Cyber Risk and Security in Canada

Authors
Brian O'Donnell & Richard Nesbitt

GLOBAL RISK INSTITUTE

Canada can become a haven against cyber attacks if we invest in and further coordinate efforts.

- *The risk of cyber attacks on Financial Institutions in Canada and around the globe is increasing, both in frequency and complexity.*
- *Countries that are leading in the cyber security space are continuously evolving their approach, which are anchored in public / private cooperation and partnership in communication, research and development and cyber technology incubation.*
- *The Global Risk Institute, a Canadian based risk research group whose members include Canada's major financial institutions, has concluded that Canada should continue and accelerate our coordination and investment in cyber security, so that Canada can be at the forefront of cyber developments and defences.*

The risk of cyberattacks is growing throughout the global economy, as governments, companies and individuals increasingly become reliant on mobile and on line, applications based technology. While millions of attacks are launched each day, the current state of cyber defences and processes is such that most are repelled. Still, the attackers are growing in numbers and sophistication, meaning that all countries and companies need to mount continuous defenses. Leaders in cyber defense, including the United States and Israel, take a National Security perspective to the problem, and have instituted partnerships across government, business and academic institutions; this approach comes from a clear understanding that cyberattacks can range from isolated hack attempts to steal data from a particular individual, all the way up to a massive, state sponsored attack targeting critical infrastructure. We think that it is imperative for Canada to advance to the leading edge of a coordinated cyber security strategy, or risk becoming an even more focused target as attackers continuously seek the weakest link.

> Canadian financial institutions have a successful history of collaboration and innovation, including in defense against financial crimes.

Canadian financial institutions have a successful history of collaboration and innovation, including in defense against financial crimes. A strong example of such cooperation was the introduction of chip technology into debit and credit cards back about ten years ago. The results are impressive, with declining fraud losses in the Canadian industry, which compares favourably to the United States and other jurisdictions, which lagged in chip technology investment. Fraudsters, like hackers, take advantage of such vulnerabilities and redirect their efforts accordingly.

Financial Institutions, like most large, sophisticated organizations, have made significant investments and advances in cyber security. Threats come in many forms, from individual hackers, nation states, organized crime, hacktivists and even insiders. Defenses developed to date include user account controls, cryptography, intruder detection software and firewalls. But still the number and severity of breaches are increasing at an alarming rate. One

such example was JP Morgan in July of 2014 and which is believed to have persisted through mid-August of that year. In this incident the hackers gained access to information on approximately 83 million customers, including names, addresses, emails and phone numbers; this left customers exposed to phishing attacks, where the fraudsters attempt to gain even more critical data (e.g. credit and debit card numbers) by posing as legitimate service providers using the personal information gained through the hack. Another major breach, the Target hack in the retail space, was even more alarming. In this case, in December 2013 and persisting for 19 days, hackers stole information on over 40 million (and some estimates are now at 110 million) clients, including credit and debit card information. The intrusion was not detected until a surge was recognized in the incidents of fraud against the clients, causing substantial anxiety and financial losses to Target and their clients. In addition, firms that are victims of such breaches suffer significant financial and reputation damage.

More recently the financial services industry experienced an even more striking breach. In March 2016 the Central Bank of Bangladesh was hacked via an intrusion that lasted weeks. The hackers used malware to cover their tracks and allow multiple re-entry points into the Bank's network. The hackers attempted to make off with over $1 billion through a series of international transactions, with only a typo calling attention to the transfer and tripping them up. Still, $80 million of the hacked funds are unaccounted for.

> The recent cyber breach at Panamanian firm Mossack Fonseca signals that hackers are after more than just credit cards and customer information.

The cyber breach dubbed as 'Panama Papers' leaked documents containing information on how wealthy individuals globally, including public officials, used the Mossack Fonseca to hide assets from public scrutiny using offshore companies. The sheer amount of data stolen could only logistically happen through an online hack: 11.5 million files totalling 2.6 terabytes equates to loads of books requiring 2,600 pickup trucks. This latest cyber breach raises concerns about "hacktivism," cyberattacks that are politically or ideologically motivated, and inherently takes decision-making away from the legal system.

Here in Canada, Goldcorp Inc. was recently victimized by anonymous hackers who stole nearly 15 gigabytes of company information, including payroll information and bank account data. Still, a couple of the most pointed Canadian examples were the attacks on the Federal Government and the Canadian Security Intelligence Service (CCIS). In June 2015 the Federal Government was attacked by the hactivist group Anonymous, basically shutting down a number of key Federal Government websites; around the same time, CCIS suffered 3 denial of service attacks over a 2 day period, bringing down their site as well. The CCIS attacker described the attack as "child's play".

> Clearly sophisticated, organized crime elements are on the prowl for any sign of weakness in jurisdictions around the world.

And it is also clear that network technology and hacking approaches will continue to evolve. In terms of technology, very advanced Canadian research and development efforts in quantum computing has significant implications for cyber defenses down the road. While quantum computing holds tremendous promise in the advancement in computing speed and complexity, it could well make obsolete the encryption technology that is so prevalent and effective in cyber defense today; we need to also coordinate our cyber defenses to continuously evolve and protect against new technologies.

The Canadian ecosystem is well suited to take a leadership position in cyber security, as clearly we don't want these type of attacks against government or industries. Cyberattacks take on many forms ranging from foreign intelligence agencies, terrorists, organized crime groups, hacktivists, lone hacker and even insiders. So an actual cyberattack could be seeking personal and financial information of an individual or group of clients of a particular firm, or at the other extreme, the attack could be a massive coordinated Denial of Service Attack, attempting

to shut down a critical network (for example a company's client service website, or a component of Canada's critical infrastructure, such as a payment system or the power grid). The Global Risk Institute considers Canada's public and private institutions to be well advanced and sophisticated in the cyber battle, but as the threat is ever-changing we need to continue to adjust and adapt. The following is a summary overview of both formal and informal institutions currently focused on cyber defense in Canada:

Public Safety Canada:

Has overall federal government responsibility for cyber security, and in 2010 developed Canada's Cybersecurity Strategy. This strategy seeks to protect the federal government's network, promote communication and cooperation across Canadian institutions, and to help all Canadians to be secure on line. The Canadian Cyber Incident Response Centre (CCIRC) under Public Safety Canada assists in securing the vital cyber systems of provinces, territories, municipalities and private sector organizations while collaborating closely with partners, including international counterparts and information technology vendors. It is understood that Public Safety Canada is also working on a new piece of legislation, Protection of Canada's Vital Cyber Systems Act. The new legislation is expected to set standards for companies operating "vital cyber systems" to safeguard their network's security, meet "robust" security goals and report hacking incidents to the federal government.

Canadian Security Intelligence Service (CSIS):

One of CSIS's key priorities is cybersecurity and infrastructure protection. In this regard they investigate threats against critical information systems and infrastructure, posed by foreign countries, terrorists and hackers. CSIS sees serious attempts to penetrate vital networks every day.

RCMP and Local Police Authorities:

Police forces across Canada investigate cybercrime as it is reported, and are actively increasing their resources for cyber investigation. One concern voiced by the Canadian Association of Chiefs of Police is that as individuals report cybercrimes, average police stations are not always equipped to respond.

Bank of Canada – Joint Operational Resilience Task Force (JORM):

The JORM was created by the Bank of Canada to protect Canada's financial infrastructure. The JORM is a collaboration across eight large financial institutions, three payment systems, the Department of Finance and the Office of the Superintendent of Financial Institutions. We expect that, similar to this Department of Finance initiative, other federal departments are implementing similar public- private forums to protect vital systems. A concern we have is how will these various forums coordinate, on a timely basis, to ensure all major industry players (finance, telco, retail and vital infrastructure such as hydro) have ongoing dialogue and information sharing on cyber threats and attacks.

Canadian Cyber Threat Exchange (CCTX):

The CCTX has been established by the Business Council of Canada (formerly the Canadian Council of Chief Executive Officers), in order to share cyber threat information across firms. The CCTX includes members from financial services, telecommunications and retail industries, and therefore should be a helpful forum in coordination across industry lines.

But cyberattacks are on the rise, from both criminal

and state-sponsored agents. According to the latest Verizon Data Breach Investigation Report, in 2015 there were 2,260 confirmed data breaches in the United States, 795 of which were in the financial services industry.

> Globally, cyberattacks have increased 38% since 2014, with the annual cost estimated up to $1 trillion.

As a result, it's not surprising that in a 2016 PwC survey of Canadian bank executives, cyber risk was identified as their top risk – not low oil prices. The top ranking of cyber risk is consistent with GRI's survey of our members, who include the leading financial services companies across Canada.

> The United States is currently a global leader in cyber security, and continues to evolve and invest in the space.

In the U.S., the Department of Homeland Security has been given the mandate to monitor, assess and coordinate cyber response, including cross industry coordination. Also, a Director of Cybersecurity position has been created in the Executive Branch, and has been added to the National Security Council. And just recently, in February 2016, the Obama Administration unveiled its Cybersecurity National Action Plan, which builds on previous legislation and makes it easier for cross sector of critical industries to share cyber threat information between themselves and government agencies; it also calls for partnering with leading private sector firms, including Google, Facebook and Microsoft. The CNAP also calls for a significant increase in funding, both for network security upgrades and ongoing detection, prevention and mitigation efforts. In addition, the National Institution of Standards and Technology (NIST) has developed a Cybersecurity Framework, which is a set of common standards, guidelines and practices to help critical institutions (examples include finance, energy and healthcare) manage and coordinate cyber risk; clearly a common set of standards is essential in helping diverse institutions communicate and share information on threats and attacks. The US also regularly runs cyber war games on well-known Wall Street firms, codenamed "Quantum Dawn", which is designed to test their defences against internet attack, and see how well financial institutions respond and co-ordinate with each other in the event of a serious cyber attack such as hacks of exchanges, breaches of customer data and outages. We believe this type of central leadership and cross industry cooperation will be even more critical in protecting nations, institutions and citizens as cyber threats evolve.

Another good example of public / private partnership in cybersecurity is Israel. Israel has been very effective in coordinating public, private, Israeli Defense Forces and academia in the research, development and implementation of cyber defenses. Their ecosystem includes research collaboration, a very deep venture capital market which funds start up cyber firms, and a talent collaboration. As a result Israel is known for its technology start up success, with Israel having more firms listed on the NASDAQ than all of Europe combined. Through a number of initiatives, most recently the launch of the Advanced Technology Park on the campus of Ben Gurion University, Israel successfully promotes the development of cyber research centres, cooperation on research and development projects and information and data sharing. In addition, Israel has created two agencies to promote cyber security. First, the National Cyber Security Authority is a government agency focused on the protection of civilian activities in cyberspace. They set out standards that all private institutions, including financial institutions, must follow, and they deal with threats in real time; they also partner closely with the Israeli Defense Forces' Cyber Force (the second agency, which is a key component of Israel's national defense forces). So clearly Israel takes national cooperation and incubation of cyber capabilities to a very high level.

> The new Liberal government has committed to developing and implementing a new innovation strategy for Canada.

They have committed to investing $900 million to boost high tech innovation and fund start up

incubators. The GRI thinks this is a crucial policy for Canada, and encourages a bias towards action in moving the policy forward. Furthermore, in the cyber space, innovation must include a focus towards cybersecurity, including research, development and education.

> Technology innovation will only proceed so far unless it is coupled with innovation in cybersecurity.

The Global Risk Institute believes that Canada should take a cue from the U.S. and Israel. In particular, we need to do more to coordinate key industry and government players across the country. We must accelerate cross-industry coordination, step up cyber research and development, and encourage cyber industry incubation. Specifically we call for the following immediate steps by Public Safety Canada:

- *Expedite the roll-out of their Cybersecurity strategy across all Federal Departments;*
- *Establish a cross-industry cyber forum, with participation of all major firms and critical infrastructure divisions;*
- *Establish clear standards, guidelines and practices across all Departments and industries, and adopt the Cybersecurity Framework developed by NITS (such standards are critical to effective communication);*
- *Work with the Canadian Universities to further build out undergraduate and advanced degree programs in cybersecurity, while also seeking support from Canadian businesses and institutions in both curriculum development and co-op program placements (as practical experience is critical to building the appropriate skill base).*
- *Incent all players in the cyber ecosystem (including supporting organizations such as venture capital, start-ups, and academia) to invest and cooperate in ongoing research and development, in order to build on Canada's cyber incubation efforts. Further, coordinate a delegation visit to both the US Department of Homeland Security and Israel's Advanced Technology Park at Ben Gurion University, seeking to share insights and opportunity to build cybersecurity partnerships.*

With the number, sophistication and severity of cyberattacks continuing to rise, Canada needs to bring its great institutions together to develop a leadership position in cybersecurity. Our universities, financial institutions, telecom companies and government agencies are among the strongest in the world. We should harness their resources.

Brian O'Donnell

Brian is an Executive in Residence at the Global Risk Institute, after retiring from CIBC in 2015. Most recently Brian was CIBC's Executive Vice President and Chief Data Officer, where he developed their data strategy and governance framework. Prior to the CDO position Brian lead the Bank's Enterprise Risk Management group, including balance sheet and capital management.

Read Brian's full Bio on GRI Website >

Richard Nesbitt

Richard is the President and CEO of Global Risk Institute in Financial Services, as well as an Adjunct Professor of the Rotman School of Management, University of Toron-to and chair, of the Advisory Board of the Mind Brain Behaviour Hive at the same University. He serves on a number of community and corporate boards of directors.

Read Richard's full Bio on GRI Website >