

Assisting Small Business with Minimizing the Risk and Recovery from Cybercrime

Issue

The cost and maintenance of cyber security measures is prohibitive to small and medium-sized enterprises (SMEs). There are solutions available, but the challenge is encouraging businesses to incorporate those solutions to protect their data.

Background

The internet is the road on which the majority of business is conducted in the 21st century and while business is responsible for its own portion of that road help is needed to make sure it is maintained.

Earlier this year the Canadian Chamber of Commerce (CCC) release a report called "Cyber Security in Canada". Within that report it was found that "the primary concern for SMEs is resources – most have no or limited financial or human resources (technical expertise) to address the challenges presented by cybercrime; therefore, there is little inclination to invest in protection".

The Canadian economy is comprised primarily of SMEs (98%) and representing about 51% of Canada's GDP and that is reason for concern. By incentivizing the adoption of cyber security solutions, the federal government can ensure that small and medium-sized business is not only protected, but if attacked can recover quickly and effectively. The CCC report lays out the three main reasons criminals target smaller business:

1. Due to a lack of resources, small businesses are less equipped to handle an attack.
2. The information hackers want – credit card credentials, intellectual property, and personally identifiable information – is often less guarded on a small business's system.
3. Small businesses' partnerships – the value chain – with larger businesses provide back-channel access to a hacker's true target

According to StaySafeOnline.org, 71% of data breaches happen to small businesses, and nearly half of all small businesses have been the victim of a cyber attack (Cyber Security in Canada pg 25).

At the same time, the dollar value of [cyber security] incidents is also on the rise, according the CCC report. It goes on to say, in a recent PwC survey, business executives note the cost of cybercrime on the bottom line is increasing. These costs include downtime, compensation for breached records and loss of intellectual property. The Ponemon Institute surveyed 24 companies across all sectors for IBM in a report called 2016 Cost of Data Breach Study. It noted that the average cost of a data breach was \$6.03 million.

Given the numbers and the three points above it's clear to see why helping SMEs protect themselves is important to the Canadian economy.

Recommendation

That the federal government allow SMEs to write off 100% of their business investments in cybersecurity-related software, equipment and other costs (support services and outsourcing costs) in the year those investments are made.