Canadian Law Enforcement
Cybercrime Priorities and Needs

Author:
Kevin Wennekes, Chief Business Officer, CATAAlliance

November 2015
Special Acknowledgement

The author would like to recognize Mr. Norm Taylor, President, Global Network for Community Safety, and Program Director, Canadian Association of Chiefs of Police Executive Global Studies Program, for his important contributions to the Summit and this report. Mr. Taylor was instrumental in facilitating discussions, encouraging engagement, and summarizing the main themes arising from the Summit. Mr. Taylor was also a valued sounding board, advisor, and editor to the author in finalizing this report.
# TABLE OF CONTENTS

Executive Summary..................................................................................................................1

1.0 – Introduction ..................................................................................................................3
   1.1 – Summit Project Team .................................................................................................4
   1.2 – Summit Speakers .......................................................................................................4
   1.3 – The Executive Boardroom Series .............................................................................5
   1.4 – Representative Organizations ..................................................................................6

2.0 – Cybercrime Summit Analysis .......................................................................................7
   2.1 – Critical Themes Emerging from Summit Discussions ..............................................7
   2.2 – Cybercrime Summit Bear Pit Summary ....................................................................7
       2.2.1 – Education ...........................................................................................................7
       2.2.2 – Create an International Cybercrime Network Centre .......................................8
       2.2.3 – Collaboration with Other Stakeholders ..............................................................8
       2.2.4 – National Strategy – Regional Delivery Centres ...............................................8
       2.2.5 – Modernized Policies and Strategies .................................................................9
       2.2.6 – Need the “Document” – But Just Do It Approach ...........................................9
       2.2.7 – Modernized Policing – Change the Culture .....................................................9

2.3 – Post Summit Evaluation Interviews ........................................................................10
   2.3.1 – Event Ratings .......................................................................................................10
   2.3.2 – Most valuable outcome .......................................................................................12
   2.3.3 – Areas for improvement .......................................................................................13
   2.3.4 – Future Topics and Speakers ...............................................................................14

3.0 – Cybercrime Priorities .................................................................................................17
   3.1 – Collaboration and Information Sharing ....................................................................17
   3.2 – Apply Needed Resources and Training ..................................................................18
   3.3 – Education ................................................................................................................18
   3.4 – Research ..................................................................................................................19
   3.5 – Advocacy and Policy Needs ....................................................................................20
   3.6 – Identify Champions .................................................................................................21
   3.7 – Critical infrastructure – Protection & Investments ..................................................21

Appendix A – Detailed Agenda

Appendix B – Summit Attendees
On October 19 & 20, 2015, the inaugural National Policing Cybercrime Summit\(^1\) was held in Toronto and featured over two dozen law enforcement, government, and industry speakers and attended by over 100 delegates. The Summit was hosted by founding partner organizations the Canadian Association of Chiefs of Police (CACP) and the Canadian Advanced Technology Alliance (CATAAlliance).

The aim of the Summit was to bring together cybercrime experts from law enforcement, industry, government and academia to share information and expertise towards the ends of identifying opportunities for a collaborative Canadian response.

The Summit was very well received with almost all rated aspects receiving a combined 90% Excellent to Outstanding rating by the 36 delegates interviewed.

This report summarizes the findings of three key deliverables resulting from the Summit: 1) a 13-point Theme Identification Summary; 2) a summary of the conversations that took place during open town-hall session, and; 3) a summary of findings of the post-Summit evaluation interviews.

Based on the above, the following priorities for addressing cybercrime in Canada have been identified:

1. **Collaboration and Information Sharing**
   a. develop regional cybercrime centres of excellence
   b. Capture, analyze, and report on cybercrime incidents and trends
   c. Continue offering annual and regional summits bringing multiple national and international stakeholders together
   d. More collaborative relationships among law enforcement agencies, industry, academia, and various provincial/federal government organizations

2. **Apply Needed Resources and Training**
   a. Human resources and technology acquisition
   b. Build internal capacity
   c. Develop common lexicon and definitions related to cybercrime
   d. Change culture in regards to hiring and training

3. **Education**
   a. Specific needs for training, knowledge-sharing and common learning among all stakeholder groups, including Policing Executives and Front Lines, among agencies, external stakeholders and the general public

---

\(^1\) [http://www.cata.ca/Media_and_Events/cybercrimesummit/default.html](http://www.cata.ca/Media_and_Events/cybercrimesummit/default.html)
4. **Research**
   a. Centralized, rigorous collection of national cybercrime statistics
   b. An environmental scan of cybercrime capabilities and resources
   c. Identify top cybercrime demands impacting on policing, categorize, focus on sharing solutions
   d. Quantify socio-economic impacts; better understand hacker motivations for early intervention; work more proactively with Universities

5. **Advocacy and Policy Needs**
   a. Updated lawful access policy
   b. Launch of national cybercrime strategy
   c. Engage with new government: advocate for cybercrime needs
   d. Jurisdictional and MLAT policies

6. **Identify Champions**
   a. Executive decision makers
   b. Subject matter experts

7. **Critical infrastructure – Protection & Investments**
   a. Internal and external threats
   b. Physical and data security infrastructure investments
On October 19 & 20, 2015, the inaugural National Policing Cybercrime Summit was held in Toronto and featured over two dozen law enforcement, government, and industry speakers and attended by over 100 delegates. The Summit was hosted by founding partner organizations the Canadian Association of Chiefs of Police (CACP) and the Canadian Advanced Technology Alliance (CATAAlliance).

The objective for this Summit was: to add tangible value to the fight against cybercrime by bringing police, industry, government and academic leaders together to exchange information on current cybercrime trends, offer demonstrations of forensic tools, share case studies, and receive updates from experts working in the field, towards the ends of identifying opportunities for a collaborative Canadian response.

The Summit aimed to bring a trifecta of key stakeholder groups together: 1) law enforcement; 2) industry providers; and, 3) other business, institutions and public service organizations, in the anticipation that key benefits could be unlocked. These included:

- Gaining a shared understanding of the current operational environment
- Learning about recent case studies
- Sharing best practices
- Broadening professional networks
- Discovering latest tools, technologies, and investigative techniques
- Developing new partnerships, prospects and collaborators
- Contributing to discussions by offering insider and outsider perspectives

This report summarizes the findings of three key deliverables resulting from the Summit:

1. A Theme Identification Summary as compiled by the Summit’s facilitator, Mr. Norm Taylor, Program Director and co-founder of the CACP Executive Global Studies Program, which was presented to delegates at the commencement of the second day of the Summit and validated by those in attendance as an accurate reflection of the key messages shared by the opening day speakers

2. A summary of the conversations that took place during the 60-minute Bear Pit session: an open town-hall session inviting open commentary from all Summit delegates, and moderated by Mr. Taylor

3. A summary of findings of the post-Summit evaluation survey: a telephone-based interview conducted with over three dozen Summit delegates

Along with identifying common themes, this report concludes with a set of recommended priorities and strategies as provided directly by delegates through these various consultation processes.
1.1 ― **SUMMIT PROJECT TEAM**

A dedicated core of individuals assisted in the planning and execution of this Summit. This report has also been reviewed and validated by them as an accurate summary of the themes, priorities and recommended strategies identified herein. Special thanks and consideration are offered to:

- **Eldon Amoroso**, Special Advisor, Canadian Association of Chiefs of Police
- **Alice DeBroy**, Webmaster & Production Manager, CATAAlliance
- **Cathie Malette**, Manager, Member Services, CATAAlliance
- **Christine Robson** MSIS, PMP, CMM III, I.T. Manager, Durham Regional Police Service
- **Guy Slater**, Superintendent, Calgary Police Service
- **Norm Taylor**, Program Director, CACP Executive Global Studies Program
- **Katherine Thompson**, VP Cyber Security, CATAAlliance
- **Kevin Wennekes**, Chief Business Officer, CATAAlliance
- **Kathy Wunder**, Director, Vancouver Police Service

1.2 ― **SUMMIT SPEAKERS**

The following speakers provided invaluable insights and helped spark thought-provoking conversations through their contribution of thought leadership and expertise.

The full agenda including speaker topics is included in Appendix A.

- **Jeff Adam**, Chief Superintendent & Director General, National Technical Investigation Services, Royal Canadian Mounted Police
- **Marie-Claude Arsenault**, OIC National Intelligence Priorities, Royal Canadian Mounted Police
- **Paul Beesley**, Superintendent, Director - Behavioural, Forensic and Electronic Services, Ontario Provincial Police
- **Ryan Broll**, Dr., Assistant Professor of the Department of Sociology and Anthropology, University of Guelph
- **Cory Dayley**, Sergeant, Cybercrime Support Team, Calgary Police Service
- **Dr. Mourad Debbabi**, President, National Cyber Forensics and Training Alliance
- **Bryce Evans**, A/ Staff Superintendent, Toronto Police Service
- **Erik Griffin**, Forensic Audio/Video Analyst, Durham Regional Police Service
- **Michael Haring**, Staff Sergeant, Royal Canadian Mounted Police
- **Peter Henschel**, Deputy Commissioner, Specialized Policing Services, Royal Canadian Mounted Police
- **Floor Jansen**, Dutch National Police Liaison Officer, Dutch National Cyber Security Center; and Strategic Advisor, High Tech Crime Unit, Dutch National Police
- **Ryan Jepson**, Staff Sergeant, Electronic Surveillance Unit, Calgary Police Service
- **John Menard**, Detective, Intelligence Technological Crime Unit, Toronto Police Service
- **Roger Merrick**, Director, Public Safety Investigations, Public Safety & Security Division, Department of Justice – Nova Scotia
- **Mark Patterson**, A/Inspector, Duty Inspector Program, Ottawa Police Service
- **Fraser Phillips**, Forensic Cellular Phone Analyst, Durham Regional Police Service
- **Troy Phillips**, Detective Constable, Durham Regional Police Service
- **Tony Reeves**, Staff Sergeant, Halifax Regional Police Service
• **Remco Ruiter**, Dutch Banking & Finance Liaison Officer, Dutch National Cyber Security Center; and Information Security Officer, Rabobank Group
• **David J. Roberts**, Senior Program Manager, IACP Technology Center, International Association of Chiefs of Police
• **Doug Ross**, Head, Technical Analysis Team (Digital Forensic Labs), Royal Canadian Mounted Police
• **Michael Russell**, Detective Constable – Forensic Computer Analyst, Durham Regional Police Service
• **Dave Seglins**, Reporter, Canadian Broadcast Corporation
• **Frank Skubic**, Detective Sergeant, Toronto Police Service
• **Peter Sloy**, Deputy Chief, Toronto Police Service
• **Scott Tod**, Deputy Commissioner, Ontario Provincial Police
• **Matthew Torigian**, Deputy Minister of Community Safety, Ontario
• **Joseph Yuhasz**, Supervisory Special Agent, Federal Bureau of Investigations

1.3 – THE EXECUTIVE BOARDROOM SERIES

The Summit featured CATAAlliance’s exclusive Executive Boardroom series: compared as being the "Dragon’s Den/Shark Tank" experience linking innovators to public safety experts. These offer private 25-55 minute sessions with a panel of 15-20 senior, cybercrime policing experts and allow Industry, Academic and other public safety organizations an opportunity, in focus-group like sessions, to showcase products or services, raise awareness or educate, and engage in meaningful dialogue in a private setting.

The invaluable contribution provided these “Dragons” cannot be understated and are recognized with special distinction as:

• **Jeff Adam**, Chief Superintendent & Director General, National Technical Investigation Services, Royal Canadian Mounted Police
• **Eldon Amoroso**, Special Advisor, Canadian Association of Chiefs of Police
• **Marie-Claude Arsenault**, OIC National Intelligence Priorities, Royal Canadian Mounted Police
• **Paul Beesley**, Superintendent, Director, Behavioural, Forensic & Electronic Services, Ontario Provincial Police
• **Peter Cuthbert**, Executive Director, Canadian Association of Chiefs of Police
• **Michael Haring**, S/Sgt. National Cyber Forensics and Training Alliance
• **Floor Jansen**, Special Advisor, Dutch National High Tech Crime Unit
• **Ryan Jepson**, Staff Sergeant, Electronic Surveillance Unit, Calgary Police Service
• **Richard MacCheyne**, D/Sgt. Cybercrime Unit, Toronto Police Service
• **Roger Merrick**, Director, Public Safety Investigations, Department of Justice - Nova Scotia
• **Troy Phillips**, Detective Constable, Durham Regional Police Service
• **Tony Reeves**, Staff Sergeant, Halifax Regional Police
• **David J. Roberts**, Senior Program Manager, International Association of Chiefs of Police
• **Christine Robson**, IT Manager, Durham Regional Police
• **Doug Ross**, Head, Technical Analysis Team (Digital Forensic Labs), Royal Canadian Mounted Police
• **Guy Slater**, Superintendent, IT Division, Calgary Police Services
• **Joseph Yuhasz**, Supervisory Special Agent, Federal Bureau of Investigation
1.4 – REPRESENTATIVE ORGANIZATIONS

The following is a list of organizations represented at the Summit. The complete delegate list is provided in Appendix B.

ADGA Group
B.R.A.K.E.R.S
Birch Forest Projects Inc.
BlackBerry
Calgary Police Service
Canada Post Corporation
Canadian Advanced Technology Alliance
Canadian Association of Chiefs of Police
Canadian Broadcasting Corporation
Canadian Radio-television & Telecommunications Commission
CISCO
Collaborative Centre for Justice and Safety
Department of Justice, Nova Scotia
Digital Boundary Group
Durham Regional Police Service
Dutch National Police
Federal Bureau of Investigations
Global Network for Community Safety
Halifax Regional Police
Halton Regional Police
International Association of Police Chiefs
La Cité
Motorola Solutions
NCFTA Canada
NCI
Niagara Regional Police Service
nTerop Corporation
Ontario Centres of Excellence
Ontario Police College
Ontario Provincial Police
Ottawa Police Service
Peel Regional Police
Philip Morris International
PRIMECorp
Ministry of Community Safety, Province of Ontario
Q9
Rabobank
Radius Security
Royal Bank Canada
Royal Canadian Mounted Police
SAS Canada
Service de police de la Ville de Montréal
SERENE-RISC
Sûreté du Québec
Surrey RCMP Detachment
Toronto Police Service
Unisys Canada
University of Guelph
University of Waterloo
Vayyoo Inc
York Regional Police

SPECIAL THANKS TO SPONSORS
This portion of the report reveals the key summative findings from the three principle sources: 1) Mr. Norm Taylor’s summary of themes arising from the presentations and conversations that took place on the first day of the Summit; 2) the Bear Pit summary; and, 3) the post-Summit evaluation interviews.

2.1 – Critical Themes Emerging from Summit Discussions

These are the 13 key themes captured and presented by Norm Taylor at the commencement of the second day of the Summit. These were individually reviewed and the assembly asked to validate, repudiate or elaborate on recommended changes or additions. The final list is as follows:

1. The ‘cyber’ shift in crime and victimization – becoming a recognized priority at policy level
2. Police are in the information business … Police must mature into the digital age
3. Social engineering – currently a one-way battle, occurring in a relative vacuum
4. Collaboration – trust and cooperation can be built upon the business case
5. Mobilization works
6. Without reporting, we are flying blind
7. Without collaboration and coordination, we are spinning our collective wheels
8. An engaged and informed public is a potentially powerful resource
9. Public engagement and police legitimacy are interconnected issues
10. We know what needs to be done … need the will and the engagement
11. Secondary victimization compels the business case
12. Information sharing is vital to prevention and intervention
13. Without public education … our systemic responses are inadequate

2.2 – Cybercrime Summit Bear Pit Summary

The following key themes arose from the Bear Pit session – a town hall type conversation facilitated by Norm Taylor.

2.2.1 – Education

2.2.1.1 – For all Law Enforcement Agents

A common lexicon and definition of what is “it” (cybercrime.) An understanding on the pervasiveness of cybercrime in that a digital footprint can be found in almost any modern crime. Information on tools, techniques and processes for investigating cybercrime and preservation of evidence. An understanding of what does and does not constitute a crime requiring a police response.
2.2.1.2 – For Chiefs/Senior Executives
The need to educate senior law enforcement executives on the all-encompassing impacts of cybercrime and its impact on the front lines with respect to time, resources and skills. Offer some basic lessons in appropriate lexicon and provide exposure to common social media and internet-based threats i.e. bots, Dark web, Going Dark, phishing, etc.

2.2.1.3 – For Front Line
Need to share case studies, best practices, and recommended tools/techniques. Need access to a global network of subject matter experts and law enforcement contacts for the purposes of information sharing and collaborative response to cross-jurisdictional crimes.

2.2.1.4 – For General Public
Need education campaigns to demonstrate how to protect themselves and how to report instances of cybercrime. Need to educate the public on what constitutes a cybercrime requiring police intervention, and those that do not.

2.2.2 – Create an International Cybercrime Network Centre
Similar to what has been done with the National Child Exploitation Coordination Centre, create an online portal serving as a global epicentre for law enforcement to:

- Access a global network of peers and subject matter experts
- Share best practices, case studies, tools and tips
- Facilitate multi-jurisdictional investigations
- Coordinate investigative files
- Access training or online briefings with key cybercrime experts
- Act as a cybercrime reporting centre for the public
- Identify emerging trends and threats
- Host special events such as Hackathons, Cybersprints, etc.
- Conduct and disseminate research – develop the “So What?” stories

2.2.3 – Collaboration with Other Stakeholders
As important as collaboration among law enforcement agencies and breaking down silos is noted, so too is the need for greater collaboration with private sector, other government agencies (Public Safety Canada, Industry Canada, CRTC, CSEC, CSIS) and non-traditional groups such as the Canadian Association of Retired Persons and Canadian Bankers Association.

2.2.4 – National Strategy – Regional Delivery Centres
Need the release of the national cybercrime strategy, which can help facilitate adoption of key strategies by any sized detachment.

An identified need for 3-4 Regional Delivery Centres (RDC) that can serve as a cybercrime lab providing timely, higher-end services (i.e. decryption, audio/video analysis, big data analysis) and allowing for local services to focus on more thorough investigatory and evidentiary collection techniques.

---

2 When these themselves have been fully established/understood by Law Enforcement
This RDC should also be able to provide funding for training and technology to the Departments in the region they serve, as well as act as an information hub.

2.2.5 – Modernized Policies and Strategies
A need to bring lawful access into the 21st Century: seeking balance between privacy and the need for timely response to a potential mortal threat situations.

A modernized policy to enable the interception and decryption of messages and data.

More MLATs to better enable prosecution of cybercriminals in foreign jurisdictions.

2.2.6 – Need the “Document” – But Just Do It Approach
Work towards creating the needed cybercrime doctrine, but not at the sake of discouraging action and learning on the ground. These two needs can be developed concurrently, with the learnings developed in action applied to a living document that as a result is continually evolving. Cybercrime requires immediate responses and is ever-evolving and as such any documentation of cybercrime definitions and techniques must be continually evolving as well.

2.2.7 – Modernized Policing – Change the Culture
Frequently mentioned that policing culture requires dramatic shifts in two key areas:

1. Recruitment:
   a. May not be necessary to own or develop policing capacity for certain cybercrime needs: contracting to outside experts can be less costly and more effective
   b. When hiring key talent who have specialized skills, do not have them walk a beat or drive a patrol car in Whitehorse for three years – may need to employ greater number of civilians with these specialized skills
   c. Find ways to convert gray hats to white hats in the service of law enforcement: leverage the appeal and influence that becoming a police officer can offer

2. Communications:
   a. Break down silos – share data, information, expertise and resources more readily within/between Departments. Can help in deconfliction.
   b. More bottom-up accessibility: allow lessons from the front lines to be more immediately shared and acted on by senior executives
   c. Check egos at the doors and seniority does not always reflect superiority: especially with matters relating to the internet, the younger generation of officers will be far better informed and equipped to manage the challenges of cybercrime. They will likely be familiar with and users of most recent developments in social media and other open source communication tools
2.3 – Post Summit Evaluation Interviews

In the two-week period following the Summit, CATAAlliance’s Chief Business Officer, Kevin Wennekes, conducted 36⁴ telephone interviews with Summit delegates. The interview-based survey contained a minor number of quantitative questions, while relying more on open-ended questions to solicit detailed, qualitative responses to key questions related to perceived priority areas to advance and what future Cybercrime Summits should address.

2.3.1 Event Ratings

A strong sample of each of the respondent groups participated in the evaluation.

⁴ 39 total interviews conducted however 3 took place after the initial analysis was complete
The chart above reveals the results of a series of questions that asked respondents to rate each area on a scale of 1 – 7 where 1 = Extremely Poor and 7 = Outstanding.

As demonstrated in these results, almost without exception, every aspect of the Summit was collectively rated either Excellent or Outstanding by more than 90% of respondents.

Those interviewed were asked to elaborate on any of the areas they had rated. The following outlines some common themes.

2.3.1.1 – Audience Participation Levels

- Many remarked on the effectiveness on the part of Norm Taylor to engage the audience and encouraging conversation and questions: recommended continued use of facilitation at any future Summits as a positive means of ensuring continued engagement
- Respondents offered a number of reasons identifying possible challenges in getting people to speak up or ask questions, including:
  - Challenges in speaking ‘above their pay grade’ given the mix of executive and front line officers (it should be noted that many respondents commented the intermingling of executive and front lines was one of the most valued aspects of participating in the Summit)
  - Having Dragon’s Den run concurrent to plenaries sometimes resulted in not having the right authorities in the room to speak further on an issue raised
  - Some found the audience size of 100 too intimate to ask questions, whereas others felt it was perfect and cautioned against creating too large a crowd which would make it more difficult to engage
  - Fear of asking a stupid question or looking thus as a result of engaging in the discussion
2.3.1.2 – Forum as a Networking Opportunity
Clear consensus on the superior level and quality of networking that took place during the Summit. This was also mentioned by a clear majority of respondents as one of the most valued outcomes of their participation in the Summit, which is explored in greater detail further in this report.

2.3.1.3 – Forum Venue & Refreshments
The venue and quality of refreshments were uniformly seen as Excellent to Outstanding. The Pearson Convention Centre was seen as an ideal venue for a 2-day Summit of this nature offering a professional, functional and esthetically pleasing surrounding, easy access to the Summit’s designated hotel, with ample free parking and wi-fi access.

The one recurring complaint, even among those who rated it highly, was over the lack of nearby (walkable) entertainment and dining options in the immediate area surrounding the venue. That said, respondents did agree that as this was only a 2-day event with a well-catered reception on the first evening and the designated hotel’s restaurant described as offering excellent dining options, it wasn’t deemed detrimental to the fuller Summit experience.

In fact, some delegates reflected the lack of surrounding distractions created more frequent opportunities for networking as most delegates attended the reception and were otherwise found in the hotel restaurant or bar where conversations started during the Summit program could be continued in a more relaxed setting.

2.3.1.4 – Amount of new information learned
But for only a handful of respondents, the Summit provided an abundance of new information and insight. Those relative few who rated this in the middle-high categories typically identified themselves as senior authorities with long-standing experience in the area of cybersecurity or cybercrime.

2.3.1.5 – Summit Rating Overall
As revealed, 98% of respondents rated the Summit in the Excellent to Outstanding ranges. When questioned if they would be interested in taking part in future Summits, 100% identified they would, with some qualifying this as depending on the specific content. The topic of what future summits should include in order to make it even more relevant to delegates is explored further in the report.

2.3.2 – Most Valuable Outcome
Respondents were asked what the most valuable outcome was to them as a result of their participation in the Summit.

The responses to this question overwhelmingly fell into one of two distinct categories: the networking opportunities and/or the level of new information or understanding that was gained as a result.

2.3.2.1 – Networking
Almost half of delegates interviewed remarked that the level of quality networking they were able to engage in was the most valued outcome. Interviewees often stressed the importance of 4 key networking relationships:

1. Among law enforcement community
2. Emphasized not only peer-to-peer, but those that allowed for dialogue between executive and front line members

2. Law enforcement and industry exchanges – the value of the conversations which took place during Executive Boardroom were highlighted by most who participated and law enforcement respondents appreciated having industry representatives who are typically at the forefront of innovative solutions taking part

3. Enhancing international networks – many remarked on the valuable lessons shared by the international speakers

4. Building national networks – law enforcement delegates appreciated meeting other Canadian law enforcement agents outside of their normal circles

2.3.2.2 – Gaining New Learning and Understanding

In conducting an analysis of the comments provided, there were 43 instances where respondents identified having learned something new or arrived at a new shared understanding. The most common themes and areas are identified below, and listed in order of frequency of mention:

- There were 19 mentions where respondents indicated obtaining a new shared understanding that they were not alone in their cybercrime challenges and in fact like most of their peers “were in a similar boat” in the sense of similar needs for funding, resources, strategies, tools and training
- There were 9 mentions of appreciating learning of senior executive views and being able to share views with them
- There were 9 mentions where respondents indicated hearing from the front lines on their challenges and the case studies offered brought tremendous value
- The arrival at the 13 themes presented on Day 2 was specifically cited by four respondents
- Mentioned on a couple of occasions were:
  - The realization that in Canada the banks and police are in completely different places with little to no collaboration
  - Appreciating that cybercrime is an interest among stakeholders outside of law enforcement
  - Learning obtained from the international speakers
  - Hearing more about the pending national cybercrime strategy

2.3.3 – Areas for Improvement

Delegates were asked what could have been done better at the Summit or if any expectations were left unfulfilled. Most of the comments provided were in fact suggestions for future speakers and topics, which are explored in greater detail further in the report.

There were some common recommendations and the most repeated include:

- **Summit Objectives/Action Plan**
  - A number of respondents spoke to wanting to see more substantive objective setting and action planning take place. Suggestions included the need for a clear statement or declaration at the outset of the Summit describing what was hoped to be achieved and
which could have helped focus group discussions towards a set of clear action items that could have been agreed to and adopted in the Bear Pit and provide takeaways for attendees to act upon
  o Look at creating sub-committee or working groups to address specific challenges resulting from the Summit and a reporting back function

• Agenda Recommendations
  o While most delegates believe the Summit must continue bringing executive and front line staff together, it was recommended that future summits have different streams that would speak to the specific interests of each group while bringing everyone together for speakers whose messaging would resonate with the entire audience
  o Consider breaking group into roundtables to address specific topics/issues
  o More industry speakers, potentially partnered with a law enforcement customer, describing how they have effectively implemented the product/service
  o More cybercrime related technology demonstrations from vendors
  o More federal government representation
  o Moving the focus of discussions from what we are not doing, to what we could/should be doing

• Executive Boardroom Series
  o Should consider holding these sessions on the day before or after the Summit to avoid removing these experts from the plenary
  o Populate with a greater number of cybersecurity technology providers

• Encourage even greater levels of conversation/networking
  o Consider assigned seating for meals and in plenary
  o Instead of asking for questions from the audience, ask individuals a specific question to engage/begin the conversation

2.3.4 – Future Topics and Speakers
In anticipation that another Summit will be held in 2016, interviewees were asked what topics they like to see added to the agenda or further explored, and which organization or individual would they recommend be featured on the agenda.

The list below provides an overview of these results.

• More case studies – a clear majority of delegates indicated wanting to hear more examples similar to the Ashley Madison presentation offered by Toronto Police Services. From case management challenges, timelines, and technical perspectives
  o While some indicated having TPS come back next year to update Summit attendees on progress in the Ashley Madison case, most simply recommended watching the news for latest stories and asking those involved to take part
• **More front line stories** – the presentations from Durham and Calgary police services and the narratives they provided were of significant interest to both law enforcement and industry attendees. Law enforcement agencies appreciated learning about what their peers were undertaking and the challenges to prepare to address in similar pursuits, while industry members appreciated the better understanding of what technology was being used and by inference what else was needed to assist
  o Organizations recommended to approach include RCMP, TPS, OPP, QPP, VPS

• **More international speakers**: seek out cybercrime authorities from other countries to continue sharing best practices and unique programs being undertaken around the world and the lessons that can be adopted here in Canada.

• **Industry Partnerships** – a significant number of interviewees identified learning more about how technology has been applied in the field was of interest and these presentations should include the law enforcement and industry partners sharing their story together. Not meant to be a sales pitch, rather a technology success story that details the problem and how collaboratively a solution was implemented

• **External experts** – many suggestions for bringing in speakers representing organizations who are also playing a critical role in cyber security.
  o Banks, insurance agencies, vendors, media and federal government organizations were frequently mentioned as potential candidates.
  o Prosecutors – stories about successful/failed prosecutions based on digital evidence – how are defence attorneys attempting to discredit evidence
  o CSIS, CBA, Utilities, Oil & Gas, PSC, CCIRC, Pan Am or Olympics, Canada Post, NSA, FBI, DHS, IC4, NCFTA (U.S. version), Industry Canada, CRTC, SERENE, DHS, INTERPOL, Scotland Yard

• **Research findings/opportunities** – many suggested attempting to include presentations revealing the results from relevant research studies or from sources of various funding to discuss how to access and or what relevant research is currently underway through these groups
  o DRDC, Universities, SERENE

• **Lawful Access** – a roundtable that brings together law enforcement, telco’s and privacy commissioner for open and candid discussion towards arriving at mutual understanding and ideally policy directions for the future. Raise and debate the R v. Spencer\(^5\) decision.

• **Prevention versus reaction**: workshops that educate law enforcement agents on how to prepare for and quickly respond to cyberattacks against their systems. How to prevent/protect against social engineering hacks. How to effectively use social media to communicate with the public. what new strategies are in place, threats in the pipe and techniques to address new threats

---

• **Vendor showcase** – more cybercrime solutions vendors to demonstrate related products and services: not much is known about existing innovation

• There were a number of **infrequently recommended** topic areas, including:
  
  o Darkweb
  o Going Dark
  o Creating culture change in policing environments
  o Encryption threats – partnered with Apple or Blackberry representative
  o Creating more effective MLATs
  o Infrastructure
  o More detailed review on the National Cybercrime Strategy
  o Progress report on Summit’s 13 Themes and initiatives undertaken as a result of the Summit
The following priorities are based on the feedback collected during the interviews and also takes into consideration the preceding analysis provided in this report. They are provided in order of frequency of mention during the interviews and in accordance with the common themes resulting from the other source information derived from the Summit.

3.1 – Collaboration and Information Sharing

The need for greater collaboration among law enforcement agencies, and with external partners including industry, academia, and international partners was mentioned in 50% of the interviews conducted and a recurring theme throughout the Summit.

One of the most frequently identified means of accomplishing this is through the development of regional cybercrime centres of excellence, which could allow for:

- the development of national and international community of subject matter experts that can be easily referenced and provide points of contact
- information and resource pooling
- foster and maintain equipment and expertise
- spearheading cybercrime initiatives: provide funding and training
- Provide advanced cybercrime expertise and services allowing local departments to focus on building generalist capabilities
- Offer national big data services and large file information sharing
- Provide virtual networking, training, videoconferencing, etc.
- Act as a centralized reporting centre for cybercrime incident reporting among all Canadian organizations and individuals
  - Capture, analyze, and report on cybercrime incidents and trends

In terms of collaboration, Summit delegates identified a number of suggestions and recommendations:

- Share knowledge and expertise among law enforcement agencies, such as:
  - More criminal case studies sharing lessons learned and recommended best practices
  - Tools and technologies that can be used – testimonials/demonstrations of these in practice
  - Organize international visits/exchanges
  - Create specialized working groups who conduct regular (monthly, quarterly) updates to the broader community
  - Enable bottom-to-top information sharing and learning opportunities
- Continue offering annual summits bringing multiple national and international stakeholders together towards identifying latest advancements, techniques, solutions, etc.
Consider offering a series of regional workshops, featuring a base of recognized subject matter experts and including localized expertise at each session, thus resulting in broader participation and a means of creating a preliminary catalogue of national cybercrime capability

- Create needed national/provincial dialogues among agencies to allow for coordinated responses, learning, strategies
- Seek to make better use of university research facilities and funding: have universities come to better understand unique law enforcement cybercrime needs
- More involvement of banks, telcos, insurance stakeholders
- Seek positive, collaborative relationships with industry: change the business model to allow for joint R&D and subsequent commercialization dividends

### 3.2 — **APPLY NEEDED RESOURCES AND TRAINING**

Almost a third of interviewees indicted the immediate application of resources (funding, tools, community building platform) was required.

There was an urgency relayed for the need to begin identifying capability gaps, hiring/training required subject matter experts, and building capacity among all responders to understand and address cybercrime and the digital footprint that can be exploited in almost any type of crime.

There was also a repeated need to better understand what tools exist to help in the field, and validation of their effectiveness.

A handful of respondents identified there was a need for a common lexicon and set definitions of cybercrime, which will help demystify cybercrime and enable the development of general cybercrime capability and understanding among all agencies and personnel.

Finally, the need for organizational culture change in hiring and training practices was mentioned as a requirement for securing, deploying, and retaining highly qualified cyber skilled talent. The current practice of having new recruits walk the beat or serving in remote areas for the first 3-5 years of their career needs to change, especially in regards to recent computer sciences graduates. Alternately, it was recommended that law enforcement hire more civilian staff and leverage the singularly unique career environment – having a true positive social impact and “catching bad guys” – as a means of acquiring skilled talent in the challenge that typically higher-paid salaries in the private sector can offer.

### 3.3 — **EDUCATION**

This was frequently mentioned by almost a third of all interviewees. As in the Bear Pit session, the need for education exists for all stakeholders, ranging from executive and front line officers, and including federal and provincial governments, police boards and civilians. The common themes from those groups cited most frequently are captured below.

**Executive level staff** were the predominantly mentioned group during the interviews, as all final decision making in terms of deployment of funding, resources and training are approved by them. Delegates found the Summit, in its approach to bringing front-line and executive officers together, helped enable for
some much-needed bottom-up information sharing and exchange, but there were many obstacles in place, including:

- Most senior executives not of the information generation and ‘everyday’ social media, internet, and digital technology terminology/understanding continues to elude them
- Need to break down information silos internally and among other jurisdictions: historically demonstrated to be a challenge and one that persists
- More bottom-up communications required in an environment that typically does not provide or culturally allow for speaking above one’s pay-grade: as such, Chiefs need advisors, but who precisely can and should advise them?
- Need to avoid having Chiefs promote any one solution as the final or only way to address a cybercrime response – many solutions needed to an ever-changing hacker toolkit

Among law enforcement agents more broadly, there is a need to understand that it is one thing to be an officer and uphold the law, but without the understanding of the technology, and if one’s finger is not on the pulse on how people are infringing the law using digital means, it’s impossible to uphold the law or build a strong case using evidence one doesn’t understand exists.

Interviewees stressed that while specialized response teams were required, it should not be at the expense of generalized training for all officers as every crime committed will have a digital evidence trail that can be exploited, often without leaving one’s desk, and further need to understand how to capture and preserve digital evidence for eventual trial.

Calls for more information sharing and case study examples were often cited by respondents. Law enforcement agents need to be sharing best practices, lessons learned and commonly used tools and techniques more frequently and openly, while where possible pooling resources and talent among jurisdictions.

Education of the general public and of political leaders was also frequently identified as a key need. The education in these instances took on two primary areas of focus: 1) Increasing awareness of Canadians on the types of cybercrimes they can become victims to, how to protect themselves and ultimately how to report it to the proper authorities; and 2) education about and advocacy of the needs of the law enforcement community to effectively address cybercrime to generate the necessary political will to enact change.

3.4 – RESEARCH

The need for valid, evidence-based research was another common area cited by almost a third of respondents. Similarly themed study areas emerged along with a variety of unique suggestions. Most are identified below:

- Need a more rigorous and comprehensive collection of cybercrime stats across the spectrum of offences. Potential to stake a claim in this space where Canada can make a difference. Currently, underreporting is a serious problem and could be partly resolved through the provision of a national online reporting system
• Conduct an environmental scan of cybercrime capabilities and resources in Canada: who is doing what, where are individual Canadian police forces in terms of existing cybercrime capability, what tools are in the toolkit and who are using them?
• Identify the top priorities from among law enforcement cybercrime experts. Categorize these and determine which impact on policing the most then focus on identifying/sharing solutions
• Study why hackers choose to commit cybercrimes and combat it through early prevention and/or encouraging them to become white hats in service of the law
• Studying the total socio-economic impacts of cybercrime: quantify the economic metrics and impacts to personal lives
• Identify those truly unique cybercrime challenges and partner with universities to help research and resolve

3.5 – Advocacy and Policy Needs
Almost a third of respondents identified the need for adequate policy to address cybercrime, and having effective advocacy plans in place to encourage support, public understanding and adoption of these needs.

The most frequently mentioned policy need related to those around lawful access and working to ensure law enforcement receives timely responses to lawful access requests, especially in situations (i.e. suspected abductions, missing persons, child exploitation) where delays could result in fatal consequences. Law enforcement agents understand the need to balance privacy concerns and invite more open dialogue with telecommunication providers and federal regulatory and oversight bodies towards forming policies that embrace protecting an individuals’ privacy versus the safety and security of those related to the lawful access request.

Two other key mentions related to a formal launch of the national cybercrime strategy similar to that undertaken for child exploitation, as well as a need to immediately begin advocating cybercrime needs to the new Federal government.

Other items of note:
• Seek standardization of approaches and policy in conjunction with training and resources
• Define who has jurisdiction and responsibility when involving multiple agencies
• Improve the effectiveness of and expand mutual legal assistance treaties (MLATs)
• Need to work with smartphone manufactures to address encryption needs: should there be a back door exploit in light of current approach by some to create encryption processes they themselves cannot decrypt?
• Suggestion to call the providers to ‘freeze’ the data until legal authorization was received to send it to the police. This would prevent the data from being erased due to any time delay.
3.6 – IDENTIFY CHAMPIONS

Seven interviewees remarked on the need to identify national champions to drive the issue forward. Most agreed it was critical to identify senior leaders who will passionately advance cybercrime awareness by rallying peers, subject matter experts, and key government stakeholders to act on a unified front.

These champions need to be decision-makers with the authority to mobilize action, direct funding, and work with others to claim ownership over key issues and challenges.

Seek those who are ready to form a “coalition of the willing” and rally them to advance specific priorities and needs.

3.7 – CRITICAL INFRASTRUCTURE – PROTECTION & INVESTMENTS

A handful of interviewees remarked that while it was not heavily discussed during the Summit, the need for the protection of critical infrastructure (i.e. gas, hydro, telecommunications) and of law enforcement databases and networks were also mission-critical components to the broader cybercrime picture.
### APPENDIX A

**DAY 1 - OCTOBER 19**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:30 a.m.</td>
<td>Registration - Networking Breakfast</td>
</tr>
<tr>
<td>8:15 a.m.</td>
<td>Opening Remarks</td>
</tr>
<tr>
<td>8:30–9:00 a.m.</td>
<td>Opening Keynote Speaker</td>
</tr>
<tr>
<td></td>
<td><strong>Matthew Torigan</strong>, Deputy Minister of Community Safety, Ontario</td>
</tr>
<tr>
<td>9:00–9:30 a.m.</td>
<td><strong>Joseph Yuhasz</strong>, Supervisory Special Agent, Federal Bureau of Investigations</td>
</tr>
<tr>
<td></td>
<td><em>Business E-mail Compromise – A Global Perspective</em></td>
</tr>
<tr>
<td></td>
<td>This presentation will introduce the audience to one of the most prolific and damaging Cyber scams seen today. The business E-mail Compromise (BEC) scam primarily targets businesses of various sizes and affects countries all over the world. Although the BEC scam is primarily a sophisticated social engineering scam, the BEC scam has cost victims over $1 billion to date. To date, the FBI has identified at least four variations of the scam as well as a variation that primarily targets individuals.</td>
</tr>
<tr>
<td>9:30–10:15 a.m.</td>
<td><strong>Remco Ruiter</strong>, Dutch Banking &amp; Finance Liaison Officer, Dutch National Cyber Security Center; and Information Security Officer, Rabobank Group</td>
</tr>
<tr>
<td></td>
<td><strong>Floor Jansen</strong>, Dutch National Police Liaison Officer, Dutch National Cyber Security Center; and Strategic Advisor, High Tech Crime Unit, Dutch National Police</td>
</tr>
<tr>
<td></td>
<td><em>Always change a winning team! Or: How building alliances changed two great teams into an even better one.</em></td>
</tr>
<tr>
<td></td>
<td>It's 2013: online payment systems are down for weeks because of massive DDoS attacks on Dutch banks. In 2014 the same banks lost billions and billions of Euro’s on Russian APT attacks. ATM’s seem to spontaneously spit out Euro’s that disappear into the pockets of money mules. It's 2015 and things are really getting out of hand; small businesses are going bankrupt because they have been targeted by criminals who were able to alter their payments using Remote Access Trojans. Remco and Floor will draw a picture of what could have happened if Dutch banks and Law Enforcement Agencies would not have cooperated closely on the fight against cyber crime over the last years.</td>
</tr>
</tbody>
</table>
Confronting Law Enforcement Cyber Threats: Assessing Risk, Building Resiliency, Managing Resources

Law enforcement agencies and their personnel are increasingly being attacked by individuals, special interest groups, organized criminal enterprises, and even nation states. The attacks range from posting offensive material online to defacing websites, denial of service (DDOS) attacks, seizing and encrypting critical agency systems through the use of ransomware malware, identity theft, and evidence destruction. The challenge facing law enforcement is amplified as agencies enhance their online presence, increase their use of mobile devices, and expand the array of digital evidence generated through the growing adoption of body-worn cameras and other technologies. This session will include a discussion of key trends and issues, and feature an overview of the IACP Law Enforcement Cyber Center (www.IACPCyberCenter.org). The Center is an online portal designed to address three principal areas: 1) cybercrime investigation, 2) digital evidence collection and management, and 3) information systems security. The objective is to focus on messaging and outreach activities to engage law enforcement practitioners and to channel users to emerging news, established training, technical assistance, investigative tools and support, and online resources with strategic partners, including the Canadian Association of Chiefs of Police.

CACP Global Studies Group – Collaborative Cybercrime Framework Study

Challenge of Public Engagement
A panel featuring noted mainstream media and senior police executives discussing the current cultural and systemic barriers preventing the open and free exchange of information, and exploring the means by which these can potentially be overcome.

Dave Seglins, Reporter, Canadian Broadcast Corporation
Doug Ross, Head, Technical Analysis Team (Digital Forensic Labs), Royal Canadian Mounted Police

Paul Beesley, Superintendent, Director - Behavioural, Forensic and Electronic Services, Ontario Provincial Police
The Future of Cybercrime – positioning a law enforcement organization for the new paradigm.

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
</table>
| 2:00 – 2:30 | **Jeff Adam, Chief Superintendent, Director General, National Technical Investigation Services, Royal Canadian Mounted Police**  
**The RCMP National Cybercrime Strategy**  
An overview of the national Force’s cybercrime strategy currently under development and the importance for input and consultation with those outside of the policing community. |
| 2:30–2:45 p.m. | **Break** |
| 2:45–3:30 p.m. | **Frank Skubic**, Detective Sergeant (Case Manager)  
**John Menard**, Detective (Intelligence Technological Crime Unit)  
**Bryce Evans**, A/ Staff Superintendent, Toronto Police Service  
**Avid Life Media (Ashley Madison Hack) investigation**  
A discussion around the challenges in the investigative process, jurisdiction issues/concerns, technology challenges and other aspects related to this high-profile data and ID theft case. |
| 3:30–4:15 p.m. | **Roger Merrick**, Director, Public Safety Investigations, Public Safety & Security Division, Department of Justice – Nova Scotia  
**Ryan Broll, Dr.**, Assistant Professor of the Department of Sociology and Anthropology, University of Guelph  
**Tony Reeves**, Staff Sergeant, Halifax Regional Police Service  
**Cyberbullying: Issues and Opportunities for Law Enforcement**  
Cyberbullying consists of bullying behaviours perpetrated electronically, such as over the Internet or by text message. Addressing cyberbullying is increasingly becoming a police responsibility in Canada, the United States, and elsewhere. This panel will introduce police members to current issues in cyberbullying prevention and response. Topics addressed include the challenges of policing cyberbullying, the potential value of enhanced collaboration with relevant stakeholders, and innovative strategies being used by select Canadian police agencies. Relevant data on youth technology use and the prevalence of cyberbullying will be provided. |
| 4:15–4:30 | **Day 1 Wrap Up** |
| 6:00 p.m. | **Cocktail Reception and Networking**  
Check-in starts at 5:45 p.m.  
Reception ends at 9:00 p.m. |
# DAY 2 - OCTOBER 20

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:30 a.m.</td>
<td>Registration - Networking Breakfast</td>
</tr>
<tr>
<td>8:30-9:00 a.m.</td>
<td>Day 1 Summary and Setting the Stage for Town Hall Discussions– Norm Taylor</td>
</tr>
<tr>
<td>9:00-9:30 a.m.</td>
<td>Peter Sloly, Deputy Chief, Toronto Police Service</td>
</tr>
</tbody>
</table>
| 9:30-10:15 a.m. | Dr. Mourad Debbabi, President, NCFTA Canada  
                             Michael Haring, Staff Sergeant, Royal Canadian Mounted Police |
| 10:15-10:30 a.m. | Break                                                                 |
| 10:30-11:15 p.m. | Michael Russell, Detective Constable – Forensic Computer Analyst  
                           Fraser Phillips, Forensic Cellular Phone Analyst  
                           Erik Griffin, Forensic Audio/Video Analyst  
                           Troy Phillips, Detective Constable, Durham Regional Police Service |
| 11:15 - 12:00 | Ryan Jepson, Staff Sergeant, Electronic Surveillance Unit, Calgary Police Service  
                             Cory Dayley, Sergeant, Cybercrime Support Team, Calgary Police Service |
| 12:00-1:00 p.m. | Lunch                                                                  |
| 1:00-1:30 p.m. | Diamond Sponsor Presentation - NCI                                      |
| 1:30-2:45 p.m. | "What Do I Do" – Senior Law Enforcement led panel & townhall  
                             Peter Sloly, Deputy Chief, Toronto Police Service |
Scott Tod, Deputy Commissioner, Ontario Provincial Police
Jeff Adam, Chief Superintendent, Director General, National Technical Investigation Services, Royal Canadian Mounted Police

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:45–3:00 p.m.</td>
<td>Break</td>
</tr>
<tr>
<td>3:00–4:00 p.m.</td>
<td>Bear Pit Session: What are we doing - what should we be doing? Moderated by Norm Taylor</td>
</tr>
</tbody>
</table>
| 4:00-4:30 | Peter Henschel, Deputy Commissioner, Specialized Policing Services
  
  RCMP Deputy Commissioner Peter Henschel, Specialized Policing Services, will discuss cybercrime within the context of the 'Going Dark' problem, which refers to a continued decline in law enforcement's ability to collect digital evidence despite having obtained court authority to do so. This problem extends across a broad spectrum of investigative, technological and jurisdictional challenges, such as intercept gaps for electronic communications, and an inability to 'see' evidence that is concealed by encryption and related technologies. These and similar challenges - including links between the Going Dark problem and cybercrime, and an urgent need for civil society outreach - will form the basis of Deputy Commissioner Henschel's remarks. |
### APPENDIX B – REGISTRANTS AND ASSESSMENT INTERVIEW PARTICIPANTS

Those containing an ‘Ω’ participated in the post Summit assessment interview process.

<table>
<thead>
<tr>
<th>First</th>
<th>Last</th>
<th>Job Title</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeff</td>
<td>Adam Ω</td>
<td>Director General</td>
<td>RCMP</td>
</tr>
<tr>
<td>Mark</td>
<td>Alder Ω</td>
<td>Public Safety &amp; Defence Lead</td>
<td>SAS Canada</td>
</tr>
<tr>
<td>Eldon</td>
<td>Amoroso Ω</td>
<td>Consultant</td>
<td>Birch Forest Projects Inc.</td>
</tr>
<tr>
<td>Marie-Claude</td>
<td>Arsenaulet Ω</td>
<td>OIC National Intelligence Priorities</td>
<td>RCMP</td>
</tr>
<tr>
<td>Akram</td>
<td>Askoul</td>
<td>Director Information &amp; Communication Technology</td>
<td>Niagara Regional Police Service</td>
</tr>
<tr>
<td>Nathalie</td>
<td>Barussaud</td>
<td>Directrice</td>
<td>La Cité</td>
</tr>
<tr>
<td>Paul</td>
<td>Batista</td>
<td>Sergeant, Computer Forensic Unit</td>
<td>Ottawa Police Service</td>
</tr>
<tr>
<td>Robert</td>
<td>Baxter Ω</td>
<td>CEO</td>
<td>Radius Security</td>
</tr>
<tr>
<td>Marie</td>
<td>Bedard</td>
<td>sergent enquêteur</td>
<td>Sûreté du Québec</td>
</tr>
<tr>
<td>Paul</td>
<td>Beesley</td>
<td>Director, Behavioural, Forensic and Electronic Services</td>
<td>Ontario Provincial Police</td>
</tr>
<tr>
<td>Don</td>
<td>Bell</td>
<td>Chief Superintendent - Bureau Commander</td>
<td>Ontario Provincial Police</td>
</tr>
<tr>
<td>Jeff</td>
<td>Black Ω</td>
<td>Business Development</td>
<td>Digital Boundary Group</td>
</tr>
<tr>
<td>Ryan</td>
<td>Broll Ω</td>
<td>Assistant Professor</td>
<td>University of Guelph</td>
</tr>
<tr>
<td>Jean-Philippe</td>
<td>Caron Ω</td>
<td>Chief Postal Inspector</td>
<td>Canada Post Corporation</td>
</tr>
<tr>
<td>Steve</td>
<td>Clegg</td>
<td>Inspector</td>
<td>Ontario Provincial Police</td>
</tr>
<tr>
<td>Caroline</td>
<td>Cloutier</td>
<td>Agent de recherche</td>
<td>Service de police de la Ville de Montréal</td>
</tr>
<tr>
<td>Sean</td>
<td>Collins</td>
<td></td>
<td>Institute for Quantum Computing, U. Waterloo SERENE-RISC</td>
</tr>
<tr>
<td>Heath</td>
<td>Crichton</td>
<td>A/Staff Sergeant</td>
<td>Ontario Provincial Police</td>
</tr>
<tr>
<td>Vern</td>
<td>Crowley</td>
<td>A/S/Sgt Tech Crime Unit</td>
<td>Ontario Provincial Police</td>
</tr>
<tr>
<td>Peter</td>
<td>Cuthbert</td>
<td>Executive Director</td>
<td>Canadian Association of Chiefs of Police</td>
</tr>
<tr>
<td>Cory</td>
<td>Dayley</td>
<td>Sgt. Cybercrime Support Team</td>
<td>Calgary Police Service</td>
</tr>
<tr>
<td>Mourad</td>
<td>Debbabi</td>
<td>President</td>
<td>NCFTA Canada</td>
</tr>
<tr>
<td>Lysandre</td>
<td>Derry</td>
<td>Intelligence Manager</td>
<td>RCMP - CISC</td>
</tr>
<tr>
<td>Bradley</td>
<td>Edwards</td>
<td>Constable - Digital Field Triage Examiner</td>
<td>Surrey RCMP Detachment</td>
</tr>
<tr>
<td>Bryce</td>
<td>Evans</td>
<td>A/Staff/Superintendent</td>
<td>Toronto Police Service</td>
</tr>
<tr>
<td>Stephen</td>
<td>Foad Ω</td>
<td>Public Sector Manager</td>
<td>Unisys Canada</td>
</tr>
<tr>
<td>Crystal</td>
<td>Foubert</td>
<td>Intelligence Analyst</td>
<td>RCMP - CISC</td>
</tr>
<tr>
<td>Danny</td>
<td>Fournier</td>
<td>Security Manager</td>
<td>Philip Morris International</td>
</tr>
<tr>
<td>Frank</td>
<td>Goldschmidt Ω</td>
<td>Director/Superintendent</td>
<td>Ontario Provincial Police</td>
</tr>
<tr>
<td>Erik</td>
<td>Griffin</td>
<td>Forensic Audio/Video Analyst</td>
<td>Durham Regional Police</td>
</tr>
<tr>
<td>First name</td>
<td>Last name</td>
<td>Job Title</td>
<td>Company</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>Paul</td>
<td>Grigoriou</td>
<td>Det/Cst</td>
<td>Durham Regional Police</td>
</tr>
<tr>
<td>Michael</td>
<td>Haring</td>
<td>Ops NCO C division Integrated Technological Crime</td>
<td>Royal Canadian Mounted Police</td>
</tr>
<tr>
<td>Peter</td>
<td>Henschel</td>
<td>Deputy Commissioner</td>
<td>Royal Canadian Mounted Police</td>
</tr>
<tr>
<td>Deanna</td>
<td>Hollister</td>
<td>Det/Cst</td>
<td>Durham Regional Police</td>
</tr>
<tr>
<td>Ron</td>
<td>Huber</td>
<td>Ω I.T. Manager</td>
<td>York Regional Police</td>
</tr>
<tr>
<td>floor</td>
<td>Jansen</td>
<td>Strategic Advisor</td>
<td>Dutch Police</td>
</tr>
<tr>
<td>Greg</td>
<td>Jenson</td>
<td>Director, Information Security</td>
<td>ADGA Group</td>
</tr>
<tr>
<td>Ryan</td>
<td>Jepson</td>
<td>Staff Sergeant</td>
<td>Calgary Police Service</td>
</tr>
<tr>
<td>Maire</td>
<td>Johnston</td>
<td>Manager</td>
<td>Ontario Provincial Police</td>
</tr>
<tr>
<td>Shailesh</td>
<td>Kaul</td>
<td>CEO</td>
<td>Vayyoo Inc</td>
</tr>
<tr>
<td>Sang</td>
<td>-rae</td>
<td>Manager, Enterprise Architecture</td>
<td>Toronto Police Service</td>
</tr>
<tr>
<td>Dan</td>
<td>Kral</td>
<td>Constable</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>Roland</td>
<td>Lendzian</td>
<td>Multimedia Developer</td>
<td>Ontario Police College</td>
</tr>
<tr>
<td>Richard</td>
<td>MacCheyne</td>
<td>Detective Sergeant</td>
<td>Toronto Police Service</td>
</tr>
<tr>
<td>David</td>
<td>Mander</td>
<td>Detective</td>
<td>Niagara Regional Police Service</td>
</tr>
<tr>
<td>Michael</td>
<td>Martin</td>
<td>General Manager</td>
<td>Motorola Solutions</td>
</tr>
<tr>
<td>Philip</td>
<td>Ouimet</td>
<td>Manager investigations</td>
<td>Cisco</td>
</tr>
<tr>
<td>Christopher</td>
<td>Pallister</td>
<td>S/Sgt, NCO I/C Operational Intake Unit</td>
<td>Royal Canadian Mounted Police</td>
</tr>
<tr>
<td>Steve</td>
<td>Palmer</td>
<td>Executive Director</td>
<td>Collaborative Centre for Justice and Safety</td>
</tr>
<tr>
<td>Jordan</td>
<td>Menard</td>
<td>Detective</td>
<td>Toronto Police Service</td>
</tr>
<tr>
<td>Amer</td>
<td>Merchant</td>
<td>Manager</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>Bridget</td>
<td>Mancini</td>
<td>Senator Industral Liaison Officer</td>
<td>University of Waterloo</td>
</tr>
<tr>
<td>Roger</td>
<td>Merritt</td>
<td>Director, Public Safety Investigations</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>John</td>
<td>Martin</td>
<td>Detective</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>Dan</td>
<td>Merchant</td>
<td>Manager</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>Ryan</td>
<td>McKeen</td>
<td>Manager</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>Philip</td>
<td>O'nuan</td>
<td>Manager</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>Chris</td>
<td>Pallister</td>
<td>S/Sgt, NCO I/C Operational Intake Unit</td>
<td>Royal Canadian Mounted Police</td>
</tr>
<tr>
<td>Paul</td>
<td>Grifoni</td>
<td>Director</td>
<td>Peel Regional Police Service</td>
</tr>
<tr>
<td>Peter</td>
<td>McShean</td>
<td>Police Commissioner, Specialed Policing Services</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>Lee</td>
<td>Noman</td>
<td>CEO</td>
<td>nTerop Corporation</td>
</tr>
<tr>
<td>Mike</td>
<td>Novelli</td>
<td>Secturer, Systms &amp; Information Security</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>B.R.A.K.E.R.S</td>
<td></td>
<td>General Manager</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>Eugene</td>
<td>Ng</td>
<td>CIO</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>Marco</td>
<td>Novelli</td>
<td>Systems &amp; Information Security</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>Lee</td>
<td>Nowlan</td>
<td>Q9</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>Shae</td>
<td>O'nuan</td>
<td>Manager investigations</td>
<td>Peel Regional Police</td>
</tr>
<tr>
<td>Christopher</td>
<td>Pallister</td>
<td>S/Sgt, NCO I/C Operational Intake Unit</td>
<td>Royal Canadian Mounted Police</td>
</tr>
<tr>
<td>First</td>
<td>Last</td>
<td>Job Title</td>
<td>Company</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Tony</td>
<td>Reeves</td>
<td>Staff Sergeant</td>
<td>Halifax Regional Police Service</td>
</tr>
<tr>
<td>David</td>
<td>Roberts Ω</td>
<td>Senior Program Manager, IACP Technology Center</td>
<td>International Association of Police Chiefs (IACP)</td>
</tr>
<tr>
<td>Christine</td>
<td>Robson</td>
<td>I.T. Manager</td>
<td>Durham Regional Police</td>
</tr>
<tr>
<td>Doug</td>
<td>Ross</td>
<td>OIC Technical Analysis Section</td>
<td>RCMP Technical Investigation Services</td>
</tr>
<tr>
<td>Ian</td>
<td>Rubel</td>
<td>Detective</td>
<td>Niagara Regional Police Service</td>
</tr>
<tr>
<td>Remco</td>
<td>Ruiter</td>
<td>Information Security Officer and Liaison Banking a</td>
<td>Rabobank</td>
</tr>
<tr>
<td>Michael</td>
<td>Russell</td>
<td>Forensic Computer Analyst</td>
<td>Durham Regional Police</td>
</tr>
<tr>
<td>Dave</td>
<td>Seglins</td>
<td>Journalist</td>
<td>CBC</td>
</tr>
<tr>
<td>Joel</td>
<td>Shapiro</td>
<td>Vice President, Sales</td>
<td>Digital Boundary Group</td>
</tr>
<tr>
<td>Frank</td>
<td>Skubic</td>
<td>Detective Sergeant</td>
<td>Toronto Police Service</td>
</tr>
<tr>
<td>Guy</td>
<td>Slater Ω</td>
<td>Superintendent</td>
<td>Calgary Police Service</td>
</tr>
<tr>
<td>Peter</td>
<td>Sloly Ω</td>
<td>Deputy Chief of Police</td>
<td>Toronto Police Service</td>
</tr>
<tr>
<td>Chris</td>
<td>Stewart</td>
<td>Sergeant</td>
<td>Niagara Regional Police Service</td>
</tr>
<tr>
<td>Lisa</td>
<td>Taylor</td>
<td>Manager/Inspector</td>
<td>Ontario Provincial Police</td>
</tr>
<tr>
<td>Norm</td>
<td>Taylor Ω</td>
<td>President</td>
<td>Global Network for Community Safety</td>
</tr>
<tr>
<td>Andrew</td>
<td>Thompson Ω</td>
<td>Senior Instructor</td>
<td>RCMP - Canadian Police College</td>
</tr>
<tr>
<td>Katherine</td>
<td>Thompson</td>
<td>Chair, CATA Cyber Council</td>
<td>CATAAlliance</td>
</tr>
<tr>
<td>Danny</td>
<td>Timmins Ω</td>
<td>CEO</td>
<td>NCI</td>
</tr>
<tr>
<td>Scott</td>
<td>Tod Ω</td>
<td>Deputy Commissioner</td>
<td>Ontario Provincial Police</td>
</tr>
<tr>
<td>Matthew</td>
<td>Torigian</td>
<td>Deputy Minister of Community Safety</td>
<td>Province of Ontario</td>
</tr>
<tr>
<td>Alan</td>
<td>Treddenick Ω</td>
<td>Director, National Security and Law Enforcement Li</td>
<td>BlackBerry</td>
</tr>
<tr>
<td>Pankaj</td>
<td>Tripathi Ω</td>
<td>Team Lead, Web&amp;Graphics Services</td>
<td>OPP</td>
</tr>
<tr>
<td>Gaëtan</td>
<td>Vaillancourt</td>
<td>Commandant</td>
<td>Service de police de la Ville de Montréal</td>
</tr>
<tr>
<td>Ron</td>
<td>Van Holst Ω</td>
<td>Director, Research Development, HPC</td>
<td>Ontario Centres of Excellence</td>
</tr>
<tr>
<td>Leslie</td>
<td>Waldron Ω</td>
<td>D/Sergeant</td>
<td>OPP</td>
</tr>
<tr>
<td>Jeff</td>
<td>Ward</td>
<td>Detective</td>
<td>Durham Regional Police Service</td>
</tr>
<tr>
<td>Kevin</td>
<td>Wennekes</td>
<td>Chief Business Officer</td>
<td>CATA</td>
</tr>
<tr>
<td>Grant</td>
<td>Woodward Ω</td>
<td>Public Safety &amp; Defence Specialist</td>
<td>SAS</td>
</tr>
<tr>
<td>Tony</td>
<td>Yaacoub</td>
<td>Chief Technology Officer</td>
<td>Royal Canadian Mounted Police</td>
</tr>
<tr>
<td>Jie</td>
<td>Yin</td>
<td>Security Architect, Enterprise Architecture</td>
<td>Toronto Police Service</td>
</tr>
<tr>
<td>Joseph</td>
<td>Yuhasz`</td>
<td>Supervisory Special Agent</td>
<td>FBI</td>
</tr>
<tr>
<td>David</td>
<td>Zamlmer</td>
<td>Manager, digital forensic investigations</td>
<td>RBC</td>
</tr>
</tbody>
</table>