# Countering the Cyber Threats against Financial Institutions in Canada: A Qualitative Study of a Private and Public Partnership Approach to Critical Infrastructure Protection

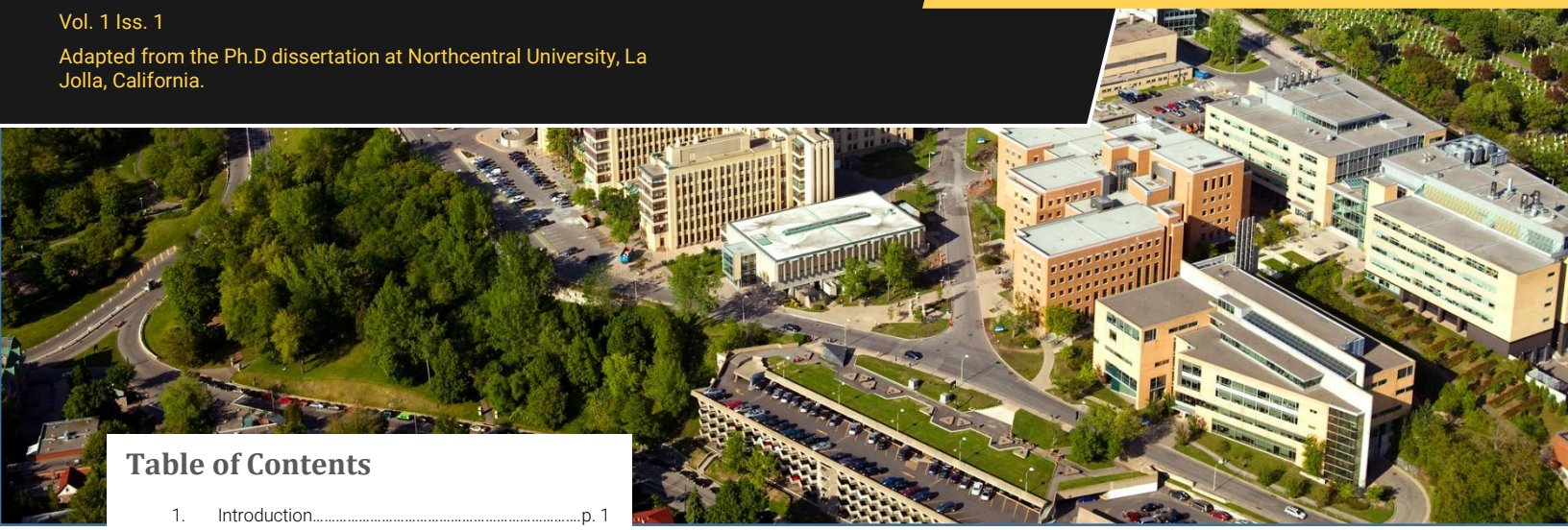
Pierre-Luc Pomerleau, Ph.D, MBA

Briefing Note

Vol. 1 Iss. 1

Adapted from the Ph.D dissertation at Northcentral University, La Jolla, California.

RCCP | Research Chair in Cybercrime Prevention



## Table of Contents



Pomerleau, P.-L. (2019). *Countering the Cyber Threats against Financial Institutions in Canada: A Qualitative Study of a Private and Public Partnership Approach to Critical Infrastructure Protection* (Order No. 27540959). Retrieved from https://www.proquest.com/products-services/pqdtglobal.html.

The Research Chair in Cybercrime Prevention was created on the initiative of the University of Montreal, Desjardins and the National Bank of Canada. Led by Benoît Dupont, researcher at the International Centre for Comparative Criminology at the University of Montreal, its mission is to contribute to the advancement of research on cybercrime phenomenafrom the perspective of its prevention.

## Introduction

Infrastructure protection is a shared responsibility between the government and private companies working together to improve its resilience. More specifically, cybersecurity is a public good that must be framed as a collective action problem between both groups of actors[1]. The private sector in Canada owns approximately 80% of the critical infrastructure in the country, so its role is essential in the management of these threats[2 3]. Homeland Security is the responsibility of various groups of "security nodes" and actors from the public and the private sectors[4].

The consequences of cyber-attacks on critical infrastructure can have significant economic, social, and environmental impacts[5]. Currently, Canadian banking security professionals have a dynamic framework structure to collectively combat various threats against their organization, while readily sharing information to protect the banking industry. As such, Canada's private sector is quickly adapting to the rapid changes in the cyber threat landscape in near real-time.

Even though banking security professionals share information, the specific intelligence or warnings they regularly share with the public sector is mostly organic, omitting the vast amount of data and intelligence available in the private sector. This situation leaves the government with a myopic view of the actual cyber threat landscape, which inherently increases risks to critical

As Carr[6] argues, there is still a fundamental disjuncture between the expectations of private and public security partners regarding roles, responsibility, and authority in protecting critical infrastructure from cyber-threats.

## Problem statement

In recent years, the threat landscape of financial institutions has changed, not only from a criminal and profit-oriented threat actor standpoint, but also from a state and non-state actor using cyberspace directing attacks towards financial institutions[7]. Public Safety Statistics show that Canadians are affected by a ransomware attack approximately 3,200 times a day[8] [9]. According to Statistics Canada[10], one-fifth of Canadian businesses were impacted by a cyber-security incident, and only 10 percent are reporting it to law enforcement. The cost of cybercrime in Canada is equivalent to 0.17% of its Gross Domestic Product (GDP), which represents annual losses of CAD$3.2 billion per year[11]. Additionally, non-state actors continue to invest in their cyber capabilities to enable cyber-attacks on financial institutions and pose a risk to the national security and economic objectives of Canada[12].

The problem to be addressed is why private, and public partnership (PPP) relationships have been ineffective in monitoring, detecting, and reacting to these incidents?[13] [14].

The probability of companies to detect hackers is low, and the perceived risk of threat actors of being caught is[15]. Due to the international nature of cybercrime, law enforcement struggles to prosecute cybercriminals and to assist banks in preventing these incidents[16]. The banking sector does not have the necessary intelligence collection authorities and capabilities to protect its network and infrastructure, while the government does possess these necessary authorities and abilities to do so — however, it does not have a banking-specific expertise of the cyber threats affecting the financial industry[7] [15].

## Purpose statement

The purpose of this qualitative study was to conduct interviews with key corporate security and cybersecurity working professionals for major financial institutions to understand:

- What factors contribute to the current system not functioning?;
- To provide recommendations to improve public and private partnerships to protect the financial industry from various cyber-threats;
- To determine if the Network Security Governance Framework first proposed by Dupont[4]and adapted by Whelan and Dupont[17], allows to better understand the phenomenon, and to identify best practices for information sharing.

Survey participants (N = 10) included Chief Security Officers (CSO) and Chief Information Security Officers (CISO) or their immediate subordinates working for Canadian financial institutions. Interviews (N=9) were conducted in Toronto, Ontario and Montreal, Quebec. The final sample represented 23 percent of cybersecurity executives in large Canadian financial institutions. Five participants in the interviews were currently working for one of the six largest banks in Canada.

## Findings from Interviews

A total of 12 core themes emerged from the data collection and analysis of the interviews:

Theme 1: To prevent incidents, financial institutions security professionals need to receive information or actionable intelligence, and they would like to receive in near real time or as frequently as possible.

Theme 2: Study participants explained that it would be essential to create a virtual fusion center as people from both public and private sectors do not necessarily need to be physically sitting in the same location to share information with each other.

Theme 3: Even if meeting each other in person, verbal communications over the phone, and exchanging secure emails are still commonly used between public and private partners. According to participants, virtual private platforms are the most appropriate communication mechanism to exchange information securely.

Theme 4: All nine participants in the interviews were unanimous in emphasizing the actual legal framework as a critical challenge in sharing information with the public sector to be efficient in preventing crime against the financial institutions.

Theme 5: When it comes to crime prevention, most of the participants expressed the public, and the private sectors have different missions and organization objectives, which significantly reduce the efficiency of current PPPs.

Theme 6: Study participants have trust in their private security colleagues to exchange information to assist them in preventing crime against their respective organizations. However, participants cited trust as being a challenge (when compared with the trust of their private sector colleagues) in having efficient information-sharing with public sector stakeholders.

Theme 7: As private entities such as financial institutions own most of the financial sector's risk, the specific roles that the private and the public sectors hold in relation to the protection of financial institutions assets are unclear. Each financial institution ensures its own security, but the government must protect the industry as a whole.

Theme 8: Most participants agreed that multiple cyber-attacks on banks in a short period of time could have significant negative impacts on investors, the customer's confidence in the financial system, the reputation of organizations under attack as well as on the stock markets.

Theme 9: Study participants confirmed the financial industry should share information with other Canadian critical infrastructures since some of them are highly interconnected and might be dependent on each other. Most participants stressed the banking industry is closely interconnected with the telecommunication sector.

Theme 10: A total of eight participants agreed it is essential to continue to increase information-sharing capabilities between public and private partners.

Theme 11: The Bank Crime Prevention and Investigation Framework (BCPIF) framework is perceived as the governance model in place for financial institutions to share information with other BCPIF members, and study participants do agree this framework is the best tool they have to share information.

Theme 12: All participants confirmed information-sharing PPPs between financial institutions and its public sector stakeholders should be categorized as security networks as per Dupont's[4] definition. Various types of security networks are necessary to manage security effectively.

## Recommendations and Lessons learned

A total of 19 recommendations for practices were identified throughout this study. The recommendations were in line with the modification of the legislation to allow information-sharing, the creation of fusion centers, the clarification of roles and responsibility between public and private actors, the mechanism to share information, and the governance of security networks. The most important recommendations for practices are related to the modification of the legislation to clarify roles and responsibilities, to allow information-sharing between private and public actors for prevention purposes, to share timely information and to provide a safe harbor for

security actors of both sectors to share information to prevent crime, protect infrastructures such as financial institutions as well as for national security purposes.

A total of 11 recommendations for future studies were identified throughout this study. Future research should study how security networks are organized to increase effectiveness and efficiency in cybersecurity and financial crime governance[18]. Legal frameworks in the U.K. and the U.S. as well as the success factors of PPP projects such as the National Cyber-Forensic and Training Alliance (NCFTA), the Financial Services Information Sharing and Analysis Center (FS-ISAC), the National Cybersecurity and Communications Integration Center (NCCIC), and the U.K. Joint Money Laundering Intelligence Taskforce (JMLIT) should be evaluated further. The evidence-based cybersecurity research approach in the context of financial institutions should also be prioritized to evaluate common tools and policies used by security networks to achieve goals, to manage cybersecurity incidents, and to investigate cybercrimes against financial institutions as there is an absence of universally accepted metrics to measure security controls and policies[19 20 21 22].

## Conclusion

This study addressed the central problem of why private and public partnership relationships have been ineffective. The legislation is a major challenge in Canadian PPPs. The Network Security Governance Framework first proposed by Dupont[4] and adapted by Whelan and Dupont[17] does allow for a better understanding of this phenomenon, as well as to identify best practices for future information sharing PPPs. A total of 12 significant themes, 19 recommendations for practices, and 11 recommendations for future studies were identified in this study

## References

[1] McCarthy, D. R. (2018). Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order. *Politics and Governance*, *6*(2), 5-12.
[2] Etzioni, A. (2017). The fusion of the private and public sectors. *Contemporary Politics*, *23*(1), 53–62.
[3] Vroegop, R. (2017). *The state of information and intelligence sharing in Canada*. The Conference Board of Canada.
[4] Dupont, B. (2004). Security in the age of networks. *Policing & Society*, *14*(1), 76.
[5] Mezher, T., El Khatib, S., & Sooriyaarachchi, T. M. (2015). Cyber-attacks on critical infrastructure and potential sustainable development impacts. *International Journal of Cyber Warfare & Terrorism*, *5*(3), 1.
[6] Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62.
[7] Borghard, D, E. (2018). *Protecting financial institutions against cyber threats: A national security issue*.
[8] Royal Canadian Mounted Police. (2019). *Ransomware*.
[9] Tunney, C. (2019). *With ransomware on the rise, RCMP urging victims to 'be patient with police'*. CBC.
[10] Statistic Canada. (2018). Impact of cybercrime on Canadian businesses, 2017.
[11] Public Safety Canada. (2018). New cybersecurity strategy bolsters cyber safety, innovation, and prosperity.
[12] Communications Security Establishment. (2018). Canadian Centre for Cyber Security, National cyber threat assessment 2018.
[13] Bures, O. (2013). Public-private partnerships in the fight against terrorism? *Crime, Law & Social Change*, *60*(4), 429-455.
[14] Dunn-Cavelty, M., & Suter, M. (2009). Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *2*, 179-187.
[15] Boes, S., & Leukfeldt, E. R. (2017). Fighting cybercrime: A joint effort. *Cyber-physical security*, 185.
[16] Holt, J. T. (2018). Regulating cybercrime through law enforcement and industry mechanisms. *Annals of the American Academy of Political and Social Science*, *679*(1), 140–157.
[17] Whelan, C., & Dupont, B. (2017). Taking stock of networks across the security field: a review, typology and research agenda. *Policing &* Society, *27*(6), 671-687.
[18] Rondelez, R. (2018). Governing Cyber Security through Networks: An Analysis of Cyber Security Coordination in Belgium. *International Journal of Cyber Criminology*, 300–315.
[19] Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*(1), 33.
[20] Wilson, T., Maimon, D., Sobesto, B., & Cukier, M. (2015). The Effect of a Surveillance Banner in an Attacked Computer System: Additional Evidence for the Relevance of Restrictive Deterrence in Cyberspace. *Journal of Research in Crime and Delinquency*, *52*(6), 829–855.
[21] Testa, A., Maimon, D., Sobesto, B., & Cukier, M. (2017). Illegal roaming and file manipulation on target computers: Assessing the effect of sanction threats on system trespassers' online behaviors. *Criminology and Public Policy*, *16*(3), 687-726.
[22] Maimon, D., Testa A., Sobesto B., Cukier M., & Wuling, R. (2019) Predictably deterrable? The case of system trespassers. In G. Wang, J. Feng, M. Bhuiyan, & R. Lu, (eds.), *Security, privacy, and anonymity in computation, communication, and storage*. Springer, Cham.