BRIEF

Cybersecurity in the Canadian Financial Sector as a National Economic Security Issue

BY

MICHEL BOUTIN &
MATHIEU CHOUINARD

IN FIDEM ASSOCIATES AND REPRESENTATIVES FOR IN-SEC-M

Canada’s financial institutions and the encompassing legislation and regulations under the Bank of Canada and the Department of Finance are globally renowned as the Standard of Excellence. However the current and potential threat by rogue as well as state funded hackers put the viability and sustainment in jeopardy unless robust action is taken.

Furthermore, to retain our sovereignty in our financial institutions, Canada must rely primarily on its Canadian cyber security industry for software, hardware and human resources and implement smartly funded programs to produce a robust cadre of cybersecurity Canadians.

Today In Fidem inc. and on behalf of In-Sec-M, the originally based cyber security association in Ottawa Gatineau, but with corporate and academic members from across Canada, will outline robust recommendations to ensure the dynamic growth and sovereign protection of our Financial Institutions as well as the Canadian cybersecurity industry.

IF
PROTÉGER
POUR PERFORMER™

Our brief begins with an overview of the ongoing changes in the Canadian financial industry with the integration of “open banking” and the fintechs in their internal and client facing business operations.

It then follows with the recognition that banks cannot modernize without the contribution of cybersecurity. By digitizing their business processes, banks are multiplying vulnerabilities and attack areas. As a result, banks are increasingly relying on cybersecurity.

Subsequently, the brief discusses the requirements for banks to invest huge sums in technology and cybersecurity. It also challenges the fact that banks, as a vital infrastructure in Canada, nonetheless acquire most of its new solutions from abroad: This is without ignoring capital flight and the shortfall for Canadian cybersecurity companies. Therefore, where does Canada’s sovereignty lie? How can the dynamic and innovative Canadian cybersecurity industry develop if its main outlet ignores it?

And, in conclusion, we propose a series of recommendations :

1 THE STATE OF THE FINANCIAL INSTITUTIONS

Banks and financial institutions are working hard to contain the numerous attacks against them. One can remember the leak of confidential personal data that affected the 40,000 CIBC and 50,000 BMO clients in May 2018. In general, cyber-attacks in the financial sector have tripled over the past five year and the average cost of containment has increased by 40%.

The Bank of Canada sums up the situation and points to the solution: «The digital economy is expanding, computer threats will not disappear and attacks have become more sophisticated. Banks need to rely on external experts, automation, analysis and other tools to really improve security and cyber security based on risk[1].

The Bank of Canada is referring to the systematic digitization of all banking services, both to provide online services to clients and to automate internal management functions. In total, Canadian banks have invested $ 84.5 billion over the past decade in new technologies.

The digitization of all banking services has created a series of new vulnerabilities. Offering online services to customers means giving them access to internal databases. The financial institution must now consider its customers as its own employees and educate them, train them and even provide them with tools to secure transactions.

[1] Filipe Dinis, Chief Operating Officer, Bank of Canada "Strengthening Our Cyber Defences", Toronto, Ontario, May 9, 2018.

The vulnerability caused by the digitization of all financial processes has increased with the advent of “open banking”. Not only do banks offer their services online, but they allow third-party developers to build applications and services around their financial infrastructure. The use of application programming interfaces (APIs) allows all banking players to connect to the bank’s services to develop their own applications.

2 THE PRESENCE OF FINTECHS IN THE FINANCIAL SECTOR

A new international industry was born out of this openness and took the name of «fintech» from the contraction of the words «finance» and «technology». Most Fintech companies are start-ups with a strong command of ICT. The model is given by PayPal who is in a way the ancestor of the fintechs. There are also industry giants like Apple who started deploying its Apple Pay app in 2015.

Fintechs are developing a business model based on cooperation and even co-management of new technologies. They also offer several new services for the banks with the aim in particular to support them in the digital transformation of their own services.

In Canada, 62 major financial institutions are actively involved in fintechs and 88% have indicated that they will increase their participation over the next few years. Banks do not hesitate to collaborate with each other to find the start-up that will give them access to a service or product that can support their massive dematerialization effort.

The most significant fintech example is the company Fintech SecureKey Technologies. The largest financial institutions in Canada, including Royal Bank, TD Group, Scotiabank, CIBC, Bank of Montreal and Desjardins Group, collectively invested $ 27 million in SecureKey.

This Toronto-based company, which was founded in 2008, is also a member of In-Sec-M. It acts as an identity and authentication provider for financial institutions to provide online services. It is a cloud-based authentication and identity validation system that uses blockchain technology to connect consumers to online services using a digital identity they already own and trust.

3

FINTECHS, THEIR SECURITY WEAKNESSES AND THE BANKS' REACTION: THE PARADOX

All fintechs do not follow SecureKey's faultless model. Indeed, the counterpart of the agility and capacity of fintechs has a price. Many of them focus too much on the quick launch of their product without exercising due diligence to security measures.

Fortinet, a cybersecurity firm, believes that «fintech companies generally have fewer human and financial resources for security, not to mention other regulatory requirements (...) Indeed, fintechs have been able to innovate quickly because they are not linked by inherited information technologies or, in particular, by extreme governance[2].

The result is a general mistrust of banks towards fintechs. According to a survey conducted by the Simmons & Simmons law firm, 71% of global financial institutions report that cybersecurity is the main risk associated with fintech partnerships. However, these same financial institutions say that collaboration with fintechs is essential.

There is therefore a crucial paradox. On the one hand, banks need fintechs to meet their business objectives. On the other hand, fintechs sometimes carry risks. The response of the banks to this paradox is both bold and cautious: they decided to mentor the fintech startups during their initial steps.

As a result, Canadian financial institutions are investing in incubators and accelerators across Canada to access the best talent. In Ontario, there are four incubators; British Columbia, Alberta and New Brunswick each have an incubator. In addition to the support of financial institutions, start-ups that are incubated are funded by a combination of governments, academics, consultants and various organizations. The principle is to give entrepreneurs in residence access to mentors, management tools and a network of venture capital investors.

[2] Filipe Dinis, Chief Operating Officer, Bank of Canada «Strengthening Our Cyber Defences», Toronto, Ontario, May 9, 2018

MAIN CANADIAN INCUBATORS AND ACCELERATORS AND THEIR SPONSORS

FREDERICTON	TORONTO				CALGARY	VANCOUVER
CyberNB	MaRS Discovery District	OneEleven	Rotman's Creative Destruction Lab (CDL)	Ryerson's Digital Media Zone (DMZ)	Innovate Calgary	Launch Academy
IBM Cirrus CGI Siemens Gvt NB Gvt Canada Bell UNB	AMEX CIBC Ebay Equifax Manulife P&G Paypal TMX	Aviva Deloitte OMERS Ontario RBC Rogers Ryerson	BDC Comcast KPMG Mastercard National Bank RBC Scotiabank	Accenture BMO City of Toronto Google IBM Microsoft TD Bank	Canadian Digital Media Network RBC Telus City of Calgary University of Calgary	BC IC Creative Technology Solutions EY Google for entrepreneurs RBC

Source: Global Risk Institute, 2018 (tailored for our needs to include Fredericton)

In Quebec, two major financial institutions, Desjardins Group and National Bank, have created a different concept. They decided to pool their research projects. Under the name of CyberEco, this non-profit organization's mission is to develop solutions of all kinds without using fintechs. Without being an incubator or an accelerator, CyberEco innovates in its own way.

4 THE CYBERSECURITY INDUSTRY IN CANADA

It is a fact, there is Canadian talent. Ottawa estimates the size of Canada's cyber security industry at $ 1.7 billion, and expects global growth of 66% over the next three years to expand Canada's position in this sector.

Canada's cybersecurity industry has more than 700 companies, many of which are internationally renowned. For example, the SNOW ARC4DIA platform used by a major satellite operator and the US military to protect their equipment and identify attackers and their motivations, among other things. TERRANOVA video clips are used by companies around the world to educate employees about cybersecurity. CORSA TECHNOLOGY has reinvented the concept of firewall by segmenting the network to limit the movement of attackers upstream of the perimeter to protect.

As an example of Canada's high-level expertise in cybersecurity, Arc4dia's SNOW solution outscored several international competitor solutions during a recent benchmarking test

FEATURES	Mandiant	Crowdstrike	root9B	CabonBlack	Windows Defender	Tanium	SNOW
Host-Based Sensor	✓	✓	✓	✓	✓	✓	✓
Big Data Analytics	✗	✓	✗	✗	✓	✗	✓
Live Monitoring & Response	✗	✗	✓	✓	✗	✓	✓
Stealth	✗	✗	✗	✗	✗	✗	✓
Custom Sensor Signature	✗	✗	✗	✗	✗	✗	✓
Remote Incident Response	✗	✗	✗	✓	✗	✓	✓
Joint Operational Console	✗	✗	✗	✗	✗	✗	✓

One could go on and list more achievements of the Canadian cybersecurity industry. It unfolds the spirit of innovation and entrepreneurship that characterize all high-tech industries. These are relatively young companies as they were mostly created after 1995, the first year the Internet made its impact on the economy, and especially after 2005, when the first version of the safety standard of the payment card industry or PCI DSS came into effect.

In terms of employment, it is difficult to accurately quantify the total number of people working in the Canadian advanced security industry. The data collected in the 2010 cited study indicated a population of more than 23,000. The authors of the study in question already considered that this figure was undervalued because it did not include the large number of independent consultants and cyber security professionals employed by private companies, public organizations and governments.

Moreover, all companies complain about the shortage of qualified cybersecurity personnel. Positions to fill remain vacant. Projects are rejected due to lack of staff. Occupying about 10% of jobs, women are almost absent from the Canadian advanced security industry. The replacement time of a security analyst is often close to three months. This industry could easily double its workforce in a few years.

It also faces major challenges with the relatively recent introduction of new technologies such as blockchains, artificial intelligence, machine learning and increasingly powerful analytical tools. The potential arrival of quantum computing, which is no longer science fiction, will pose a certain risk for the confidentiality of information and make obsolete current encryption algorithms. It will have to pass the test of secure quantum cryptography.

5 ONE PROBLEM: CAPITAL FLIGHT

The Canadian cybersecurity industry has many strengths to address all of these challenges because of the close cooperation between university and business. In full swing, however, it knows a problem of substance. Our financial institutions barely know its existence. We reported earlier that in ten years banks have invested $ 84.5 billion to make their digital transition. This does not mean that this money has been invested in Canada. It is the opposite. Most of the goods and services thus acquired are foreign. This is a real and significant capital flight.

In the area we are particularly interested in, that of cybersecurity, we must mention the names of Check Point Software Technologies, PaloAlto Networks, Fortinet or Cisco, who keep coming back when we talk about buying solutions from major financial institutions. All these companies are American, except for Check Point which is Israeli. It goes without saying that we do not pretend to blame banks for sourcing where excellence is. It is their most absolute right and it must be respected.

Without a doubt, Canadian cybersecurity companies often go under the radar of major financial institutions. Most of them are small businesses. The vast majority of cyber security companies have fewer than 25 employees. This is the case for more than 70% of them.

The solution is to bring together these dispersed forces by multiplying partnerships. We have seen that this is exactly what happens in the financial cyber security sector with the incubators or accelerators mentioned in the previous table.

All of these initiatives have been initiated by local initiatives. This is a bottom-up approach that demonstrates the vitality of Canada's cybersecurity industry and its willingness to tackle the problem head on with its obvious limitations. However, there is no overall coherence between the different initiatives with the risk of overlaps. Under these conditions competition usually prevails over cooperation, complementarities and emulation.

Moreover, these local initiatives have a weak branding. The cybersecurity market is global and it requires images of strong national brands. At present, three countries have acquired such a cybersecurity branding: the United States, Great Britain and Israel. The presence of this small country with the two traditional giants provides a model that Canada should learn from.

6

THE ISRAELI MODEL

The model began with the creation in 2012 of the Israel National Cyber Bureau (INCB) which reports directly to the Prime Minister's Office. INCB's mission is to develop Israel's cybersecurity policy and strategy. Its work culminated in the creation in 2015 of the National Cyber Security Authority (NCSA), a government entity responsible for Israel's cybersecurity operational efforts[3]. To create efficiencies, NCSA also reports directly to the Prime Minister.

Israel's cybersecurity program has two components: educational and financial. Awareness of cybersecurity begins in kindergarten and transforms into training from the fourth grade to continue to the doctoral level. Thus, Israel was the first country in the world where students could obtain a doctorate in cybersecurity as an independent discipline.

In practice, the government is doing everything possible to encourage the creation of start-ups. In 2018 alone, Israel has created 60 new cybersecurity companies. With the help of the government, these companies have managed to grow to a level where they are already attracting the interest of international venture capital funds. "Last year, Israeli cyber security firms raised more than US $ 1.03 billion at all stages of funding. This represents 20% of the total venture capital funds invested in cyber businesses around the world, just behind the United States[4].

Of course, it is obvious that Canada's socio-political environment is very different from that of Israel. No model can be reproduced as is. What needs to be remembered from the model is the great cooperation between government and business. It is not only a question of financial support, but of a constant accompaniment that implements all the services of the State. The entire state apparatus, including the Israeli secret services, shares its information with cybersecurity firms.

7 THE STRATEGY OF THE CANADIAN GOVERNMENT

The top-down approach has so far been lacking in Canada. The local initiative already exists. Toronto has four cybersecurity incubators. New Brunswick is mobilizing to become the epicenter of Canadian cybersecurity. Where is the structuring action of the federal government?

Canada devised a national strategy in 2018 and centralized several organizations under one roof called the Canadian Cybersecurity Center (CCC), whose resources from the Canadian Cyber Incident Response Center of the Department of Public Safety, Shared Services Canada's Security Operations Center, as well as the Information Technology Security Division of the Communications Security Establishment (CSE). It is a big step forward. Will it be able to achieve significant results?

All the ingredients are in place. The new center is under the responsibility of the CSE, which in turn reports to the Department of National Defense. The CSE is an intelligence agency that is part of the Five Eyes uniting Canada with the United States, Australia, New Zealand and the United Kingdom. Established in 1946, it is the world's largest intelligence organization[5]. If the CSE can share with the CCC all or part of the information on civil cyber security to which it has access, it is certain that the impact on the Canadian economy will be significant.

Finally, the federal government is working to renew the cybersecurity framework. One of the elements of this framework will allow small and medium-sized businesses that wish to obtain easily recognizable certification to demonstrate to their customers businesses or consumers, that they adhere to a well-established set of cybersecurity practices. Obtaining this certification will help participants gain a competitive advantage.

Canada is beginning with undeniable delay on the three leaders in cybersecurity, but it is entering a new phase where it has a real strategy. It remains to translate this strategy into concrete projects.

[5] J. Vitor Tossini, «The Five Eyes – The Intelligence Alliance of the Anglosphere», UK Defence Journal, November 14, 2017

CONCLUSION AND RECOMMENDATION LEADS

CONCLUSION

Cybersecurity is above all a matter of cooperation in the face of the humongous resources and structures available to hackers, cybercriminals and pirate nation-states. Facing these threats, Canada cannot afford to act in dispersed order. The keystone of Canada's cybersecurity strategy is the creation of a framework in support of a coherent national ecosystem. Its heart should be the financial sector. Banks have already built local ecosystems. It remains to jell these efforts in a top-down approach to make it a great national ecosystem.

This challenge should fall on In-Sec-M, the national cybersecurity industry cluster. In-Sec-M brings together companies, research centers, educational institutions, government actors and industry associations. Its role is to mobilize them to set up structuring projects to meet the needs of major clients. It is also dedicated to creating research consortia with several companies and research centers to develop customized products.

For example, In-Sec-M has an agreement with NRC to find and hire the best cybersecurity experts to meet the needs of the IRAP program. The generalization of this type of intervention across Canada will create a perfectly transparent market where demand responds to supply efficiently.

RECOMMENDATION LEADS

To contribute to the development of the Canadian cybersecurity industry, the federal government should factor in some elements:

IN THE FINANCIAL SECTOR

a. Establish a process for financial institutions to look first to Canadian content when acquiring cybersecurity solutions. An organisation such as In-Sec-M would act as the enablement vehicle. It would mobilize the Canadian cybersecurity ecosystem to respond to calls for tenders, either individually or in a grouped manner. Any purchase made in this context would be eligible for a subsidy equal to a percentage of the contracts thus agreed;
b. Provide cybersecurity start-ups focusing on the financial sector with a non-repayable grant along the lines of BCIP to be funded by the Treasury Board Secretariat.
c. Launch a visibility campaign on the theme «Canada = Financial Cybersecurity»
d. In international markets formalise a linkage between In-Sec-M and the Trade C ommissioner Service

IN THE CYBERSECURITY SECTOR

a. Enhance the PSPC purchasing policy to strengthen national cybersecurity firms based, when possible, on the principle of national security exemption.
b. Encourage cyber security R & D with accelerated depreciation and tax credits on software and equipment solutions.
c. Instill and fund a STEM equivalent program for cybersecurity.
d. Provide scholarships for women and aboriginals to encourage them to join the cybersecurity field.
e. Promote Security Education in Canadian universities and colleges by all means available to the government (scholarships to replace student loans, research funds, government contracts, etc.),
f. Introduce a multiple times tax credit valid for 10 years to solicit companies to invest in the cybersecurity sector.
g. Establish and promote a certification process under the leadership of federal organisation such as CCCS.

With these final comments, we conclude our brief. We trust that it shall reach out to the people and organisations who yearn to develop an industry that is vital to Canada’s economy and more so for the protection of our Canadian way of life.

THANK YOU

Based in Montreal and Quebec City, In Fidem, **infidem.biz,** is a company dedicated solely to information security. Founded in 2005, it has since been recognized by Canadian financial players and government stakeholders. Today, it employs more than 80 experts serving its clients. It is In Fidem's belief that information protection is one of the key drivers of industry performance. By protecting their information, organizations inspire the trust of the people and and organizations they deal with.

IF
PROTÉGER
POUR PERFORMER

infidem.biz

Founded in 2017, In-Sec-M, **insecm.ca**, is a non-profit organization based in the Ottawa-Gatineau region. It aims to foster the emergence of an innovative cybersecurity ecosystem across Canada

IN·SEC·M insecm.ca