National approach to Cyber intrusion

A COMPARISON OF UNITED KINGDOM AND CANADA

Authors: **Alston Perianayagam**, *Special Advisor, Global Risk Institute*
Richard Nesbitt, *CEO Global Risk Institute, and*
Mark Caplan, *President GRI Global Risk Institute*

The Global Risk Institute in Financial Services annually surveys the Chief Risk Officers of its members to assess the risks which they view as having the most serious impact on their organizations should they occur. For both 2017 and 2018 the top risk identified is cyber risk. Vulnerability to cyber crime is serious and it is rising, as are the threats of cyber attacks:

- ***New technologies**, including new uses for data, are being increasingly adopted.*
- ***The functioning of critical infrastructure** is increasingly dependent on networked technology. (Power plants, communication systems, transportation services, hospitals, payment systems, etc.)*
- ***Financial systems and networks** are interconnected on an increasingly global basis.*
- ***Cyber intrusions** are happening more frequently, with increasing levels of damage.*
- **Cyber criminals** *are becoming more and more sophisticated.*

- ***Cyber criminals target:***
  - ***Individuals** - for access to personal information and financial assets.*
  - ***Companies** - for trade secrets/R&D, confidential corporate and client information.*
  - ***Governments** - for national defense secrets and citizen information.*
  - ***Academic Institutions** - for leading-edge research.*
- *Foreign powers with significant financial resources are using cyber intrusion techniques to steal information, influence outcomes of elections and build foreign currency reserves.*
- *Advances in technology, specifically quantum computing, could render obsolete much of the cryptography that protects current commercial (including financial) platforms.*

In a recent interview, the head of the UK's National Cyber Security Center warned that it was just a matter of when, not if, additional attacks would occur in the country, and that some attacks will get through, at which point the objective becomes cauterizing the damage.

> *"There are 100 countries that can deliver APT's (advanced persistent threat) and live on your network and do anything they wish".*

Combatting this increasing risk requires a coherent strategy, clear structure and practiced response that provides effective coordination at the institutional, industrial, national and international levels.

This paper explores the national level landscapes within Canada and the United Kingdom as they relate to financial services. While national priorities, timing, and approach will always vary to some extent, we believe it to be a fair comparison given the UK and Canada are described as the third and fourth largest cybersecurity innovation hubs in the world. [1]

While there are similarities in the approaches there are also differences. It is our belief that cyber risk management response strategies are most effective with significant cooperation across industry groups, governments, regulators and academia. We examine the developments over the past several years which led to the current national approaches. It is our hope that through a better understanding of differing national approaches we can advance the learning and discussion of the optimal way to protect the citizens, corporations, vital infrastructure, and economies.

1 *Deloitte, "Harnessing the cybersecurity opportunity for growth" October 2016*

National Cyber Security Infrastructure in the UK:

1. GOVERNMENT INITIATIVES:

The National Cyber Security Strategy 2016-2021[2] is the UK Government's cabinet level document which outlines the vision for the UK by 2021 to be secure from and resilient to cyber threats, while prosperous and confident in the digital world. The document highlights the need:

- ***To defend the UK against evolving cyber threats,***
- ***To deter cyber criminals and,***
- ***To develop nation-wide cyber expertise.***

In total, the UK government earmarked and committed an investment of £1.9 billion over the period of 2016-2021. This amount is in addition to the £860m National Cyber Security Programme already spent as part of the 2011 National Cyber Security Strategy.

The cornerstone of the UK national strategy is the introduction of the National Cyber Security Center (NCSC) - established in October 2016. NCSC is the central body for cyber security at a national level, reporting to the GCHQ (Government Communications Headquarters).

NCSC was created as an amalgamation of various government entities, including CPNI (the Center for the Protection of National Infrastructure) responsible for managing Critical National Infrastructures, CERT-UK (Computer Emergency Response Team) and CCA (the Center for Cyber Assessment) that conducts cyber assessment for the UK government.

In exercising its mandate, NCSC collaborates with other government entities, including the intelligence agencies – the Security Service (MI5) and the Secret Intelligence Service (MI6)- and National Crime Agency (NCA). The NCA addresses Serious and Organized Crimes including organized crimes, fraud, money laundering, border policing, human trafficking and child exploitation (amongst others). A department within NCA, called the National Cyber Crime Unit (NCCU) was set up to lead and coordinate the national investigative response to cyber crime.

At the regional level, ROCU (Regional Organised Crime Units) was set up to support the national effort as well as local forces.

Separately, Action Fraud is run by the City of London police and provides a national reporting centre for fraud and cyber crime. As part of the 'Deter' action plan in the National Cyber Security Strategy 2016-2021, a new 24/7 reporting and triage capability will be set up between Action Fraud, NCSC, NCCU and other law enforcement agencies.

In September 2015, the Global Cyber Alliance,[3] a partnership between government and international law enforcement agencies, was established. The organization was founded by the City of London Police, District Attorney of New York County and the Center for Internet Security.

One of Global Cyber Alliance's initiatives is DMARC (Domain-based Message Authentication Reporting and Conformance) protocol. This program helps to authenticate emails from the government entities to the general public. NCSC adopted this program across government entities and in its first year, was able to block at least 120,000 fake emails from a spoof @gov.uk address.

2 *UK Government, National Cyber Security Strategy 2016-2021, (2016)*

3 *Global Cyber Alliance, www.globalcyberalliance.org*

The 2017 NCSC Annual Report [4], dated October 2017, highlights its first year's progress, including:

1. The launch of Active Cyber Defence, which has prevented thousands of attacks and reduced the average time a phishing site is online from 27 hours to 1 hour,
2. A coordinated response of more than 590 significant cyber incidents,
3. Coordinated an active UK response to the global WannaCry incident.

Prior to the introduction of National Cyber Security Strategy 2016-2021, the UK government, through the UK Trade and Investment, published the Cyber Security Strategy – the UK Approach to Exports. [5] This initiative is now being driven by DIT (Department for International Trade).

2. INDUSTRY INITIATIVES:

A key component of a successful national cyber strategy is the proactive and dynamic engagement within the private sector to allow individual corporations to be on alert through the exchange of information.

The CiSP (Cyber-Security Information Sharing Protocol) is a joint industry and government sharing protocol initiative to exchange cyber threat information. The CiSP program is run by the NCSC. It is a resource in the event of large scale cyber attacks, such as the WannaCry ransomware attack of May 12th 2017. [6]

Within the sharing protocol, the CiSP Fusion Cell refers to a joint government and industry organization of analysts, who examine cyber information and data feeds, conduct analysis and provide contextual cyber threat and vulnerability assessments.

In addition to CiSP, Industry 100 is another initiative launched by NCSC. It provides an opportunity for companies to embed staff into NCSC (based on NCSC needs) for industry expertise and collaboration. The NCSC targets 100 staff, hence the name, embedded by the industry.

The UK also has the cyber growth partnership and the Cyber Exchange. [7] The Cyber Growth Partnership is composed of representatives from academia, government and industry. The Partnership works on behalf of the wider industry to achieve three strategic objectives:

- *Increasing export market understanding and access*
- *Develop the UK's offer and brand for overseas markets*
- *Skills, Research & Innovation* [8]

There are also a number of UK government-funded activities to support small cyber businesses such as the Cyber 101 programme [9] and the Cyber Security Academic Startups programme [10].

Separate from the initiatives outlined above, the Cyber Defence Alliance (CDA) is a collaborative effort between banks and law enforcement agencies. The CDA was created in 2015 by 4 banks and since then, more banks have joined the effort. [11] In addition to CDA there are other trade association sharing initiatives such as with the UK Finance and the Investment Association.

The Cross-sector Safety and Security Communications (CSSC) initiative is a partnership between law enforcement agencies, local and national government agencies and private sector. CSSC was founded in June 2011 by a team of senior security experts with an initial focus of business preparation during the London Olympics in 2012.

4 *National Cyber Security Center, "National Cyber Security Centre: a year of protecting the UK", (2017)*

5 *Gov. UK, "Cyber security: the UK's approach to exports", (2014)*

6 *NCSC's 2017 annual report reported that there were more than 23,000 visitors to CiSP online platform following the WannaCry attack, including 15,000 during the first weekend.*

7 *Cyber Growth Partnership UK, https://www.cyberexchange.uk.net*

8 *TechUK, https://www.techuk.org/cyber-growth-partnership*

9 *Digital Catapult, "Digital Catapult and DCMS launch Cyber 101", (Feb 2017)*

10 *https://apply-for-innovation-funding.service.gov.uk/competition/100/overview*

11 *Gov. UK, "Cyber security academic startups programme", (Jan 2018)*

Another initiative underway that brings together key players from Government and Industry is CyberInvest. CyberInvest encourages and promotes cyber security research at UK universities and has created a community of industry, government and academia committed to cyber security research in the UK. [12]

RESPONSE TEAM AND INCIDENT MANAGEMENT

In most cases, Cyber incidents require quick response. The centralized role of NCSC provides leadership in a crisis situation that is triggered by a cyber attack. NCSC provides active support to the impacted organizations and if necessary, inter-governmental coordination.

For corporations that are experiencing a cyber attack, there are two options available. The Cyber Incident Response (CIR) is certified by NCSC and CPNI and it is reserved for large cyber breaches and critical infrastructures. The Cyber Security Incident Response scheme (CSIR) is approved by CREST (Council of Registered Ethical Security Testers) and can be used by most corporations.

3. REGULATORY INITIATIVES:

Financial firms handle massive amounts of data, including transaction data, personal wealth records and personal identities (such as ID, address, etc.). Data and privacy protection are an important part of maintaining the public trust in the financial system and as such maintaining cyber resilience should be a top priority for any financial organization and their regulatory overseers.

The responsibility for ensuring a sound cyber defense rests within the Board of Directors of the corporations and regulators rely heavily on governance arrangements. Regulatory guidance highlights the importance for organizations to have proper safeguards in place against cyber attacks. These safeguards should be created by a holistic cyber awareness culture and deliberate framework that govern acceptable practices and controls in the organization.

The FCA (Financial Conduct Authority) and the PRA (Prudential Regulation Authority), the market and prudential regulators in the UK's financial services sector respectively, play a key role in continuously monitoring that financial services firms have sufficient cyber resilience by conducting Risk and Control Assessments to ensure financial services abide by or adhere to the processes within their own Cyber Security Risk Appetite sandbox.

The Bank of England introduced CBEST (the Bank of England Cyber Security Framework). It is the first of its kind effort by a central bank or federal financial authority and helps prepare for systemic attacks on the whole financial system. CBEST was practised on 35 Financial Institutions, 24 supervised Banks and a selection of building societies and insurance companies.

The Bank of England, FCA and the British Government's Treasury coordinated a simulation of cyber attacks on the financial sector known as Waking Shark (2011) and Waking Shark II (2013). Participants included investment banks, financial market infrastructure and the regulators. [13]

The document Cyber Security Regulations and Incentives Review [14] outlined regulations governing Cyber Security in the UK.

Other legislation and regulation relevant to Cyber Security for financial services in the UK and EU include:

- *General Data Protection Regime (GDPR), May 2018*
- *Payment Services Directives 2 (PSD2), Jan 2018*
- *FCA's - Financial Services and Markets Act 2000*
- *The Network and Information Security Directive is a proposed regulation by the European Commissions.*
- *Communication Act 2003*
- *Data Protection Act (DPA) 1998*
- *Computer Misuse Act 1990*

12 *National Cyber Security Centre, "CyberInvest" (Aug. 2016)*

13 *For more detail reports, please refer to https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity*

14 *Gov. UK, "Cyber Security Regulation and Incentives Review", (Dec 2016)*

4. THE ROLE OF ACADEMIA:

DEVELOP TALENT AND CONDUCT RESEARCH

A large portion of the UK's national Cyber Security strategy includes a plan to develop cyber expertise and increase general awareness of the Cyber Security risks.

The NCSC and the Engineering and Physical Sciences Research Council (EPSRC) have developed the Academic Centers of Excellence in Cyber Security Research (ACE-CSR) program. It is a certification program to recognize UK universities that meet the minimum requirement of:

- *Commitment from the university's leadership team to support and invest in the university's cyber security research capacity and capability*
- *A critical mass of academic staff engaged in leading-edge cyber security research*
- *A proven track record of publishing high impact cyber security research in leading journals and conferences*
- *Sustained funding from a variety of sources to ensure the continuing financial viability of the research team's activities*

There are 14 universities recognized as ACE-CSR. The NCSC and GCHQ have also certified 20 Cyber Security Masters degree courses at 15 universities across the UK. Over 20 universities now offer either a Bachelors or Masters Degree in Cyber Security as noted in Appendix 4.

As part of its commitment to develop talent within the UK, NCSC is also funding approximately 30 Doctoral students from ACE-CSRs.

Additional programmes include:

- **The certified degrees programme** [15]
- **Government funded research institutes** [16]
- **The DCMS backed programme for schools** [17]

As importantly, identifying talent is being done at a young age. The £20m cyber schools programme funded by the UK government [18] is trying to identify and nurture cyber talent in 14-18 year old students and also the £40m Institute of Coding initiative [19] is looking to support increased computer science education in 18+ higher education initiatives. Both are billed as a mechanism to increase the talent pipeline in the UK over the next 4-6 years.

At the pre-university level, NCSC conducts a CyberFirst program to students 14-18 years of age. The program includes classroom-based activities, after-school sessions with expert mentors, challenging projects and summer school. By 2021, the NCSC expects that cyber security will be taught effectively as an integral part of relevant courses from the primary to post-graduate level.

In additional to the talent development strategies outlined above, innovation in the technology sector requires a climate that fosters entrepreneurship. The NCSC strategy includes incubation of start-ups in the Cyber Security area. The NCSC is planning to set up two innovation centers. The first center, Cheltenham Accelerator, was opened in 2017 and was joined by seven start-up companies.

15 *NCSC, "NCSC-certified degrees", (Aug 2017)*

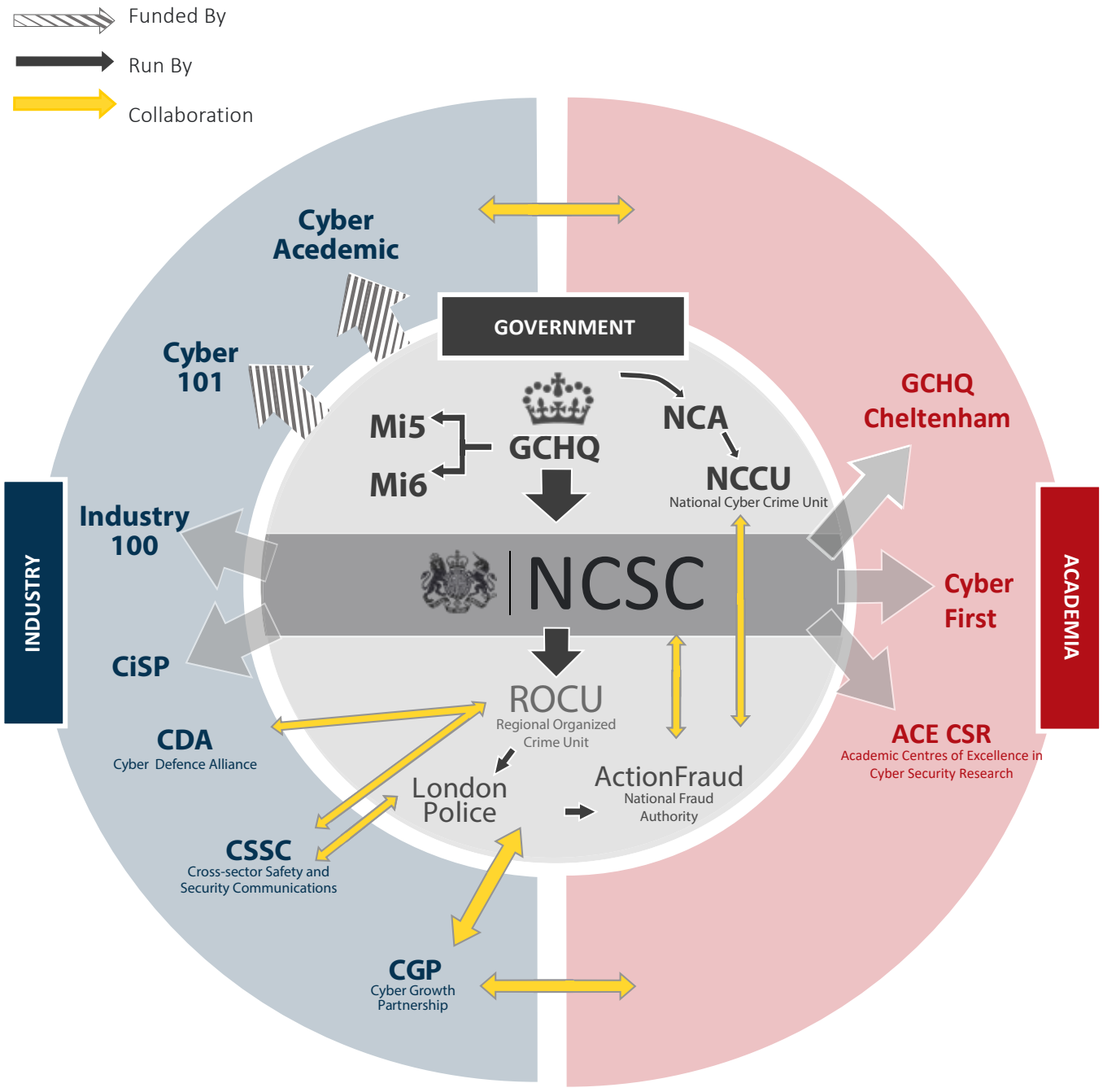
16 *NCSC, "Research institutes"*

17 *Gov. UK, Press Release, Students urged to apply for pioneering Cyber Schools Programme" (July 23, 2016)*

18 *Gov. UK, "Cyber Schools Programme" (Feb 2017)*

19 *Gov. UK, News Release, "Prime Minister announces £20 million Institute of Coding", ((Jan 2018)*

DIAGRAM OF UK NATIONAL CYBER SECURITY INFRASTRUCTURE



NATIONAL CYBER SECURITY INFRASTRUCTURE IN CANADA:

1. GOVERNMENT INITIATIVES:

Canada's Cyber Security Strategy (2010), outlines how the Government of Canada is working with all levels of government, private sector organizations and international partners to strengthen cyber security in Canada. It is focused on three pillars:

- ***Securing government systems,***
- ***Partnering to secure vital cyber systems outside the federal Government, and***
- ***Helping Canadians be secure online.*** [20]

This document is currently under review. In 2016-2017, an evaluation of Canada's Cyber Security Strategy was undertaken as a collaborative effort between various government departments. [21]

In the 2018 February budget, the federal government allocated over $500 million, spread out until 2022-23, to cyber security. The bulk of the funds will be used by the CSE to create the new Canadian Centre for Cyber Security and by the RCMP to establish a National Cyber Crime Coordination Unit. Previously, no single organization had been given an overarching national mandate on cyber coordination. A number of Government departments currently play key roles as described in the following write up about Cyber Security in the Canadian Federal Government (taken from the website of PSC): [22]

Public Safety Canada (PSC) *as part of its mandate to keep Canadians safe from a range of risks such as natural disasters, crime and terrorism has a cyber directorate. The department houses the Government Operations Centre as the hub of the National Emergency Response System (NERS). PSC operates the Canadian Cyber Incident Response Centre (CCIRC) which escalates cyber incidents of national significance to the Government Operations Centre which then helps coordinate a national response. IT and security professionals who need to engage with the federal government on cyber security issues but are unsure of who to contact can always contact CCIRC.*

The ***Communications Security Establishment (CSE)*** *is the Government of Canada's cryptologic agency responsible for the collection of cyber foreign intelligence and Canada's interface with the international cryptologic community. It undertakes classified research and development for cyber security. CSE monitors and defends Government of Canada networks by detecting, discovering and responding to sophisticated cyber threats to the Government, and provides mitigation and recovery advice and guidance to Government departments to help them recover from cyber incidents.* [23]

The ***Royal Canadian Mounted Police (RCMP)*** *leads the criminal investigative response to suspected criminal cyber incidents, such as the unauthorized use of a computer and mischief in relation to data. It leads the investigative response to suspected criminal national security cyber incidents and assists domestic and international partners with advice and guidance on cyber crime threats.*

20 *Government of Canada, Public Safety Canada, "Cyber Security"*

21 *Government of Canada, Public Safety Canada, "Summary of the 2016-2017 Evaluation of Canada's Cyber Security Strategy (CCSS)"*

22 *Government of Canada, Public Safety Canada, "Cyber Security in the Canadian Federal Government"*

23 *For further information on CSE's approach to cyber defence - https://www.cse-cst.gc.ca/en/group-groupe/cyber-defence*

*The **Canadian Security Intelligence Service (CSIS)** conducts national security investigations, reports to and advises the Government of Canada of activities constituting a threat to the security of Canada as defined in the Canadian Security Intelligence Service Act. It provides analysis to assist the Government of Canada in understanding cyber threats, and the intentions and capabilities of cyber actors operating in Canada and abroad who pose a threat to the security of Canada. This intelligence enables the Government of Canada to improve its overall situational awareness, better identify cyber vulnerabilities, prevent cyber espionage or other cyber threat activity, and take action to secure critical infrastructure.*

The Department of National Defence (DND) is responsible for the provision of defence intelligence to inform the Government of Canada threat and risk assessment process. DND Contributes to Government situational awareness during the monitoring and analysis, mitigation, and response phases of the Government of Canada Information Technology Incident Management Plan by providing cyber security information from military allied sources, monitoring and reporting on technological IT threats, and providing options analysis for potential military response.

***Industry Canada (IC)** is responsible for spectrum management in Canada and for fostering a robust and reliable telecommunications system. IC develops policies to ensure a safe and secure online marketplace and helps to ensure the continuity of telecommunications during an emergency.*

Defence Research and Development Canada (DRDC) *leads the development of military cyber security science and technology (S&T) in support of the Canadian Forces. Furthermore, the DRDC Centre for Security Science (DRDC CSS) leads, in partnership with Public Safety Canada, cyber security S&T efforts that are not specifically assigned to another department or agency. These activities fall under the Canadian Safety and Security Program (CSSP), which is a federal effort, delivered in partnership with all levels of government, industry, academia and allies, to strengthen Canada's ability to anticipate, prevent/mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism through the convergence of science and technology (S&T) with policy, operations and intelligence.*

*The **Treasury Board Secretariat (TBS)** establishes and oversees a whole-of-government approach to cyber security, including: setting government-wide direction and establishing priorities for securing government IT systems and networks; providing direction and advice to lead security agencies on the approach and implementation of measures for managing IT security incidents; and providing oversight of IT incident management, including post-mortem reviews and lessons learned.*

***Shared Services Canada (SSC)** streamlines and consolidates information and communications technologies in the areas of email, data centres and networks, and ensures the confidentiality, integrity and availability of common information technology (IT) services provided to departments. SSC provides IT security services and other solutions to enable departments to exchange information with citizens, businesses and employees. SSC also gathers, analyzes, consolidates and facilitates the sharing of operational threat and vulnerability information related to the common IT services and Government IT critical infrastructure they manage, and communicates the information to the Canadian Cyber Incident Response Centre and, as authorized, to departments and cyber security partners.*

***Canadian Radio-television and Telecommunications Commission (CRTC)** ensures that Canadians have access to a world class communications system, while protecting Canadians from unsolicited communications and contributing to a more secure online environment for consumers and businesses.*

The Office of the Privacy Commissioner of Canada (OPC) *oversees compliance with both the Privacy Act, which covers the personal information-handling practices of federal organizations, as well as the Personal Information Protection and Electronic Documents Act, the federal private sector privacy law. In accordance with Treasury Board policy, the OPC receives data breach reports from departments and agencies and reviews and advises on privacy impact assessments (PIAs) of new and existing government initiatives. The security of federal technological infrastructure is often at the heart of PIAs and the OPC works with departments and agencies to advise on appropriate safeguards.*

The ***Canadian Anti-Fraud Centre (CAFC)*** *is Canada's central repository for data, intelligence and resource material as it relates to fraud. The CAFC commits to providing timely, accurate and useful information to assist citizens, businesses, law enforcement and governments in Canada and around the world. The primary goals are prevention through education and awareness, disruption of criminal activities, providing assistance with regard to enforcement, and strengthening partnerships between the private and public sectors with the aim of maintaining Canada's strong economic integrity.*

Other individual departments/ministries, such as the Department of Finance, Global Affairs Canada, and Natural Resource Canada (to name but three), have oversight for cyber related matters that relate to the industries and activities within their mandates.

RESPONSE AND INCIDENT MANAGEMENT

Incident response is coordinated through three organizations at a Federal level – CCIRC (PSC), the Information Protection Centre (SSC) and the Cyber Threat Evaluation Centre (CSE).

As noted above, RCMP and CSIS are responsible respectively for criminal and intelligence investigation related to cyber crime. The two large Provincial Police forces (OPP and SQ) may also be engaged in the investigation of cyber incidents relating to their jurisdictions.

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is Canada's financial Intelligence unit. Its mandate is to facilitate the detection, prevention and deterrence of money laundering and the financing of terrorist activities, while ensuring the protection of personal information under its control. [24]

2. INDUSTRY INITIATIVES:

Proactive and dynamic engagement within the industry domestically, in partnership with the official sector and in conjunction with the global players is a feature of the cyber landscape in Canada.

Many of the largest, most technologically mature financial institutions are engaged directly with CSE in a relationship of information sharing on practices and threats. Given the highly sensitive nature of the information shared, these relationships are typically governed by non-disclosure agreements which allow all parties to ensure security while facilitating a worthwhile exchange.

Many financial services companies are members of the Canadian Cyber Threat Exchange (CCTX), a not for profit organization that helps Canadian businesses and consumers detect and mitigate cyber attacks. CCTX operates as a cybersecurity information sharing centre and

24 *Government of Canada, Financial Transaction and Reports Analysis Centre of Canada*

aims to provide timely cybersecurity analysis.[25] Up and running since late 2016, CCTX brings private sector, public sector, law enforcement and academia together to share information and analysis.

At least 20 Canadian institutions are also involved in the Financial Services – Information Sharing and Analysis Centre (FS-ISAC), a US-based financial services initiative with a global membership of over 6300 members. Its mission is

> *"To help assure the resilience and continuity of the global financial services infrastructure and firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the global economy."* [26]

FS-ISAC often has activities organized in Canada.

Closer to home the industry has come together to form the Canadian Financial Services – Cyber Security Governance Council (CFS-CGC) whose aim is to provide a consolidated industry view of the issues facing the industry and to make recommendations as to the actions required to mitigate them. The CFS-CGC is due to put out a position paper on cyber security shortly.

2014 saw the creation of the Digital ID & Authentication Council of Canada (DIACC). Created following the federal government task force for the payment system review, DIACC brings together participants from governments and agencies (federal and provincial), financial institutions, telecommunications and ID solutions providers to

> *"Develop a Canadian digital identification and authentication framework to enable Canada's full and secure participation in the global digital world".* [27]

Coordinating incident response is highly developed in the banking sector in Canada. Created in the early 2000s by the Canadian Bankers Association (CBA), the Canadian Financial Institutions – Computer Incident Response Team

> *"Coordinates the exchange of information between banks and other industry partners or regulators during cyber related security incidents".* [28]

Membership of this organization includes 59 domestic and foreign banks, branches and other key financial stakeholders of the financial system.[29]

The CBA also plays a coordinating role in the investigation of cyber related incidents through its Bank Crime Prevention and Investigation Office (BCPIO).

3. REGULATORY EFFORTS IN FINANCIAL SERVICES:

The regulatory landscape in financial services in Canada has a number of institutions overseeing risks.

The Office of the Superintendent of Financial Institutions (OSFI) provides prudential oversight of federally registered banks and trust companies, insurers, and pension plans. Provincially registered entities (such as credit unions and insurers) are regulated by a variety of provincial bodies.

Market conduct is regulated at a provincial level by securities commissions who work together in coordination under the umbrella of the Canadian Securities Administrators (CSA). Asset managers and broker-dealers are overseen by the Investment Industry Regulatory Organization of Canada (IIROC). The Bank of Canada (BOC) is the domestic monetary authority and is the

25 *Canadian Cyber Treat Exchange, https://cctx.ca/*

26 *FS-ISAC Financial Services Information Sharing and Analysis Centre https://www.fsisac.com*

27 *DIACC, Digital ID & Authentication Council of Canada, https://diacc.ca*

28 *Government of Ontario, Legislative Assembly of Ontario, "Committee Proceedings Transcript - 2004-08-17"*

29 *For more information on cyber security forums - "Inventory of Canadian Cyber Threat Mitigation Initiatives Final Report", B. Dupont, March 2016*

regulator for designated payment systems. The BOC has oversight responsibility for all designated Financial Market Infrastructures (FMIs).

Consistent with regulatory practice in much of the developed world, regulators place heavy reliance on board governance, disclosure, and management self-assessment in discharging their oversight obligations in cyber security. OSFI (in 2013) for example issued

> *"Cyber security self-assessment guidance to assist federally regulated … financial institutions in ensuring their cyber risk management policies and practices…"* [30]

The Joint Operational Resilience Management (JORM) is a public-private partnership seeking to enhance resilience across the financial sector. Members include payment and clearing system participant FIs, FMIs, the Department of Finance, OSFI, and the Bank of Canada (Chair). In 2017 JORM conducted a large scale cyber intrusion exercise aimed at assisting the members in assessing their internal escalation, communication protocols, and readiness in the event of a severe cyber incident.

Finally, the OPC (mentioned in the government section above) has responsibility for overseeing compliance with the Digital Privacy Act. New requirements around data breach disclosure are coming into force in Canada shortly and the OPC will, in all likelihood, play an increasingly important role in cyber preparedness and response.

30 *The Office of the Superintendent of Financial Institutions (OSFI) , "Cyber Security Self-Assessment Guidance"*

4. THE ROLE OF ACADEMIA:

DEVELOP TALENT AND CONDUCT RESEARCH

Canada has a vibrant academic community which conducts research and training on cybersecurity.

Hosted by the Université de Montréal, Smart Cybersecurity Network (SERENE-RISC) is a knowledge mobilization network created to improve the general public's awareness of cybersecurity risks and to empower all to reduce those risks through knowledge. The Networks of Centres of Excellence of Canada (NCE) federal funding agency announced the release of SERENE-RISC's funding on April 15, 2014. SERENE-RISC network partners include more than 40 academics across 10 disciplines at 24 post-secondary institutions from Quebec, Alberta, Ontario, British Columbia and Nova Scotia, more than 24 public and private sector members, and 6 not-for-profit organizations. [31]

Another not for profit effort that brings together academic thought leaders is Quantum-safe Canada. [32] Forward looking by design and leveraging on Canada's leadership from the Institute for Quantum Computing in Waterloo, Quantum-safe Canada is focused on raising awareness regarding the threat to encryption and cybersecurity through advances in quantum computing.

According to a Deloitte report on cybersecurity opportunities, Ontario alone has 9 university level cyber security degree programs and 30+ college level cyber security diploma programs. [33] Ryerson University, for example has established a Privacy and Big Data Institute which launched as a hub for research education and events in 2014. [34] Other provinces are also promoting academic thought leadership in the field as can be evidenced by the Canadian Institute for Cybersecurity at the University

31 *The Smart Cybersecurity Network (SERENE-RISC)*

32 *Quantum-Safe Canada, https://quantum-safe.ca/*

33 *Deloitte "Harnessing the cybersecurity opportunity for growth", (October 2016)*

34 *Ryerson University, Privacy and Big Data Institute*

of New Brunswick. And activity is not only at the post-secondary level. The Canadian Cyber Defense Challenge, [35] which began as a Winnipeg based pilot program in 2011, is engaging high school level students in the realities of modern day cyber issues.

CONCLUSION

Technological change represents great promise to societies including solving many challenges that exist in our environment, economies and societies. Rewards of technological development also bring with them challenges. One of these challenges is the propensity of some to use technology for self-enriching or destructive acts. Cybersecurity prevention, detection and remediation is a requirement that is a current and future necessity for all. National arrangements in every country will play a significant role in determining the effectiveness of combatting cybercrime.

35 *Cyber Defence Challenge, CCDC event*

APPENDIX 1

LIST OF ABBREVIATIONS UK:

ACE-CSR: Academic Excellence in Cyber Security Researches

CBEST: Bank of England Cyber Security Framework

CCA: Center for Cyber Assessment, a unit within NCSC

CDA: Cyber Defence alliance

CiSP: Cyber Security Information Sharing Protocol

CSSC: Cross-sector Safety and Security Communications

DMARC: Domain-based Message Authentication, Reporting and Conformance protocol

CIR: Cyber Incident Response

CSIR: Cyber Security Incident Response Scheme

CREST: Council of Registered Security Testers

CPNI: Center for Protection for National Infrastructure

DPA: Data Protection Act

DIT: Department for International Trade

FCA: Financial Conduct Authority

GCA: Global Cyber Alliance

GCHQ: Government Communications Head-Quarter

GDPR: General Data Protection Regime

MI-5 & MI-6: Intelligence Agencies in the UK

NCA: National Crime Agency

NCCU: National Cyber Crime Unit – a division within NCA that handles Cyber Crimes

NCSC: National Cyber Security Strategy

NIS Directive: Network and Information Security Directive

PRA: Prudential Regulation Authority

PSD2: Payment Service Directive 2 (regulation)

UK CERT: UK Computer Emergency Response Team

APPENDIX 2

LIST OF ABBREVIATIONS CANADA:

BCPIO: Bank Crime Prevention and Investigation Office (CBA)

BOC: Bank of Canada

CAFC: Canadian Anti-Fraud Centre

CBA: Canadian Bankers Association

CCIRC: Canadian Cyber Incident Response Centre (PSC)

CCSS: Canada's Cyber Security Strategy (PSC, TBS, SSC, GAC, JC, CSE, CSIS, DND, RCMP)

CCTX: Canadian Cyber Threat Exchange

CFI-CIRT: Canadian Financial Institutions, Computer Incident Response Team (CBA)

CFS-CGC: Canadian Financial Service Cyber Security Governance Council

CRTC: Canadian Radio-television and Telecommunications Commission

CSCP: Cyber Security Cooperation Program

CSA: Canadian Securities Administrators

CSE: Communications Security Establishment (DND)

CSIS: Canadian Security Intelligence Service (PSC)

CTEC: Cyber Threat Evaluation Centre

DIACC: Digital ID & Authentication Council of Canada

DND: Department of National Defence

DoF: Department of Finance

DoE: Department of Energy

DRDC: Defence Research and Development Canada (DND)

FERP: Federal Emergency Response Plan (PSC)

FINTRAC: Financial Transactions and Reports Analysis Centre

FMI: Financial Markets Infrastructure

FS-ISAC: Financial Services – Information Sharing and Analysis Centre

GAC: Global Affairs Canada

IC: Industry Canada

IIROC: Investment Industry Regulatory Organization of Canada

IPC: Information Protection Centre (SSC)

JC: Justice Canada

JORM: Joint Operational Resilience Management (BOC)

NRCAN: Natural Resources Canada

NDA: Non-Disclosure Agreements

OSFI: Office of the Superintendent of Financial Institutions

OPC: Office of the Privacy Commissioner

OPP: Ontario Provincial Police

PSC: Public Safety Canada

PSPC: Public Services and Procurement Canada (formerly Public Works & Government Services Canada)

RCMP: Royal Canadian Mounted Police (PSC)

SERENE-RISC: Smart Cybersecurity Network (part of the Network Centres of Excellence of Canada)

SSC: Shared Services Canada (PSPC)

SQ: Sûreté du Québec

TBS: Treasury Board of Canada Secretariat

APPENDIX 3

LIST OF ADDITIONAL READINGS:

- ***National Cyber Security Strategy 2016-2021:*** *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf*
- ***NCSC's 1st year Annual Report:*** *https://www.ncsc.gov.uk/news/national-cyber-security-centre-year-protecting-uk*
- ***G7 Fundamental Elements on Cyber Security:*** *https://www.fin.gc.ca/n16/docs/g7-1014-eng.pdf*
- ***G-7 Fundamental elements for effective assessment of cybersecurity in the financial sector:*** *https://www.treasury.gov/press-center/press-releases/Documents/(PRA)_(BCV)_4728453_v_1_G7%20Fundamental%20Elements%20for%20Effective%20Assessment.pdf*
- ***FCA's approach to Cyber Security in Financial Services firms****. A speech by Nausicca Delfas, Director of Specialist Supervision at the FCA (Sept 2016): https://www.fca.org.uk/news/speeches/our-approach-cyber-security-financial-services-firms*
- ***Industry-100 blog:*** *https://www.ncsc.gov.uk/information/industry-100*
- ***CREST:*** *http://www.crest-approved.org/*
- ***ACE CSR:*** *https://www.ncsc.gov.uk/articles/academic-centres-excellence-cyber-security-research*
- ***Cyber Security Capacity Review in the UK****, a report by Global Cyber Security Capacity Center as requested by the UK Government: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf*
- ***Harnessing the Cybersecurity opportunity for growth*** *– Cybersecurity innovation & the financial services industry in Ontario http://www.oce-ontario.org/docs/default-source/default-document-library/oce-tfsa_cyber-brochure-exec-summary-online-oct19.pdf?sfvrsn=4*
- *Inventory of Canadian Cyber Threat Mitigation Initiatives Final Report, B. Dupont, March 2016*