Cyber-crime is growing exponentially. So why have so few Canadian businesses and government adapted to that? New Policy School report

For Immediate Release March 15, 2018

Calgary – Cyber attacks in 2017 were some of the most devastating in recent history. From the CIA to ransomware attacks on hundreds of thousands of computers they cost untold millions in damage. Personal data leaks from Equifax to Yahoo and Uber - even government organizations were breached. Cyber-crime is growing exponentially and Canadian governments at all levels have not kept pace quickly enough to protect both themselves and the private sector. What does 2018 hold?

Today, The School of Public Policy with author Goran Samuel Pesic released a report that explores and analyzes three broad categories of top cyber-issues which may impact the Canadian economy in the immediate to near term with solid recommendations for protection. Cyber issues include: Private sector concerns in intellectual property (IP), E-commerce, Smart cities, cyber-space threats and beyond.

According to Pesic "Protection should start with educational campaigns about the scope and varieties of risk that permeate the private sector, e-commerce and smart citie. All levels of government need to proactively make cyber-security education and awareness-building campaigns a top priority for the public service. Canada's political parties also need to accept that they must move on from traditional thinking. The knowledge economy has indeed arrived, and proper and meaningful policy articulation around protecting Canadian business interests from cyber-threats requires new ideas and legislative safeguards."

Government can assist with cyber-security in Canada's private sector through awareness campaigns, rewarding businesses for best practices, providing tax credits to offset the cost of security measures, and offering preferential lending and insurance deals from government institutions. E-commerce merchants must protect themselves by ensuring the security of their clients' computers, communication channels, web servers and data encryption.

The federal government's 2015 *Digital Privacy Act* was a good first step, but there is much territory left to be covered. The act offers little assistance in making the leap from a pre-internet governmental model of doing business with the private sector. Nor does it acknowledge the full costs organizations must face when contemplating improving their cyber-security.

The key to keeping ahead of the cyber-criminals is to recalibrate our understanding of the threats accompanying the technology. New ideas, new economic policies, new safeguards, new regulations and new ways of doing business will all help to keep Canada safe in the burgeoning knowledge economy.

The paper can be downloaded at https://www.policyschool.ca/publications/

-30-

Media contact:

Morten Paulsen
morten.paulsen2@ucalgary.ca
403.220.2540