Addressing the risks and challenges of cyber: Inaugural ITAC Cyber Tech Summit looks at industry and government collaboration opportunities

Cyber attacks have already had a measurable adverse impact on Canada, totaling billions of dollars. Protecting assets from cyber attacks requires a whole of community approach and collaboration between the public and private sector. It is critical that the federal government play a key role as convener of the community and is an example in which cyber criminals can exploit gaps that exist within organizations as well as between the public and private sectors.

The need for greater focus on cyber was a catalyst for ITAC hosting its inaugural *Cyber Technology Summit* in Ottawa on October 30th, which sought to bring together information, communications and technology (ICT) industry and government leaders together to reinforce the importance of and need for a strong understanding of cyber security by Government that will include engagement of Canadian industries and individuals. There are significant challenges ahead that will directly impact the Canadian economy, government, large industry, and small and medium sized enterprises.

The Summit organizing committee featured key members of the cyber industry, as well as senior officials from Federal departments, including Public Safety Canada, the Communications Security Establishment and Innovation, Science and Economic Development.

Our Summit aligned closely with the theme of the final week of the Government of Canada's *Cyber Security Awareness Month: Our Future in Cyber Security*. It had approximately 150 attendees for the full day event.

Since the federal government last developed a cyber strategy in 2010, the threat landscape has evolved significantly. New applications of technologies have created a host of new vulnerabilities and attack vectors. Major actors from international organized crime, nation-state cyber-espionage organizations and hacktivists have escalated the severity and complexity of the threat, applying significant resources and skills to defeat enterprises that do not have robust cyber security.

The event featured a keynote from the ADM of the Canadian Cyber Security Centre, Andre Boucher, who discussed how the Cyber Centre will engage with the Canadian tech industry; and he promises that we will be hearing more from him. Also, the keynote speakers examined how moving to cloud technologies can make your systems safer, but not without risk. Attendees also heard from a technical panel that discussed the current cyber challenges in the public and private sectors, and how we must work together to combat risks. There were three breakout sessions that examined more

specific cyber topics: the need to develop cyber talent, international export opportunities for Canadian industry and the government adoption of cutting edge cyber tech.

A major take-away was the openness of senior government officials who work on the cyber file to engage with industry and their interest in partnering to work towards Canada's cyber defences. This is a sea-change of behaviour from especially CSE and we hope to continue to engage in 2019 and beyond.

Thank you to our sponsors:
- AWS
- Bell
- Calian
- Cisco Canada
- Digital Boundary Group
- Oracle
- RSA
- SecureKey
- TeraMach