COUNTERING COSTLY CYBERCRIMES

Opening Statement

The cost of cybercrime perpetrated on businesses is rising. However, there is insufficient data to determine accurately what those costs are. When asked at a recent cybercrime dialogue if the attendants knew where to report a cybercrime, most did not. Canada does have websites where business can report a breach of their data, however, it is not well known. Businesses need to report cybercrime and provide the data that the federal agencies require to accurately measure the costs and develop strong countermeasures. Conversely, the federal agencies could and should do more to engage businesses as part of their planning and outreach strategies and promote their webpage for reporting cybercrime through education and awareness campaigns.

Background

The fact that cybercrime is on the increase is indisputable. What becomes challenging is measuring the impact on Canada's economy. In 2018, 57% of Internet users reported experiencing a cyber security incident. Just over one-fifth (21%) of Canadian businesses reported that they were impacted by cyber security incidents which affected their operations in 2017. About 19% of small businesses reported being impacted compared to 28% of medium-sized businesses and 41% of large businesses.[1]

Of those businesses that were impacted by cyber security incidents, 39% could not identify the motive of the attack, while 38% identified the motive as an attempt to steal money or demand a ransom payment. Just over one-quarter (26%) of businesses experienced incidents where perpetrators attempted to access unauthorized or privileged areas, while 23% experienced incidents where there was an attempt to steal personal or financial information.[2]

Sectors which reported the highest level of cyber security incidents included banking institutions (47%), universities (46%) and pipeline transportation (45%). Businesses in these sectors were mostly impacted by incidents to steal money or demand ransom payments in 2017.[3]

Canadian businesses spent an average of $16,000 to recover from all impactful cyber security incidents in 2017, these average costs were substantially higher for businesses in critical infrastructure sectors. Businesses in the pipeline transportation sector spent $131,000, followed by businesses in the natural gas distribution sector ($118,000) and banking institutions ($87,000). Comparatively, universities ($13,000) spent less than the average. [4]

In Federal Budget 2019, the Government of Canada invested $144.9 million over five years to the Communications Security Establishment (CSE) to help improve protection of critical infrastructure, $80 million to fund several university-affiliated cyber security networks to promote collaboration between cyber security centres of excellence, $67.3 million over five years, and $13.8 million per year ongoing, to Public Safety Canada; Innovation, Science and Economic Development Canada; Global Affairs Canada; and the Royal Canadian Mounted Police to raise cyber security awareness, $30.2 million over five years to

[1] https://www150.statcan.gc.ca/n1/pub/89-28-0001/2018001/article/00015-eng.htm
[2] https://www150.statcan.gc.ca/n1/pub/89-28-0001/2018001/article/00015-eng.htm
[3] https://www150.statcan.gc.ca/n1/pub/89-28-0001/2018001/article/00015-eng.htm
[4] https://www150.statcan.gc.ca/n1/pub/89-28-0001/2018001/article/00015-eng.htm

protect democracy and elections from foreign interference and election misinformation. $19.4 million to over four years to the Heritage department to help educate Canadians to recognize online disinformation.

Currently, there are initiatives that the federal government has put forward such as the Mandatory Breach Notification legislation for organizations subject to The *Personal Information Protection and Electronic Documents Act* (PIPEDA). However, the general public has incomplete knowledge of which companies are subject to reporting breaches and are largely uninformed as to what information has been compromised. There are several models used elsewhere which can improve Canada's reporting and information dissemination procedures, for example, Australia's ACORN program (Australian Cybercrime Online Reporting Network) collects citizen complaints so that police and industry can monitor trends, thwart organized criminal groups and arrange incidents for further investigation.

To conclude, the research is not consistent on cost or number of incidences in Canada as this data is not fully tracked and not all breaches are reported. It is safe to guestimate that cybercrime has cost the Canadian economy up to $3.12 billion dollars annually (Huffington Post, quoting NORTON, 2013). The time taken (averaging 19 hours for individuals, according to Norton) to deal with an incursion as well as the cost to salvage data, the cost to develop a more secure system, the cost to update employee training to avoid further breaches, and ultimately, the cost to a business's brand as client trust is lost along with their data, is incalculable. Cybercrime has become a barrier to economic growth.

THE CHAMBER RECOMMENDS

That the Provincial Government and Federal Government work collaboratively with stakeholders and business to:

1. strengthen and promote the Canadian Cyber Incident Response Centre (CCIRC) and the Canadian Anti-Fraud Centre (CAFC):
    a. as collectors of data including type and number of incidences;
    b. to develop awareness and education strategies for businesses in a format that is easily accessed and understood; and
    c. to pro-actively engage businesses and the public in awareness and education campaigns;

2. ensure that the newly formed Electronic Crime Committee (ECC) includes business association representatives to assist with communications and outreach strategies to businesses;[9] and

3. invest additional resources required to increase the RCMP's or other Municipal Police's ability to investigate and prosecute criminal activities with collaborating investigative agencies and local authorities.

Submitted by the Surrey Board of Trade