

## **Fighting Cybercrime beyond ID Theft and Spam**

Cybercrime is focused, in the public eye, mainly on Identity Theft and the problem of Spam email. The problem is broader than that and the resolutions contained herein are intended to deal with the issues beyond those two serious problems.

In a meeting with Janet Napolitano, Secretary of Homeland Security, Canadian Public Safety Minister Peter Van Loan likened cyber security to “the new arms race” as the government fights to protect its information systems from threats from around the world.

In 2008, the Canadian Association of Police Boards (CAPB) commissioned a nationwide survey by Deloitte which identified cybercrime as the most significant challenge facing law enforcement organizations in Canada.

The Internet has grown to be a vital piece of the fabric of all aspects of the day to day operation of society, as well as an indispensable vehicle for international commerce. It has brought a myriad of opportunities for enormous financial opportunity and success among entrepreneurs around the world, both legitimate and criminal. Unfortunately, the game, and the laws that govern law enforcement world wide favour the criminal. With enormous financial resources (often rivaling and even exceeding many countries) these criminals can hire the brightest talent, acquire the latest technologies, and harness archaic legal systems to work to their benefit by not keeping pace with criminal developments, by not instituting legal remedies at the pace the criminals can generate new modes of operation, and by shackling the enforcers with these inadequate and antiquated legal systems unsuited to the modern world.

Identity theft and subsequent fraud is rapidly challenging drug trafficking as the main generator of money from crime, and Spam, has become the greatest threat to overloading the system, stealing time and resources as well as being the vector for fraud and malicious attacks on the world’s cyber systems.

### **The CAPB Deloitte findings include:**

- 49% of respondents have been a victim of cyber crime (cyber crimes include computer viruses, banking and personal information being lost or stolen through the Internet, children being bullied or sexually abused through online contact, businesses being hacked and held for ransom, identity theft and interference with critical infrastructure such as power grids, water systems or telephone services).
- 70% of victims of cyber crime have not reported the crime as they were unsure who to report to or did not think any justice would occur.
- 86% of respondents indicate that cyber crime has become a concern.
- 95% of respondents believe they are being targeted for cyber crime (most respondents believe the greatest threats are identity theft, financial fraud and computer viruses).
- 89% of respondents believe that preventing cyber crime should be a priority of government and law enforcement agencies.

**Some additional considerations include:**

- a recent IBM survey of healthcare, financial, retail and manufacturing industries, nearly 60% of businesses believe that cyber crime is more costly to them than physical crime
- 2007 research from the U.S. Cyber Consequences Unit shows that the destruction from a single wave of cyber attacks on critical infrastructures could exceed \$700 billion - the equivalent of 50 major hurricanes hitting U.S. soil at once.
- According to a 2007 Symantec study, Canada ranks ninth as a country targeted for malicious cyber activities while the U.S. holds the #1 position. This same study discovered more than 700,000 new malicious code threats for 2007, up from only 125,000 in 2006

The Canadian Chamber of Commerce has spoken to the issues of Identity Theft and Spam in previous resolutions (2007); however, there is much cyber crime, outside of these two aspects including espionage and terrorism which obviously pose a threat to commerce as well as the integrity of the country and need attention by our government.

**Recommendations**

That the federal government in concert with the recommendations on Identity Theft (2007) and Spam Control (2007):

1. Amend the Criminal Code to modernize search and seizure and intercept provisions (particularly Part 6) in keeping with changes in technology by:
  - requiring telephone and internet service providers to include interception capability in new technology once North American standards have been developed;
  - requiring telecommunications service providers to make customer name and address information available on request from law enforcement personnel;
  - requiring service providers to ensure that specified information in relation to a particular subscriber is preserved and produced in response to a court order;
  - engaging in discussions with providers to identify reasonable costs arising from meeting the foregoing requirements, and develop a process of compensation for said costs.
2. Establish a centralized mechanism for the mandatory reporting of designated cyber security incidents to enable quantification of the potential damage to the Canadian economy
3. Establish a national educational program to increase awareness, among children, of cyber crime and prevention programs for introduction into school curricula
4. Develop and implement a national campaign to educate both the general population and the business community to the relevant risks in not being adequately aware of, and protected from, the activities of cyber criminals

5. Establish a web site to act as a clearing house for the most current information on cybercrime in Canada, for public information and education, with monitored links to similar central information points around the globe.