Cambridge Forums Inc.

2016 Cyber Security Forum

Addressing the Internet of Things Security and Privacy Challenges

Editor: Gregory Higgins, Castlebar Communications

8/31/2016

The 2016 *Cyber Security Forum*:
Addressing the Internet of Things Security and Privacy Challenges

Executive Summary

Canadians are facing an ever growing number of cyber threats. Denial of service attacks and data breaches cost the Canadian economy billions annually, and individual Canadians are increasingly exposed to identity theft and the loss of valuable personal information at the hands of cyber criminals.

While the nascent Internet of Things ("IoT") industry offers the promise of tremendous efficiency and convenience gains for businesses and consumers, security and privacy must be made paramount in the development of IoT solutions for widespread use.

In light of these concerns, the *Cyber Security Forum ("Forum")* brought select cyber industry leaders together in May 2016 to identify challenges and make recommendations to protect Canadians from cyber threats and increase cyber awareness and resilience.

For IoT Security, *Forum* participants recommended the following actions:

Increase Canadians' Cyber Savviness

For government and industry, this means working together to promote a cyber savvy workforce and cyber savvy consumers through targeted public awareness and education programs.

Develop a National Cyber Policy Framework

The Government of Canada ("GC") and Canadian private and Non-Governmental Organizations ("NGO") sectors can turn challenge into opportunity by building a national cyber policy framework that supports cyber innovation and capacity building, while helping businesses and consumers detect and mitigate cyber threats and vulnerabilities.

Adopt an Enterprise Risk Management Approach

Government and industry stakeholders must reach agreement on IoT network security priorities, identifying where and how critical data should be stored and how it should be shared among IoT network stakeholders. Collaboration will also be key in establishing sector *risk profiles* and corresponding security standards and protocols for prevention of and response to IoT security failures.

Incentivize Security Innovations

The GC can show creativity and commitment by incentivizing industry to incorporate security features into IoT networks through tax credits and targeted funding. Industry can play a complementary role by leveraging its IoT networking presence in Canada to influence foreign IoT suppliers to adopt greater security consciousness in product design and production.

For IoT Privacy, *Forum* participants recommended the following actions:

Develop a New IoT Social Contract

Network and product providers should initiate a new *IoT social contract* in which consumer privacy concerns and expectations are recognized as an implicit 'duty of care'. For their part, consumers must demand plain-language end-user license agreements and features that allow them to better gauge privacy threats and vulnerabilities.

Achieve Clarity on Use of Secondary Data

Government, industry and consumer advocacy groups must work together to clarify current uses of secondary data and establish parameters for acceptable secondary data use, storage and exchange.

Set Standards for Data Validity and Reliability

Industry and government must establish a data validity/reliability model in which IoT devices and applications are classified according to common standards of data accuracy and reliability. This model could encompass standards of data longevity, placing time limits on data use to protect individual privacy.

Incorporate 'Privacy by Design' Principles

The Province of Ontario's *Privacy by Design* concept – which aims to protect personal privacy by embedding it into IoT technology design, business practices and physical infrastructures – should be adopted as a universal privacy standard by government, industry and IoT consumers.

Forum participants identified two key future steps in IoT Security and Privacy:

Develop a 'Secure Canada' Approach

Using a shared leadership approach, Canadian industry and government could improve Canada's cyber posture by creating and funding an entity charged with developing a 'Secure Canada' approach to IoT security and privacy. This entity would collaborate with senior GC policy makers to develop a national framework for cyber competencies, roles and responsibilities at all levels of society – from consumers and small businesses to large corporations and government.

Promote Responsible Cyber Behaviours

Industry, government, NGO and education stakeholders must demonstrate their commitment to cyber security and privacy by investing in programs that promote increased workforce capacity through digital literacy and technological awareness as well as greater personal responsibility for behaviours on IoT devices and networks.

The 2016 Cyber Security Forum:
Addressing Internet of Things Security and Privacy Challenges

Context:

A Rapidly Expanding Digital Universe

The IoT, which connects the physical world and human beings to the digital cloud, promises huge efficiency and convenience gains and enormous social and economic benefits in the decade ahead.

By 2020, experts estimate that at least 50 billion smart devices will be connected to the cloud. With built-in digital sensors and actuators, these devices enable scalable cyber-physical systems such as personal e-health monitoring and smart appliances in homes, cloud computing and advanced data analytics at work, and smart systems for managing public services such as transportation and healthcare in communities. Together, these IoT technologies are revolutionizing the way Canadians live and work.

Objectives:

A Collaborative Approach to Cyber Threats and Vulnerabilities

As IoT efficiency and connectivity spark rapid technology uptake, security and privacy are taking a back seat to consumer convenience and industry growth. With a view to addressing this imbalance, Cambridge Forums Inc. invited select corporate CEOs, CIOs, and other in-house cyber resources, along with a select group of external regulatory, legal, compliance, information technology and security experts, to Langdon Hall in Cambridge, Ontario from May 29-31, 2016 to discuss IoT security and privacy challenges.

About the *Cyber Security Forum*

The annual *Cyber Security Forum* is an exclusive retreat of leaders in the industry aimed at addressing current and emerging cyber threats and vulnerabilities, benchmarking best practices for safeguarding against such threats, and shaping Canadian public cyber security and compliance policies and industry practices. The *Forum* is owned and operated by Cambridge Forums Inc., who develops similar learning opportunities for executives and professionals in a variety of sectors nationally and internationally.

The "*Forum* Community" provides members with an opportunity to discuss common challenges and those specific to their industry under the Chatham House Rule:

"When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."

The *Forum*'s private learning environment allows participants to candidly discuss common issues, learn from different perspectives and receive guidance from peers and professional advisors.

This report, which summarizes *Forum* discussions and recommendations, represents an important first step in the development of a comprehensive framework for collaborative action on IoT security and privacy challenges across private, public and non-governmental sectors in Canada.

Internet of Things — Security Scene Setter and Discussions

The *Forum*'s Internet of Things security discussions began with scene-setter presentation from a senior Government of Canada representative on cyber threats to IoT infrastructure sectors vital to Canadians' health, security and prosperity, including transportation, telecommunications, food and water, energy and healthcare.

Government of Canada Cyber Security Review

"I expect all ministers to do their part … to improve economic opportunity and security for Canadians. In particular, I will expect you to:

Lead a review of existing measures to protect Canadians and our critical infrastructure from cyber-threats."

— From the Prime Minister's Mandate Letter to the Minister of Public Safety and Emergency Preparedness, November 2015.

In 2015, direct attacks and data breaches against critical infrastructure ("CI") from threat actors ranging from cyber hacktivists to hostile states to organized crime cost the Canadian economy billions in lost sales and productivity and untold damage in loss of business reputation and consumer confidence.

While CI network owners have taken significant steps to protect electronic technologies from increasingly sophisticated cyber intrusions, the growing interconnectivity and interdependence of the IoT – and proliferation of IoT network devices across medical, transportation, health, food and retail sectors – is amplifying threat vulnerabilities.

Identifying Cyber Threat Drivers

In the face of IoT-related threats, the GC representative called on government and industry to adopt a holistic, collaborative approach to identifying cyber threat drivers.

The Government of Canada has taken the first step with its launch of a cyber security review under the direction of the Minister of Public Safety and Emergency Preparedness. The review is engaging CI owners and operators on multifaceted policy and regulatory measures aimed at increasing Canada's cyber resilience, while facilitating increased digital innovation and capacity building among IoT network operators.

The Government of Canada presentation was followed by small group discussions on specific threats to Canada's IoT data collection, use and storage and the types of policy and regulatory measures that may be required to address them, with an underlying emphasis on balancing IoT security and privacy concerns.

IoT Security Recommendations

1) Reverse a Broken Risk Model

Today's IoT devices are designed at the top of the industry-driven risk model to favour convenience over security, resulting in an ever-widening gap between digital device use and end-user security. *Forum* participants agreed that this top-down risk model is broken. A more security-centric, bottom-up model – beginning with security savvy end users and working upward to device designers and manufacturers – is required, along with practical incentives for consumers, such as bundling convenience and security features into one package.

Participants pointed to the Canadian Standards Association's product ratings and guidelines as an example of an effective consumer-driven risk model in the non-virtual world, noting that a similar, consumer-driven risk model could be applied to products and services in the virtual world.

Risk Modelling Lessons From the Auto Sector

The auto industry experience over the past several decades shows that security standards and innovations are primarily "event-driven". When the consequences of product security failures (i.e. highway fatalities) were made clear, they sparked a shift in societal attitudes, which in turn drove demand for risk mitigation features such as turn signals, seatbelts and air bags.

When IoT consumers become comparatively well aware of potential harm from cyber threats and vulnerabilities they are likely to force a similar shift to risk mitigation/security features for IoT network devices.

2) Increase Canadians' Cyber Awareness

On a macro level, Industry and government must work together to promote a cyber savvy workforce and cyber savvy IoT consumers through targeted awareness programs.

Organizations – from private companies and NGOs to community groups and schools – must also be active promoters of cyber security protocols and practices. At the individual level, Canadians must take greater responsibility for own technological awareness, informing themselves of security risks and vulnerabilities associated with IoT device use and governing themselves accordingly. Better informed stakeholders at every level of the IoT continuum is the best means of ensuring a secure and productive IoT ecosystem in Canada.

3) Develop a National Cyber Policy Framework

Security threats and vulnerabilities inherent to the global IoT ecosystem are too diverse and complex for technology solutions alone. They require a multisectoral cyber policy framework, with contributions from Canada's regulatory, technical, educational and judicial sectors.

Canada's current cyber security strategy, adopted in 2009, needs to be updated and incorporated into a national cyber policy framework that takes account of emerging IoT security risks. This framework would take a *proactive* IoT security approach at the front end of the IoT risk continuum and a collaborative *response* approach at the back end to address cyber system failures.

Canada's private sector has taken positive steps with the creation of the Canadian Cyber Threat Exchange (CCTX), a not-for-profit organization that supports the sharing of cyber threat information and analytics across sectors and helps Canadian businesses and consumers detect and mitigate cyber attacks. CCTX's collaborative goal – to strengthen Canada's economic prosperity by better protecting Canadian businesses, governments and consumers from cyber threats and vulnerabilities – is one that resonates with all IoT stakeholders.

Following the CCTX example, *Forum* participants agreed that senior-level dialogue across government, private, NGO and educational sectors on the development of an effective national cyber policy framework is something Canadian industry must be prepared to initiate and support.

4) Anticipate Impacts of Quantum Computing

If properly implemented, a national cyber framework – and related cyber risk models, standards and protocols – can assist Canada in "future-proofing" its IoT networks.

A strong rationale for prioritizing development of this framework is that it will assist IoT network operators' adaptation to quantum computing and associated security challenges. Many *Forum* participants expressed the view that the window for action is narrow, as quantum cryptography has the potential to overtake current cyber encryption standards within the next five years.

5) Adopt an Enterprise Risk Management Approach

Equally important to IoT network integrity is the adoption and implementation of an enterprise risk management approach to IoT data security among large stakeholders such as government and the financial and telecommunications sectors.

An enterprise risk management approach identifies which IoT network areas are to be prioritized, where and how critical data is to be stored, and how it is to be shared among IoT network stakeholders.

The GC can serve as a catalyst for collaborative enterprise risk management by working with industry to establish *risk profiles* for critical infrastructure. *Forum* participants noted that risk profiling, and the adoption of corresponding security standards and protocols for the prevention of and response to IoT security failures, is particularly relevant to sectors where critical interdependence is such that a single security failure can lead to cascading failures, resulting in major industry impact.

IoT Device Regulation: Prioritizing Actuators

Forum participants were in agreement that data device security standards and protocols should focus primarily on IoT device *actuators* as the consequences of actuator failures (i.e. heart defibrillators) are much more significant than those of IoT device sensor failures (i.e. malfunctioning smartphone screen).

6) Incentivize Security Innovations

Recognizing that government legislation lags behind industry growth and innovation, *Forum* participants agreed that the most effective way for government to narrow the regulation/innovation gap is to incentivize Canadian industry to incorporate security features and sound business practices into IoT networks such as routers, switches and access points.

GC tax credits and/or targeted funding measures were seen as effective means of bolstering IoT security standards and encouraging security related research and development.

Forum participants acknowledged that incentivizing the incorporation of security features into IoT products fabricated outside of Canada, such as cars, appliances, clothing and shoes, is a significant challenge. Nevertheless, Canadian companies can play a role by leveraging their IoT networking presence in this country to influence suppliers toward greater security consciousness in IoT product design and production.

Internet of Things — Privacy Scene Setter and Discussions

The *Forum*'s IoT privacy discussion was prefaced by a scene-setter presentation from a national telecommunications executive on cyber security and privacy issues within the rapidly expanding digital healthcare sector.

A significant trend within the IoT health model is the rapid transfer of health data ownership from health providers to consumers. This transformation has given rise to numerous security and privacy concerns around third-party access to personal information, the management of personal healthcare devices – i.e. insulin pumps and implantable defibrillators – linked to IoT health networks, and the appropriate use of personal information in secondary data, including aggregate data and data analytics aimed at achieving better population health outcomes.

The presentation was followed by small-group discussions on how big data and cloud-linked devices are impacting data governance, including data consent, collection, disclosure, use and control. Particular attention was directed to the question of how to embrace the benefits data analytics without compromising individual privacy.

Health Information: a Hacker's Goldmine

Electronic health records are a popular target for cyber criminals and identity thieves because they contain valuable personal information — social insurance numbers, birth and death dates, family information, and billing information, including credit card data — that allow hackers to gain control of a person's identity and do major damage.

According to a recent Symantec *Internet Security Threat Report,* health services accounted for the largest percentage (39 percent) of data breaches in 2015.

As the Symantec report observes, "Just like any other business … in hacking it boils down to the bottom line, and hackers want the most payout for their efforts. Healthcare organizations are the latest gold mine."

Within the broader cyber privacy spectrum, participants examined the impact of industry's increasing use of cloud computing on consumer privacy and the rights of specific jurisdictions to safeguard citizen privacy by ensuring that personal data stored on cloud-based host services is afforded protection under local laws.

Participants also examined the question of whether privacy and residency concerns could be addressed by technology solutions alone, or by alternative methods such as a multi-national policy framework or strong independent oversight and transparency.

IoT Privacy Recommendations

1) Develop a New IoT Social Contract

Forum participants observed that, as with cyber security, IoT connectivity and convenience have largely trumped privacy concerns. If personal privacy is to be protected, IoT network and product providers must entertain the idea of a new *IoT social contract* in which the privacy concerns and expectations of consumers are recognized as an implicit 'duty of care'.

For their part, consumers must demand plain-language end-user license agreements that allow them to better gauge and track privacy threats and vulnerabilities and protect themselves accordingly.

Toward a Common Understanding of Privacy

Cyber privacy is a global issue that requires international collaboration to establish a common understanding of the concepts of 'privacy' and 'anonymity' in the digital age.

A common digital understanding of privacy would allow IoT consumers to distinguish between what is 'personal' and what is not, and jurisdictions to reexamine and potentially expand upon key privacy concepts such as a citizen's 'right to be forgotten'. It would also allow IoT network managers to identify which IoT components are 'privacy-sensitive' and therefore subject to enhanced security standards and protocols.

2) Introduce a Privacy Metric

IoT device transparency could also be achieved with the introduction of an IoT privacy 'metric' attached to a product labelling system. This labelling system could be similar to the one employed by the food industry, which uses the metric of 'nutrition' to indicate the intrinsic health risks/benefits of a given product.

A more personalized privacy model could also be developed in which a user defines his or her own privacy profile and adjusts IoT device settings accordingly to ensure that current applications, and future purchases, meet a pre-configured privacy comfort level.

3) Achieve Clarity on Use of Secondary Data

There is greater need for clarity in privacy and consent in relation to the use of secondary data. Individuals may consent to public access to their personal information for one particular IoT use (i.e. Facebook, Twitter), only to see their information used for other purposes, sometimes quite intrusively, further down the IoT network chain. Government, industry and consumer advocacy groups must work together to clarify current uses of secondary data and establish parameters for acceptable secondary data use, storage and exchange.

4) Develop a Modern Cyber Privacy Framework

When it comes to data governance, *Forum* participants noted that Canada's current legislative framework (*Access to Information* and *Privacy* Acts) needs modernizing in order to address IoT technological realities and to meet the requirement for greater transparency on the use, retention and sharing of IoT cloud data. Legislative amendments must also take into account the true value of electronic information, while incorporating a more modern definition of information "sensitivity".

In a global data world, Canada must work with the international community to harmonize Canadian policies with global norms on privacy governance, including basic approaches to privacy (i.e. Is it a human right or simply a preventive measure?), the reasonable expectation of privacy, which varies from jurisdiction to jurisdiction, and the prioritization of community rights and individual privacy rights (Is my data my own personal property or the property of the cloud?).

5) Segregation of Data

Effective data governance may also require the segregation of data itself into separate clouds (i.e. Justice Cloud, Energy Cloud or Transportation Cloud) to better protect personal privacy.

6) Set Standards for Data Validity and Reliability

A key challenge in the age of big data is validating data sources in the cloud. A potential solution is to identify and categorize web sites, applications and devices according to previously agreed upon standards of data accuracy and reliability. An established data validity/reliability model would add significant credibility to the notion of informed end-user consent. It could also encompass agreed-upon standards of data longevity, with a view to placing time limits on data use to protect individual privacy.

7) Incorporate 'Privacy by Design' Principles

The Province of Ontario's *Privacy by Design* concept – which aims to protect personal privacy at the front end of the IoT risk model by embedding it into IoT technology design, business practices and physical infrastructures – was observed by *Forum* participants to be the most promising approach for establishing a universal privacy standard for use by government, industry and stakeholders.

Privacy by Design: Foundational Principles

- Proactive not reactive;
- Preventative not remedial;
- Privacy embedded into design;
- Privacy as default setting;
- Full functionality – positive-sum, not zero-sum;
- End-to-end security – full lifecycle protection;
- Visibility and transparency – keep it open; and
- Respect for user privacy – keep it user-centric.

— Ann Cavoukian, Ph.D. , Executive Director, Privacy and Big Data Institute, Ryerson University and, former Information and Privacy Commissioner of Ontario.

8) Focus on Security and Privacy

The most compelling aspect of the *Privacy by Design* approach for *Forum* participants is that it avoids the false dichotomy of privacy *versus* security by viewing privacy as a natural corollary of security.

Internet of Things Security and Privacy — Future Steps

Develop a 'Secure Canada' Approach

Forum participants observed that the Government of Canada's (GC's) current cyber security strategy is focused too narrowly on threats and vulnerabilities to government departments and agencies. With the GC's current cyber security review in mind, consensus was reached on the need for increased government-industry collaboration, with the private sector taking the lead in creating and funding a new entity tasked with developing a comprehensive, cross-sectoral 'Secure Canada' approach to IoT security and privacy. With a shared leadership approach, this entity would be linked to senior GC officials (within the Prime Minister's office or the Privy Council Office) to ensure ongoing government consultation and input.

Ideally, this 'Secure Canada' approach would draw upon insights and experiences of allied countries that have already gone down this road. The United Kingdom, for example, has created a successful information sharing environment that delineates cyber security/privacy roles and responsibilities across an entire society – from individuals and small businesses to corporations, governments and the public safety and security intelligence communities. Canada can draw upon important lessons learned in creating its own 'Secure Canada' approach to cyber security and privacy across Canadian society.

'Secure Canada' and Canadian Prosperity

A successful 'Secure Canada' approach to cyber security and privacy is one that underlines the important link between cyber security and Canadians' long-term well-being and economic prosperity. While the financial costs of inaction on cyber security are enormous, so too are the prospective social and financial benefits of a nationally coordinated 'Secure Canada' approach to cyber policy and practices, standards and protocols. A cost-benefit analysis of this approach is simply too important for Canadians to ignore.

The private sector can take action by providing leadership on awareness, enterprise risk management and IoT privacy, and by promoting responsible behaviours, without waiting for government intervention.

Quantum Computing and Security/Privacy Issues

Quantum computing and associated asymmetrical encryption/decryption will have a significant impact on Canada's IoT ecosystem in coming years. In view of this paradigm shift, *Forum* participants agreed that quantum computing, and its implications for cyber security and privacy, should be a key element of the 2017 *Cyber Security Forum*.

Promote Responsible Cyber Behaviours

While businesses are fully aware of the financial costs associated with cyber security breaches, individual Canadians lag behind in their understanding of the potential impact of cyber intrusions on their digital profiles, including identity theft and the loss of important health and financial information.

Industry, government, NGO and education stakeholders must demonstrate their commitment to cyber security and privacy by investing in programs that promote increased workplace capacity through digital literacy and technological awareness as well as greater personal responsibility for behaviours on IoT devices and networks.

Annex

List of Participating Organizations

While participating organizations contributed to the discussions that took place at the Cyber Forum, the full content of this report does not necessarily reflect the perspective of each individual participating organization.

ACT Canada

Accipiter Radar Technologies Inc.

ADGA Group

Bell Canada/BCE

Bennett Jones LLP

Blake, Cassels & Graydon LLP

Bruce Power

Canadian Association of Defence and Security Industries

Canadian Bankers Association

Canadian Chamber of Commerce

Canadian Gas Association

Canadian Nuclear Safety Commission

Canadian Security Intelligence Service

Carillon Information Security Inc.

CISO Sun Life Financial

Communications Security Establishment

Conestoga College Institute of Technology and Advanced Learning

Crumpton Group LLC

Force Multiplier

FundSERV Inc.

HealthCareCAN

I-Sec Integrated Strategies

Industry Canada

Institute for Quantum Computing

Intact Financial Corporation

ISARA Corporation

International Cyber Security Protection Alliance

Linchpin Labs Inc.

Microsoft Canada

Miovski Group Inc.

NIKSUN Inc.

Ontario Community Safety

Ontario Provincial Police

Port of Vancouver

PricewaterhouseCoopers LLP

Public Safety Canada

Rogers Telecommunications Ltd.

Royal Canadian Mounted Police

RSA Security EMC2 Corporation

SAS Canada

Shared Services Canada

Telus

Treasury Board of Canada