Grigsby, Alexandre

From: Claude.Gagne@ic.gc.ca
Sent: Wednesday, January 11, 2012 6:51 PM
To: Guy.Mitchell@ic.gc.ca; Grigsby, Alexandre; Gordon, Robert; Jacqueline.Jones@ic.gc.ca; Lewis.robart@crc.gc.ca; Nancy.Macartney@ic.gc.ca; Alexander.Hughes@ic.gc.ca; James.Fulcher@ic.gc.ca; Felix.Berezovsky@ic.gc.ca; pamela.moss@nserc-crsng.gc.ca; s.bourgi@ictc-ctic.ca
Cc: Alain.Beaudoin@ic.gc.ca; n.mcdevitt@ictc-ctic.ca
Subject: RE: Exploratory Meeting on Cybersecurity Skills Issues and Opportunities for Collaboration

Colleagues,

Thank you for the note, Norm. It's good to know that connections have been made and that people are collaborating across organizational boundaries.

If the answers one is seeking can be provided by the ICTC study, it would be unfortunate not to take advantage of Norm's offer. I don't "own" the talent file nor the cybersecurity file, but some of you have stewardship of either or both themes.

As a general policy advisor for the ICT sector, I do look forward to the outcomes of all your studies and efforts, and I do hope we will alert one another when they become available.

Claude

From: Norm McDevitt [mailto:n.mcdevitt@ictc-ctic.ca]
Sent: 10 janvier 2012 17:41
To: Gagné, Claude: ICT-TIC; Mitchell, Guy: DGEPS-DGGPN; Alexandre.Grigsby@ps-sp.gc.ca; Gordon, Robert: CSTAC; Jones, Jacqueline: ECOM-DGCE; Robart, Lewis: CRC; Macartney, Nancy: ICT-TIC; Hughes, Alexander: DEPC-PCEN; Fulcher, James: ICT-TIC; Berezovsky, Felix: ICT-TIC; pamela.moss@nserc-crsng.gc.ca; Sam Bourgi
Subject: RE: Exploratory Meeting on Cybersecurity Skills Issues and Opportunities for Collaboration

Dear Claude,

Thank you for the follow up. It was a pleasure meeting all of you last week, getting a better understanding of what is happening in their departments and sharing ICTC's work in the area of cyber security. The meeting also served as a connection point which has facilitated a few one on one meetings for additional collaboration already!
As a reminder, over the next few months we will be moving ahead with our cyber security roadmap study in order to define the occupations, skills requirements and trends of cyber security professionals in Canada. Our goal is to also raise awareness regarding the impacts of cyber insecurity on the Canadian economy. We will be collecting primary data beginning at the end of this month in the forms of working groups, surveys and conference calls with experts in finance, government services, ICT and education. We will then develop a report that captures their feedback, as well as the research ICTC has completed to-date.

If you or any of your colleagues from the roundtable wish to contribute to this study or would like the study to highlight aspects of critical importance to the Federal Government, please contact myself or Sam Bourgi (s.bourgi@ictc-ctic.ca) so that we may discuss your concerns and build surveys/working group questions around your needs.

We look forward to staying in touch on this important matter. Please contact myself or Sam if you would like more information.

Regards,

Norman McDevitt, PMP
Vice President
Information and Communications Technology Council (ICTC)

116 Lisgar Street, Suite 300, Ottawa, ON K2P 0C2
Phone: 613-237-8551 Ext. 137
Fax: 613-230-3490
Email: n.mcdevitt@ictc-ctic.ca
Website: www.ictc-ctic.ca

The Information and Communications Technology Council (ICTC) is a not-for-profit sector council funded in part by the Government of Canada's Sector Council Program. We are dedicated to creating a strong, prepared and highly educated Canadian ICT industry and workforce.

From: Claude.Gagne@ic.gc.ca [mailto:Claude.Gagne@ic.gc.ca]
Sent: Thursday, January 05, 2012 7:49 PM
To: Guy.Mitchell@ic.gc.ca; Alexandre.Grigsby@ps-sp.gc.ca; robert.gordon@ps-sp.gc.ca; Jacqueline.Jones@ic.gc.ca; Lewis.robart@crc.gc.ca; Nancy.Macartney@ic.gc.ca; Alexander.Hughes@ic.gc.ca; James.Fulcher@ic.gc.ca; Felix.Berezovsky@ic.gc.ca; pamela.moss@nserc-crsng.gc.ca; Norm McDevitt; s.bourgi@ict-ctic.ca
Subject: Exploratory Meeting on Cybersecurity Skills Issues and Opportunities for Collaboration

Dear all,

Thank you for your contributions to the meeting earlier today. Feedback so far was that it was helpful to find out what other stakeholders are doing, what their concerns may be and what are some of the outstanding questions. As summarized by Guy Mitchell, converging interests appear to be in the following areas:

1) Are there shortages in terms of people or skills?

Public Safety Canada hopes to document shortages at the level of the government, with the view of to addressing issues of recruitment, attraction, training and retention. It will meet with CSE, TBS and other departments and agencies. It is also interested in knowing more about the situation in the private sector and how it might impact cybersecurity talent in government. Finally it needs to produce a report on the state of play in various countries and opportunities for international collaboration. (Contact for details: robert.gordon@ps-sp.gc.ca)

Industry Canada considers that talent is the lifeblood of the ICT industry and that Canada must develop, attract and retain ICT talent in order to be competitive. The Statistics Canada National Occupations Classification (NOC) system in use for labour market surveys does not offer enough granularity to identify gaps or shortages. StatsCan has started to track enrolment and grads in systems security, and we have the following data:

MSc enrolments in Computer and Information Systems Security

2005	2006	2007	2008
51	138	207	231

And graduates in this field

2005	2006	2007	2008
0	3	30	60

It's impossible to say anything about existing/future shortage of professionals in this field. There is, however, anecdotal evidence that shortages exist. A contract has been let to conduct a study on talent issues in 6 ICT clusters (BC, Calgary, Toronto, Ottawa, Waterloo and Montreal). In 2008, Statistics Canada reports that 60 students graduated at the Masters level in cybersecurity, but Industry Canada has no data on PhDs. There will be more students coming out of graduate programs in cybersecurity in coming years. It is not clear where these students go, nor what the demand is for more. (Contact for details: felix.berezovsky@ic.gc.ca)

The Information and Communications Technologies Council (ICTC) is developing a Cyber Security Strategy that identifies the cyber security skills and human resource needs of Canada's digital economy. In collaboration with industry, education and government, ICTC is investing in strategies for developing a highly skilled and diverse cyber security workforce to address ICT security issues in the digital economy. There are labour shortages and skills shortages. Cybersecurity is an important component of digital literacy for all Canadians; IT professionals need cybersecurity skills; and there are needs for highly qualified professionals in cybersecurity. Three emerging occupations are in high demand: critical infrastructure engineers; IT security specialists; and, ethical hackers. Huge shortages in the USA and India have been documented. In Canada, a review of secondary data points to significant gaps. Focus groups will be done in Montreal, Toronto and Vancouver in order to identify requirements. A study is also being done of requirements in the financial sector. A report on cybersecurity skills will be issued in March (Contact for details: n.mcdevitt@ictc-ctic.ca and s.bourgi@ictc-ctic.ca).

The Communications Research Centre (CRC) of Industry Canada has 7 researchers, some of which are adjunct professors at universities, who mentor students.

The Electronic Commerce Branch of Industry Canadarecognizes the importance of cybersecurity skills for fighting spam and Internet threats. Its website http://fightspam.gc.ca is helpful for does not address skills directly (Contact for details: jacqueline.jones@ic.gc.ca)

The Digital Economy Policy Branch of Industry Canada is interested in basic digital literacy for all Canadians and in making Canadian business more competitive. The Digital Technology Adoption Pilot Program (DTAPP) being delivered by NRC-IRAP from October 2011 to March 31, 2014 might help Canadian business be more savvy in terms of cybersecurity. (Contact for details: alexander.hughes@ic.gc.ca).

2) Is there potential formore research collaboration in Canada, in particular with universities?

NSERChas a budget of a billion dollars each year to fund demand-driven research in the natural sciences and engineering, and most of the funding is for students and research equipment. After 9/11, Safety and Security was identified as a target area for NSERC funding. Three universities offer programs in various areas of cybersecurity:

- Carleton University – Centre for Security & Defense Studies
- University of New Brunswick – Information Security Centre of Excellence
- Concordia University – Institute for Information Systems Engineering – Computer Security Lab

In addition the following research groups are also active:

- BCIT – Centre for Forensics and Security Technology
- University of Waterloo – Centre for Applied Cryptography Research
- University of Calgary – Institute for Security, Privacy, and Information Assurance (formerly Centre for Information Security and Cryptography)
- York University – Program in Computer Security
- University of British Columbia – Networks, Systems, and Security Lab
- University of Ontario Institute of Technology (UOIT) – Networking and IT Security Specialization Program

Using a series of keywords provided by Industry Canada, but excluding defence-related terms, NSERC was able to identify active projects in cybersecurity that are worth $104 million (listing available on demand). NSERC has a program with DND where for jointly funding CRD projects with university professors but only when there are non-defence related goals and where the results of the research could be exploited in the public market.

In addition, NSERC provides $5 million over 5 years to the Internetworked Systems Security Network (http://www.issnet.ca) under the Strategic Partnership Programs. Managed out of Carleton University since January 2008, the research team consists of about 20 researchers from 9 universities. Its expected end date is August 31, 2013, unless it is renewed. (Contact for details: pamela.moss@nserc-crsng.gc.ca)

CRC works with the Department of National Defence, its Defence Research and Development Canada, as well as with allied organisations and international standards bodies to develop improved defence communications.CRC also works with Public Safety Canada to improve the communications capabilities of Canada's first responder community, and with the Communications Security Establishment and the telecommunications industry to prevent, identify and mitigate cyber attacks.
(Contact for details: lewis.robart@crc.gc.ca)

3) What are other countries doing and what is the potential for cooperation?

Public Safety Canada is interested in knowing what other countries are doing and how Canada might be involved.

- Pamela Moss toprovide contacts for the European Commission FP7 and Horizon Program 2020 initiatives on cybersecurity that are international in scope. Some target cooperation in cybersecurity with emerging countries such as China, India and Brazil.
- Jacqueline Jones to provide links topolicy work on cybersecurity at the OECD, APEC, etc.

NEXT STEPS FOR CONSIDERATION:

- Continue to liaise electronically and share findings and reports. Meet again depending on findings.

- Consider supporting the creation of a Canada Excellence Research Chair in cybersecurity at a Canadian university
to attract one of the world's top researchers in cybersecurity to Canada. The Canada Excellence Research Chairs (CERC) Program awards world-class researchers up to $10 million over seven years to establish ambitious research programs at Canadian universities.Time is of the essence. Phase One of the program will end on May 28, 2012. Substantial industry, government and community financial and in-kind support is key for success. There needs to be a significant industry cluster and receptor capacity, as in the Ottawa region. For details, see
http://www.cerc.gc.ca/hp-pa-eng.shtml

- Consider promoting the NSERC Collaborative Research and Training Experience Program (CREATE) for cybersecurity, as a means to enhance linkages between industry and academia with the view of increasing the supply of highly qualified personnel (HQP) who are "employer-ready" and can generate immediate results after graduation, improving job readiness as an immediate benefit to the industrial employer. Up to 50 percent of the CREATE grants will be dedicated to the industrial stream. There are two competitions in 2012. Funding is significant, up to $1.6 million, and the program is open to international collaboration. See http://www.nserc-crsng.gc.ca/professors-professeurs/grants-subs/create-foncer_eng.asp

- For Industry Canada in particular, the tracking through NSERC (Pamela Moss) of students/employers in the area of cybersecurity would provide invaluable understanding of their employment outcomes and existing/future shortage, better clarity on the number students in this area and determine if there is a need to improve Canada's ability to retain graduates and foreign students in this field.

Please do not hesitate to send amendments, links or additions to this report.

Best regards,

Mme Claude Gagné
Senior Advisor | Conseiller principal
Information and Communications Technologies Branch | Direction générale des technologies de l'information et des communications
Spectrum, Information Technologies and Telecommunications Sector | Secteur du Spectre, des technologies de l'information et des télécommunications
Industry Canada | Industrie Canada
300 Slater Street, Ottawa ON K1A 0C8 | 300, rue Slater, Ottawa ON K1A 0C8
Claude.Gagne@ic.gc.ca
Telephone | Téléphone 613-990-4288
Facsimile | Télécopieur 613-957-4076
Teletypewriter | Téléimprimeur 1-866-694-8389
Government of Canada | Gouvernement du Canada

Industry Canada Industrie Canada

Canada

Pages 7 to / à 8

are duplicates

sont des duplicatas

Pages 8 to / à 9

are duplicates

sont des duplicatas

Pages 9 to / à 10

are duplicates

sont des duplicatas

Pages 10 to / à 11

are duplicates

sont des duplicatas

Pages 11 to / à 12

are duplicates

sont des duplicatas

Grigsby, Alexandre

From: Sam Bourgi <s.bourgi@ictc-ctic.ca>
Sent: Monday, January 09, 2012 12:59 PM
To: Grigsby, Alexandre
Subject: RE: Follow-up on the IT/cyber security skills shortage meeting at IC

Good afternoon, Alex,

I just double checked with Norm McDevitt and that would be a great time to meet. Norm and I will see you tomorrow at 2:00 at the Second Cup.

My best,

Sam Bourgi, ICTC

From: Grigsby, Alexandre [mailto:Alexandre.Grigsby@ps-sp.gc.ca]
Sent: Monday, January 09, 2012 10:28 AM
To: Sam Bourgi
Subject: RE: Follow-up on the IT/cyber security skills shortage meeting at IC

Hi Sam,

We can get together tomorrow PM over coffee if that works for you, say 2:00? There's a Second Cup on the corner of Bank and Somerset which is effectively at the mid-point between our two offices. Is that suitable for you?

Cheers,

alex

Alexandre Grigsby
tel. 613.949-4243

From: Sam Bourgi [mailto:s.bourgi@ictc-ctic.ca]
Sent: January-06-12 4:03 PM
To: Grigsby, Alexandre
Subject: RE: Follow-up on the IT/cyber security skills shortage meeting at IC

Good afternoon, Alexandre,

Thank you for your email. I would be more than happy to assist you in your deliverables. However, the amount of research/information we have on this subject is overwhelming. I am currently navigating the information in order to frame our whitepaper study and provide better guidance to our Cyber Security strategy.

Would you like to meet with me next week regarding your request? That way I can pinpoint the information you need and provide you with relevant material. After speaking with our vice president, Norm McDevitt (whom you met yesterday), he expressed a great deal of interest in discussing what your needs are. Tuesday, Thursday or Friday of next week would be a great time for us to meet you and/or any of your colleagues. Please let me know your availability.

As for our other Cyber Security initiatives, we are in the process of collecting primary data in order to overcome the shortcomings of the NOCs. We are also in the process of navigating the NOC codes in order to identify Cyber Security occupations and estimate current/projected trends. Our first round of primary data collection will

commence later this month in Toronto at our finance sector working group. I am also designing a Cyber Security survey to disseminate to our ICT contacts.

Should you have any other questions or collaboration requests regarding your February deadline, I would be happy to assist. I look forward to hearing from you.

Regards,

Sam

Sam Bourgi
Research Analyst, Labour Market Intelligence | Immigration Initiatives
Information and Communications Technology Council (ICTC)
116 Lisgar Street, Suite 300, Ottawa, ON K2P 0C2
Phone: 613-237-8551 Ext. 152 | Fax: 613-230-3490
E-mail: s.bourgi@ictc-ctic.ca
Web: http://www.ictc-ctic.ca/

ICTC CTIC

From: Grigsby, Alexandre [mailto:Alexandre.Grigsby@ps-sp.gc.ca]
Sent: Friday, January 06, 2012 2:48 PM
To: Sam Bourgi
Subject: Follow-up on the IT/cyber security skills shortage meeting at IC

Hi Sam,

It was nice to meet you at the IT/cyber security skills shortage meeting we attended yesterday at Industry Canada.

I'm following up on some of the work you said you were doing with regards to the White Paper on cyber security skills shortages. Recognising that you're looking to have paper released in March, are there any working documents or bibliographical information that you may be able to send my way so I can wrap my head around the issue?

As Bob Gordon noted in the meeting yesterday, Public Safety is on the hook for putting together a short paper on how to attract IT/cyber security professionals in the public and private sectors for delivery in February. The work that you're doing seems to be really interesting and given that I won't be able to wait until the White Paper is released, I was hoping you could share some background reading material.

Should you have any questions, please don't hesitate to get in touch.

Cheers,

alex

Alexandre Grigsby
Policy Analyst | Analyste des politiques
National Cyber Security Policy | Cybersécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel: 613.949.4243

Pages 14 to / à 15

are duplicates

sont des duplicatas

Pages 15 to / à 16

are duplicates

sont des duplicatas

ICTC PRELIMINARY SCAN

CYBER SECURITY

CRITICAL ICT HUMAN RESOURCES IN THE DIGITAL ECONOMY

Prepared by:

Sam Bourgi,
Information and Communications Technology Council (ICTC)

ICTC CTIC

Information and Communications Technology Council
Conseil des technologies de l'information et des communications

300-116 Lisgar Street, Ottawa, ON, Canada K2P 0C2
Phone: (613) 237-8551 | Fax: 613-230-3490
E-mail: lmi@ictc-ctic.ca
Web: http://www.ictc-ctic.ca/

INTRODUCTION

The Internet has made it easier than ever for people to bank, shop, connect with others and find the information they need at any time. According to a 2008 survey by Statistics Canada, approximately three-quarters of Canadians aged 16 or older—roughly 19.2 million people—used the Internet over the past 12 months.[1] As Internet use among Canadians continues to grow, so too does online criminal behavior such as fraud and identity theft. According to Nancy Hughes Anthony, President and CEO of the Canadian Bankers Association, "criminals unfortunately have an even greater number of options to obtain and illegally use individuals' personal information."[2]

The growth of cyber threats has created high demand for human resources capable of developing reliable digital communications infrastructure that can safeguard the privacy of Canadians and protect the sensitive information of critical infrastructures.

WHAT IS THE CYBER THREAT?

Cyber security refers to ICT security services that are utilized to apply "safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information."[3] Attacks by hackers are on the increase and are becoming ever more sophisticated. [4] Serious consequences can occur due to the illicit use of personal information. Identity theft, health information leaks and unauthorized financial disclosures exemplify the issues that Canadians are concerned about. Public Safety Canada, a federal agency, expounds upon the issue of IT security in the following passage:

> "The Internet, computers and mobile devices are an integral part of our daily lives: from banking and making purchases using debit and credit cards to socializing and sharing personal information online. Yet many Canadians do not take the proper precautions to protect personal information online, leaving themselves open to fraud, identity theft and serious financial loss. Protecting our digital identity and the personal information we post online is becoming just as important as protecting our personal information offline."

Canada's dependence on digital communication infrastructure is ever growing; digital communications allow Canadians to make bill payments, transfer money, file tax returns and exchange sensitive information. The integration of ICT has moved Canada toward a digital economy, as exemplified by the following:

- 74% of Canadian households and 87% of businesses use Internet services;
- 59% of all personal tax filings are done electronically;
- 67% of Canadians bank online;
- Canadian online sales generate $62.7 billion; and

- The federal government relies on the Internet to provide consumers with 130 online services.[5]

The expansion of Canada's digital economy has created new security challenges for critical ICT infrastructure, including sub-sectors which rely on ICT to improve their products and services.[1] **The risks associated with digital communications extend far beyond personal banking and online business; critical infrastructures such as transportation and health care are similarly dependent on digital communications**, where security breaches and/or critical data disruption have greater consequences.[6]

The top three attack methods hackers employ to retrieve sensitive information are:

1. Remote Access Application

2. Third Party Connectivity

3. SQL Injection

A GLOBAL APPROACH TO CYBER SECURITY

In order to develop cyber security best practices in Canada, including investing in a highly qualified cyber security labour force, cyber security must be approached from a global perspective in order to learn from, and build on, the strategies of similar economies facing similar challenges.

United Kingdom (U.K.)

The British approach to cyber security is embodied in the Information Assurance (IA) program, which is a response to mounting public scrutiny over the government's ability to provide effective services. According to Roger Styles, Central Sponsor for Information Assurance for the U.K. Cabinet Office, the U.K. government relies heavily on ICT advancements to deliver services to the public and to ensure a more efficient public service, a phenomenon he calls **'Transformational Government.'**[7]

The resulting IA strategy is a response to the increasing mobility of the U.K. labour force, as well as the increasing usage of Internet services at a time when digital communications infrastructure is vulnerable to criminal behavior. The IA strategy is designed to deliver a risk management framework to all segments of British society. According to Styles, the IA strategy:

- reflects the government's commitment to **risk management** as opposed to **total security** because no network can be considered totally secure in an absolute sense;

- is contained in the government's cyber standards and policies, which includes building in-house capacity to manage ongoing cyber threats;

- reflects the need to reform security procedures as part of the overall risk management strategy;

- addresses governance concerns by forcing organizations to assign

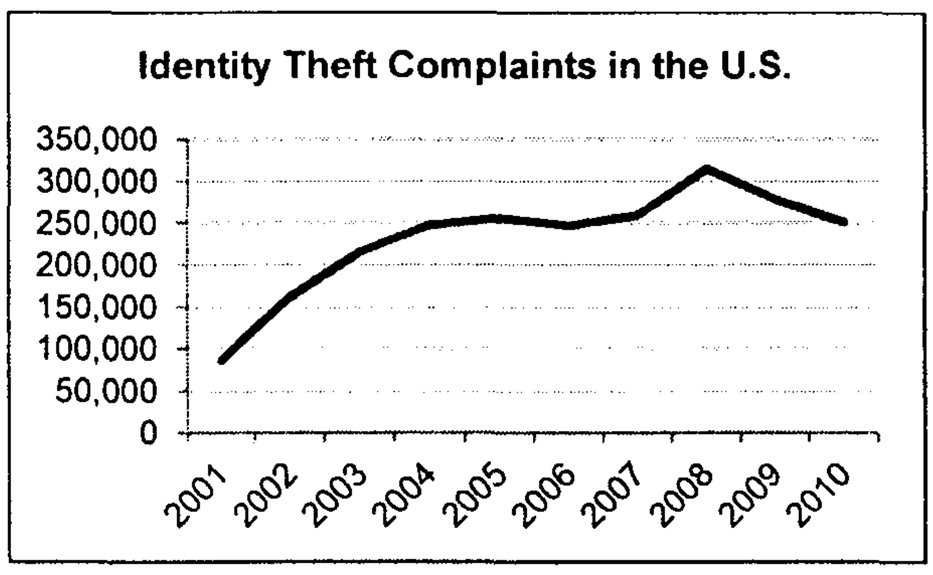
[1] For more information on the role of ICT in key sub-sectors, please view ICTC's *Sub-Sector Series*, a series of reports which address the role of ICT human resources in areas such as wireless communications, e-Health, digital media, nanotechnology and finance.

responsibility in the event of a security failure; and

- ensures a common framework and understanding across all sectors of the U.K. economy.[8]

United States (U.S.)

According to Booz Allen, a U.S.-based consulting firm, the U.S. is facing a cyber war, with the White House, Pentagon, State Department a nd New York Stock Exchange all targets of elaborate and sophisticated cyber attacks. Current President Barrack Obama has declared that cyber security is one of most challenging concerns facing the U.S.[9]



Source: Federal Trade Commission (2011). 2010 Consumer Sentinel Network Data Book. Retrieved November 15, 2011 from: http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf.

Over the 2001 to 2010 period, identity theft rose substantially in the United States. In 2010, the Federal Trade Commission reported 250,854 identity theft complaints. The number of complaints peaked in 2008 at 314,521. As a comparison, in 2008 Phone Busters reported that 12,142 identity theft complaints were reported in Canada, resulting in the loss of more than $9.5 million.[10] In 2010, total losses were close to $30 million.[11] The Canadian Council of Best Business Bureaus estimates that identify theft costs the Canadian economy approximately $2.5 billion annually.[12]

According to a study of the U.S. federal cyber security labour force conducted by Booz Allen, **the federal government is experiencing significant skills shortages in cyber security professionals**.[13] However, shortages at the federal level have not discouraged industry leaders from addressing shared concerns about network security and the growing cyber threat.

Industry Responds: Network Centric Operations Industry Consortium (NCOIC)

The NCOIC was established by industry leaders from various sectors to develop strategies around common network problems and to resolve online-centric policy concerns. The government entered the dialogue shortly after NCOIC's inception in 2004 in order to provide clearer guidelines for cyber policy.

The NCOIC added cyber security as a key policy issue shortly after its inception in order to address common security concerns and collaborate around shared solutions.

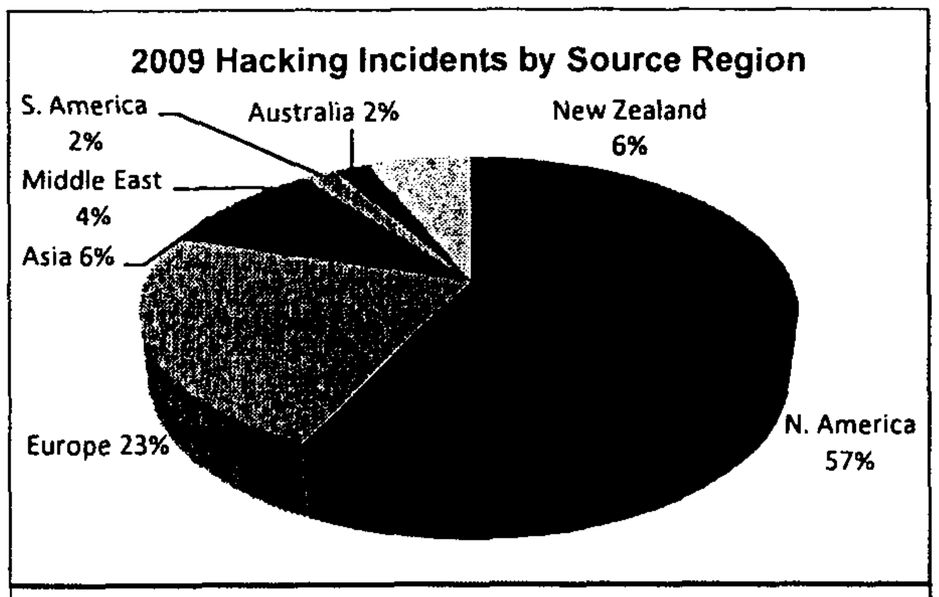
According to former chairman of NCOIC, Harry Raduege Jr., the U.S. Chamber of Commerce has engaged its network of more than three million businesses on the issue of cyber security, a clear sign that cyber security has become a critical issue.

U5 Countries

International cooperation is one of the most important strategies for addressing the vulnerability of digital communications infrastructure. Cyber threats are an international phenomenon; yet, policymakers seeking to address the issues operate in national jurisdictions that do not permit cooperation and information exchange beyond national borders. Because sensitive information is usually at stake,

international guidelines and regulations pertaining to information sharing and cyber security are scarce.

According to Michael Aisenberg, Chair of the U.S. IT Sector Coordinating Council, EWA Information and Infrastructure Technologies, Inc., the so called **U5 Countries** (U.S., U.K., Canada, Australia and New Zealand) are a great place to start building international cooperation around such issues as information sharing and cyber security.[14]



Source: The Web Hacking Incident Database 2009.

THE GROWING DEMAND FOR CYBER SECURITY IN CANADA

The need for cyber security human resources will absolutely continue to grow in Canada as ICT expands in organizations, government and personal banking. In response, Public Safety Canada has established a Canadian Cyber Incident Response Centre (CCIRC), which is responsible for the protection of national critical infrastructure against cyber incidents. CCIRC is responsible for:

- monitoring cyber threats;
- providing mitigation strategies against such threats; and
- coordinating the national response to cyber security incidents.[15]

According to Ron Deibert, Director at the Canada Centre for Global Security Studies and the Citizen Lab,[16] Canada absolutely needs a stronger approach to cyber security. **The growing concern with security has already created a massive cyber security market** (between $80 and $150 billion U.S. annually), which provides filtering, data mining and fusion and computer attack capabilities to security services worldwide.[17]

The Conference Board considers cyber insecurity an "economic and national security crisis." It notes that advancements in cyber security represent a "strategic advantage" for organizations and the nation.[18] Raising public awareness about the risks of online activity, investing in the ICT skills that are needed to support a cyber-secure nation and developing a highly skilled cyber security workforce represent a strategic advantage for organizations and the nation.

HOW CYBER SECURITY WILL CONTRIBUTE TO LABOUR FORCE EXPANSION IN CANADA

In a recent report, Sapphire, a global provider of IT staffing services, revealed that projects related to collaboration, security and cloud computing are among the most common contributors to labour force expansion in Canada. The report also stated that large firms have the greatest need for security and privacy specialists.[19]

The U.S. Bureau of Labor expects growth in Computer Security Specialists to exceed growth in the U.S.' economy-wide labour force over the 2008 to 2018 period [20] Demand for IT security is expected to increase as organizations' need for data security accelerates– especially as more databases become connected to the Internet. Moreover, **the growing reliance on wireless networks will also increase the need for cyber security specialists**. According to the Bureau, those with knowledge of information security will likely be in high demand, as computer networks transmit an increasing amount of sensitive data.[21] Security concerns are particularly important issues in the context of cloud computing, where virtualization is a fundamental technology. Virtualization tends to raise security requirements, making security management much more complex.[22]

SHORTAGES IN CYBER SECURITY LABOUR MARKET

The growing threat of cyber infractions has created a new market for ICT professionals with the skills to design and operate critical systems infrastructure that can withstand sophisticated attacks. According to industry and government stakeholders interviewed by Professional Engineers Ontario (PEO), cyber security professionals are in very short supply. **Communications Infrastructure Engineering (CIE) has emerged as a possible solution to the ongoing threat posed by sophisticated hackers**.[23]

CRITICAL RESOURCE: CIE PROFESSIONALS

CIE is an engineering discipline that supports critical infrastructures by designing and managing secure networks for mission-critical and safety-critical applications.

ESSENTIAL ACITIVITY OF CIE PROFESSIONALS

- System-level design and management of secure communications networks, which have the following characteristics: **availability, confidentiality, integrity** and **privacy**.

PRINCIPAL PRACTICES OF CIE PROFESSIONALS

- Design and oversight of secure communications networks; and

- Perform risk analysis for critical network infrastructure.

ESSENTIAL SKILLS AND KNOWLEDGE CIE PROFESSIONALS NEED

- Background in other Electrical Engineering sub-disciplines, such as Communications Engineering, Computer Engineering and Software Engineering;

- Knowledge of IP and related technology;

- Knowledge and application of network security, standards and risk assessment;

- Critical infrastructure protection; and

- Compliance and governance standards.[24]

The CIE practice requires further development by the professional engineering community in order to define the standards and licensing procedures for CIE professionals. With growing security concerns affecting all segments of Canadian society, human resources committed to the protection and maintenance of communications infrastructure are necessary. CIE expertise has the potential to strengthen federal government policy initiatives around cyber security by establishing guidelines and best practices for secure communications networks.

The growing threat of cyber infractions has created a new market for ICT professionals. **CIE has emerged as a possible solution to the ongoing threat posed by sophisticated hackers.**

EMERGING OCCUPATIONS

IT Security Specialists

Threats to information security are especially problematic for government departments which house sensitive information. In dealing with the evolving threat posed by sophisticated hackers, government departments in the U.S., for example, have taken a proactive approach to mitigating risks. IT Security Specialists can protect federal networks and critical infrastructures by pinpointing key areas (i.e., communications, endpoint protection, or other threat areas) in which security has been breached. Identifying the nature of the breach is critical in order to craft an effective response and mitigate future attacks. IT Security Specialists have the knowledge and skills to identify the nature of the threat and respond accordingly.[25]

Ethical Hackers

The international market for ethical hackers, sometimes referred to as white hats or penetration testers, is growing among multinational corporations and government agencies. According to Cyber Media Research, India's Information Technology Enabled Service Business Process Outsourcing (ITES-BPO) is expected to grow 16.6% in 2012, creating a large market for security specialists and ethical hackers. According to the Indian Computer Emergency Response Team, 2011 phishing attacks reached 3,458 by May, compared to the 5,432 cases reported in all of 2010 and 549 reported in 2009.

According to Narayanan Ramaswamy, executive director with KPMG, the demand for ethical hackers in India will grow 20 times by 2015. This growth will not be limited to IT companies; financial services, retail chains and government agencies will all experience growing demand for ethical hackers. Nasscom estimates that India needs over 77,000 ethical hackers every year to satisfy labour demand; however, the country is only producing between

20,000 and 25,000 ethical hackers annually.[26]

While skills shortages of ethical hackers have not been reported in North America, these trends should be monitored to assess potential demand requirements in future years. With the majority of hacking incidents originating in North America, Canada must ensure that it has the resources to combat the growing cyber threat. The growing demand for ethical hackers in India is a clear indication that Canadian employers, governments and ICT associations must be proactive in safeguarding Canada's critical networks and digital infrastructures.

NEXT STEPS

Cyber security is one of the most important issues facing society. It impacts the public safety of Canadians, the commercial integrity of organizations and ultimately Canada's global competitiveness. The HR and labour market implications of cyber security are undeniable and worthy of further consideration by government, industry and ICTC.

STRENGTHENING CYBER SECURITY INFRASTRUCTURE THROUGH PARTNERSHIP

1. Cross-sector cooperation and partnerships within national jurisdictions are absolutely necessary to reach consensus and develop best practices in a critical area such as cyber security.

2. Facilitate international cooperation around information sharing and cyber security and develop guidelines for mitigating risks to critical infrastructure.

3. Cyber security must be approached holistically; effective responses to cyber threats must consider every spectrum, including infrastructure, technology, privacy, information management and individual behaviour.[27]

4. In order to safeguard Canada's critical infrastructure from sophisticated cyber attacks, government and industry must invest in the cyber skills they need; as security concerns become more serious, the Canadian economy requires a highly-skilled ICT labour force capable of designing, maintaining and safeguarding digital communications infrastructure.

DEVELOPING CYBER SECURITY LABOUR FORCE

1. Industry and academia should support CIE as a discipline by raising awareness of the growing demand for cyber security professionals.

2. Industry and government should invest in industry- and domain-specific cyber security professionals who can address cyber threats to critical infrastructures such as transportation, health care and finance.

3. Support cyber security networks for ICT professionals in various industries to address common security concerns and develop best practices for designing and overseeing communications networks.

CALL FOR ACTION

ICTC believes that the ICT sector, including industry, education and government, must invest in strategies for recruiting, retaining, integrating and developing a highly-skilled and diverse cyber security labour force. These critical players must stimulate the number of young students, including women, entering into ICT and ICT related secondary and post-secondary programs. These programs must reflect the needs of industry and shift to integrated, cross-discipline, post-secondary programs with practicum components including professional development opportunities for returning students. ICT employers must ensure diversity and inclusion of both Canadian and Global talent, which are essential elements of their HR practices. Without diversity and inclusiveness, we limit the pool of workers industry can recruit from and this compounds the skills shortage in Canada.

Raising public awareness about the risks of online activity, investing in the ICT skills that are needed to support a cyber-secure nation and developing a highly skilled cyber security workforce represent a strategic advantage for organizations and the nation.

NEXT STEPS

In the next phase of its Cyber Security Study, ICTC will collect primary data in order to assess the growing field of cyber security in the Canadian economy. Primary data will be collected in the forms of working groups, surveys and telephone consultations with representatives from ICT, Government Services and Finance. Primary data, supplemented by secondary sources, including Census and LFS data, will allow ICTC to determine the trends of cyber security specialists in the Canadian economy. Primary data will also uncover the cyber security HR requirements of select industries and the leading edge skills employers look for when recruiting security specialists.

The Information and Communications Technology Council (ICTC) is a not-for-profit sector council dedicated to creating a strong, prepared and highly educated Canadian ICT industry and workforce. ICTC is a catalyst for change, pushing for innovations that will provide skills definitions, labour market intelligence, career awareness and professional development for the Canadian ICT industry, educators and governments. ICTC also believes that increased career awareness and professional development is the pathway to a successful ICT sector. ICTC forges partnerships that will help develop the quantity and quality of ICT professionals needed to maintain and improve Canada's position as a leader in the global marketplace.

END NOTES

[1] Statistics Canada (2008). Canadian Internet Use Survey. *Statistics Canada, The Daily* (2008). Retieved November 21, 2011 from http://www.statcan.gc.ca/daily-quotidien/080612/dq080612b-eng.htm.

[2] Andrew Addison (2008). "Banks team up for Cyber Security Awareness Month to help Canadians avoid online threats from social networking." Retrieved November 14, 2011 from http://www.reuters.com/article/2008/10/06/idUS144776+06-Oct-2008+MW20081006

[3] http://www.tbs-sct.gc.ca/cio-dpi/webapps/technology/profil/profil-eng.pdf

[4] "Cyber-security lax, experts warn; Government and industry are vulnerable to large-scale loss of data, they caution", Gazette, December 1, 2010.

[5] Government of Canada (2010). Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada. *Government of Canada* Cat. No.: PS4-102/2010E-PDF

[6] George Comrie (2011), "Cyber Security: Protecting digital infrastructure through CIE," *Dimensions* Sept (*2011*). Retrieved November 14, 2011 from http://www.peo.on.ca/DIMENSIONS/septoct2011/Cyber%20security.pdf.

[7] Matthew Gravelle (2008). Cyber Security: Developing a Canadian Strategy. *Public Policy Forum.* p. 12.

[8] Ibid, pp. 13-4.

[9] Booz Allen (2009). "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce," *Booz Allen*. Retrieved November 17, 2011 from http://www.boozallen.com/media/file/CyberIn-Security_2009.pdf.

[10] CBC News (2009). "Stolen Identity." *CBC News*. Retrieved November 17, 2011 from: http://www.cbc.ca/news/story/2009/01/21/f-idtheft.html.

[11] Terry Reith (2010). "Canadian fraud cases rose in 2010." *CBC News*. Retrieved November 17, 2011 from: http://www.cbc.ca/news/story/2010/12/31/con-fraud-2010.html.

[12] Carrie Davis (2009). The High Cost of Identity Theft in Canada. *Spend on Life*. Retrieved November 17, 2011 from: http://www.spendonlife.ca/blog/high-cost-identity-theft-canada.

[13] Booz Allen (2009). "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce," *Booz Allen*. Retrieved November 17, 2011 from http://www.boozallen.com/media/file/CyberIn-Security_2009.pdf.

[14] Matthew Gravelle (2008). Cyber Security: Developing a Canadian Strategy. *Public Policy Forum*. pp. 13-5.

[15] Public Safety Canada. (2011, June 17). Canadian Cyber Incident Response Centre (CCIRC). Retrieved June 24, 2011 from http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx.

[16] Ron Deibert (2011, May 2011). *Cyber Security: Canada Is Failing The World* http://deibert.citizenlab.org/2011/05/huffington-post-cyber-security-and-canadian-policy/.

[17] Ron Deibert and Rafal Rohozinski. (2011, Mar 28). *The new cyber military-industrial complex*. Retrieved June 22, 2011 from http://www.theglobeandmail.com/news/opinions/opinion/the-new-cyber-military-industrial-complex/article1957159/.

[18] The Conference Board of Canada (2010). Study Tours: Cyberspace and National Security – CNS Research Mission. http://www.conferenceboard.ca/topics/security-safety/studytour.aspx.

[19] Sapphire (2010). Canadian IT Staffing Outlook.

[20] O Net Online (2010). Summary Report for Information Security Analysts. Retrieved November 30, 2011 from http://www.onetonline.org/link/summary/15-1071.01.

[21] Bureau of Labor Statistics (2011). Occupational Outlook Handbook 2010-11 Edition. Retrieved December 1, 2011 from http://www.bls.gov/oco/ocos305.htm.

[22] OECD (2010). OECD Information Technology Outlook. *OECD*.

[23] George Comrie (2011), "Cyber Security: Protecting digital infrastructure through CIE," *Dimensions* Sept (*2011*). Retrieved November 14, 2011 from http://www.peo.on.ca/DIMENSIONS/septoct2011/Cyber%20security.pdf.

[24] Ibid.

[25] Mary Mosquera (2008). "Security specialists in demand: Increasing network threats drive the need for professional experience and certifications," Federal Computer Week (Nov 12, 2008). Retrieved December 5, 2011 from http://fcw.com/articles/2008/11/12/security-specialists-in-demand.aspx.

[26] The Times of India (2011). "Ethical Hackers: Gov't, MNCs want you," The Times of India (July, 25, 2011). Retrieved December 6, 2011 from http://articles.timesofindia.indiatimes.com/2011-07-25/job-trends/29812403_1_ethical-hackers-cyber-security-ankit-fadia.

[27] Matthew Gravelle (2008). Cyber Security: Developing a Canadian Strategy. *Public Policy Forum*, pp. 14-5.