55. The Risks of Cyber Crime — Electronic and Digital Issues

From the individual consumer to large corporations, cyber crime has cost the Canadian economy up to $3.12 billion dollars annually. The cost of protecting oneself and one's business from being detrimentally affected is escalating; as precious resources are used for security, it is a barrier to economic growth.

Cyber crime is not a new phenomenon, but there is still a lot to learn in order to effectively respond to the threat. The nature of cyber crime continues to change faster than public institutions can fully understand them, regulate them and mobilize against them. For example, one of the most prolific and damaging cyber scams seen is the Business E-mail Compromise (BEC) scam which primarily targets businesses of various sizes and affects countries all over the world. Although the BEC scam is primarily a sophisticated social engineering scam, the BEC scam has cost victims over $1 billion to date.

According to the National Cyber Security Alliance, one in five small businesses are hit by cyber crime annually. In 2013, cyber attacks on small businesses rose 300% comprising 31% of all targeted attacks. Small businesses are particularly vulnerable without the resources to combat such attacks such as Remote Access Trojans used by criminals who were able to alter their online or payment terminals. On a larger scale, cyber criminals often target smaller business that have partnerships with larger organizations for the purpose of back door access to the larger partner's stores of more valuable personal data, critical infrastructure and intellectual property. 71% of cyber crime attacks happen to small businesses, which do not have the same security levels as larger organizations. Almost half of small businesses have been victim of a cyber attack with the hackers seeking credit card credentials, intellectual property, and personally identifiable information.[1]

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. Canada does have a Spam Reporting Centre and a government operated Canadian Anti-Fraud Centre, but neither is equipped to handle the exploding array of cyber-scams and malware that are targeting home and business computers.[2]

The Surrey Board of Trade has been leading awareness of, and action against, cyber crime for several years, recent recommendations requested that the federal government:

- Establish a centralized mechanism for the mandatory reporting of designated cyber security incidents to enable quantification of the potential damage to the Canadian economy.
- Establish a national educational program to increase awareness, among children, of cyber crime and prevention programs for introduction into school curricula.
- Establish a website to act as a clearinghouse for the most current information on cyber crime in Canada, for public information and education, with monitored links to similar central information points around the globe.

Cyber crime is occurring exponentially in keeping with the growth of the digital marketplace. The federal strategy is focused primarily on national security threats and does little to combat the dramatic growth in email scams, online extortion and breaches at corporate computer networks. It will require all levels of government, RCMP and business to play a part in reducing and eliminating cyber crime in a coordinated strategy.

---

[1] Canadian Chamber of Commerce
[2] Canadian Advanced Technology Alliance

Recommendations

That the federal and provincial governments work in a coordinated way with stakeholders and business to:

1. Increase integration amongst governments and policing agencies on cyber crime to effectively punish cyber criminals
2. Promote digital literacy by establishing best practices for cyber resilience, including education on more sophisticated and specialized crime
3. Invest additional financial and skilled human resources to the national cyber-security centre set up by government, industry and policing agencies to help investigate and warn the public about new and emerging cyber-threats