Surviving and Thriving in the Digital Economy

Goran Samuel Pesic
David Pratt & Associates
March 23, 2017

Good afternoon ladies and gentlemen, before I begin my remarks allow me to thank the University of Calgary, the Canadian Institute for Global Affairs, event sponsors and our moderator, David Bercuson, for this opportunity to present a private sector viewpoint.

As a management consultant, international business advisor and US national security scholar, I look to frameworks to understand our current reality and gauge tomorrow's business environment. This is particularly challenging when assessing cyber threats as they relate to Canada's international trade and commerce interests.

But before I begin my comments on the top cyber-issues which create challenges, problems and issues facing Canadian companies who are, or are planning to export and do business overseas, allow me to preface my remarks that the opinions, analysis and predictions presented here today are strictly my personal views and do not reflect those of David Pratt and Associates.

This afternoon I'm going to structure my presentation in three broad categories:

1. Private sector concerns in Intellectual Property (IP)
2. E-Commerce
3. Smart cities, cyberspace threats and beyond

Intellectual Property

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. 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.

According to the Harvard Law School, in 1985, 32% of the market value of S&P 500 companies was based on intangible assets, mostly in the form of intellectual property. In 2005, these assets represented almost 80% of the same companies' market value. Today, IP plays an increasingly important role in business. As such, considerations relating to the protection of IP are assuming greater importance for business, government and academia.

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.

When it comes to cyber threats, research suggests that while the private sector has significant economic value at risk from intellectual property theft, neither the high value of the IP, nor its susceptibility to cyber-attack is fully appreciated by business of all sizes.

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 purely seeking profit, hackers are also seeking intellectual property. 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.

I believe this is a critical area where joint emphasis needs to be placed given the potential for huge economic and industry losses attributed to this modern form of cyber threat against Canadian domestic and international trade interests.

In sum, the cyber threat to IP is poorly understood by many in government and business, but very real nonetheless.

E-Commerce

As of 2016, there were roughly three billion Internet users globally or almost half the world’s population. In reports issued by the US-based Boston Consulting Group and Merrill Lynch, it has been highlighted that the Internet economy has reached about $4.2 trillion US in the G-20 economies.

The reports assert that if the “Internet-of-Things” were a national economy, it would rank in the world’s top five, behind only the US, China, Japan, and India, and slightly ahead of Germany. Put another way, the Internet is contributing up to 8% of GDP in some economies, running national growth and creating jobs.

Out of the $4.2 trillion just cited, about $2 trillion was retail e-commerce (B2C) sales and $2.2 trillion in business-to-business (B2B) e-commence. Putting these figures in perspective, Canada’s 2016 GDP measured $1.6 trillion according to Statistics Canada.

So, what are the main concerns facing Canadian business and exporters when it comes to e-commence?

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.

Issues that are being currently discussed by business and government include:

- Privacy
- Data sovereignty and locations of data centers
- Data protection / Security
- IP rights
- Applicable Law / Jurisdiction
- Taxes
- Standardization

B2B e-commerce will also undoubtedly affect Canadian international trade. It allows companies to select the best suppliers for their needs regardless of their geographical location, and to 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 – companies of all sizes must protect their e-commerce assets including but not limited to:

- Client computers;
- Computer communication channels;
- Web servers (which are highly susceptible to security threats);
- Communication channels, in general, and the Internet, are especially vulnerable to attacks; and
- Encryption, which provides some level of privacy and secrecy.

So, what can Canadian firms engaged in e-commence proactively do to mitigate cyber threat risks to their business?

My recommendation is to develop a sound “Security Plan with Cyber Management Policies” around the following framework:

1. Risk assessment
2. Security policy
3. Implementation plan (such as)
    a. Security organization
    b. Access controls
    c. Authentication procedures, including biometrics
    d. Authorization policies, authorization management systems
4. Security audit

In sum, I envision a very important information awareness and education role for the Canadian government when it comes to helping e-commence businesses secure their competitive position in the local, regional and global supply chains.

Try to imagine a well thought out process where government can reward SMEs and exporters for best and secure practices, either through a new cyber security tax credit, or preferable lending terms and rates through its crown corporations such as EDC and BDC. Typically, banks, insurance companies and other government entities ask for a company's managerial, financial and technical expertise when assessing transactional risk.

Why not include a new risk category for cyber security preparedness?

Smart cities, cyberspace threats and beyond

The world is experiencing a period of extreme urbanization. According to research by the Massachusetts Institute of Technology (MIT) considering the implications of smart cities, in the near future, cities will account for nearly 90% of global population growth, 80% of wealth creation, and 60% of total energy consumption. Our changing landscape will have a great impact on future cyberspace threats and beyond.

Therefore, the Canadian government and business alike need to develop and prepare better strategies for the creation of new cities.

In broad terms, smart cities will provide Canadian businesses with unprecedented economic opportunities. However, 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.

Ericsson of Sweden 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".

Securing these cities needs to be a joint project involving local government and private sector organizations with an immediate stake in the continuation of a city's stable functioning.

Ensuring that these smart cities are cyber secure will require the identification and prioritization of critical assets, behaviour based security – establishing a benchmark of normal operation of critical assets and continuously ensuring that all parts of the city adhere to benchmarks, rapid component replacement in the event of compromise, or failure and the secure segmentation of critical private assets from the city network.

Addressing immediate and future cyber threats to Canadian business interests at home and broad will include:

- Machine learning will enable faster fraud detection over legacy expert rules.
- Probabilistic tools will rise, replacing current blacklists and expert rules. This will redefine how risk is measured, how actions are coordinated, and how risk reporting is conducted.
- Wider and deeper application of biometrics technologies for authentication.
- Greater use of contactless payment system currently in use in Canada, the UK and Australia.
- Mobile fraud will be on the rise, particularly in Asia, as more people turn to mobile banking.

What does this mean for cybercriminals and others engaged in commercial clandestine cyber activities?

Cybercriminals will certainly engage in greater levels of sophisticated mimicry of legitimate brands by imitating logos, emails, websites, and mobile applications. This is already happening. That means companies need to pay closer attention to social media, establish domain monitoring, protect email chains, and remove rogue mobile applications.

To conclude my presentation, ladies and gentlemen, I offer this simple advice: To meaningfully address the potential negative economic and commercial impacts of cyber threats to Canadian domestic and international trade, the Canadian government must proactively educate and provide financial and tax incentives to SMEs and exporters to help them level the global playing field.

Let us all be reminded here that businesses create jobs, governments do not. But governments can play a vital and critical role in setting the economic policies, changing regulatory and tax regimes as well as investing in public infrastructures, which will better prepare Canada to survive and thrive in the digital economy.

Thank you.