Security Day – November 08, 2017
"*Demystifying* Defensible Security"

Interim Agenda Only – subject to change

8:00 – 9:00	**Registration - *refreshments sponsored by Microsoft***
9:00 – 9:15	**Logistics and Welcome from Government Chief Information Security Officer** Gary Perkins, Government Chief Information Security Officer, OCIO, Information Security Branch, CITZ
9:15 – 9:45	**Defensible Security "DefSec" 101** Paul Falohun, Senior Security Analyst, OCIO, Information Security Branch, CITZ Dan Lathigee, Senior Project Manager, OCIO, Information Security Branch, CITZ *Implementing a high value security control does not necessarily mean you have a strong security posture however ensuring proper foundational (hygiene) level controls are in place can stop 80% of the challenges.*
9:45 – 10:25	**Risk Management** Kent McDonald, Security Software Sales, IBM
10:25 – 10:40	**Coffee Break - sponsored by Microsoft**
10:40 – 11:20	**A Strategy for Success: How Building a Security Strategy can help Achieve your Security Goals** Nick Corcoran, MISO, Security Architect, Corporate Services for the Natural Resource Sector *Through the development of the first ever information security strategy in BC Government, the NRS is finding success in raising management engagement and implementing security technologies to improve their defensibility. Nick Corcoran will describe this approach and what the NRS has achieved to date.*
11:20 – 12:00	**DevSecOps – Security at the Speed of Code!** Jeff Michaud, Senior Consultant, MNP Michael Aldor, Senior Manager, MNP *DevSecOps weaves security checks and balances into all aspects of DevOps and promotes ongoing identification of correction of security flaws and vulnerabilities. How is this done? Who becomes responsible for security? Are there tools? Answers to these questions and more will be provided in a question and answer style session delivered by MNP's Jeff Michaud and Michael Aldor.*
12:00 – 1:00	**Lunch - sponsored by Check Point and MNP**
1:00 – 1:40	**Achieving Defensible Security in a Global Digital World** John Hewie, National Security Officer for Microsoft Canada *Digital transformation has created a complex set of challenges for traditional information security. How do you enable end user and organizational productivity with mobile, cloud and IoT while still protecting sensitive information? Achieving Defensible Security in 2017 requires an evolution in how you must think about the security perimeter, threat and information protection and security management. This session will lay out some of these fundamentals and how Microsoft itself and many of our largest customers are addressing them.*
1:40 – 2:20	**Getting to Defensible** Don Costello, Director Security, Privacy and Compliance, Social Development & Poverty Reduction *'Getting to Defensible' will tell the tale of a sector's journey from hearing about Gary's Defensible Security strategy to where we are at today. This will include our initial communications plan, development of an assessment approach, re-development of an assessment approach, our initial evaluation and measurement of the "elements" and our partnership with OCIO to make quick improvements and develop a longer term plan to get to green…*
2:20 – 2:30	**Coffee Break - sponsored by KPMG**

2:30 – 3:10	**Telus and Defensible Security** Mike Vamvakaris, Head of Cybersecurity Consulting, TELUS *The rise of digital transformation has created new opportunities for the public sector to explore efficiencies and economies of scale for providing new electronic services to their citizens. Governments, ministries and municipalities alike now more than ever need to be aware of the emerging cyber risks and threats that can undermine innovation, create a loss of confidence and result in service disruptions, outages and increased costs. The stakes are high and getting cyber security right or wrong is the difference between knowing and not knowing the minimum set of actions and guidelines that can defend your organization against cyber-attacks. A Defensible Security approach ensures that at a minimum you have a formal plan and framework in place to prevent, detect and respond to the majority of cyber-attacks such as spear-phishing and malware. How does one start and what are the main pitfalls to avoid when rolling out a Defensible Security strategy? Learn first-hand how TELUS is utilizing industry best practices, frameworks and in-house security technologies to defend against today's emerging threats and beyond tomorrow's next cyber-attack.*
3:10 – 3:50	**Tradition of Security** Benoit Gagnon, Senior Security Engineer, Check Point Software Technologies *We do things in a certain way because we know how it's done; we do security the way we know it works. Our way of doing things is almost to a point of tradition. What are the impacts, how do we evolve in defending our networks.*
3:50 – 4:30	**Defensible Security in a Day!?** Guy Rosario, Manager, IT Advisory/Cyber Security, KPMG *If you had a one day to improve security, what could you do? What would you start with? How would you do it? The majority of ways security fails, is not getting basic stuff in place. In this talk, Guy guides the audience through this.*
VANCOUVER GROUPCAST SPONSORED BY IBM	***VICTORIA GROUPCAST SPONSORED BY TELUS***

Special thanks to our sponsors …

IBM

Check Point SOFTWARE TECHNOLOGIES LTD.

TELUS

Microsoft

KPMG

MNP LLP