20 October, 2016

ITAC RESPONSE TO PUBLIC SAFETY CANADA'S CYBER SECURITY REVIEW

The Information Technology Association of Canada (ITAC) appreciates the opportunity to participate in Public Safety Canada's consultations on Canada's approach to Cyber Security. ITAC is the authoritative national voice for Canada's $170 billion information and communications technology (ICT) industry. Canada's 36,000 ICT firms generate over 1.1 million jobs directly and indirectly. The ICT industry in Canada also creates and supplies goods and services that contribute to a more productive, competitive and innovative economy and society.

Cyber security has long been a central issue for ITAC. ITAC's membership includes a significant number of businesses operating across the cyber security ecosystem. ITAC has been providing technical and policy advice to advance critical issues in cyber security field for decades and our quarterly Cyber Security Forum has been a bridge between industry, government and academia for over 16 years. This submission has been developed through a working group of ITAC members with broad consultation across the Association. The first section considers key challenges facing Canada and the cyber security industry and puts forward 12 recommendations under three themes. The second section provides direct responses to 14 of the consultation questions posed through the government's consultation document *Security and Prosperity in the Digital Age*.

As Canada's economy has become increasingly digital, protecting critical assets from criminal threats and international espionage needs to become a national priority on par with traditional physical defense. Cyber attacks have already had a measurable adverse impact on Canada, totaling billions of dollars. The ICT sector is the nervous system of Canada's economy. Over $174 billion in electronic funds traverse Canada's telecommunications network every day, and cyber crime has already had negative impacts on Canada's economy totaling billions of dollars.[1] Protecting assets from cyber attacks requires the collaboration of a wide range of actors and technologies across the public and private sector. It is critical that government and Canadian society recognize that Canada is now a fully digital economy and cyber security is itself critical infrastructure.

Trends and Drivers

Cyber threats are nothing new–the first virus was discovered 30 years ago. However, since the federal government last developed a cyber policy in 2010, the threat landscape has evolved significantly. New applications of technologies–whether through the expansion of mobile devices, smart buildings and cities, autonomous devices or the rapidly expanding Internet of Things– have created a host of new vulnerabilities and attack vectors.

Major actors from international organized crime, nation-state cyber-espionage organizations and hacktivists have escalated the severity and complexity of the threat, applying significant resources and skills to defeat enterprises that do not have robust defence-in-depth security. Over the past year, a number

[1] Study on the Analysis of Darknet Space for Predictive Indicators of Cyber Threat Activity –Communication Security Establishment, Bell Canada and Secdev Cyber Corp, 31 Mar 2011

5090 Explorer Drive, Suite 510, **Mississauga**, Ontario, Canada L4W 4T9
Phone 905-602-8345, Fax 905-602-8346
220 Laurier Ave. West, Suite 1120, **Ottawa**, Ontario, Canada K1P 5Z9
Phone 613-238-4822, Fax 613-238-7967

of large public institutions, including several hospitals and the University of Calgary, have found themselves victims of ransomware. In particular, the insider threat vector continues to pose a growing concern, whether from disgruntled employees or hacking of credentials by external actors.

In the face of these persistent threats, old concepts of cyber security based on prevention and protecting the perimeter are becoming quickly outdated. Discussions around security often emphasise resiliency, emergency management and disaster recovery, thus establishing a policy of failure as the starting point to a strategy on cyber and critical infrastructure protection. Understandings of cyber vulnerabilities needs to proactively expand and consider networks, storage and endpoints throughout the supply chain. Businesses need to move from the mindset that getting hacked is an inevitability and refocus their efforts on the fabric of cyber security shifting the unit of protection from network to data. In the face of these rapidly evolving and persistent cyber threats, Canada has a long way to go to secure our physical, economic and digital assets. Canadian businesses across industry sectors do not view cyber threats or vulnerabilities with the seriousness appropriate to the risk. There is clear evidence of aggressive and sophisticated cyber threats, widespread attacks and measurable losses affecting all critical public and private sectors in Canada.[2] The combined costs of attacks by nation-states, organized crime and hacktivists in one year against the public sector were estimated at $8.5B. Leading with a react and recover strategy is unaffordable. Currently only 50% of companies have documented incident procedures that are followed and tested and 43% are performing only periodic vulnerability assessments.[3] While the federal government has worked for over a decade to raise awareness of cyber threats among citizens and businesses, stronger measures are needed to meet the growing threat and to ensure the physical, economic and digital security of Canadians.

Governments' Unique Role

The international, intelligence-driven nature of cyber security gives government a unique and central role to play. Certain areas government has sole responsibility for include:

- Law enforcement
- Access to privileged cyber intelligence.
- The ability, through Statistics Canada, to collect valuable economic data, including on cyber security incidents.
- The ability to support the development and deployment of civic and economic protections, including cyber security technologies, which may not have a market outside of government.

It is important that government recognize these unique roles and abilities, and consider how to leverage partnerships with industries without duplicating activities in the private sector. For instance, governments have unique views of cyber attacks. However, rather than developing solutions in-house, the government should develop mechanisms to share information with industry in order to help industry develop products to meet emerging situations.

[2] Darkspace Project, Combating Robot Networks and their controllers Study, Night Dragon, Aurora, Koobface, Shadows in the Cloud, McAfee Annual threat report and GhostNet et.al.
[3] Deloitte 2015 Cybersecurity Survey. http://www2.deloitte.com/ca/en/pages/risk/articles/cybersecurity-survey-2015.html

Major Challenges Facing Canada's Cyber Security and Cyber Industry Growth

1. Shortage of Cyber Security Talent

A common challenge across the technology industry is the lack of talented staff to build, integrate and deliver the services that keep businesses productive and secure. Nowhere is this more the case than in the highly specialized field of cyber security.

While 65 Canadian post-secondary institutions offer courses on cyber security, unlike our competitor nations Canada has not developed a national strategy to ensure an adequate supply of trained cyber security professionals.[4] This not only presents a barrier to the growth of Canada's cyber security industry but also has implications for Canada's long term security.

2. Cultural Challenges with Cyber Security

Cultural issues also play a large part in the adoption and implementation of effective cyber defence. Many organizations have policies and procedures in place, but fail to effectively implement and maintain them. Security is still focused at the technology level and there is a perception that another security product will solve all security problems. This is a failure to understand that no single technical safeguard alone can secure an enterprise. Instead there must be an integrated approach between security-by-design, the application of proven standards and processes, and a culture of compliance and accountability.

In addition, senior management at the executive level needs to be engaged and accountable for ensuring that significant cyber risks are addressed to maintain a balanced and managed state of risk. Above all else, cyber security must be seen as enabling, not impeding, business. Properly designed enterprises must provide a secure environment that facilitates business innovation and scalability. Security processes must never be seen as so expensive, complex and tedious that they discourage adoption and implementation. This is a significant problem at present in industry, and particularly in government.

3. Lack on Dependable Cyber Data and Information Sharing

Cyber security is heavily reliant on information sharing between government and among competitors to ensure mutual safety and security. There is, however, a completely understandable reluctance among businesses to share information and publicize that they've been hacked. If businesses want to share information with law enforcement or government, it is often unclear who businesses should contact and how information could be shared confidentially. There is also a lack of dependable statistics on the scope of cyber threats facing Canadian citizens and businesses.

4. Uncoordinated Approach to Cyber Innovation and Industry Development

Cyber security is a fast growing global industry, and Canada is fortunate to have developed an international reputation for our innovative cyber security firms. Clusters of companies have formed

[4] For more information on post-secondary cyber security courses and programs in Canada see SERENE-RISC's Canadian Cybersecurity Course Directory: https://www.serene-risc.ca/en/news/current-cybersecurity-education-in-canada

across the country. Between 2011 and 2015, Canada had the 3rd highest number of cybersecurity venture capital deals behind the US and Israel.[5] Because of the state-level involvement and investment in cyber security technologies, government has an important role to play in growing Canada's cyber industry. Competitors including the US, Israel and the UK have made significant investments in cyber innovation centres as well as coordinated industry and export development activities. If Canada hopes to realize the potential of our cyber industry, government needs to work with industry to take a more strategic approach to sector development.

5. Lack of Coordination within the Federal Government

Across the federal government, multiple departments have seemingly overlapping mandates around cyber security. This can make it very challenging for businesses to know who in government they should be reaching out to and working with. Federal cyber procurement can also be frustrating for industry. For instance, while Treasury Board Secretariat establishes some uniformity of standards for purchasing security products – departments still seem free to make purchasing decisions outside of those standards. The Treasury Board Policy for Security Assessment and Authorization (SAA) is also burdensome, costly and time consuming for industry as well as somewhat outdated as allies are increasingly adopting active cyber defense approaches which can better adapt to emerging threats.

ITAC Recommendations

In the section of the consultation document entitled "Canada's Way Forward on Cyber Security" the government sets out five principles "for a renewed cyber security approach." Overall, ITAC supports these principles. They provide a balanced approach and recognize the broad challenges, threats, vulnerabilities and opportunities facing Canada in the cyber realm. This section also sets out three potential areas for action: Resilience; Cooperation and Capability, and; Cyber Innovation. ITAC would like to put forward the following recommendations for potential actions in these action areas.

1. Resilience: Encourage Business Adoption of Cyber Protections and Public Awareness of Threats

The government has an important responsibility to ensure that Canadian businesses are adopting appropriate cyber protections that guarantee the physical and economic safety of Canadians. Government cyber security awareness plans have been around for years, but many businesses are still unaware, unable or unwilling to implement appropriate cyber protections. Government needs to develop a multipronged strategy for improving the cyber resiliency of Canadian business and public awareness of basic cyber hygiene. This should include:

1.1. Implement a cyber certification program as a basic minimum standard

A government sponsored certification program will help demystify the complexity of the cyber security environment and will make it easier for businesses ensure they meet basic cyber security protections. It will also help individuals and other companies establish trust that the businesses they work with take cyber security seriously and create a mechanism to protect their supply chain. The UK's Cyber Essentials program provides a strong base on which the federal government can learn and

[5] Source: CB Insights.

build. There could also be an opportunity to build on the OFSI Cyber Security Guidance self-assessment that was rolled out to federally regulated banks in 2013.

Whatever standards or practices are developed, the focus should be on establishing affordable, cost-effective and operationally practical guidance if it to be adopted on a broad basis. The guidance should be pragmatic and avoid unnecessary burden, reporting or process for process sake.

1.2 Implement tax incentives and other nudges to encourage businesses to regularly conduct basic cyber risk assessments.

The federal government interacts commercially with businesses in a wide range of avenues, ranging from procurements to R&D funding. The government should use these leavers to create nudges that encourage businesses to regularly undertake cyber risk assessments and incentivize material mitigations. For example:

- Federal R&D funding, through SR&ED, IRAP or other programs, should require cyber risk assessments prior to funds being delivered–both as a best practice and as a way to protect taxpayer investments in the creation of IP from industrial espionage.
- Risk assessment or Canadian Cyber Essentials certification should be required to participate in the federal government supply chain and bid on government projects.
- Introduce a tax credit for companies that can demonstrate compliance with higher-level cyber standards, especially in areas of critical infrastructure, to help offset the costs of establishing and maintaining compliance.
- The government should work with large Canadian organizations to encourage basic cyber assessments or Canadian Cyber Essentials certification to participate in their supply chain.
- The government should work with financial institutions to help Canada develop a mature cyber insurance market based on regular cyber risk measurement and mitigation.

1.3 Invest in Cyber Protections without a Broad Market

Some cyber security technologies can provide broad protection to Canadians but on their own have limited market outside government. The government should be willing to work with industry to develop, fund and purchase intelligence or protections as a public good and protection for the digital economy. Specific technologies government should invest in include:

- Upstream cyber protections to "clean the pipes" at the telecom level.
- Government specific technologies aimed at protecting critical infrastructure and resources from espionage.
- Purchasing and disseminating proprietary cyber intelligence gathered by private industry to help protect businesses that may not have resources to acquire the intelligence independently.

1.4 Reinvent Cyber Awareness and Hygiene Programs

Canadian citizens and businesses need to be better informed about cyber threats and basic hygiene that can help protect them from common threats, like changing defaults and applying complex passwords. Part of this should be a new, higher profile cyber awareness strategy that uses clear messaging and

techniques like design thinking and behavioural economics to encourage Canadians to implement best practices. The federal government should also work with provinces to improve cyber security education throughout the school curriculum especially middle and high school.

Canada needs leaders promoting a new approach to fighting cybercrime. The new approach is to create a "Cyber Safety Culture" in businesses and for individual citizens. This can be accomplished after realizing that technology solutions can only solve part of the problem because the vast majority of cyber vulnerabilities are created by individuals' behavior, hence the need for focus on cultural change:

- Present the risk clearly and accurately in simple business terms.
- Provide solutions that are accessible and understandable.
- Provide solutions that are affordable and non-disruptive.
- Provide solutions that find the balance between running a business and making that business secure**.**
- Constantly refresh the messaging using engaging and interesting ways to overcome the sterile messaging usually associated with cyber security.

Canada should also make a more concerted effort to work with industry to more visibly promote October as cyber security awareness month at a national level.

2. Cooperation and Capability: Develop Cyber Talent and Centralize Cyber Security

2.1 Address Cyber Talent Gap

Canada has a significant gap in cyber security talent. Ensuring a steady supply of cyber professionals needs to be a priority for the federal and provincial governments. Other jurisdictions (e.g. U.S., Israel, U.K.) are far ahead of Canada in deploying coordinated strategies to develop cyber talent. Canada should follow and build on these examples by:

- Supporting youth cyber training and national-level competitions to help identify talent early, and encouraging young people to pursue cyber security careers.[6] Canada should work to help our young people "own the podium" in cyber sports.
- Supporting undergraduate, post-graduate and experiential learning programs to help Canadians train and re-train for careers in cyber security. ITAC has long worked to facilitate industry involvement in the development of talent development initiatives that ensure learning outcomes that meet the needs of employers.[7]

[6] The largest cyber youth program in the world is the U.S. Cyber Patriot program which in 2015 had 3,379 teams of high school students participating in national competitions. Cyber Patriot has also expanded to include a middle school/jr. high program. The U.K. has created its Cyber Centurion program, which aligns with the U.S. initiative. For several years, students from Winnipeg have competed in the Cyber Patriot competitions through an initiative called the Canadian Cyber Defense Challenge. Earlier this year ICTC announced the creation of a larger Canadian initiative, dubbed Cyber Titan, which aims to take the competition national across Canada.

[7] ITAC has a proven track record of working with government and post-secondary institutions to deliver programs that meet the needs of employers (including our Business Technology Management program, currently at 19 universities, which has a specialty stream in cyber security). We are currently working with the Munk School at the University of Toronto to develop

2.2 Centralize Federal Government Cyber Security Functions and Communications

ITAC members have raised concerns that there is currently too little communication and coordination of cyber security initiatives across federal departments. The federal government needs to take a more holistic approach to protecting its own cyber risks and coordinating security efforts with provinces, municipalities, the broader public sector and private industry.

To this end, ITAC recommends the federal government follow the example of the United States and appoint a federal **Chief Information Security Officer.** The federal CISO, based in Treasury Board Secretariat CIO branch, would work with federal CIO and CTO to coordinate cyber protection across federal departments, be the lead for coordinating activities with industry and other orders of government, and serve as the public face of cyber security in Canada (along with the Minister of Public Safety and Emergency Preparedness). A federal CISO would centralize accountability and ensure collaboration and coordination across PSC, CSE, DND, SSC, TBS and other departments. The CISO should also regularly meet with CISOs of major Canadian corporations and key government and industry groups—potentially through the creation of a National Cyber Security Advisory Group—to ensure cyber coordination and collective security.

Part of the CISO's mandate should be working with industry to improve the federal government's accreditation program by moving away from the current Treasury Board Policy for Security Assessment and Authorization and instead look at how other jurisdictions provide security on an active basis that is efficient, adaptive and flexible.

2.3 Centralize Cyber Law Enforcement Capabilities

Canadian law enforcement should centralize their cyber crime resources into a single-window National Cybercrime Coordination Centre. A single-window centre will make it easier for businesses to know who to call when their systems have been compromised, and will help law enforcement investigate and respond to cyber crime across jurisdictions. This should include a secure exchange mechanism and strong data protection arrangements so private sector organizations feel comfortable sharing potentially confidential information with law enforcement. Most importantly, for a coordination centre to get business to voluntarily report incidents of cyber crime, it needs to be able to demonstrate results and prove its value to businesses and Canadians.

2.4 Improve Cyber Security Communications with Industry and the Public

Presently the federal government's industry communications initiatives on cyber security issues are relatively low profile. The federal government should work to improve the business value of its cyber security communications with industry. For example, the U.S. Department of Homeland Security has a very visible and useful cyber security alert program. Bulletins and alerts issued through U.S. Computer Emergency Readiness Team (CERT) are critical information for all cyber security organizations and IT

new industry standardized curriculums focusing on cyber security. The government should continue to support industry and employer involvement with post secondary institutions to ensure graduates have the cyber skills employers need.

infrastructure operators. The U.S. National Institute for Standards in Technology (NIST) is also extremely proactive with industry in the U.S. at developing standards and best practices for both government and industry.

One potential option is that Canada develop a parallel, shared, or coordinated program with the U.S. The net effect would be visibility and support for effective cyber security in Canada, and a stronger alignment with U.S. partners on our shared security interests.

3. Cyber Innovation: Create Platforms for Government-Industry Collaboration

The global cyber security industry is expected to grow to over $170 billion by 2020.[8] Canada already has a strong global reputation as a trusted provider of cyber security products and services. There are several clusters of innovative cyber firms established across the country and leading-edge cyber research at our post-secondary institutions. While growing this industry is a focus for several departments at both the federal and provincial level, ITAC believes there are several gaps in the cyber innovation ecosystem that the federal government should work to address.

3.1 Create a National Centre for Cyber Security Innovation

The U.K., Israel and the U.S. have all created cyber innovation centres aimed at connecting industry with experts in the government security establishment.[9] In several of these examples, industry and government security experts collocate to help facilitate information sharing and the demand-driven development of new protections and products. ITAC believes Canada should pursue a similar model by creating a centre or network of centres, so industry is able to benefit from government expertise and develop new, leading-edge cyber products.

3.2 Fund Cyber R&D

The government has invested, both directly and through R&D tax credits, in developing innovative cyber security technologies in Canada. These investments in industry and academia need to continue. Direct investment should focus on emerging areas where Canada can form a niche, including: AI and machine learning, quantum secure cryptography, the internet of things and fintech security. The government should also continue to support academic/industry collaboration though organizations like the National Research Council and SERENE-RISC.

3.3 Expand Federal Pilot and Cyber Technology Demonstration Programs

It can be extremely challenging for Canadian firms to successfully export cyber security products and services without first having proven the technology at home. Sales and certification by government add unique credibility that can dramatically improve a business's chances of selling technology to foreign governments. The federal government currently has several programs aimed at piloting new technologies, but they are small compared to similar programs in competitor jurisdictions.[10] The federal

[8] See: ww.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity-market-reaches-75-billion-in-2015-expected-to-reach-170-billion-by-2020/. Gartner predicts cyber spending will grow 7.9% to reach $81.6 billion world wide in 2016. See: http://www.gartner.com/newsroom/id/3404817.

[9] For examples see the UK's GCHQ Cyber Innovation Centres or Israel's CyberSpark.

[10] For example, for example, the U.S. Small Business Innovation Research (SBIR) program allocates between $2-3 billion annually for procurements from SMEs. See Section 7 of: Independent Panel on Federal Support to Research and

government should either create a new program to facilitate the piloting of new cyber technologies within the federal government or increase funding for technology demonstration programs, like the Build in Canada Innovation Program[11]. DND should also use their Tech Demo program to encourage the wide-scale demonstration of cyber security technologies.[12]

An expansion of demonstration programs should also align with general efforts to streamline the technology procurement process across the federal government so it is easier for technology vendors to inform the federal government of their products and compete for projects.

3.4 Develop a Canadian Cyber Export Strategy

Many areas of the federal and provincial governments are doing a great job at helping cyber firms access foreign markets and attend international trade events; however, compared to other jurisdictions, like Israel or the UK, Canada's could take a more strategic approach to building our cyber industry.[13] The federal government should work with provinces to develop a more holistic strategy for growing Canadian cyber exports, including:

- Working with industry to develop a Canadian cyber brand.
- Make it easier and less costly for cyber products to get the Canadian government's "seal of approval," either through demonstration programs or certification by CSE or another body.[14]
- Coordinated trade missions abroad and innovation showcases domestically so growing Canadian cyber firms are able to establish anchor customers at home.

Conclusion

Now is an important moment for cyber security in Canada. As our work and lives become increasing connected, the federal government has an essential role to play to ensure the physical and economic security of Canadians. There is also a real opportunity for the Canada to take advantage of new market opportunities and make the cyber industry a part of our sustained prosperity.

ITAC and our members look forward to working with government to advance the outcomes of this consultation. While the topics in this consultation are broad, we would be pleased to provide specific details on any recommendations put forward at the government's convenience.

Development. 2011. *Innovation Canada: a call to action*: http://rd-review.ca/eic/site/033.nsf/vwapj/R-D_InnovationCanada_Final-eng.pdf/$FILE/R-D_InnovationCanada_Final-eng.pdf

[11] The Build in Canada Innovation Program currently has a dedicated envelope of $40 million annually. This is significantly smaller than the $2-3B invested in SMEs by the U.S. Federal Government through various technology demonstration programs. Guidance for cyber products also highlights that the program is not a substitute for certification. See: https://www.ic.gc.ca/eic/site/icgc.nsf/eng/07483.html

[12] While some cyber security applications may be eligible for the DND TechDemo program, the program does not explicitly encourage demonstrations of cyber technologies. TechDemo also have very low profile within the cyber industry.

[13] The U.K. Cyber Growth Partnership is a great approach Canada could seek to emulate. See: https://www.techuk.org/cyber-growth-partnership

[14] ITAC members have noted that it currently takes months and costs hundreds of thousands of dollars to get certification from CSE.

Part B: Answers to Specific Questions

Trend 1: Evolution of the Cyber Threat

How can law enforcement better address the growing challenge posed by cybercrime (for example, through training and capacity-building, equipment, partnerships, innovative initiatives)?
Are there barriers to reporting cybercrimes (or suspected cybercrime) to law enforcement agencies? If so, what are they?

For law enforcements to better fight cybercrime ITAC recommends the creation of a single-window Cyber Crime Coordination Centre to serve as a dedicated, centralized law enforcement resource. This should include a secure exchange mechanism and strong data protection arrangements so private sector organizations feel comfortable sharing potentially confidential information with law enforcement.

Law enforcement will also have to form a stronger relationship with Canada's cyber security industry. Elements like innovation, capacity building and cyber intelligence gathering should be outsourced to experts in the industry who will be able to help police more effectively respond.

How can public and private sector organizations help protect themselves from cybercrime, such as the threat of ransomware attack, fraud and identity theft, and what tools do they need to do so?
What do public and private sector organizations need to protect themselves from advanced cyber threats (for example, tools, capacity, information)?

To start, many organizations need to improve their basic cyber hygiene and put in place baseline controls and protections to keep their systems safe. A government sponsored security scheme similar to the UK's Cyber Essentials will help cut through the complexity and establish a minimum security standard across the economy. While this will not protect all organizations from attacks, it will at least help protect less sophisticated organizations from the most common attack vectors.

The government also needs to play a role in helping organizations acquire information about potential attack vectors by acquiring and disseminating threat intelligence through channels like CCIRC and improved cyber bulletins to industry. It also needs to help organizations ensure they have the capacity to onboard that intelligence by ensuring Canada has an adequate supply of cyber security professionals.

More broadly, all organizations need to foster a better understanding of current and emerging threat actors and attack vectors. Frontal attacks on public-facing perimeters are becoming less common and instead major threat actors are seeking to penetrate and exploit their targets from within using hijacked credentials and privileges (e.g. phishing) and establishing covert exfiltration channels. Endpoints throughout the supply chain, including the emerging internet of things, can also create new vulnerabilities. Most worrisome is that, with that the time between compromise and discovery (i.e. 'dwell' time) is often 1-2 years. It is time both government and industry stopped relying solely on perimeter 'bastion' defences and instead consistently adopted security by design, data centric security and layered defence in depth.

There are new technologies now available that can provide aggregated information from endpoint threat detection software. This information can be organized, visualized and presented to show cyber

metrics/posture across an entire organization, customized to targeted viewers. This enables preventative action before breach, and rapid detection and effective response after a breach.

Policing in Cyberspace

In a digital age, security and privacy go hand in hand. How can cybercrime be addressed in a manner that respects Canadians' privacy rights and protects public safety?

In any democracy, balancing security and freedom, including privacy, is a constant challenge. Openness and transparency play key roles in establishing trust and helping law enforcement strike the right balance.

Earlier in this document we suggest the creation of a "blue ribbon" Canadian National Cyber Security Advisory Group, led by a new Chief Information Officer for Canada. This group, which could include industry and government leadership as well as representatives from civil society and the Office of the Privacy Commissioner of Canada, would provide input on proposed policy approaches, including on how cyber responses impact personal privacy. The government should also avoid imposing any non-voluntary requirements on IT service providers which could potentially impact the confidentiality and security of their clients. Failure to do so could drive clients away from Canadian providers to offshore services and undermine trust in Canada as a secure IT partner.

What are the constraints to information sharing on advanced cyber threats and associated vulnerabilities?

Culture: Many organizations are still avoid sharing sensitive information outside their organization out of fear of a stigma that will come from being the victim of a hack. This makes it much harder to establish mutual verification on threats and vulnerabilities. To improve our collective cyber security, Canadian businesses need to move from a "need-to-know" culture to a "need-to-share."

Government: There is currently a lack of uniform data classification within the public sector (protected status vs. classified) which makes it challenging to share information externally. There is also ambiguity in mandates to combat cyber crime across the public and private sectors. Government and law enforcement lack a secure exchange mechanism for sharing data on cyber crime. The creation of a federal CISO and a Canadian Cybercrime Coordination Centre should help address these challenges.

Cost: Sharing information on cyber crime can be very costly and time consuming for an organization. To encourage more businesses to devote resources to sharing information, the value proposition needs to be improved.

How can public and private sector organizations work together to build Canadian' awareness of cyber security issues (e.g. joint online training initiatives)?
How can individuals be better informed about how to recognize and react to a cybercrime or a cyber security vulnerability?

Greater efforts need to be made by government to raise general awareness, through initiatives like Cyber Security Awareness Month and online training programs. Cyber security is complex, but the government should make efforts to simplify messaging to focus on cyber hygiene essentials like changing passwords

and checking attachments. Techniques like behavioural economics should also be used. The creation of a Canadian CISO, to act as the face of cyber security in Canada could also help with awareness efforts.

Canada needs leaders promoting a new approach to fighting cybercrime. The new approach is to create a "Cyber Safety Culture" in businesses and for individual citizens. This can be accomplished after realizing that technology solutions can only solve part of the problem because the vast majority of cyber vulnerabilities are created by individuals' behavior, hence the need for focus on cultural change:

- Present the risk clearly and accurately in simple business terms.
- Provide solutions that are accessible and understandable.
- Provide solutions that are affordable and non-disruptive.
- Provide solutions that find the balance between running a business and making that business secure**.**
- Constantly refresh the messaging using engaging and interesting ways to overcome the sterile messaging usually associated with cyber security.

Trend 2: Increasing Economic Significance of Cyber Security

How can Canadian businesses be encouraged to adopt better cyber security regimes – particularly SMEs?

The government should develop a certification scheme similar to the UK's Cyber Essentials that cuts through complexity and helps establish a baseline standard for all business. Government funding programs and other government interactions with business (e.g. procurement) should encourage cyber risk assessments and mitigation as a common industry practice.

What steps should be taken to ensure that networked and emerging technologies (e.g. IoT) are cyber secure?

Government should support, through bodies like the Standards Council of Canada, industry-led efforts towards the development of standards and protocols that ensure security and privacy by design. As multiple standardization projects are currently in process around the world, the government should avoid introducing regulatory requirements that limit innovation or restrict businesses to particular approaches or technologies. The government should also work with industry to ensure consumers are aware of how to improve the security of their protected devices (e.g. changing default passwords).

What are the barriers to strengthening cyber systems in critical infrastructure?

A first step needs to be recognizing that cyber security protections are critical infrastructure, and potential cyber vulnerabilities need to be considered at the core of any infrastructure development project.

Currently, the Government of Canada has a Supply Chain Integrity Program (SCIP). However, it is fractured and its implementation poses challenges from an industry standpoint. SCIP vetting is done on a project by project basis and industry has no knowledge of what products/technologies have been previously vetted and approved, making the design and selection of technologies for government bids problematic. It is likely that a winning bid could find that they are forced to undertake an expensive

redesign after the contract has been award, as certain technologies are not approved. It is therefore strongly recommended that the Government publish a running list of vetted products from which industry suppliers could chose components. Vendors should be able to request that their products be vetted and added to the list to ensure a level playing field.

What are the constraints to information sharing and engagement related to protecting cyber systems of Canada's critical infrastructure?

See the above comments for "Policing in Cyberspace."

Currently, certain regulatory schemes in critical infrastructure, such as SCADA, are managed from the US and operate as revenue-generating businesses. Many Utility providers find that they do not adequately reflect the Canadian context and are very expensive to participate in. For these reasons, some large utility operators opt for alternate standards–either their own, or others. The net result is an inconsistent patchwork of standards related to critical industry.

Trend 3: Expanding Frontiers of Cyber Security

What information (data, metrics) would contribute to a better understanding of cyber security issues in Canada?

The U.S. Department of Homeland Security has a very visible and useful program for cyber security. Bulletins and alerts issued through the US CERT are critical information for all cyber security organizations and IT infrastructure operators. Moreover, the U.S. NIST is extremely proactive with industry in the U.S. to develop standards and best practices for both government and industry.

By contrast, Government in Canada takes a low profile approach and gives the impression that cyber security is not a priority. We recommend Canada develop a parallel program, possibly shared/coordinated with the U.S. The net effect is visibility and support for effective cyber security for government and industry in Canada. It would tell our U.S. partners that we are a player, that we take this pervasive threat seriously, and would demonstrate that Canada and the U.S. are working together to deal with our mutual security and interests.

What is needed to improve Canadian innovation in cyber security?

Canada should follow the lead of competitor nations by developing platforms for the government security establishment and industry to collaborate on developing innovative cyber security technologies, similar to the UK's GCHQ Cyber Innovation Centres and Israel's CyberSpark. Canada should continue broad funding (e.g. SR&ED) as well as targeted direct investments into cyber security fields where Canada can develop a niche.

Canada should help cyber businesses demonstrate and prove their new products by providing innovation focused pilot/procurement programs, including expanding the Build in Canada Innovation Program and opening the DND Tech Demo program to include cyber security products.

Canada should develop a holistic cyber export strategy including national branding, coordinated domestic and international trade missions, and more accessible certification programs through CSE or other agencies.

What measures could be taken to improve the availability, relevance and quality of cyber security training?

Cyber security training should begin at a young age, building general awareness in middle and high school. The government should follow the lead of other leading jurisdictions by supporting youth cyber competitions that identify talent and encourage young people to pursue cyber careers. The government should work with industry and post-secondary institutions to develop common core learning outcomes for cyber security programs across the country that ensure graduates have the skills businesses need. The government should also support post-graduate and experiential learning programs to create a leading-edge cyber workforce. The ICT industry, through ITAC's Talent division, has been actively working with post-secondary institutions for many years on similar programs, and we would be interested in opportunities to collaborate on building Canada's cyber talent base.

For further information, please contact David Messer, Sr. Director Policy, ITAC at dmesser@itac.ca