

**Written Submission for the Pre-Budget Consultations in  
Advance of the 2020 Budget**

**Electronic Transactions Association**



## Recommendation

- **Recommendation 1:** That the Government of Canada create a 15 per cent non-refundable tax credit for small businesses to purchase cyber security insurance.
  - The policy would be available for small businesses up to 99 employees and self-employed individuals.
  - Only firms which have successfully undertaken Innovation, Science, and Economic Development Canada's Cyber Assessment and Certification program would be eligible.
  - The credit would be reviewed after 5 years.
  - The credit would encourage small business owners to protect their livelihoods as cyber attacks and risks continue to increase as the digital economy grows.

# Helping Canadian Small Businesses Mitigate Cyber Risks

## About ETA

[The Electronic Transactions Association](#) (ETA) is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services. Its membership spans the breadth of the payments industry to include independent sales organizations, payments networks, financial institutions, transaction processors, mobile payments products and services, payments technologies, equipment suppliers, and online small business lenders. ETA member companies are creating innovative offerings in financial services, revolutionizing the way commerce is conducted with safe, convenient and rewarding payment solutions and lending alternatives. ETA advocates for the payments industry in Canada to help drive innovation in the global market for payments technology services.

## ***Small businesses drive the economy***

Small businesses are the backbone of Canada's economy — and are key to building thriving and prosperous communities. In fact, a staggering 98 per cent of Canadian businesses are small businesses, employing over 8 million Canadians, and constituting almost 70 per cent of the total private labour force. In 2014, small businesses contributed 42 per cent of Canada's GDP. Combined with medium sized businesses, the number reached 53 per cent.

As such a key driver of Canada's economic future, when increasing numbers of small businesses experience a hack or data breach the entire Canadian economy takes a hit. In recognition of this, ETA and its members are working directly with entrepreneurs and small business owners to find ways to help them address their cyber security needs, enhance their business' resilience and ensure they thrive.

## ***Vulnerability of small businesses***

While Canada is one of the most entrepreneurial countries in the world, the federal government is often called upon to help small businesses grow and prosper. This is particularly the case with the growing importance of the digital economy – where the need for small businesses to protect themselves against cyber threats becomes more fundamental to their continuing success each day.

The Government has recognized how a lack of cyber preparedness has the potential to hurt Canadians. For example, in 2015, both the Minister of Public Safety and Emergency Preparedness and the Minister of Innovation, Science and Economic Development were given mandates to review existing measures to protect Canadians and critical infrastructure from cyber-threats. More recently, Budget 2019 stated that “as rapid growth in the digital economy continues, safeguarding cyber security has become a priority for governments, businesses and individuals, [and that] Canadian businesses reported spending \$14 billion in 2017 to prevent, detect, and recover from cyber security incidents.” According to Statistics Canada, this includes approximately \$4 billion on cyber security software and related hardware alone.

Despite these significant investments by Canada's business community, small businesses remain at a high risk of cyberattacks and are vulnerable to all manner of cyberthreats - from DDoS (Distributed Denial-Of-Service) to ransomware. Innovation, Science and Economic Development Canada estimates that approximately 71 per cent of data breaches in Canada involve a small or medium sized enterprise,

while the U.S. Securities and Exchange Commission stated in 2015 that 60 per cent of all targeted cyber attacks were against small firms. These attacks put small businesses at a disadvantage and cost them significant resources to recover and lead many to falter. Simply put, small businesses are the most vulnerable to cyber attacks.

A [2017 Canadian Survey of Cyber Security and Cybercrime](#) by Statistics Canada shows that 19 per cent of small businesses and 28 per cent of medium-sized businesses were impacted by cyber security incidents. – while a full five per cent of businesses stated that they had no cyber security measures in place at all. The survey showed that while a majority of businesses (all sizes) have cyber security measures in place like anti-malware, email and network protection, the resilience around other areas like data and point-of-sale protection continues to lag behind what is necessary. This paints a picture that shows many Canadian businesses are woefully unprepared for any sort of cyber attack, particularly small businesses that do not have the resources to put mitigation measures in place.

Government studies have also acknowledged that more support is needed. One of the recommendations from the Senate Committee on Banking, Trade and Commerce's October 2018 [report](#) on cyber threats, is that "... businesses should be given incentives to invest in cyber security improvements, for example, by making these investments tax deductible". Further, in June 2019 the House of Commons Standing Committee on Public Safety released a [report](#) which stated that while large financial firms have sufficient protection against potential cyberattacks, small firms do not.

It is also important to note that Canada is a recognized hotspot for fintech start-ups; the report states that Canada is projected to continue to see a 55 per cent annual growth rate in this sector, expected to continue through 2020. The smaller players in this sector are extremely vulnerable to targeted cyberattacks that could have a crippling effect on Canada's fintech sector and the economy.

### ***Protecting small businesses from cyber threats***

Small businesses already face tough challenges for survival. In Canada, only 63 per cent of small businesses survive their first five years, with that number dropping to 43 per cent by the tenth year. There is also a correlation between the number of employees and survival rate, where businesses with 50-99 employees see a 55 per cent survival rate after ten years, compared to only 42 per cent of businesses with one to four employees surviving past year 10.

The growing threat of cyberattacks will only make success harder to achieve for small businesses as the failure to provide adequate security can lead to profound economic consequences including monetary losses, theft of valuable intellectual property, and leaked consumer data. Cyber attacks also have a direct correlation with the viability of a small enterprise, with the U.S. National Cyber Security Alliance indicating that 60 per cent of small businesses go bankrupt within six months after a cyberattack.

The Government of Canada has recognized the urgency and economic importance of enhancing the cyber resilience of small businesses by initiating a program to develop a voluntary, recognizable certification that would enable small businesses to meet a baseline set of security practices. To incent faster adoption of these practices by small businesses, ETA believes there would be value in providing a 15 per cent non-refundable tax credit for small businesses to purchase "cyber insurance" – provided they have met the requirements of the voluntary cybersecurity certification program.

ETA's proposal would encourage participants to strengthen the cyber resilience of their businesses, while also enhancing public trust in the digital economy. To target the businesses that need this

assistance the most, the credit would only be available to small businesses with up to 99 employees and self-employed individuals. The program would be reviewable after five years.

This proposed tax credit would be akin to the Mineral Exploration Tax Credit, which is aimed at spurring investment in junior exploration companies. The Mineral Exploration Tax Credit is a 15 per cent non-refundable tax credit.

### ***Examples in other jurisdictions***

Examining global practices that promote enhanced cyber security measures for small business, there are several examples for Canada to draw on should government put in place a tax mechanism to reduce the costs of enhancing the cyber resilience of small companies.

In Australia, there is a [Cyber Security Small Business Program](#) that supports small businesses with fewer than 19 employees. The program provides a grant equal to 50 per cent of the cost of a micro, small or standard certified small business check. The cyber security must be tested by a provider that has been approved by the Council of Registered Ethical Security Testers Australia New Zealand. The maximum amount of the grant is \$2100.

In the State of New York, there is a proposed law to provide a 25 per cent tax credit to small businesses with under 100 employees for premiums for qualified data breach insurance. The requirements would include small businesses being in compliance with National Institute of Standards and Technology (NIST) or New York security standards.

### ***Conclusion***

Small businesses are increasingly relying on the digital economy to grow and succeed. The digital economy touches all sectors, from goods and services to products and manufacturing. While large firms have the ability to spend significant resources to protect themselves against increasing cyber threats, small businesses do not have that option and become much more vulnerable to business crippling attacks, whether it be ransomware or data breaches. By providing a cyber insurance tax credit, the government can play a role in encouraging small businesses to mitigate cyber risks and protect themselves properly. The two-fold benefit is that jobs are preserved and confidence in Canada's digital economy is enhanced.

ETA welcomes the opportunity to provide comments in response to the Committee's Pre-Budget Consultations in Advance of the 2020 Budget and would be happy to answer any questions on the recommendation or supporting information contained herein.

For further information please contact:

Scott Talbott  
Senior Vice President  
Electronic Transactions Association  
[stalbott@electran.org](mailto:stalbott@electran.org)