Lena Klassen
1005477128
INF301
November 15th, 2019

Canada's Evolving Cybersecurity Strategy

Introduction

The term "cybersecurity" encompasses the efforts and processes in place to secure digital information and technologies. Canada's National Cybersecurity Strategy from 2018 defines cybersecurity as "the protection of digital information and the infrastructure on which it resides."[1] Since digital technologies are utilized in personal, business, and governmental domains, cybersecurity impacts all of these areas. Examples of efforts to improve cybersecurity include using anti-virus software on personal computers, implementing a network intrusion and response system at businesses, and governments initiating digital literacy programs to keep their citizens safe online.

Canada's 2010 Cybersecurity Strategy

The Canadian government recognized the importance of cybersecurity in its release of Canada's first national cybersecurity strategy in 2010.[2] This strategy was initiated by Vic Toews, the Minister of Public Safety at the time, [3] who was working in the conservative government led by Stephen Harper. The three main goals of the strategy were "Securing Government systems,"

[1] "National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age," Ottawa, 2018, 7, http://publications.gc.ca/collections/collection_2018/sp-ps/PS4-239-2018-eng.pdf.
[2] "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada," Ottawa, 2010, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-cbr-scrt-strtgy-eng.pdf.
[3] "National Cyber Security Strategy," 2010, 1.

"Partnering to secure vital cyber systems outside the federal Government," and "Helping Canadians be secure online."[4]

The goal of "Securing Government systems" was deemed a priority in Canada's 2010 cybersecurity strategy since these systems handle highly sensitive information, such as Canadian citizens' personal data and classified military information, and had already been subject to numerous cyberattacks.[5] The plan for strengthening the cybersecurity of government systems primarily focused on clearly outlining the specific roles that various federal departments, such as The Department of National Defence and the Canadian Forces, for example, would play in developing and improving the government's cybersecurity architecture.[6] Other aspects of the plan included implementing cybersecurity related technical improvements,[7] providing cybersecurity training for government employees,[8] and creating foreign, as well as local, cybersecurity policies.[9]

Although securing governmental systems was a priority, the other two main goals outlined in Canada's 2010 cybersecurity strategy, securing non-federal governmental systems through partnerships and keeping Canadians cybersafe, were crucial since they dealt with protecting Canada's economy, infrastructure, and individual citizens from cybercrime.[10] The strategy's second main goal, "Partnering to secure vital cyber systems outside the federal Government," focused on partnering with three key parties: provinces and territories, the private

[4] "National Cyber Security Strategy," 2010, 7.
[5] "National Cyber Security Strategy," 2010, 9.
[6] "National Cyber Security Strategy," 2010, 10.
[7] Ibid.
[8] "National Cyber Security Strategy," 2010, 11.
[9] "National Cyber Security Strategy," 2010, 10.
[10] "National Cyber Security Strategy," 2010, 11-13.

sector, and the critical infrastructure sector. [11] Through partnering, the Canadian government intended to assist provinces and territories with keeping citizens' private data secure, assist the private sector with securing sensitive business information such as intellectual property, and assist the critical infrastructure sector with securing their systems from various attacks, including cyber.[12] The protection of individual Canadian citizens from cybercrime was addressed by the third main point in Canada's 2010 cybersecurity strategy, "Helping Canadians be secure online."[13] To accomplish this goal, the Canadian government planned to provide Canadian law enforcement with better resources for combating cybercrime and educating Canadians on cybersecurity best practices.[14] By addressing the cybersecurity needs of individual citizens, key partners, and the federal government, Canada's 2010 cybersecurity strategy aimed to provide all-encompassing national cybersecurity.

Canada's 2018 Cybersecurity Strategy

In 2018, Canada's second national cybersecurity strategy was announced by Ralph Goodale, the Minister of Public Safety at the time.[15] While Canada's first national cybersecurity strategy was released under a conservative government and had a budget of roughly $430 million for 10 years,[16] the second strategy was released under a liberal government, headed by Justin Trudeau, and currently has a budget of $500 million for 5 years.[17] Although Canada's 2018

[11] "National Cyber Security Strategy," 2010, 11-12.
[12] "National Cyber Security Strategy," 2010, 12.
[13] "National Cyber Security Strategy," 2010, 7.
[14] "National Cyber Security Strategy," 2010, 13.
[15] "New Cyber Security Strategy Bolsters Cyber Safety, Innovation and Prosperity," press release, June 12, 2018, https://www.canada.ca/en/public-safety-canada/news/2018/06/new-cyber-security-strategy-bolsters-cyber-safety-innovation-and-prosperity.html.
[16] "Canada's Cyber Security Strategy," 2018, 6.
[17] "Canada's Cyber Security Strategy," 2018, ii.

national cybersecurity strategy was built on the platform established by the strategy from 2010, it promises to "be more extensive and inclusive."[18] The three main themes of the 2018 cybersecurity strategy are "Security and Resilience," "Cyber Innovation," and "Leadership and Collaboration."[19]

The government of Canada aims to implement the three themes in the 2018 cybersecurity strategy through a variety of approaches. To improve the "Security and Resilience" of Canada's digital systems, the Government of Canada will focus on hardening the federal departments' cybersecurity, improving the law enforcement's ability to fight cybercrime, assisting small and medium enterprises with cybersecurity, and defending Canada's "critical networks" from foreign cyberattacks.[20] The Canadian government will drive "Cyber Innovation" by promoting Canada's existing flourishing cybersecurity industry,[21] supporting cybersecurity research, especially relating to "quantum computing and blockchain technologies,[22] and encouraging students to enter cybersecurity related fields of study.[23] To further establish its role in cybersecurity "Leadership and Collaboration," the government of Canada will closely partner with provinces and territories, as well as the private sector, to provide them with cybersecurity assistance and to collaborate on a national plan for responding to cyberattacks.[24] Additionally, the Canadian government will work to educate Canadian organizations as well as individual citizens on the

[18] "Canada's Cyber Security Strategy," 2018, 4.
[19] "Canada's Cyber Security Strategy," 2018, 3.
[20] "Canada's Cyber Security Strategy," 2018, 17.
[21] "Canada's Cyber Security Strategy," 2018, 19.
[22] "Canada's Cyber Security Strategy," 2018, 24.
[23] "Canada's Cyber Security Strategy," 2018, 22.
[24] "Canada's Cyber Security Strategy," 2018, 31.

importance of cybersecurity."[25] All of the aforementioned initiatives aim to improve Canada's national cybersecurity, as outlined in Canada's 2018 national cybersecurity strategy.[26]

Impact of Cybercrime on Canadians

Canadian citizens continue to be increasingly impacted by cybercrime, even with the 2018 national cybersecurity strategy touting that, since 2010, the Canadian governmental systems have experienced a decreasing number of data breaches despite an increasing number of attacks. [27] The number of cybercrime incidences reported to the police has steadily increased over the past few years from roughly 15,000 incidents reported in 2014, to almost 33,000 incidents reported in 2018.[28] In 2018, the categories with the highest number of cyber-related incidences were fraud, child-porn related crimes, and harassment or indecency related crimes, with fraud accounting for roughly half of all reported cybercrime incidences.[29] According to a Canadian Anti-Fraud Centre manager, identity theft related financial losses incurred by Canadians spiked from $11.7 million in 2017, to $21.2 million in 2018.[30] Considering the rapidly increasing number of cybercrimes committed towards Canadians, the importance of improving the cybersecurity of individual citizens cannot be overstated.

Just like Canadian citizens, Canadian businesses are also deeply impacted by cybersecurity. In 2017, over 21% of Canadian businesses experienced cybersecurity incidents

[25] "Canada's Cyber Security Strategy," 2018, 26-27.
[26] "Canada's Cyber Security Strategy," 2018.
[27] "Canada's Cyber Security Strategy," 2018, 6.
[28] "Police-Reported Cybercrime, By Cyber-Related Violation, Canada (Selected Police Services)," Table: 35-10-0001-0, https://doi.org/10.25318/3510000101-eng.
[29] Ibid.
[30] Bryan Borzykowski, "4 Things You Need to Know About Identity Theft Right Now," CPA (CPA Canada, March 14, 2019), https://www.cpacanada.ca/en/news/canada/2019-03-14-identity-theft-101.

that affected their business operations.[31] Furthermore, over half of those businesses "reported that cyber security incidents prevented employees from carrying out day-to-day work."[32] Canadian businesses with the highest number of cybersecurity incidences were banking institutions, universities, and pipeline transportation related businesses.[33] It is clear that businesses are aware of the importance of cybersecurity, since already in 2017, 94% of Canadian businesses spent money on improving their cybersecurity, and the average amount spent per business was $78,000.[34] All the aforementioned figures about the impact of cybersecurity on Canadian businesses were collected in the largest scale cybersecurity survey conducted for Public Safety Canada, [35] showing the Canadian government's increasing interest in this area. Since businesses in Canada are extremely impacted by cybersecurity, which means the Canadian economy will also be impacted, the Government of Canada is taking initiative to understand the evolving cybersecurity threat landscape that Canadian businesses are facing.

Canadian Government National Cybersecurity Efforts

The Government of Canada is currently driving a variety of efforts that aim to address Canada's national cybersecurity needs. One of these efforts is a cybersecurity research initiative that it leads with CANARIE, a company deeply involved with Canadian digital research activities. This joint initiative is focused on providing Canadian universities, colleges, and research organizations with advanced cybersecurity tools, training, and funding to enable them

[31] Howard Bilodeau, Mohammad Lari, and Mark Uhrbach, "Cyber Security and Cybercrime Challenges of Canadian Businesses, 2017," Juristat, March 28, 2019, Statistics Canada Catalogue no. 85-002-X, 3, https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00006-eng.pdf.
[32] Ibid.
[33] Ibid.
[34] Ibid.
[35] Ibid, 16.

"to protect intellectual property and private information."[36] Another government effort related to the education sector is the plan to create cybersecurity related "Work-Integrated Learning opportunities" as part of the government led "Student Work Placement Program."[37] These opportunities will be made available to students in the following programs: science, technology, engineering, mathematics, and business.[38] Students are also encouraged to apply to attend "GeekWeek," a yearly government sponsored cybersecurity event held in Ottawa where professionals and students are issued cybersecurity challenges that they must solve.[39] By fostering a close relationship with Canadian educational institutions, the Canadian government intends to protect cutting edge cybersecurity research, as well as prepare students for working in the cybersecurity industry.

Canada's national cybersecurity efforts also extend beyond the education and industry sector to include tools and resources for individual citizens. A resource aimed at educating citizens on cybersecurity is the Government of Canada's "Get Cyber Safe" website, which includes cybersecurity tips, news, blogs, and much more.[40] Another helpful resource for Canadians is the "Canadian Anti-Fraud Centre" website, which provides information on current online scams, recent cybercrime related news, and instructions for reporting fraud incidents. [41]

---

[36] "CANARIE Issues Call to Strengthen Cybersecurity in Canada's Research and Education Community," CANARIE (CANARIE, July 30, 2019), https://www.canarie.ca/canarie-issues-call-to-strengthen-cybersecurity-in-canadas-research-and-education-community/.
[37] "National Cyber Security Action Plan: 2019-2024," Ottawa, 2019, 12, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf.
[38] Ibid.
[39] "GeekWeek Blog – October 2018," blog, https://cyber.gc.ca/en/geekweek-blog-october-2018 (accessed November 15, 2019).
[40] Get Cyber Safe (Government of Canada), https://www.getcybersafe.gc.ca/index-en.aspx, (accessed November 15, 2019).
[41] Canadian Anti-Fraud Centre (Government of Canada), http://www.antifraudcentre-centreantifraude.ca/index-eng.htm, (accessed November 15, 2019).

These resources, along with many similar ones, enable Canadians to improve their cybersecurity awareness and help them protect themselves from cybercrime.

Brief Summary

The Canadian government spearheads a vast number of cybersecurity efforts to protect Canadian citizens, businesses, and government departments, and many of these efforts were developed out of Canada's national cybersecurity strategies from 2010 and 2018. The national cybersecurity strategy from 2010, Canada's first cybersecurity strategy, created the platform on which all future initiatives, plans, and strategies could be built upon. This is reflected in the 2018 national cybersecurity strategy, which expands on the existing cybersecurity strategy, but also extends into new areas, such as quantum computing for example.[42] An aggressive, all-encompassing national cybersecurity approach is necessary for Canada, since Canadian government departments, businesses, and individual citizens are deeply impacted by cybercrime, and need the cybersecurity resources and tools that Canada currently provides, and is planning to provide.

Resources for Further Exploration of Cybersecurity in Canada

Although this work has provided a brief outline of Canada's evolving cybersecurity strategy, more resources must be reviewed to gain a deeper and more accurate understanding of Canada's past, present, and future approach to tackling national cybersecurity. "Building Canada's Cyber Security Policy" is a brief video, published by the Centre for International Governance Innovation in Waterloo, that provides an excellent explanation of Canada's recent

[42] "Canada's Cyber Security Strategy," 2018, 15.

cybersecurity policy.[43] It can be accessed here.[44] The Government of Canada website "Canadian Centre for Cyber Security" is a great resource for current cybersecurity expertise, advisories, tools, and other interesting cybersecurity content.[45] A valuable document for further exploration is Canada's National "Cyber Security Action Plan" for 2019-2024.[46] One small section of the plan was briefly mentioned in this paper, but it is certainly worth reading in full as it provides information that is essential to understanding Canada's cybersecurity future.

[43] Building Canada's Cyber Security Policy, Cyber Security (CIGI, 2019), https://www.cigionline.org/multimedia/video-building-canadas-cyber-security-policy.
[44] Ibid.
[45] Canadian Centre for Cyber Security (Government of Canada), https://www.cyber.gc.ca/en/ (accessed on November 15, 2019).
[46] "National Cyber Security Action Plan: 2019-2024."

Works Cited

Bilodeau, Howard, Mohammad Lari, and Mark Uhrbach. 2019. “Cyber Security and Cybercrime Challenges of Canadian Businesses, 2017.” *Juristat*. Statistics Canada Catalogue no. 85-002-X. https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00006-eng.pdf.

Borzykowski, Bryan. “4 Things You Need to Know About Identity Theft Right Now.” CPA. CPA Canada, March 14, 2019. https://www.cpacanada.ca/en/news/canada/2019-03-14-identity-theft-101.

Building Canada's Cyber Security Policy. *Cyber Security*. CIGI, 2019. https://www.cigionline.org/multimedia/video-building-canadas-cyber-security-policy.

Canadian Anti-Fraud Centre. Government of Canada. http://www.antifraudcentre-centreantifraude.ca/index-eng.htm (accessed November 15, 2019).

“CANARIE.” *CANARIE*. CANARIE, July 30, 2019. https://www.canarie.ca/canarie-issues-call-to-strengthen-cybersecurity-in-canadas-research-and-education-community/.

Canada. Canadian Centre for Cyber Security. *GeekWeek Blog – October 2018*. blog. https://cyber.gc.ca/en/geekweek-blog-october-2018 (accessed November 15, 2019).

Canadian Centre for Cyber Security. Government of Canada. https://www.cyber.gc.ca/en/ (accessed November 15, 2019).

Canada. Public Safety Canada. *Canada’s Cyber Security Strategy: For a Stronger and More Prosperous Canada*. [Ottawa], 2010. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-cbr-scrt-strtgy-eng.pdf.

Canada. Public Safety Canada. *National Cyber Security Action Plan: 2019-2024.* [Ottawa], 2019. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf.

Canada. Public Safety Canada. *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. [Ottawa], 2018. http://publications.gc.ca/collections/collection_2018/sp-ps/PS4-239-2018-eng.pdf.

Canada. Public Safety Canada. *New Cyber Security Strategy Bolsters Cyber Safety, Innovation and Prosperity*. press release, June 12, 2018. https://www.canada.ca/en/public-safety-canada/news/2018/06/new-cyber-security-strategy-bolsters-cyber-safety-innovation-and-prosperity.html.

Canada. Statistics Canada. *Police-Reported Cybercrime, By Cyber-Related Violation, Canada (Selected Police Services).* Table: 35-10-0001-0. https://doi.org/10.25318/3510000101-eng.

Get Cyber Safe. Government of Canada. https://www.getcybersafe.gc.ca/index-en.aspx (accessed November 15, 2019).