

# Canadian Cybersecurity Awareness Stakeholders Teleconference Report

# Canadian Cybersecurity Awareness Stakeholders Teleconference Report

The human factor is being increasingly recognised as a critical aspect of cybersecurity. The concern of developing the capability of Canadians to contribute to securing cyberspace is as complex as it is important. Communities of research and practice have long since grown to respond to similar concerns for the security of information and communications technology systems; i.e. hardware and software. These communities offer spaces for the exchange of ideas, knowledge and expertise, the establishment and challenge of consensus, as well as a launching point for endeavours. Developing effective tools and solutions for the human side of cybersecurity will require strong and diverse communities linking researchers, decision-makers, practitioners and industry.

Members from across the academic and professional community working on relevant issues such as cybersecurity public awareness, usable security and cybersecurity training and education participated in a teleconference on the 23rd of October 2018. This conference brought together a wealth of experience and knowledge in cybersecurity, awareness, education and training. Capitalising on this experience could prove key in expediting the transition to the future of cybersecurity and the development of human capacity to actively security cyberspace.

This meeting was not intended to provide resolutions or solutions. However, there are a number of issues appear to be clearly understood across the community. Further there are also opportunities for collaboration and sharing among those working on similar problems. Salient points from the conversation are summarised below.

# Children

The importance of educating children was echoed across sectors and provinces. Children are very important for cybersecurity as they are both the most vulnerable and the least informed segment of the population. Children are digital natives and have a larger part of their lives online. There is an opportunity to reach kids while they are still in school and give them tools before they become exposed to cybersecurity threats. It is important to look at this issue in a holistic manner and educate parents and teachers in cybersecurity as well. There was a general sense that cybersecurity awareness should be done through schools. A lot of schools don't have digital literacy in their curriculum. Most of the cybersecurity education materials is not mandatory therefore doesn't reach the kids. Teachers have appeared to be self-taught and are finding cybersecurity information by themselves. Therefore, the education of kids is only as good as the information their teachers were able to find on their own. Media Smarts recently published research on parents' levels of digital literacy. Their goal is to understand what parents do to integrate technology in a way that ensure their family's well-being.

Work is being done with schools and teachers to provide awareness programs and materials in a number of places across Canada. Collaborative work between UNB and Bluespurs has been done to develop curriculum in New Brunswick. In Ontario Carlton University is working with MediaSmarts and teachers at the moment to find out how they are teaching digital literacy. The province of Ontario also recently started a program that targets secondary coop programs and they have a list of schools across Canada to connect with. The ministry of education in B.C. has partnered with Palo Alto to develop awareness programs. They also worked with kindergarten to grade 6 students for Bully Day.

Several participants are also looking at promoting Science Technology Engineering and Mathematics (STEM) learning to students and particularly for girls to try to help them move into those fields. Efforts like 'Hackergal' and 'CyberTITANS' provide guidance and mentors to promote STEM and cybersecurity for students.

The lack of workforce in cybersecurity is a challenge across sectors. Building public awareness of cybersecurity is important but there is a related challenge in awareness of careers in this field and attracting talent. There is a program in New Brunswick that starts in kindergarten and there is the cyberTITANS program, which is based on the CyberPatriot program from the US. The cyberTITANS program looks very interesting from the perspective of a parent and it could be developed to help more people in Canada.

Resources have already been created to help with education for children. Blue Spurs have created <https://thebluekit.com/>. MediaSmarts have are updating resources at <http://mediasmarts.ca/digital-media-literacy/digital-issues/cyber-security>, including games <http://mediasmarts.ca/game/privacy-playground-first-adventure-three-cyber-pigs>. The Government of British Columbia has a website <https://www.cybersafebc.ca/> for schools.

Developing messaging for cybersecurity is particularly difficult. Risks and technologies

# Coordinated and Clear Messaging

change rapidly in the ICT space and consequently, related advice and recommendations have a limited shelf life. Further, the information that is generated by cybersecurity professionals is generally designed for other professionals and as such is very technical. The technicality of these communications means that people who are not familiar with the technology or with cybersecurity issues can get lost. Even within the technical community there is lack of clarity. There is also an issue with conflating cybersecurity with IT security and computer security. To push the information out to the general public, we it should be in a form that is relevant and accessible to all. The rapidly changing information must be translated in order to be useful, which is logistically challenging.

To maximise the utility of the information when performing this, we must improve term definitions, messaging alignment and consistency in messaging. Collaboration for uniform communication in terms of threats, trends, messaging and awareness would be beneficial for all.

There is the possibility of communicating this information in innovative ways. CyberEco will develop a mobile application to inform people of the settings on their device and inform them of the related risks so they can make conscious security decisions.

## Collaboration

Carleton university has been looking at how games can be used to educate people about cybersecurity. They have been working with Media Smarts to develop a game to help children develop their digital literacy.

The Canadian Anti-Fraud Centre (CAFC) identifies lot of the new fraud and scams early because of the public reporting mechanism they have. They work with partners to share information about scams and trends. The Canadian Anti-Fraud Centre (CAFC) works with SERENE-RISC to distribute the fraud awareness messaging from CAFC through the SERENE-RISC network. CAFC provide regular updates via a mailing list. They are enthusiastic to work with other networks in the same way. A lot of the new fraud and scams are identified early at CAFC because of the public reporting mechanism they have.

The Canadian Centre for Cybersecurity (CCCS) has set up a 1-888 number for cyber issues so that people can call with their questions.

Connecting for resources, information, best practices and lessons learned generates real value for all stakeholders. This group could provide a great help by connecting the CCCS with contacts in the different provinces.

## At-Risk Groups

Children, seniors and the general public are important groups for cybersecurity. Within large organisations the current focus remains on phishing and ransomware. Within universities, Academics and researchers potentially have gap in their awareness of cybersecurity risks and impacts. The work they are doing is valuable and they should ensure that their IP is protected from theft. Earlier this year the media revealed that Iran deliberately stole information from researchers (“Open Librarian”) in the US and in Canada. Universities aren't currently considered to be critical infrastructure and may not be well protected against these kinds of threats.

## Weaving the Fabric

A future of cybersecurity in Canada involves the integration of cybersecurity knowledge and tools at every level of society, business operations and government. There are decisions that need to be made about what is considered to be acceptable for Canadians in cyberspace. For example, large amounts of data are being consolidated in a few private hands without much transparency around the data and around the algorithms that generate it. There is a need for a sophisticated public conversation about privacy and rights. A wider understanding of issues related to cybersecurity would allow for a more informed a nuanced public forum for debate on very important issues.

Many more knowledgeable people are needed to build cybersecurity. The promotion of STEM, particularly to groups traditionally marginalised in technical fields is important to encourage and enable the best talent into the field. Recruiting into the cybersecurity sector is also important. Surprisingly few university students know about cybersecurity.

Through the creation of the CCCS, the Communications Security Establishment (CSE) is extending its role of helping secure the Canadian Government to help also secure citizens and enterprises. They have a mandate to raise awareness of cybersecurity among the population, to work with academia to develop the cybersecurity research portfolio and to generate talent. They have been working with partners, such as from the energy and banking industry, as well as with CyberEco to give cybersecurity career talks at different universities around Montreal. It appears that currently even students in computer science and engineering programs don't know much about potential careers in cybersecurity, pointing to a need for this kind of effort and so this is something that they will be continuing. There is also an initiative working with high school and CEGEP students led by the University of Montreal with a similar intent.

On R&D, the CCCS will be looking to work with institutions to fund research looking to work through NSERC and SSHRC to provide grants for cybersecurity research. They also hope to support innovation by providing a space at their new building to help test and validate security technologies. The CCCS aims for these efforts to be pan-Canadian and to connect with other innovation centres.

# Real-world challenges

Security is important but we still need to define what is reasonable advice and what is reasonable to ask. Most people don't sit at a computer to 'do security', they want to get on with their online activities. We need to be careful when we devise tools and security messaging. We must ensure that our recommended cybersecurity practices are reasonable. There is a paper on the Rational rejection of security advice that provides that argument that, if you were to take the time required to implement all of the current security advice, you would be better off just ignoring it all and tackle a potential attack should you be targeted. This argument, while plausible is certainly not recommended but it does whimsically highlight the practical restrictions on security activities, which is why we should target possible security and not for perfectly security.

A challenge with cybersecurity advice is that it is not evergreen. An approach to increasing the longevity of advice would be to focus on perennial skills. For example, developing mental models and decision-making skills around online information sharing might prove to be more efficient than providing specific advice that becomes obsolete. MediaSmarts approach is to base tools in the principles of digital media literacy, there is enough evidence to convince consumers that critical thinking skill is already protective and they also want the resources to be practical so that they are pertinent. Their guides also include practical advice.



# Participants

**Dawson Mossman** [dawson.mossman@bluespurs.com](mailto:dawson.mossman@bluespurs.com)

Dawson has been involved in a variety of technical roles for over 15 years. I'm currently the Director of Technology at Blue Spurs, a Fredericton-based consulting company of about 100 people. In my current role, I have a focus on understanding how we can use and leverage emerging technology such as IoT, ML, and AI. CyberSecurity is a critical component across all of these areas as they continue to evolve and move into the hands of developers. I also have a passion for using technology to help with human rights issues such as poverty, safe drinking water and food, sustainability, and housing. Over the past two years, I've helped build a TechEd starter kit that provides kids with a hands-on opportunity to use technologies like IoT and ML with the AWS platform.

**Ed Juskevicius** [ed.juskevicius@canada.ca](mailto:ed.juskevicius@canada.ca)

Ed Juskevicius joined Industry Canada's telecommunications' engineering, planning, and standards team in 2009 as Manager for Infrastructure Security. In 2015, he became Manager for ICT Resilience within the Spectrum and Telecommunications Sector of the Government of Canada's department for Innovation, Science and Economic Development (ISED). He is currently working to understand the impacts that new AI and/or quantum-based technologies will have on the cyber security of public, academic, and private-sector networks, IT systems and end-user ICT devices.

**Jeff Thomson** [jthomson@antifraudcentre.ca](mailto:jthomson@antifraudcentre.ca)

Jeff Thomson works for the Operational Support Unit at the RCMP's Canadian Anti-Fraud Centre (CAFC). CAFC works with SERENE-RISC to distribute fraud awareness messaging. Jeff looks to find other opportunities to do awareness and can provide awareness information in support of other organizations wishing to raise awareness of cyberfraud.

**Julia Le** [Julia.Le@ontario.ca](mailto:Julia.Le@ontario.ca)

Julia Le is the Cyber Security Education Coordinator for the Ministry of Government and Consumer Services, Cyber Security Division in the Ontario Public Service. As a lead for the October Cyber Security Awareness Month and Partnerships she seeks out opportunities to collaborate with different levels of government and agencies. She can be reached at [Julia.le@ontario.ca](mailto:Julia.le@ontario.ca).

**Lynn Smith** [lynn.smith@canada.ca](mailto:lynn.smith@canada.ca)

Lynn Smith, is a Senior Policy Analyst with the National Cyber Security Directorate at Public Safety Canada, with responsibilities and experience for engagement with external stakeholders in the private sector, academia, and provincial and territorial officials on a range of issues including: digital service delivery, cyber security workforce planning, standards and best practices, and emerging technologies. Lynn is also a Steering Committee member of the Security Awareness Working Group (SAWG), where security practitioners from across the Government of Canada share resources, materials, and inform policies and procedures regarding security writ large.

**Michael Joyce** [michael.joyce@umontreal.ca](mailto:michael.joyce@umontreal.ca)

Michael Joyce is the Knowledge Mobilization coordinator for Canada's SERENE-RISC (Smart Cybersecurity Network – Réseau Intégré sur la Cybersécurité) initiative. He has

# Participants

worked to develop knowledge sharing and distribution tools such as the Konnect Knowledge sharing platform, and cybersec101.ca and is the editor-in-chief of the SERENE-RISC Quarterly Cybersecurity Knowledge digest. Prior to working with SERENE-RISC, Mr. Joyce formerly formally managed a global network of cybercrime experts and investigators worldwide for the Virtual Forum Against Cybercrime (VFAC) developed under the auspices of the United Nations Office on Drugs and Crime based at the Korean Institute of Criminology.

## **Natalia Stakhanova**      [natalia@cs.usask.ca](mailto:natalia@cs.usask.ca)

Dr. Natalia Stakhanova is an Associate Professor at the University of Saskatchewan. Prior to joining UofS, she was the NB Innovation Research Chair in Cybersecurity at the University of New Brunswick. Her work revolves around building secure systems. Working closely with industry on a variety of R&D projects, She has developed a number of technologies that resulted in 3 patents in the field of computer security. Natalia Stakhanova is the recipient of the UNB Merit Award, the McCain Young Scholar Award and the Anita Borg Institute Faculty Award. She is a strong advocate of Women in IT and co-founder of CyberLaunch Academy, an initiative that aims to promote science and technology among children.

## **Renaud J Levesque**      [Renaud.Levesque@cyber.gc.ca](mailto:Renaud.Levesque@cyber.gc.ca)

Renaud Levesque is the Director General of Cyber Outreach at the Canadian Centre for Cyber Security (CCCS). The CCCS is looking to interact and foster relationships and programs with organizations to increase the development of cyber security talent and capacity in Canada.

Renaud has significant experience in the delivery of capability and organizational change in highly technical environments. His has over 30 years experience as a Systems Engineer, responsible for the development and deployment of numerous systems and in leading IT-related R&D.

## **Sana Maqsood**      [SanaMaqsood@cmail.carleton.ca](mailto:SanaMaqsood@cmail.carleton.ca)

Sana Maqsood is a PhD student at Carleton University. She has over 10-years of industry, government and academic experience in HCI, security, and web development. Her current research focuses on developing games to improve end users mental models of security and privacy. She has also worked in the area of user authentication, looking at alternative password schemes on flexible display devices. Her latest project, a web-based digital literacy game developed in partnership with MediaSmarts will be deployed to Canadian schools in the near future

## **Sonia Chiasson**      [chiasson@scs.carleton.ca](mailto:chiasson@scs.carleton.ca)

Sonia Chiasson is the Canada Research Chair in User Centric Cybersecurity and an Associate Professor in the School of Computer Science at Carleton University. Her research group has done work on understanding and improving users' mental models of security and privacy. The group's research has looked at using infographics and interactive comics to teach adults and tweens about attacks and how to protect against various risks, using an interactive ebook to teach young children about online privacy, and developing a game to teach tweens about online privacy and security. All of their work involves user



# Participants

studies assessing the effectiveness of the tools at improving knowledge and behavioural intent

**Thierry Plante** [tplante@mediasmarts.ca](mailto:tplante@mediasmarts.ca)

Thierry Plante is a Media Education Specialist at Media Smarts, a national non-profit organisation for education and digital literacy. Since the 90s, Media Smarts has been creating resources for parents and teachers to enable them to become critical users of media. Cybersecurity is an important part of digital literacy and is part of Media Smarts' tools. Media Smarts is hoping to be able to bridge the gap between the different methods used to develop digital literacy across Canada. They also hope to create desire among teachers to learn about digital literacy and teach it to their students.

Media Smarts' most recent research on the digital well-being of Canadian families: <http://mediasmarts.ca/research-policy>

**Trace Muldoon** [Trace.Muldoon@gov.bc.ca](mailto:Trace.Muldoon@gov.bc.ca)

Trace Muldoon is the Manager of Security Awareness, Office of the Chief Information Officer, Province of B.C. Trace leads the Governance and Engagement teams within the Office of the Chief Information Officer for the BC Government. Trace is a Certified Information Security Manager (CISM) with over 30 years working with information systems and more than 12 years of information security related immersion. Trace has a wealth of experience, knowledge and good ideas and is passionate about cybersecurity awareness, risk management and best practices.

**Christine Menard** [Christine.Menard@CSE-CST.GC.CA](mailto:Christine.Menard@CSE-CST.GC.CA)

Christine manages the Get Cyber Safe Public Awareness Campaign, Communications Security Establishment. An example of the Campaign Initiatives is the holiday gift guide that helps consumers choose smart devices based on their security features and privacy policies. <https://www.getcybersafe.gc.ca/cnt/rsrccs/cmpgns/cmpgn-10/gft-gd-en.aspx>

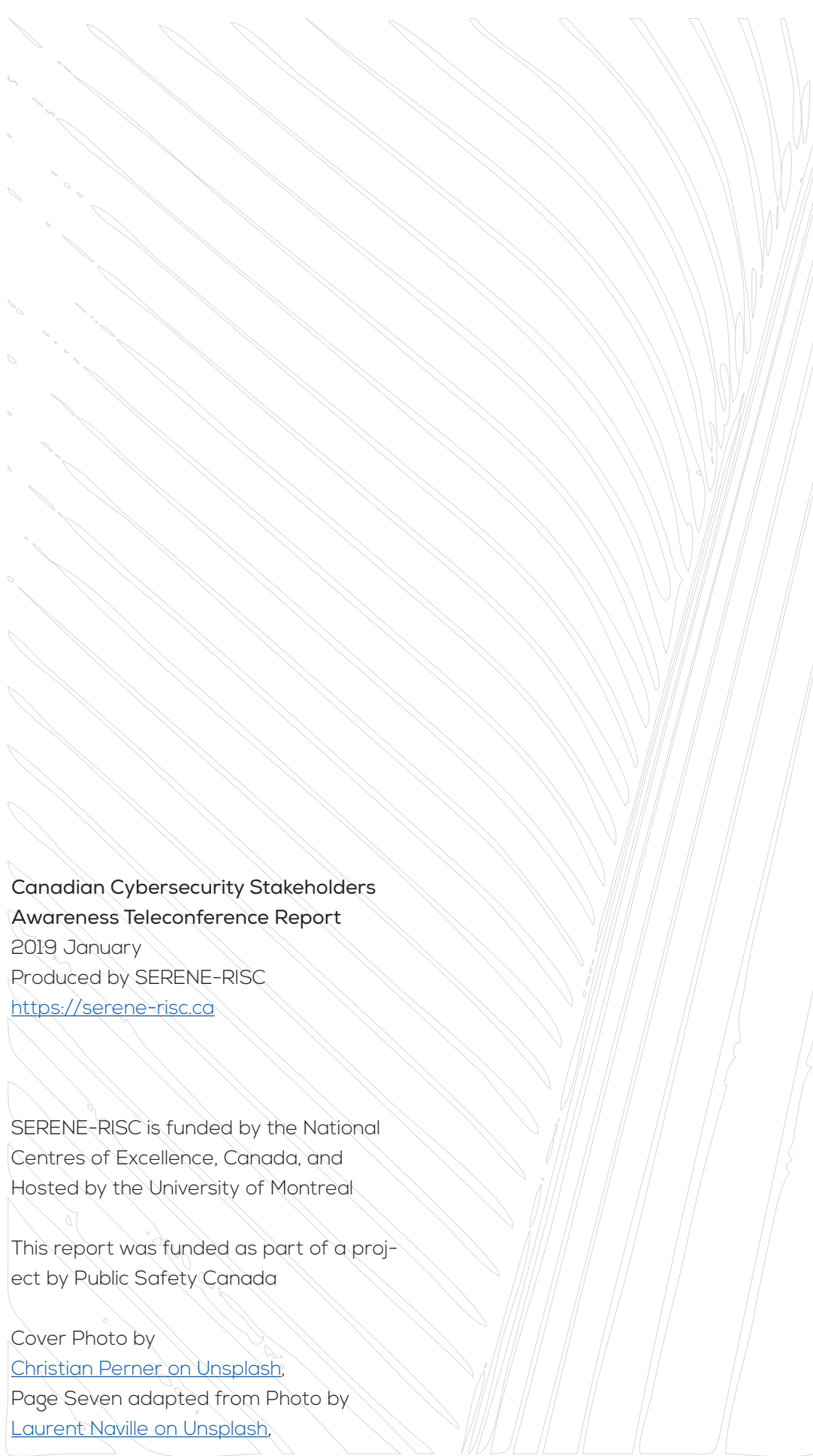
**Lauri Sullivan** [Lauri.Sullivan@CSE-CST.GC.CA](mailto:Lauri.Sullivan@CSE-CST.GC.CA)

Lauri Sullivan is the Supervisor of communications for the Canadian Centre for Cybersecurity (CCCS) at CSE.

Lauri led the communications planning for the creation of CCCS which was established on October 1st 2018. Her team works with partners across sectors to develop public communications about the CCCS and about cybersecurity.

**Veronique Menard** [veronique.menard@cyber.gc.ca](mailto:veronique.menard@cyber.gc.ca)

Véronique Ménard is the liaison officer in Montreal for the Communications Security Establishment (CSE) and for the Canadian Center for Cybersecurity (CCCS). Her goal is to establish partnerships with the industry, public sector, academia and various groups to increase awareness of cybersecurity and cybersecurity expertise across the province of Quebec. On behalf of CSE, she co-founded with SERENE-RISC the We Are Cyber network, a network aimed at advancing women in cybersecurity and STEM. She also delivers cybersecurity careers awareness talks at universities and soon in CEGEPS.



**Canadian Cybersecurity Stakeholders  
Awareness Teleconference Report**

2019 January

Produced by SERENE-RISC

<https://serene-risc.ca>

SERENE-RISC is funded by the National  
Centres of Excellence, Canada, and  
Hosted by the University of Montreal

This report was funded as part of a proj-  
ect by Public Safety Canada

Cover Photo by

[Christian Perner on Unsplash.](#)

Page Seven adapted from Photo by

[Laurent Naville on Unsplash.](#)