SURREY BOARD OF TRADE
inclusive | innovative | independent

2018

COUNTERING COSTLY CYBERCRIMES FOR BUSINESS

Introduction

The cost of cyber crime perpetrated on businesses is rising. However, there is insufficient data to determine accurately what those costs are. When asked at a recent cyber crime 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 cyber crime and provide the data that the federal agencies require to accurately measure the costs and develop strong counter-measures. 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 cyber crime through education and awareness campaigns.

Background

That cyber crime is on the increase is indisputable. What becomes challenging is measuring the impact on Canada's economy. Published only a year ago, PricewaterhouseCoopers economic crime survey found 59% respondents believe cybercrime is on the rise, with 28% confirming they've been impacted in the previous 24 months. Losses ranged between $50,000 to $5M for 16% of respondents, with another 31% losing from $1,000 to $50,000. Those tipping over $1M have increased to 12% from 5% in 2014.[1]

Norton Cyber Security Insights Report 2016 states that $1.9B (USD) was lost to cybercrime in Canada in the previous year with 26% (8.5 million Canadians) affected.[2] Another private security firm predicts cybercrime will cost more than $2.1T (yes, T for trillion) by 2019 with 60% of the breaches occurring in North America.[3] The Association of Certified Fraud Examiners puts it at $3.5T globally, now.[4]

Symantec reports that security breaches are up 2% in 2016 from 2015 with more than 10 million identities exposed, a huge 125% increase from the previous year. 62% of the business victims were small to medium enterprises. Customer details are the targets putting many individuals at risk for fraud or worse.[5] Start-ups are most vulnerable as a data breach recovery averages $38,000; with intellectual property and trade secrets compromised. Bankruptcy looms for those who lose much.

Even governments are not safe. Since 2010, Public Safety Canada has spent $245 million on defending government computer networks, safeguarding critical infrastructure and educating the public. Currently, there are no federal laws to require companies to disclose hacks, security breaches, thefts of data or money, so the general public has incomplete knowledge of which companies have been compromised. There are several models used elsewhere which can be adapted for Canada. For example, Australia's ACORN program (Australian Cyber Crime Online Reporting Network) collects citizen complaints so that police and industry can monitor trends, thwart organized criminal groups and arrange incidents for further investigation.

---

[1] Global Economic Crime Survey 2016. www.pwc.com/ca/crimesurvey
[2] https://us.norton.com/cyber-security-insights-2016
[3] https://www.canadiansecuritymag.com/news/data-security/cybercrime-will-cost-businesses-over-$2-trillion-by-2019
[4] http://www.mnp.ca/en/posts/7-shocking-statistics-on-small-business-data-theft
[5] http://www.mnp.ca/en/posts/7-shocking-statistics-on-small-business-data-theft

Canada does have a Spam Reporting Centre, which is hosted by the Canadian Cyber Incident Response Centre (CCIRC), and a government operated Canadian Anti-Fraud Centre (CAFC), but neither is equipped to handle the exploding array of cyber-scams and malware that are targeting home and business computers.[6] Recently, the Canadian Association of Chiefs of Police (CACP) and the Canadian Advanced Technology Alliance (CATAAllliance) joined forces to create the Electronic Crime Committee (ECC) to develop a national cybercrime strategy for Canada,[7] which will begin to address the need for data and a more coordinated approach with law enforcement agencies. As an advisory body, it does not have legislative powers to effect necessary changes to protect Canadian businesses, though its work will no doubt be of value in the future.

The RCMP has a cybercrime strategy (2015)[8] defining cybercrime in two categories: technology-as-target (the unauthorized use of computers and/or data, including identity theft, scams, phishing, etc.), and technology-as-instrument (criminal usage including fraud, drug trafficking, cyber-bullying, exploitation, etc.). Their data is collated accordingly as the number of incidences reported in each category. The RCMP has a broad mandate for investigating cybercrime including coordinating with local policy forces and international agencies. As part of their action plan, #8 identifies the need to enhance the Canadian Anti-Fraud Centre (CAFC) "as a trusted data and intelligence source on financially-motivated cybercrimes," and "improve victim-based reporting" to improve police information sharing on cybercrime activities and trends, "including potential links to National Police Services." Action items #9 and #10 are similarly seeking coordination of data collection across agencies. As not all incidents are reported or recorded, the true impact of cybercrimes has yet to be measured by anyone, including those charged with investigating criminal activity in cyber-space.

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 Surrey Board of Trade recommends that the federal and provincial governments 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

[6] Canadian Cyber Incident Response Centre. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx
[7] https://www.cacp.ca/electronic-crime-committee.html#122
[8] http://www.rcmp-grc.gc.ca/en/royal-canadian-mounted-police-cybercrime-strategy
[9] As per the RCMP Cybercrime Operational Framework: E5 "Engage industry to address shared cybercrime issues and foster mutually beneficial relationships." http://www.rcmp-grc.gc.ca/en/royal-canadian-mounted-police-cybercrime-strategy

3. Invest in additional resources required to increase the RCMP's ability to investigate and prosecute criminal activities with collaborating investigative agencies and local authorities.