UNIVERSITY OF CALGARY

THE SCHOOL OF PUBLIC POLICY PUBLICATIONS

SPP Briefing Paper

Volume 11:11 March 2018

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

SURVIVING AND THRIVING IN THE DIGITAL ECONOMY*

Goran Samuel Pesic

SUMMARY

Cyber-crime is growing exponentially and Canadian governments at all levels have not kept pace quickly enough to protect both themselves and private enterprise. Evolving technology allows for ever-more sophisticated cyber-threats to intellectual property, but some businesses and governments have neither changed their pre-internet thinking nor established adequate safeguards.

Protection should start with educational campaigns about the scope and varieties of risk that permeate the private sector, e-commerce and smart cities using the internet of things. Thirty years ago, just 32 per cent of the market value of Standard & Poor's 500 companies was based on intangible assets, mainly intellectual property. Today, that figure stands at 80 per cent and protecting those assets from cyber-crime is of vital importance.

While cyber-criminals look to make money off of phishing scams, their interests have also extended to infiltrating proprietary industrial designs, resource management and information affecting acquisitions. The fact that some countries see this type of crime as a normal way to gain access to foreign business information is often poorly understood by Canadian businesses accustomed to functioning under much higher ethical standards.

The e-commerce realm faces its own cyber-threats including those affecting privacy, data sovereignty, location of data centres, data security and legislation. E-commerce merchants must protect themselves by ensuring the security of their clients' computers, communication channels, web servers and data encryption. It sounds daunting, but it shouldn't be. Merchants can take steps

* This research was financially supported by the Government of Canada via a partnership with Western Economic Diversification.

such as doing risk assessments, developing security policies, establishing a single point of security oversight, instituting authentication processes using biometrics, auditing security and maintaining an emergency reporting system.

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.

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 growth of smart cities, connected to the internet of things, creates new susceptibilities to cyber-crime. By 2021, there will be approximately 28 billion internet-connected devices globally and 16 billion of those will be related to the internet of things. However, smart cities appear to be low on the list of cyber-security priorities at all levels of government. There is a lack of local guidance and commitment, an absence of funding programs and tax incentives for risk-sharing arrangements, and nothing in the way of a federally initiated smart-cities strategy.

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.

UNIVERSITY OF CALGARY

THE SCHOOL OF PUBLIC POLICY PUBLICATIONS

SPP Briefing Paper

Volume 11:11 March 2018

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

SURVIVRE ET PROSPÉRER DANS L'ÉCONOMIE NUMÉRIQUE*

Goran Samuel Pesic

RÉSUMÉ

La cybercriminalité connaît une croissance exponentielle et les gouvernements canadiens à tous les niveaux n'ont pas suivi la cadence pour se protéger eux-mêmes et les entreprises privées. L'évolution de la technologie a mis en scène des menaces de plus en plus complexes en ce qui concerne la propriété intellectuelle, or certaines entreprises et gouvernements n'ont pas changé leur mode de pensée pré-Internet, ni prévu les mesures de précaution adéquates.

La protection devrait commencer par des campagnes d'information quant à l'ampleur et à la variété des risques auxquels s'expose le secteur privé, le commerce en ligne et les cités intelligentes qui font grandement appel à la connectivité des objets et des équipements. Il y a trente ans, seuls 32 pour cent de la valeur de l'index Standard & Poor 500 sur le marché pouvait être attribuée au capital immatériel, surtout en ce qui concernait la propriété intellectuelle. Aujourd'hui, ce chiffre s'élève à 80 pour cent; protéger ces avoirs contre la cybercriminalité est d'une importance vitale.

Alors que les cybercriminels cherchent surtout à faire de l'argent avec les escroqueries d'hameçonnage, leurs intérêts se sont diversifiés à l'infiltration des procédés industriels brevetés, à la gestion des ressources et à l'information affectant les acquisitions. Le fait que certains pays considèrent ce type de criminalité comme une façon normale d'avoir accès aux informations commerciales étrangères n'est pas bien compris par les entreprises canadiennes qui sont habituées de fonctionner selon des standards éthiques beaucoup plus élevés.

Le domaine du commerce électronique est confronté à ses propres menaces,

* Cette recherche a été soutenue financièrement en partie par le gouvernement du Canada via Diversification de l'économie de l'Ouest Canada.

incluant celles concernant la vie privée, la souveraineté des données, la situation des centres de données, la sécurité des données et la législation. Les marchands du commerce électronique doivent se protéger en assurant la sécurité des ordinateurs de leurs clients, des canaux de communication, des serveurs et de l'encodage des données. La tâche semble colossale mais elle ne devrait pas l'être. Les marchands peuvent prendre diverses mesures comme l'évaluation des risques, l'élaboration de politiques de sécurité, le développement de points d'accès uniques pour la sécurité, l'instauration de processus d'indentification biométrique, les audits de sécurité et le maintien des systèmes de communication d'urgence.

Le gouvernement peut contribuer à la cybersécurité du secteur privé au Canada avec des campagnes de sensibilisation, un programme récompensant les pratiques exemplaires, des crédits fiscaux compensant le coût lié à la sécurité et l'offre de services d'assurance et de crédits préférentiels de la part des institutions gouvernementales.

La loi fédérale sur la protection des renseignements personnels numériques de 2015 était un premier pas, mais il reste beaucoup de territoire à couvrir. La loi actuelle offre peu pour s'affranchir du modèle d'affaires gouvernemental pré-Internet avec le secteur privé. Elle ne tient pas compte du coût réel auquel les entreprises font face quand vient le temps d'améliorer leur cybersécurité.

La croissance des cités intelligentes, impliquant une connectivité des objets et des équipements, créé de nouvelles vulnérabilités à la cybercriminalité. D'ici 2021, il y aura environ 28 milliards d'appareils connectés à Internet, dont 16 milliards liés à l'Internet des objets. Les cités intelligentes s'avèrent cependant tout en bas des priorités de cybersécurité, et ce, à tous les niveaux gouvernementaux. Il y a une carence d'orientation et d'engagement au niveau local, un manque de programmes de financement et d'incitatifs fiscaux en vue du partage des risques et rien du tout pour initier une stratégie fédérale au profit des cités intelligentes.

La solution pour rester à l'affût de la cybercriminalité est d'ajuster notre compréhension des menaces provenant de la technologie. De nouvelles idées, de nouvelles politiques économiques, de nouvelles mesures de sécurité, de nouveaux règlements et de nouvelles façons de mener les affaires contribueront à préserver la sécurité du Canada dans une économie du savoir en pleine croissance.

INTRODUCTION

Outlining the top cyber-issues in any given year is challenging. As in any field of study, predictions about uncertainty or surprise events are difficult. They are often, but not always, based upon experience or expert knowledge. Cyber-threats and trends are no different. They are exacerbated by the rapidly evolving nature of commercially available technology, coupled with accessing networks of expert know-how anywhere and anytime, making the digital and knowledge economies vulnerable to cyber-attacks and exploitation. This is particularly true for Canadian companies that export, or are planning to export, and that do business overseas. This paper explores and analyzes three broad categories which may impact the Canadian economy in the immediate to near term:

1. Private sector concerns in intellectual property (IP).
2. E-commerce.
3. Smart cities, cyber-space threats and beyond.

INTELLECTUAL PROPERTY

According to Harvard Law School, in 1985 32 per cent of the market value of S&P 500 companies was based on intangible assets, mostly in the form of intellectual property. Today, these assets represent almost 80 per cent of the same companies' market value (Ruttenberg, von Mehren and Yen, 2012). Thus IP plays an even more important role in business today than in any historical period. The protection of IP is thus assuming greater importance for business, government and academia.

Intellectual property is a broad category of law concerning the rights of the owners of intangible products of invention or creativity. For example, IP law grants exclusive rights to certain owners of artistic works, technological inventions, and symbols or designs. Subcategories of IP law include patent, copyright, trademark and trade secrets (Kalanje, 2006). Therefore, IP touches the very core of business operations such as licensing, royalties, technology transfer, venture capital, IP asset management, trademark and patent enforcement as well as legal action for IP infringements.

While protecting Canadian IP rights abroad is important, it is challenging because copyrights, trademarks and patents granted in Canada are not always legally enforceable abroad. Various treaties attempt to make IP rights enforceable in other countries, but the ultimate enforceability of rights depends on the laws of the country in question, the type of IP being protected and the specifics of any existing treaties.

According to John Dowdy (2012), senior partner at McKinsey and Company in London, research suggests that while the private sector has significant economic value at risk from intellectual property theft, businesses of all sizes appreciate neither the high value of the IP nor its susceptibility to cyber-attack.

Given the many competing priorities and demands corporations or SMEs have in the day-to-day running of their businesses, the reality is that many companies do not prioritize cyber-security. In addition, the government is doing less to protect Canadian IP compared to protecting its critical infrastructure or its classified information systems.

Beyond pure profit, hackers also seek intellectual property. For example, Canadian security expert Ray Boisvert (2014a), president and CEO of I-SEC Integrated Strategies and former CSIS assistant director, says that hackers' top priorities include proprietary industrial designs, processes and practices related to resource management, and information related to "valuations" that can affect acquisitions. Several countries see cyber-theft as a legitimate approach to modernization, market assurance and resource access.

Canadian business leaders need to adjust and increase their levels of security awareness when dealing with foreign businesses or their agents. Our high levels of business practices, ethics and standards are simply not the global norm outside North America, the EU and other G7 countries, as well as Australia and New Zealand. To mitigate overall risk, Boisvert (2014b) suggests seeking the assistance of the Canadian embassy in markets where IP theft levels are medium to high. Canadian officials could provide services and support ranging from briefing about local business and cultural practices to providing secure meeting facilities to discuss commercially sensitive matters. I believe this is a critical area that requires joint efforts by government authorities and business, given the potential for huge economic and industry losses from cyber-threats to Canadian domestic and international trade interests.

The cyber-threat to IP is unevenly understood by many in government, outside of the security-related agencies, poorly comprehended by Canadian businesses of all sizes and remains a very real impediment to many export sectors of the Canadian economy.

E-COMMERCE

What are the main concerns facing Canadian business and exporters when it comes to e-commerce today?

The U.S.-based Boston Consulting Group (2015) estimated that there are roughly three billion mobile users globally – or almost half the world's population – and projected that this number will exceed eight billion connections by 2020.

An earlier report issued by the same firm in 2012 predicted the internet economy will reach about US$4.2 trillion in the G20 economies by 2016. The report also asserted that if the internet of things were a national economy, it would rank in the world's top five, behind only the U.S., China, Japan and India, and slightly ahead of Germany. Put another way, the internet is contributing up to eight per cent of GDP in some economies, running national growth and creating jobs (Boston Consulting, 2012). Out of the $4.2 trillion just cited, about $2 trillion was estimated to be retail e-commerce (B2C) sales and $2.2 trillion was business-to-business (B2B) e-commerce. To put these figures in perspective, Canada's 2016 GDP measured $1.6 trillion, according to Statistics Canada (2018).

Concerns have already been raised about the legal and administrative changes that may be necessary to address new e-commerce and transaction models facilitated by the internet.

Some of the top issues which business and government authorities are currently discussing include:

- Privacy;
- Data sovereignty and locations of data centres;

- Data protection and data security;
- IP rights;
- Applicable law(s) and jurisdiction(s);
- Taxes;
- Standardization.

B2B e-commerce will also undoubtedly affect Canadian international trade. According to Praveen Gupta (2007), a fellow of the American Society for Quality and author of several books on business management, companies should select from the best suppliers for their needs regardless of their geographical location, and sell to a global market. Some of the advantages promised to users of B2B e-commerce include:

- Shorter transaction and fulfillment cycles;
- Lower procurement administrative costs;
- Reduced operating expenses;
- Increased company profits;
- Improved inventory management practices.

My advice to business clients is – on a basic technical level – that companies of all sizes must protect their e-commerce assets. There are several key considerations to ensure protection such as:

- Clients' computers;
- Web servers (which are highly susceptible to various security threats);
- Communication channels in general and the internet are especially vulnerable to attacks, given the type and variety of channel options;
- Data encryption, which provides some level of privacy and secrecy.

Canadian firms engaged in e-commerce should proactively aim to mitigate cyber-threat risks to their businesses. Developing a sound security and cyber-management plan is a good first step. It would be simple, effective and highly advisable to shape a security plan with cyber-management policies around the following framework:

1. Risk assessments – outside and inside the organization.
2. Security policy.
3. Single point of oversight and accountability in an organization such as company security officer (CSO) with an appropriate government security clearance (PSP Canada, 2017).
4. Implementation plan including:
    a) Security organization
    b) Access controls
    c) Authentication procedures, perhaps including biometrics features
    d) Authorization policies, authorization management systems.

5. Security audit process and procedures.

6. Emergency reporting measures to senior management related to security issues (and if required, media and customer engagement plans to provide information).

7. Quarterly security reporting using a dashboard to senior management.

8. Annual reporting to board of directors on security risks, mitigation measures and future considerations.

Government has a clear and important role to play in this domain both from a policy and program-delivery point of view. Government can mount an important information, awareness-building and education campaign with targeted outreach initiatives. This means reaching out to all e-commerce sectors and companies with the aim of promoting best practices, facilitating business groups or sector-related events and providing incentives for business to be more competitive and ready for cyber-security.

Government can also make an impact through a program of corporate behavioural nudges. Try to imagine a well thought-out process where government can reward SMEs and exporters for best cyber-security practices. This will certainly require changes to existing commercial laws, regulations, policies, taxes and individual government department and agency mandates. The rewards will be extensive and far-reaching. Behavioural economics is an excellent vehicle for encouraging best practices in cyber-security.

In discussions with a variety of businesses it is clear that they uniformly want to invest in more cyber-security measures to protect their competitive marketplace position, IP assets and e-commerce infrastructure. They all agree that the traditional government interaction model with business and organizations belongs to the pre-internet era. Asked what types of changes would immediately help benefit a business in today's economy, many clients agreed that a new cyber-security tax credit would be welcome. This would help to offset the growing costs of operating and maintaining effective up-to-date cyber-security measures while anticipating future security needs as technology rapidly evolves.

Another behavioural nudge that would be very effective would be preferential lending, certification or insurance rates. Cyber-security businesses that are prepared and can demonstrate their readiness should benefit from preferable lending rates and terms from government-owned institutions and Crown corporations such as EDC and BDC. When it comes to borrowing or bonding, banks, insurance companies and other government entities typically ask a firm to provide its managerial, financial and technical expertise when assessing transactional risk. Why not include a new risk category for cyber-security preparedness? In this scenario, businesses that are investing in cyber-security measures are truly encouraged to transform and evolve with technology and rewarded for their efforts, rather than burdened with the high costs associated with cyber-security expenditures. Similarly, the government and associated lending and insurance entities mitigate their exposure to risk without incurring punitive one-off costs after cyber-failures.

The federal government has taken some measures to bridge the pre-internet government model with a more responsive model that works with business. On June 18, 2015, the *Digital Privacy Act* (also known as Bill S-4) received royal assent in Parliament. This new law mandates that businesses must provide notification of data breaches. The act establishes some basic

legal requirements directed at the private sector. These are intended to respect the privacy of Canadians and to ensure in turn that Canadians trust that their privacy will be handled securely and protected in the hands of businesses (Justice Laws, 2015). Currently, the province of Alberta is the only sub-federal jurisdiction in Canada to have a similar law enacted.[1] Other comparable types of federal legislation can be found in the U.S., Australia and New Zealand. Although the legislation's general intent is for the protection of individuals, it is really only a small step forward when we consider the pressing need to effectively modernize and manage a suite of laws which govern commerce and information, but which do not address current privacy concerns and cyber-security matters in the modern context of e-commerce. For example, the new law falls short in tackling the larger issue of how to meaningfully bridge the gap between a pre-internet governmental model of doing business with the private sector, and the new realities that commercial organizations face in carrying the full costs of cyber-security in the internet age.

Addressing this new reality should be a policy priority of Canada's mainstream political parties as they attempt to achieve some form of consensus from business interests and citizenry about appropriate measures. Everyone agrees that the knowledge economy is here to stay, but the key challenge will be for government decision-makers and business leaders to make it relevant, inclusive and adaptive for the internet era. Domestic wealth creation and economic sustainability are ultimately in the national interest. Success in the effort to bridge the gap will be the key to Canada's success in the global e-commerce economy.

SMART CITIES, CYBER-SPACE THREATS AND BEYOND

The world is experiencing a period of extreme urbanization. According to research by the Massachusetts Institute of Technology (2016) on the implications of smart cities, in the near future cities will account for nearly 90 per cent of global population growth, 80 per cent of wealth creation and 60 per cent of total energy consumption. Our changing landscape will have a great impact on future cyber-space threats and beyond. Therefore, the Canadian government and Canadian businesses alike need to develop and prepare better strategies for the emergence of these new urban centres. Securing these cities needs to be a collective project involving local, provincial and federal governments and private sector organizations with an immediate stake in the continuation of a city's stable functioning.

In broad terms, smart cities will provide Canadian businesses with unprecedented economic opportunities. However, according to Nicolas Reys (2016) of Control Risks, an independent global risk consultancy specializing in political, integrity and security risk, "cyber threat actors will be presented with an unprecedented attack surface in smart cities because of the significant increase in the number of interconnected devices." The Swedish firm Ericsson (2016) predicts there will be a total of approximately 28 billion connected devices worldwide by 2021, with nearly 16 billion related to the internet of things.

It is inevitable that smart cities will effectively address a certain set of issues such as better traffic control management, optimization of micro, local and regional electrical grids as well as carbon footprint- and greenhouse gas-monitoring regimes at the household and business levels,

[1] Alberta's Personal Information Protection Act is available at http://www.qp.alberta.ca/1266.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779762507

but with everything new comes unforeseen risks. Each new internet-enabled device that comes online presents governments and businesses with threats and opportunities. How those threats and opportunities are managed will be critical for wealth creation and social stability in Canada.

According to the Brunswick Group (2016), ensuring that smart cities are cyber-secure will require the identification and prioritization of critical assets. This includes behaviour-based security. This simple idea establishes benchmarks of normal operation for critical assets and continuously ensures that all parts of a city adhere to uniform benchmarks. Should a security incident occur, then a rapid component replacement is centrally deployed in the event of compromise or failure. This would ensure the secure segmentation of critical private assets from the city network. Three key industry concerns over immediate and future cyber-threats to Canadian smart-city projects regularly emerge from discussions with businesses. These are:

- Lack of long-term local government guidance and commitment;
- No national smart-cities strategy led by the federal government;
- Absence of any local, provincial and federal funding programs and/or aggressive tax incentives to encourage better risk-sharing arrangements through public-private partnerships.

In terms of cyber-space threats, global industry experts generally agree that sources on this subject are diverse and they do not agree on the way forward. However, the following represents a summary of general ideas and predictions which have emerged over the past few years:

- Machine-learning techniques will increase, for example, enabling faster fraud detection over legacy expert rules (Guruswamy, 2015);
- Probabilistic tools will augment and replace current blacklists and expert rules. This will redefine how risk is measured, how actions are co-ordinated and how risk reporting is conducted (Ingevaldson, 2016);
- Wider and deeper application of biometrics technologies for authentication will be applied across sectors (Jain et al.,1998).This is evidenced in today's mobile devices, such as the new 2017 iPhone 8 and iPhone X models, requiring fingerprinting and facial recognition respectively as a means of authenticating the device's owner;
- Greater usage of contactless payment systems now in use in Canada, the U.K. and Australia (Webster, 2016). For example, most people in Canada are now familiar with such things as MasterCard's PayPass and Visa's payWave contactless features;
- More sophisticated and targeted mobile fraud schemes will evolve as more people turn to mobile banking applications and money transfers, particularly in hyper-growth regions such as Asia-Pacific (ThreatMetrix, 2017);
- Phishing emails are one of the biggest threats to online security for individuals and businesses conducting financial transactions. These criminally motivated scams are particularly dangerous when they do a convincing job of impersonating trusted e-commerce brands like PayPal (Mathews, 2017).

Cyber-criminals have successfully deployed and executed a variety of sophisticated mimicry schemes aimed at legitimate corporate brands by imitating their logos, emails, websites and, more recently, their mobile applications. The vast majority of us are undoubtedly unaware, or at best suspicious, of the inherent risks of viewing an email or clicking a web link. For example, last year cyber-criminals cleverly deceived Edmonton's MacEwan University into transferring

$11.8 million to bank accounts located in Montreal and Hong Kong (Wakefield, 2017). The criminals constructed a highly believable website that resembled the domain site of one of the university's major suppliers to launch their scam. Despite an increased awareness in the general population, this means companies of all sizes need to pay much closer attention to their social media presences. One straightforward recommendation for good business practice is to institute a company-wide domain-monitoring policy and procedure. Just as every employee represents their employer when dealing with customers, so too should companies encourage their employees to be vigilant about the company brand on the web. This also extends to companies protecting their email chains and detecting and removing rogue mobile applications from devices.

To conclude, I offer this simple piece of advice: To address the potential negative economic and commercial impacts of cyber-threats to Canada's domestic and international trade in any meaningful way, the Canadian government needs to recalibrate its pre-internet business interaction model by working with the private sector to reward SMEs and exporters with financial and tax incentives to help them level the global playing field in the internet era. All levels of government need to proactively make cyber-security education and awareness-building campaigns a top priority for the public service. Last, Canada's political parties 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.

Businesses create jobs; governments do not. But government can play a critical role in setting the regulatory and policy agendas. These include economic policies and changing regulatory and tax regimes, as well as investing in smart cities that leverage the benefits of public-private infrastructure projects. Taking these measures makes sound economic and national security sense and will better prepare Canada to survive and thrive in the digital economy.

REFERENCES

Boisvert, Ray. 2014. "What Every CEO Needs to Know about Cybersecurity: A Background Paper," Business Council of Canada. Available at http://www.ceocouncil.ca/wp-content/uploads/2014/04/What-Every-CEO-Must-Know-Cyber-April-4-2014-Final.pdf

Boston Consulting Group. 2012. "The Connected World: The Internet Economy in the G-20: The $4.2 Trillion Growth Opportunity." Available at https://www.bcg.com/documents/file100409.pdf

Boston Consulting Group. 2015. "The Mobile Revolution: How Mobile Technologies Drive a Trillion-Dollar Impact." January. Available at https://www.bcg.com/en-ca/publications/2015/telecommunications-technology-industries-the-mobile-revolution.aspx

Brunswick Group. 2016. "Smart Cities: The Implications for the Private Sector."

Dowdy, John. 2012. "The Cyber-Security Threat to U.S. Growth and Prosperity," *Cyberspace: A New Domain for National Security.* Aspen.

Ericsson. 2016. "Ericsson Mobility Report on the Pulse of the Networked Society." Available at https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf

Gupta, Praveen. 2007. *Business Studies Xi 6E Tata*. New Delhi: McGraw-Hill Education.

Guruswamy, Karthik. 2015. "Data Science: Machine Learning vs. Rules-Based Systems," *Forbes Media*. Dec. 15.

Ingevaldson, Daniel. 2017. "Emerging Anti-Fraud Technology Predictions," Easy Solution Inc. blog. Available at http://blog.easysol.net/emerging-anti-fraud-technology-predictions/

Jain, Anil et al., 1998. "Biometrics: Personal Identification in Networked Society," *Introduction to Biometrics*. Michigan State University. 4-16.

Justice Laws. (Government of Canada). 2016. *Digital Privacy Act*. Available at http://laws-lois.justice.gc.ca/eng/annualstatutes/2015_32/page-1.html

Kalanje, Christopher. 2006. "Role of Intellectual Property in Innovation and New Product Development," World Intellectual Property Organization. Available at www.wipo.int/export/sites/www/sme/en/documents/pdf/ip_innovation_development.pdf

Massachusetts Institute of Technology. 2016. Future Cities Hands-On Workshop. June 6.

Mathews, Lee. 2017. "Don't Fall for this Sophisticated New PayPal Phishing Scam," *Forbes Media*. Feb. 1. Available at https://www.forbes.com/sites/gradsoflife/2018/01/10/at-a-crossroads-in-life-consider-a-jump-to-a-different-future-of-opportunity/#6f8ce00c4b90

Public Services and Procurement Canada. 2017. "Appointing a Company Security Officer." Available at https://www.tpsgc-pwgsc.gc.ca/esc-src/organisation-organization/ase-cso-eng.html

Reys, Nicolas. 2016. "Control Risks. Smart Cities and Cyber Threats." Available at https://www.controlrisks.com/en/our-thinking/analysis/smart-cities-and-cyber-threats

Ruttenberg, Joan, Paige von Mehren, and Julie Yen. 2013. *The OPIA Insider's Guide to Intellectual Property and Cyberlaw 2013*. Bernard Koteen Office of Public Interest Advising. Harvard Law School. Available at http://hls.harvard.edu/content/uploads/2008/06/IP-Cyberlaw-Guide-Final-1.pdf

Statistics Canada. 2018. Gross Domestic Product at Basic Prices, By Industry. Available at http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/gdps04a-eng.htm

ThreatMatrix Inc. 2017. "Asia Pacific Cyberattacks up 35% Year on Year, as Global Organized Fraud Rings Turn their Attention to Emerging Financial Services." March 8. Available at https://www.threatmetrix.com/press-releases/asia-pacific-cyberattacks-35-year-year-global-organized-fraud-rings-turn-attention-emerging-financial-services/

Wakefield, Jonny. 2017. "MacEwan University Loses $11.8 Million to Scammers in Phishing Attack," *Edmonton Journal*. Sept. 1. Available at http://edmontonjournal.com/news/local-news/11-8-million-transferred-from-macewan-university-accounts-in-phishing-attack

Webster, Karen. "UK's Lessons for US Mobile Payments Adoption," PYMNTS.com. March 21. Available at www.pymnts.com/nfc/2016/uk-lessons-for-us-mobile-payments-adoption/

About the Author

Goran Samuel Pesic has many years of experience in political, economic, defence and security matters. He is a Senior Associate and Head of Operations with David Pratt and Associates, a government relations and strategic consultancy firm located in Ottawa, Canada. Goran is also President of Samuel Associates, where he provides strategic advice on specific issues and projects to a wide variety of clients in Canada and abroad. Goran is a U.S. National Security Fulbright Scholar from the University of California and holds a Bachelor of Arts in Political Science and History from the University of Toronto.

ABOUT THE SCHOOL OF PUBLIC POLICY

The School of Public Policy has become the flagship school of its kind in Canada by providing a practical, global and focused perspective on public policy analysis and practice in areas of energy and environmental policy, international policy and economic and social policy that is unique in Canada.

The mission of The School of Public Policy is to strengthen Canada's public service, institutions and economic performance for the betterment of our families, communities and country. We do this by:

- *Building capacity in Government* through the formal training of public servants in degree and non-degree programs, giving the people charged with making public policy work for Canada the hands-on expertise to represent our vital interests both here and abroad;
- *Improving Public Policy Discourse outside Government* through executive and strategic assessment programs, building a stronger understanding of what makes public policy work for those outside of the public sector and helps everyday Canadians make informed decisions on the politics that will shape their futures;
- *Providing a Global Perspective on Public Policy Research* through international collaborations, education, and community outreach programs, bringing global best practices to bear on Canadian public policy, resulting in decisions that benefit all people for the long term, not a few people for the short term.

The School of Public Policy relies on industry experts and practitioners, as well as academics, to conduct research in their areas of expertise. Using experts and practitioners is what makes our research especially relevant and applicable. Authors may produce research in an area which they have a personal or professional stake. That is why The School subjects all Research Papers to a double anonymous peer review. Then, once reviewers comments have been reflected, the work is reviewed again by one of our Scientific Directors to ensure the accuracy and validity of analysis and data.

The School of Public Policy
University of Calgary, Downtown Campus
906 8th Avenue S.W., 5th Floor
Calgary, Alberta T2P 1H9
Phone: 403 210 3802

DISTRIBUTION
Our publications are available online at www.policyschool.ca.

DISCLAIMER
The opinions expressed in these publications are the authors' alone and therefore do not necessarily reflect the opinions of the supporters, staff, or boards of The School of Public Policy.

ISSN
ISSN 2560-8312 The School of Public Policy Publications (Print)
ISSN 2560-8320 The School of Public Policy Publications (Online)

DATE OF ISSUE
February 2018

MEDIA INQUIRIES AND INFORMATION
For media inquiries, please contact Morten Paulsen at 403-220-2540. Our web site, www.policyschool.ca, contains more information about The School's events, publications, and staff.

DEVELOPMENT
For information about contributing to The School of Public Policy, please contact Jessika Anderson by telephone at 403-210-7968 or by e-mail at jessika.anderson@ucalgary.ca.

RECENT PUBLICATIONS BY THE SCHOOL OF PUBLIC POLICY

ENERGY AND ENVIRONMENTAL POLICY TRENDS: THE INVISIBLE COST OF PIPELINE CONSTRAINTS
https://www.policyschool.ca/wp-content/uploads/2018/03/ENERGY-trends-advisory-March.pdf
G. Kent Fellows | March 2018

FALLING THROUGH THE CRACKS: HOW THE COMMUNITY-BASED APPROACH HAS FAILED CALGARY'S CHRONICALLY HOMELESS
https://www.policyschool.ca/wp-content/uploads/2018/02/Falling-Through-The-Cracks-Milaney-FINAL-2Williams-Dutton-final.pdf
Katrina Milaney, Nicole Williams and Daniel Dutton | February 2018

SOCIAL POLICY TRENDS: INTERNATIONAL TRENDS IN FEMALE EMPLOYMENT RATES
https://www.policyschool.ca/wp-content/uploads/2018/02/Social-Trends-International-EM-Rates-February-2018.pdf
Margarita Gres Wilkins and Ronald Kneebone | February 2018

THE TIME HAS COME TO REVISIT SOLVENCY FUNDING RULES
https://www.policyschool.ca/wp-content/uploads/2018/02/Solvency-Funding-Nielson.pdf
Norma Nielson | February 2018

2017 TAX COMPETITIVENESS REPORT: THE CALM BEFORE THE STORM
https://www.policyschool.ca/wp-content/uploads/2018/02/2017-Tax-Competitiveness-Bazel-Mintz-Thompson-final.pdf
Philip Bazel, Jack Mintz and Austin Thompson | February 2018

RECENT CHANGES TO PROVINCIAL GOVERNMENT BUDGET REPORTING IN ALBERTA
https://www.policyschool.ca/wp-content/uploads/2018/02/AB-Budget-Reporting-Kneebone-Wilkins.pdf
Ronald Kneebone and Margarita Gres Wilkins | February 2018

HAS THE CITY-RURAL TAX BASE AND LAND-USE BALANCE CHANGED IN ALBERTA? EXPLORATIONS INTO THE DISTRIBUTION OF EQUALIZED PROPERTY ASSESSMENTS AMONG MUNICIPALITY CLASSES
https://www.policyschool.ca/wp-content/uploads/2018/02/Final_City-Rural-Tax-Base-McMillan.pdf
Melville McMillan | February 2018

REDUCING GREENHOUSE GAS EMISSIONS IN TRANSPORT: ALL IN ONE BASKET?
https://www.policyschool.ca/wp-content/uploads/2018/01/GHG-Emissions-Rivers-Wigle.pdf
Nicholas Rivers and Randall Wigle | February 2018

CANADA AND ASSOCIATE MEMBERSHIP IN THE PACIFIC ALLIANCE: AN IMPORTANT PART OF A GLOBAL TRADE STRATEGY
https://www.policyschool.ca/wp-content/uploads/2018/01/Pacific-Alliance-Stephens-Navarro-Jan2018.pdf
Hugh Stephens and Juan Navarro | January 2018

ALBERTA'S CHANGING INDUSTRIAL STRUCTURE: IMPLICATIONS FOR OUTPUT AND INCOME VOLATILITY
https://www.policyschool.ca/wp-content/uploads/2018/01/AB-Industrial-Structure-Dahlby-Khanal.pdf
Bev Dahlby and Mukesh Khanal | January 2018

SOCIAL POLICY TRENDS: THE ENERGY BOOM AND INCOME
https://www.policyschool.ca/wp-content/uploads/2018/01/Social-Trends-Deciles-January-Final.pdf
Margarita Gres Wilkins and Ronald Kneebone | January 2018

POLICY BRIEF – WHY IS UPTAKE OF THE DISABILITY TAX CREDIT LOW IN CANADA? EXPLORING POSSIBLE BARRIERS TO ACCESS
https://www.policyschool.ca/wp-content/uploads/2018/01/Disability-Tax-Credit-Dunn-Zwicker.pdf
Stephanie Dunn and Jennifer Zwicker | January 2018

BUSINESS SUBSIDIES IN CANADA: COMPREHENSIVE ESTIMATES FOR THE GOVERNMENT OF CANADA AND THE FOUR LARGEST PROVINCES
https://www.policyschool.ca/wp-content/uploads/2018/01/Business-Subsidies-in-Canada-Lester.pdf
John Lester | January 2018