile state threat activity. These powers were arguably important for the Canadian government to have, given the current geopolitical realities that exist with respect to cyber conflict, in which cyberattacks are involved in "intellectual property theft, privacy breaches, and the use of civilian companies or research institutions to advance military goals" (Department of National Defence 2024, 10). However, this legislation also meant that the government's ability to aid the private sector with respect to defensive cyber operations that are not part of section 21(1) were limited, effectively leaving a defensive gap for entities not defined in this section and ultimately relegating the responsibility of managing this risk to small and medium Canadian businesses.[6]

The Government of Canada is currently attempting to mitigate this defensive gap through the RCMP and the Canadian Centre for Cyber Security (CCCS). The RCMP's National Cybercrime Coordination Centre (NC3) works with "law enforcement and other partners to help reduce the threat, impact and victimization of cybercrime in Canada."[7] The CCCS is the public branch of the CSE with a mandate to provide "expert advice, guidance, services and support" on cybersecurity.[8] However, both the NC3 and CCCS provide minimal direct assistance in terms of supporting small and medium Canadian enterprises responding to cyberattacks day to day because they are not MDR providers with security operations centres (SOCs) for small and medium Canadian businesses.

What is the solution for Canadian businesses that have been left to defend themselves in this age of cyber conflict against attacks that are not protected through section 21(1) of the CSE Act? How do we scale and implement cyber defences through the creation of cybersecurity programs and ensure adequate reporting for all digitally enabled organizations in Canada to reduce the risk of cyberattacks to individual organizations and the broader Canadian economy? Canadian MDR providers are increasingly becoming the most logical choice to protect Canadian businesses from the disruption of cyberattacks and their subsequent financial impact; this is because MDR is the only way to detect, respond and recover from cyberattacks in progress.

4 *Ibid*, s 18.

5 *Ibid*, s 21(1).

6 *Ibid*, s 21(1).

7 See www.rcmp-grc.gc.ca/en/nc3.

8 See www.cyber.gc.ca/en/about-cyber-centre.

MDR

Effective cybersecurity programs that reduce the risk of negative impacts in the wake of cyberattacks should include five controls: token-based, multi-factor authentication; a vulnerability management program; incident response plans; data backups; and MDR. The last of these controls is the most important because MDR is the only way to detect, respond to and recover from cyberattacks in progress (Westman 2023).

In 2021, there were a reported 235 ransomware attacks against Canadian industry with an average cost of $6.35 million, putting the total cost to the broader Canadian economy at more than $1 billion (CCCS 2021). Ransomware is a type of malicious software or "malware" that encrypts or locks up files on a computer or network, making them inaccessible to the owner. The cybercriminal behind the ransomware then demands a ransom payment from the victim in exchange for a decryption key to unlock the files; if the ransom is not paid, the files may remain encrypted or could even be deleted.

Ransomware can spread through various means, such as malicious email attachments, infected websites or vulnerabilities in software. Once it infects a system, it can quickly spread and encrypt files, causing disruption to businesses and individuals. The cost of recovering from a ransomware attack is significantly greater than that of preventive measures to mitigate such threats; the most effective prevention strategy these threats today is to partner with an MDR firm.

What is MDR? Industry analysts define it in this way:

> Managed detection and response (MDR) services provide customers with remotely delivered security operations center (SOC) functions. These functions allow organizations to rapidly detect, analyze, investigate and actively respond through threat disruption and containment. They offer a turnkey experience, using a predefined technology stack that commonly covers endpoint, network, logs and cloud. Telemetry [from endpoints, networks, logs and cloud] is analyzed within the provider's platform using a range of techniques. This process allows for investigation by experts skilled in threat hunting and incident management, who deliver outcomes that businesses can act upon. (Shoard 2023, para 10)

Put more simply, MDR is both a service and a software. MDR firms operate SOCs, which are 24/7 teams responsible for monitoring for cyberattacks against organizations. When a cyberattack is identified by a SOC, the team responds to the cyberattack in progress to remove threat actors, whether cyber-criminal or state-sponsored, from the organization's IT environment. This service requires both large teams and specialized software in order to support its delivery. Some enterprises in Canada have the funds and talent to create their own internal SOCs, such as major Canadian financial institutions and some major Canadian retailers; however, most small and medium firms do not have the financial capital or talent to build their own internal SOCs (Cozens 2022).

The cost of employing an MDR firm depends on the size of the organization and the number of computers requiring protection in the corporate IT environment, ranging from as low as US$50,000 to upwards of US$500,000 (Cozens 2022; ForeNova 2023). IT department spending also varies depending on an organization's size and the type of industry to which it belongs; in 2023, 33 percent of organizations in the US and Canada

were freezing or cutting budgets for cybersecurity initiatives (IANS and Artico 2023). To bridge the financial cost for small and medium enterprises, the Government of Canada should consider providing incentives to these enterprise in order to increase and build their cybersecurity programs by partnering with Canadian MDR firms (Solomon 2023).

By these businesses choosing Canadian MDR firms, the Government of Canada's collaboration with these firms (in terms of security clearances, legal agreements and data residency, for example) would make reporting cyber incidents more straightforward than should these organizations choose to go with international MDR firms. The House of Commons recently completed a report titled *The Cyber Defence of Canada* in which those suggestions were echoed specifically: "the Government of Canada [should] take steps to incentivize companies, which could include tax credits, to adopt cybersecurity measures."[9] This report also advises the government to "take steps to retain Canadian-developed information technology intellectual property in Canada, including commercialization measures that maintain Canadian ownership of cyber-technologies," such as Canadian MDR firms.[10] In addition, according to the report, "the Government of Canada [should] work with provinces to establish minimum standards for cyber security for small and medium organizations and incentivize companies to adopt the latest security measures to protect from both high-risk low probability and low-risk frequent attacks" which Canadian MDR firms are excellently suited to address.[11]

The Human and Financial Challenge

The challenge for Canadian businesses is that under-resourced IT departments across different industries have been given the additional responsibility of running cybersecurity programs (Burke 2020). These IT departments are already stretched thin in most Canadian businesses due to a lack of cybersecurity investment (Saddleton 2022). The human challenge is further intensified due to the ongoing cybersecurity skills shortage, limiting the ability of organizations to retain what cybersecurity skills they have amid the personnel costs of building in-house security programs (Cozens 2022; *The Globe and Mail* 2022).

The cost of the education that individuals and organizations need to provide their employees to train and upskill is also expensive. The SANS Institute is the industry-leading training provider that specializes in "hands-on-keyboard" cybersecurity training; it is SANS's ongoing mission to empower cyber security professionals with the practical skills and knowledge they need to make businesses safer. The available training includes cyber and network defences, penetration testing, incident response, digital forensics and auditing. The Institute awards Global Information Assurance certifications to individuals who complete the training, which the CSE recognizes as advanced cybersecurity certifications (CCCS 2022a). But this training cost upwards of $13,000 for a week-long course that includes a final exam for the certification.

That amount of time and money represents a significant cost for an employee as well as a significant investment from an employer. In addition, once an

9 House of Commons, *The Cyber Defence of Canada: Report of the Standing Committee on National Defence* (June 2023) (Chair: John McKay), online: <www.ourcommons.ca/Content/Committee/441/NDDN/Reports/RP12548256/nddnrp05/nddnrp05-e.pdf>.

10 *Ibid*, 3.

11 *Ibid*, 3.

individual has that certification, that individual is then uniquely skilled in the labour market, which could then be leveraged in order to change employers for additional salary and benefits. This marketability can act as a disincentive for organizations to invest in their cybersecurity professionals.

To bridge the financial cost of training and upskilling this talent pool for Canadian MDR firms, the Government of Canada should consider using public funds to provide incentives to these firms. This would incentivize Canadian MDR firms to continue to invest in their highly skilled cybersecurity professionals by providing the necessary education, while mitigating the impact of those individuals leveraging that upskill to change employers. The Government of Canada and broader Canadian society would benefit by creating a highly skilled talent pool, and by extension, Canadian business would be better protected and less likely to experience significant financial consequences from cyberattacks. It would also minimize the financial impact on the Canadian economy and GDP by reducing the cost that organizations have to pay in responding to major cyber incidents, as was the case for Sobeys and Suncor.

CSE National Cyber Threat Assessment and the Data: The 2023 Threat Landscape

The best way to understand this problem is to look at data; however, there are significant challenges in acquiring data in this evolving policy space due to organizations not reporting cyberattacks for a variety of reasons. In 2022, eSentire reviewed ransomware name-and-shame sites and identified 232 Canadian companies; a large majority of those Canadian companies were victims of Russian-based ransomware gangs (Westman 2023). It is important to note that this list only includes companies that were affected by publicly known cyberattacks, in which the company's information leaked on the dark web. The true number of affected companies is unknown as businesses have been known to pay ransoms to have their systems restored. As of 2021, Statistics Canada estimates 90 percent of these crimes go unreported to law enforcement.[12]

This lack of reporting by organizations is partly due to the potential ramifications for businesses impacted by cyberattacks and the potential legal risk presented by publicly acknowledging or reporting these incidents. The other reason is the perceived lack of value in reporting to law enforcement. Up until very recently, law enforcement in Canada was not providing the necessary hands-on-keyboard help and support to organizations experiencing cyberattacks, and that is largely due to financial challenges as well as the sheer number of these incidents: the RCMP NC3 notes that from "April 1, 2021, until end of August 2022, the NC3 received more than 2,000 requests for operational assistance from domestic and international law enforcement partners" (RCMP 2022).

Additionally, up until very recently, international law enforcement's efforts to reduce international cybercrime were poorly coordinated and ineffective (Greenberg 2022). Many strides have been made to improve international law enforcement collaboration, such as with the LockBit 3.0 takedown; the ransomware-as-a-service operation extorted more than $US120 million in ransom from more than 2,000 victims in 2022. The operation resulted in the takeover of major pieces of the ransomware group's infrastructure, including its primary administration and public-facing leak site (Hurley 2024).

12 See https://antifraudcentre-centreantifraude.ca/annual-reports-2021-rapports-annuels-eng.htm.

Law enforcement's ability to directly target those engaged in the most significant cybercrime and cyberespionage is hampered within the borders of countries in which international law enforcement action is minimal and/or non-existent. Countries that are either indifferent to cybercrime or even actively collaborating with these threat actors include China, Iran, North Korea and Russia (Greenberg 2019; CCCS 2022b; Department of National Defence 2024).

Threat intelligence analysts often refer to the "spectrum of state responsibility" to indicate a state's level of culpability with respect to cyberattacks that originate within their borders. Cyberattacks in the countries listed above fluctuate from being state-ignored, meaning that the government knows about these third-party attacks but is unwilling to take any official action against them, to being state-integrated, meaning that the government actually coordinates these attacks by using integrated third-party proxies and government forces (Healey 2012).

There is growing and compelling evidence to suggest that certain types of malware and cyber criminals are supported by at least some of the aforementioned states. Most notable among these is Russia's Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). GRU hackers are most famously known for causing the NotPetya ransomware outbreak that targeted a variety of industries and firms around the world (including Australia, France, Germany, Italy, Poland, Ukraine, the United Kingdom and the United States) that together suffered nearly $US 1 billion in losses (Greenberg 2019; US Department of Justice 2020). Through investigative reporting and breached dark web data, it was recently disclosed that a Russian cybercrime forum was partly founded by a GRU officer. This officer was an attorney who advised some of Russia's top cyber criminals on the legal risks of their work and what to do if they were caught (Krebs 2024). More recently, in January 2024, GRU officers relied on non-GRU cyber criminals to install Moobot malware on vulnerable routers. GRU hackers then used the Moobot malware to install their own "bespoke scripts and files" that repurposed the botnet, leveraging it for a "global cyber espionage platform" (Department of National Defence 2024; US Department of Justice 2024a, para. 2).

This nexus between cyber criminals, state proxies and intelligence agencies presents a highly complex problem for Canada. Canadian MDRs sit at the nexus of cybercrime and state-sponsored activity, and the figures below build a compelling case to demonstrate the need for a Government of Canada requirement to better leverage industry subject matter experts from Canadian MDR firms. This would allow threat intelligence to be shared more rapidly between government and industry subject matter experts who have security clearances embedded in Canadian MDR firms to better protect Canadians in a whole-of-society or "national team" approach (Bruce et al. 2023, 10).

The recent House of Commons' report on *The Cyber Defence of Canada* echoed the suggestions above, specifically recommending that the Government of Canada implement a "multistakeholder platform for collaboration and engagement on cybersecurity issues."[13] That group would be able to have "ongoing dialogue with critical infrastructure owners/operators such as municipalities, Provincial, Territorial,

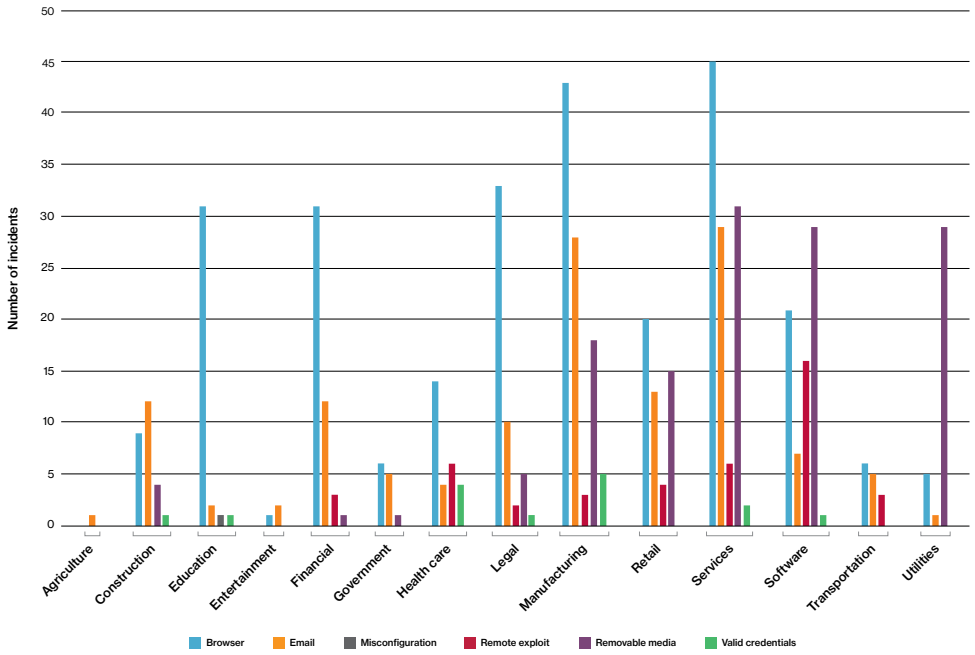
13 House of Commons, *The Cyber Defence of Canada: Report of the Standing Committee on National Defence* (June 2023) (Chair: John McKay), online: <https://www.ourcommons.ca/Content/Committee/441/NDDN/Reports/RP12548256/nddnrp05/nddnrp05-e.pdf>.

Indigenous governments, and private sector operators" with the goal of establishing "requirements for private sector critical infrastructure operators to report ransomware and cybersecurity incidents to the Canadian Centre for Cyber Security."[14] The report also suggests that the Government of Canada "expand its collaboration with Canadian security and defence industries to bolster Canada's offensive and defensive cyber infrastructure amidst the growing assertiveness of malign foreign states."[15]

The United States' approach to solving this wicked problem has been CISA's JCDC. The JCDC is a public-private cybersecurity collaborative that leverages new authorities granted by Congress in the 2021 National Defense Authorization Act to unite the global cyber community in the collective defence of cyberspace. It is comprised of a diverse team of cross-industry organizations that proactively gathers, analyzes and shares actionable cyber-risk information to enable synchronized, holistic cybersecurity planning as well as cyber defence and response.[16]

The graphs below were compiled using a subset of eSentire's 2023 data set of cyberattacks that impacted firms in North America; North America was chosen in order to sufficiently anonymize the data. This data is available because eSentire studies threat-actor behaviours and uses the resulting data to learn how to provide better detections and recommendations to reduce the risk of cyberattacks impacting their customer base. The graphs also demonstrate Canadian MDR firms' ability to conduct cybersecurity incident reporting and deal with the growing assertiveness of malign foreign state cyberthreat actors.

Figure 1: Initial Cyberthreat Access by Industry in North America, 2023



Source: Author.

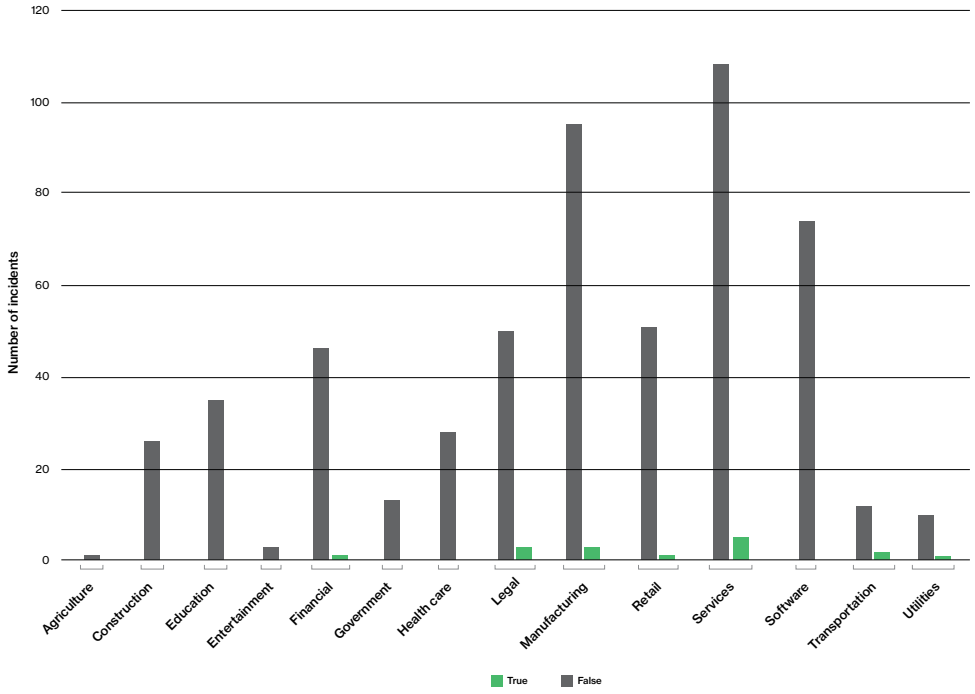
14 *Ibid*, 2.

15 *Ibid*, 3.

16 See www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative.

Figure 1 shows the ways in which threat actors are initially gaining access to organizations in North America: often, it is through a browser or email. MDR firms detect these attacks using specialized software and then respond to them by taking the appropriate measures to remove the threat from the customer's environment.

Figure 2: Incidents Responded to in North America Involving State-Sponsored Threats, 2023



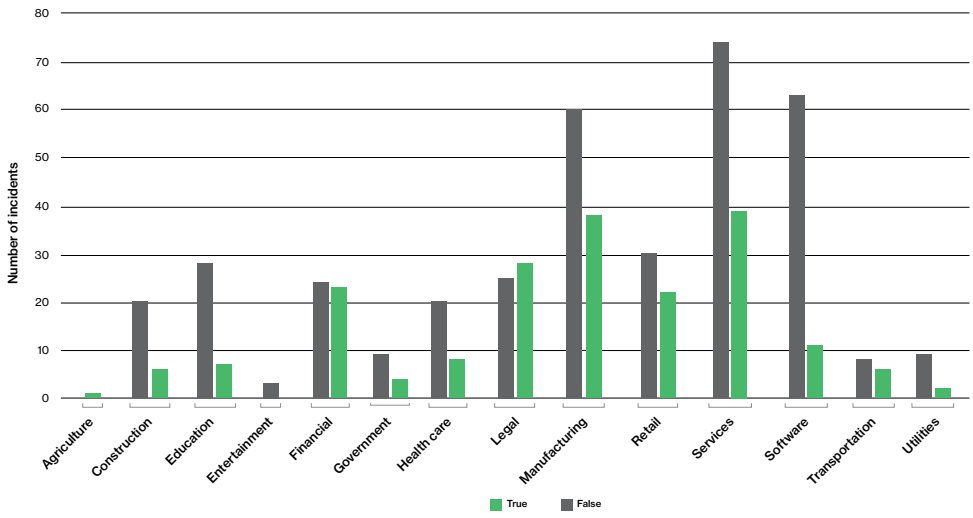
Source: Author.

Figure 2 shows the incidents that were responded to in 2023 in which malware and techniques have been tracked to state-sponsored threats, meaning that the malware and techniques used to conduct these cyberattacks in North America were consistent with those known to be used by foreign states through public reporting of these threats by CISA and other cybersecurity firms such as CrowdStrike and Mandiant. This finding is consistent with CCCS's *National Cyber Threat Assessment 2023*, which states, "We assess that the state-sponsored cyber programs of China, Russia, Iran, and North Korea pose the greatest strategic cyber threats to Canada. State-sponsored cyber threat activity against Canada is a constant, ongoing threat that is often a subset of larger, global campaigns undertaken by these states. State actors can target diaspora populations and activists in Canada, Canadian organizations and their intellectual property for espionage, and even Canadian individuals and organizations for financial gain" (CCCS 2022b, 12).

Figure 3 shows the incidents that were responded to in 2023 in which malware and techniques have been tracked to groups interested in deploying ransomware. Again, the malware and techniques used to conduct these cyberattacks against North American firms were consistent with the malware and techniques known to be used by ransomware gangs through public reporting of these threats by CISA and other cybersecurity firms such as CrowdStrike and Mandiant. Additionally, this data aligns

with the CCCS's *National Cyber Threat Assessment 2023*, which states, "Cybercrime continues to be the cyber threat activity most likely to affect Canadians and Canadian organizations. Due to its impact on an organization's ability to function, ransomware is almost certainly the most disruptive form of cybercrime facing Canadians. Cybercriminals deploying ransomware have evolved in a growing and sophisticated cybercrime ecosystem and will continue to adapt to maximize profits" (CCCS 2022b, 5).

Figure 3: Incidents in Which Ransomware Could Have Been Deployed against Organizations in North America, 2023



Source: Author.

Recommendations

This paper has highlighted three areas in which the Government of Canada could incentivize more industry collaborations, increase the base level of cybersecurity for small and medium enterprise across the country, and rapidly scale the cybersecurity talent pool in Canada. These recommendations reflect those given in the House of Commons Standing Committee on National Defence report titled *The Cyber Defence of Canada*, specifically recommendations 1, 4, 6, 8, 10, 13 and 14.

Today, the Government of Canada is attempting to support the whole of society through the RCMP NC3 and CCCS. However, the RCMP NC3 and CCCS provide minimal direct support in the defence of small and medium enterprises from cyberattacks because they are not an MDR operating a SOC for small and medium Canadian businesses. Therefore, the most effective and efficient way that the Government of Canada can rapidly scale Canadian cyber defences for the benefit of the whole of society is to use public funds to incentivize Canadian businesses to partner with Canadian MDR firms, provide those MDR firms with incentives to invest in their cybersecurity professionals and leverage those subject matter experts to collaborate with the Canadian intelligence community. These recommendations are elaborated more broadly here:

- The CCCS and RCMP NC3 should adopt a similar model to CISA's JCDC and provide a subset of Canadian MDR providers with security clearances to enable cross-collaboration with Canadian intelligence and law enforcement agencies to address threats and share information in order to start building a "national team." MDR providers are currently on the frontlines of the cyber conflict being fought by states and financially motivated, hacktivist threat actors, protecting Canadian industry with minimal support from CCCS and NC3. In order for the Government of Canada to keep pace with these varied threat actors, the CCCS and NC3 need to evolve into meaningful contributors and coordinators for the defence of Canadian industry. This role would be similar to that of CISA's JCDC, and would facilitate the Government of Canada treating Canadian MDR organizations as peers that can provide much needed advice, guidance and intelligence in order for the government to take action against these groups through international agreements and bilateral partnerships. In some instances, these relationships with Canadian law enforcement and Canadian intelligence agencies exist in an ad hoc and semi-formalized manner. In order to mature and actually put into practice the whole-of-society approach required to combat cyberthreats, the Government of Canada, specifically the NC3 and CCCS, should look to adopt measures to create a community of defence, similar to the model created by CISA with the JCDC. This would also enable more efficient and effective cyber incident reporting, while enhancing active and defensive cyber operations by the CSE and the CAF Cyber Command.

- The Government of Canada should provide a financial incentive to small, medium and enterprise firms leveraging Canadian MDR providers; this should come in the form of a non-refundable tax credit in order to directly reduce the taxes paid by Canadian businesses that are currently doing so. This approach would incentivize organizations that have previously not had the additional IT or security budget for a full cybersecurity program to consider partnering with a Canadian MDR provider. The services that should be included in the non-refundable tax credit are: managed SOCs for monitoring endpoints, networks, logs and cloud data sources; vulnerability management; and digital forensics and incident response services (including retainers).

- The Government of Canada should also give Canadian MDR providers a financial incentive to grow their talent in the form of a non-refundable tax credit. This tax credit would enable MDR providers to invest in their talent and support their development by paying for industry-standard training to keep pace with the rapid change of technology and stay competitive with international firms. The leading cybersecurity certifications and training programs are costly and can total more than $10,000; offsetting these costs for business will directly support MDR providers by enabling them to retain top talent to best protect Canadian businesses.

Acknowledgements

I would like to thank my employer, eSentire, for providing me with the opportunity to conduct my research, trusting me with this data and believing in the importance of demystifying this space for Canadian policy makers to build a more secure country. Reducing the impact of cyberattacks benefits all Canadians.

I would also like to thank my mentors Wesley Wark, J. Paul Haynes, Aaron Shull, Rahul Bakshi, Derek Watral and Kurtis Armour.

Additionally, my sincerest gratitude goes to my friends and colleagues in the Canadian intelligence and law enforcement communities who took the time to look at earlier drafts and provide me with some useful perspectives and insights on the shared challenge we both face. This policy paper is better because of your support. Together, we can solve this problem.

Finally, I would also like to thank my wife and family for putting up with my incessant need to try to solve wicked problems. None of this would be possible without your love and support. Thank you.

Ducimus. Persuade, change, influence.

About the Author

Ryan Westman is a director of threat intelligence at Waterloo, Ontario-based eSentire and leads the firm's threat intelligence team. Prior to joining eSentire, Ryan spent three years in management consulting, leading a threat intelligence and analytics team, and also worked for Public Safety Canada and the Canadian Armed Forces. Ryan holds a B.A. in political science and history from Wilfrid Laurier University, an M.Sc. in counterterrorism from the University of Central Lancashire and a master's degree from the University of Waterloo. He is a certified cyberthreat intelligence analyst, certified forensic analyst and certified security leader through Global Information Assurance Certification. As a Digital Policy Hub visiting fellow, he will focus on the impact of poor digital defences on the Canadian economy.

Acronyms and Abbreviations

CAF	Canadian Armed Forces
CCCS	Canadian Centre for Cyber Security
CISA	Cybersecurity & Infrastructure Security Agency
CSE	Communications Security Establishment
GAC	Global Affairs Canada
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
IT	internet technology
JCDC	Joint Cyber Defense Collaborative

MDR	Managed Detection and Response
NC3	National Cybercrime Coordination Centre
RCMP	Royal Canadian Mounted Police
SOC	Security Operations Centres

Works Cited

Arghire, Ionut. 2024. "Canada's RCMP, Global Affairs Hit by Cyberattacks." SecurityWeek, February 27. www.securityweek.com/canadas-rcmp-global-affairs-hit-by-cyberattacks/.

Berkow, Jameson. 2011. "Chinese hackers went after aborted Potash deal." *Financial Post*, November 30. https://financialpost.com/technology/chinese-hackers-went-after-aborted-potash-deal-report.

Blackwell, Tom. 2020. "Exclusive: Did Huawei bring down Nortel? Corporate espionage, theft, and the parallel rise and fall of two telecom giants." *National Post*, February 20. https://nationalpost.com/news/exclusive-did-huawei-bring-down-nortel-corporate-espionage-theft-and-the-parallel-rise-and-fall-of-two-telecom-giants.

Braga, Matthew. 2013. "Canada must ramp up cyber security in wake of alleged China-led attacks, experts say." *Financial Post*, February 19. https://financialpost.com/technology/canada-must-ramp-up-cyber-security-in-wake-of-china-led-attacks-experts-say.

Bruce, Shelly, John Bruce, Aaron Shull and Kailee Hilt. 2023. *Waterloo Security Dialogue: Fostering Nationwide Cybersecurity Collaboration*. Waterloo, ON: CIGI. www.cigionline.org/static/documents/WSD_Special_Report_web.pdf.

Burke, Stephen. 2020. "Cyber Security Goes Beyond the IT Department, and Across the Whole Organisation." *CPO Magazine*, June 25. www.cpomagazine.com/cyber-security/cyber-security-goes-beyond-the-it-department-and-across-the-whole-organisation/.

Calof, Jonathan. 2014. *An Overview of the Demise of Nortel Networks and Key Lessons Learned: Systemic effectis in environment, resilience and black-cloud formation*. Ottawa, ON: Telfer School of Management, University of Ottawa. March 17. https://sites.telfer.uottawa.ca/nortelstudy/.

CCCS. 2021. *Cyber Threat Bulletin: The Ransomware Threat in 2021*. Government of Canada. www.cyber.gc.ca/sites/default/files/cyber/2021-12/Cyber-ransomware-update-threat-bulletin_e.pdf.

– – –. 2022a. *Certifications in the Field of Cyber Security 2023-2024*. Government of Canada. www.cyber.gc.ca/sites/default/files/certificationsfieldcybersecurity-2022-v2-e.pdf.

– – –. 2022b. *National Cyber Threat Assessment*. Government of Canada. www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf.

CISA. 2024. "PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders." March. www.cisa.gov/sites/default/files/2024-03/Fact-Sheet-PRC-State-Sponsored-Cyber-Activity-Actions-for-Critical-Infrastructure-Leaders-508c.pdf.

Cooper, Sam. 2020. "Inside the Chinese military attack on Nortel." Global News, August 25. https://globalnews.ca/news/7275588/inside-the-chinese-military-attack-on-nortel/.

Cozens, Bill. 2022. “Is an outsourced SOC worth it? Looking at the ROI of MDR.” *ThreatDown* (blog), December 15. www.malwarebytes.com/blog/business/2022/12/are-outsourced-soc-services-worth-it-looking-at-the-roi-of-mdr.

CTVNews.ca Staff. 2013. “DND may abandon $1B move to former Nortel site because of surveillance bugs.” CTV News, September 30. www.ctvnews.ca/mobile/canada/dnd-may-abandon-1b-move-to-former-nortel-site-because-of-surveillance-bugs-1.1477766.

Department of National Defence. 2024. *Our North, Strong and Free: A Renewed Vision for Canada’s Defence*. Ottawa, ON: Government of Canada. www.canada.ca/content/dam/dnd-mdn/documents/corporate/reports-publications/2024/north-strong-free-2024.pdf.

Dougherty, Nicole. 2020. “Huawei: The Dragon That Caught Nortel Off Guard.” NATO Association of Canada, January 30. https://natoassociation.ca/why-canada-should-be-wary-of-huawei-lessons-from-nortel/.

ForeNova. 2023. “The Cost of MDR: Unveiling the True Value of Cybersecurity Expertise.” *ForeNova* (blog), August 7. www.forenova.com/blog/managed-detection-and-response-cost.

Freeze, Colin. 2014a. “Canada targeted in 2011 hacks by accused PLA unit.” *The Globe and Mail*, May 19. www.theglobeandmail.com/news/national/canada-targeted-in-2011-hacks-by-accused-pla-unit/article18750958/.

– – –. 2014b. “What a cyber attack looks like – from the target’s point of view.” *The Globe and Mail*, May 26. www.theglobeandmail.com/news/politics/globe-politics-insider/what-a-cyber-attack-looks-like-from-inside-the-government/article18853435/.

– – –. 2020. “RCMP investigating after soldiers’ personal data leaked in cyberattack at RMC.” *The Globe and Mail*, August 19. www.theglobeandmail.com/canada/article-rcmp-investigating-after-soldiers-personal-data-leaked-in-cyberattack/.

Gray, Jeff. 2011. “Hackers linked to China sought Potash deal details: consultant.” *The Globe and Mail*, November 30. www.theglobeandmail.com/technology/tech-news/hackers-linked-to-china-sought-potash-deal-details-consultant/article534297/.

Greenberg, Andy. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers*. Toronto, ON: Random House.

– – –. 2022. *Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency*. Toronto, ON: Random House.

Healey, Jason. 2012. “Beyond Attribution: Seeking National Responsibility for Cyber Attacks.” Atlantic Council Issue Brief, February 22. www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF.

Hurley, Billy. 2024. “Operation Cronos locks LockBit.” IT Brew, February 21. www.itbrew.com/stories/2024/02/21/operation-cronos-locks-lockbit.

IANS and Artico. 2023. *2023 Security Budget Benchmark Summary Report*. www.iansresearch.com/resources/infosec-content-downloads/detail/2023-security-budget-benchmark-summary-report.

Krashinsky Robertson, Susan. 2023. “Empire says cost of Sobeys cybersecurity breach higher than initial estimates.” *The Globe and Mail*, September 13. www.theglobeandmail.com/business/article-sobeys-empire-earnings-q3-cyberbreach.

Krebs, Brian. 2024. “From Cybercrime Saul Goodman to the Russian GRU.” Krebs on Security, February 7. https://krebsonsecurity.com/2024/02/from-cybercrime-saul-goodman-to-the-russian-gru/.

McKenna, Kate and Philip Ling. 2024. “Authorities investigating massive security breach at Global Affairs Canada.” CBC News, January 30. www.cbc.ca/news/politics/global-affairs-security-breach-1.7099290.

Mosleh, Omar. 2023. “SickKids attack — and apology — pulls ransomware’s ‘Robin Hood’ into spotlight.” *Toronto Star*, January 5. www.thestar.com/news/canada/sickkids-attack-and-apology-pulls-ransomware-s-robin-hood-into-spotlight/article_5ebeb7d4-4154-58d6-97ce-dbf4404f8311.html.

Moss, Neil. 2023. “Global Affairs gauged ‘very likely’ chance of another breach weeks after 2022 cyberattack: docs.” *The Hill Times*, July 19. www.hilltimes.com/story/2023/07/19/global-affairs-gauged-very-likely-chance-of-another-breach-weeks-after-2022-cyberattack-docs/392924/.

Naraine, Ryan. 2012. “Nortel hacking attack went unnoticed for almost 10 years.” ZDNet, February 14. www.zdnet.com/article/nortel-hacking-attack-went-unnoticed-for-almost-10-years/.

Payton, Laura. 2012. “Former Nortel exec warns against working with Huawei.” CBC News, October 11. www.cbc.ca/news/politics/former-nortel-exec-warns-against-working-with-huawei-1.1137006.

Pearson, Natalie Obiko. 2020. “Did a Chinese hack kill Canada’s greatest tech company?” Bloomberg, July 1. www.bloomberg.com/news/features/2020-07-01/did-china-steal-canada-s-edge-in-5g-from-nortel.

Riches, Sam. 2024. “Canada’s cybersecurity under siege and even the government is powerless.” *National Post*, March 12. https://nationalpost.com/news/canadas-cybersecurity-under-siege-and-even-the-government-is-powerless.

Rudolph, Alexander. 2022. “When Empty Promises are Literally Empty: Canadian Cyber-Defence Policy by Ad-Hoc.” Canadian Global Affairs Institute, July. www.cgai.ca/when_empty_promises_are_literally_empty_canadian_cyber_defence_policy_by_ad_hoc.

Saddleton, Lucy. 2022. “More than half of Canadian businesses plan to spend more on tech in 2023: study.” *Canadian Lawyer*, December 19. www.canadianlawyermag.com/inhouse/news/general/more-than-half-of-canadian-businesses-plan-to-spend-more-on-tech-in-2023-study/372465.

Shoard, Pete. 2023. *2023 Gartner Market Guide for Managed Detection and Response Services*. eSentire, February 13. www.esentire.com/resources/library/2023-gartner-market-guide-for-managed-detection-and-response-services.

Solomon, Howard. 2020. “Threat group posts files allegedly from Canadian military college.” IT World Canada, August 19. www.itworldcanada.com/article/threat-group-posts-files-allegedly-from-canadian-military-college/434694.

———. 2023. “Give tax break so small Canadian firms can invest in cybersecurity, Parliament told.” IT World Canada, February 8. www.itworldcanada.com/article/give-tax-break-so-small-canadian-firms-can-invest-in-cybersecurity-parliament-told/526227.

———. 2024. “Ransomware gang claims it hit Canadian oil pipeline operator.” IT World Canada, February 13. www.itworldcanada.com/article/ransomware-gang-claims-it-hit-canadian-oil-pipeline-operator/558632.

Stephenson, Amanda. 2023. “Suncor Energy cyberattack likely to cost company millions of dollars, expert says.” *Financial Post*, June 26. https://financialpost.com/commodities/energy/oil-gas/suncor-energy-cyber-attack.

The Globe and Mail. 2022. “Severe cybersecurity talent gap creates vulnerabilities.” *The Globe and Mail,* October 19. www.theglobeandmail.com/business/adv/article-severe-cybersecurity-talent-gap-creates-vulnerabilities/.

US Department of Justice. 2020. “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace.” Press release, October 19. www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

– – –. 2024a. “Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation’s Main Intelligence Directorate of the General Staff (GRU).” Press release, February 15. www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian.

– – –. 2024b. “Owners of China-Based Company Charged with Conspiracy to Send Trade Secrets Belonging to Leading U.S.-Based Electric Vehicle Company.” Press release, March 19. www.justice.gov/opa/pr/owners-china-based-company-charged-conspiracy-send-trade-secrets-belonging-leading-us-based.

US Department of the Treasury. 2019. “Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware.” Press release, December 5. https://home.treasury.gov/news/press-releases/sm845.

Vx Underground. 2024. “Lockbit Statement.” Vx Underground, February 24. https://web.archive.org/web/20240226200811/https://samples.vx-underground.org/tmp/Lockbit_Statement_2024-02-24.txt.

Westman, Ryan. 2023. “Poor Cyber Defences Are Damaging Canada’s Economy.” Opinion, Centre for International Governance Innovation, April 17.