BUILDING A **SAFE** AND **RESILIENT CANADA**

The Development of *Canada’s Cyber Security Strategy* and Lessons Learned

September 11, 2013

Association of Southeast Asian Nations Regional Forum

Workshop on Cyber Security

Canada

The Evolution of Cyber Security as an Issue

- Computer security in the late 1980s and 1990s was viewed primarily as a technical issue.
    - Managed by IT departments and only exceptional cases referred to law enforcement.
    - Malware seen as a nuisance, but not a serious security issue to be addressed by governments.

- Developments in the late 1990s and early 2000s change this.
    - The Y2K scare and its impact on national critical infrastructure.
    - The ILOVEYOU and other worms.

- The landscape becomes much more complex in the mid 2000s
    - Espionage and cybercrime become commonplace
    - The Internet becomes a critical tool that underpins economic and social prosperity

Developing the Strategy

- Private sector
    - Early engagement
    - Call for central point of contact

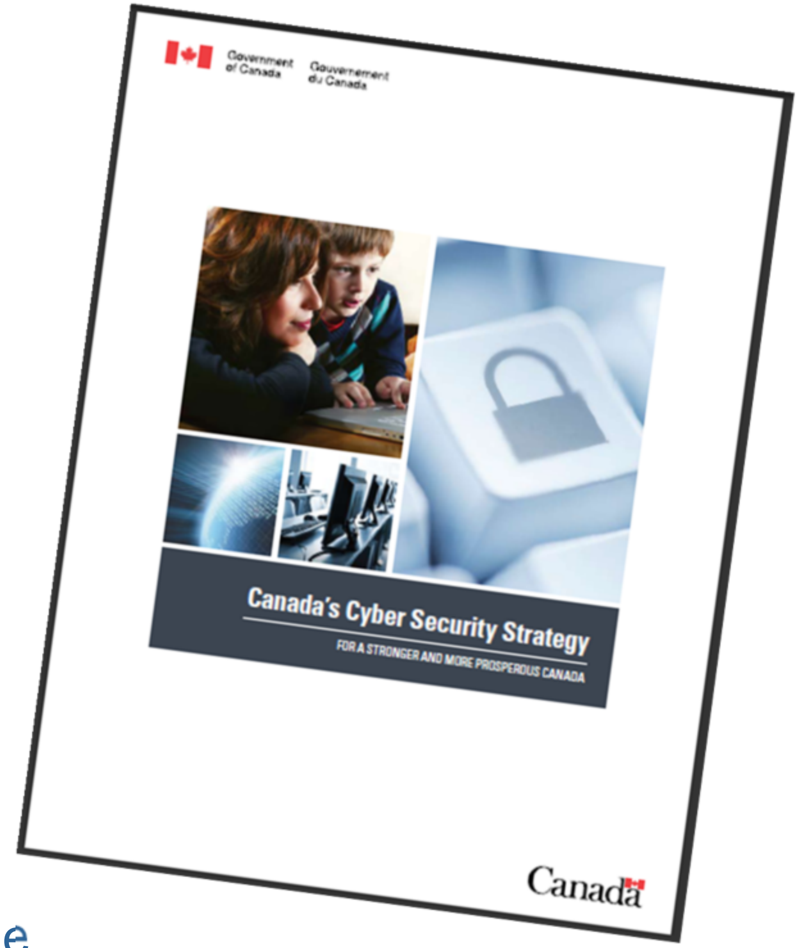
- Government
    - Develop a highly classified threat assessment for senior officials
    - Identify a lead agency and obtain senior level commitment
    - Formal and consistent inter-departmental steering committee

- Challenges
    - Limited empirical data on the impact of cyber crime
    - Cyber is “silent” – stigma of coming forward
    - Perception this is only a technical issue
    - Describing the precise nature of the threat is difficult
    - Identifying and bundling a solution is complex

Canada's Cyber Security Strategy

- Launched in October 2010.
- Signals cyber security as a priority for the Government of Canada.
- Coordinates and unifies domestic and international action.
- Built on three pillars:

  1. Secure Government systems.
  2. Partner to secure systems outside the Government of Canada.
  3. Help Canadians to be secure online.



Government of Canada Gouvernement du Canada

Canada's Cyber Security Strategy

FOR A STRONGER AND MORE PROSPEROUS CANADA

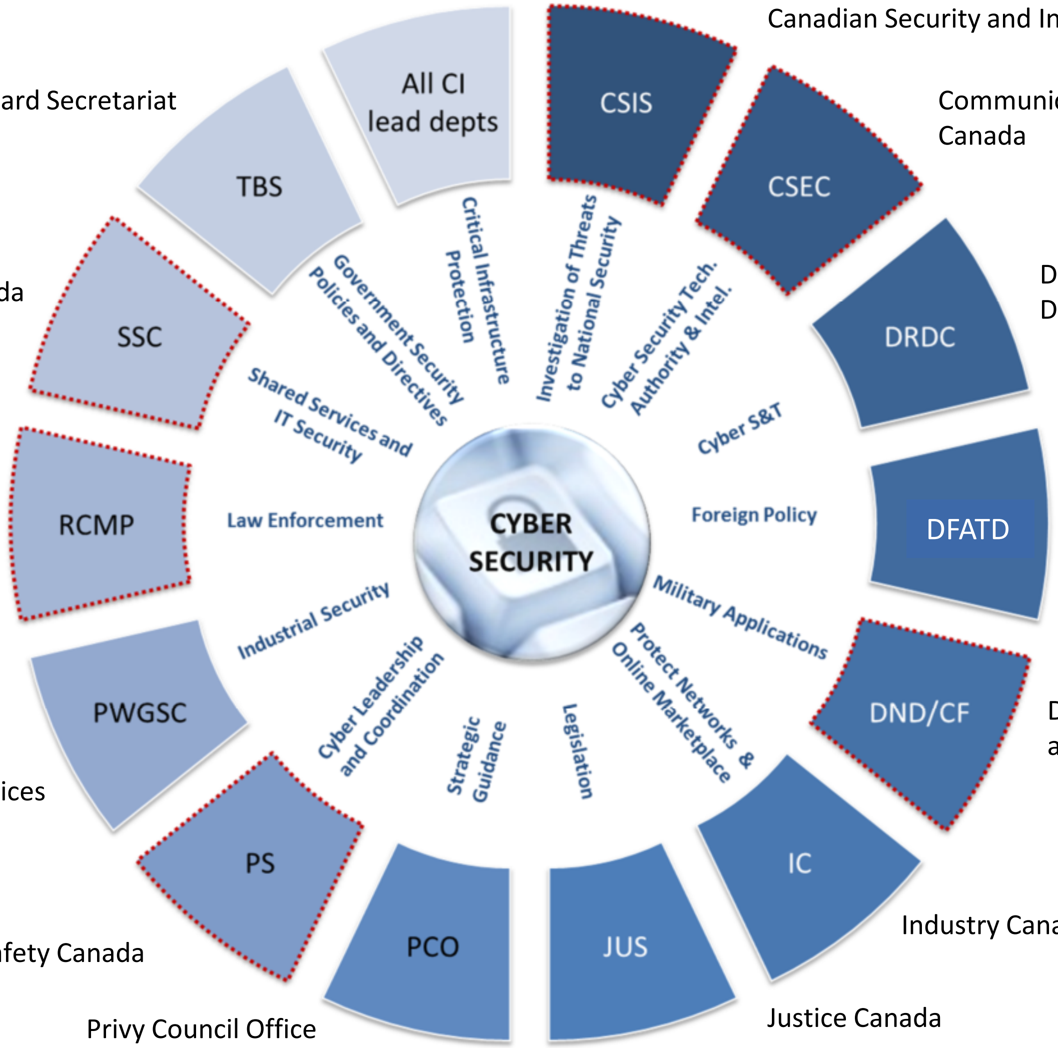
Canada

Pillar 1: Secure government systems

- Establish clear federal roles and responsibilities.
  - Refine government departments’ responsibilities for cyber security incidents affecting government networks.
- Strengthen security of federal information and systems.
  - Improve cyber hygiene throughout government.
- Strengthen international cyber security activities.
  - Deeper engagement with allies and partners.
  - Focused engagement at international forums to promote cyber security best practices and norms.

A whole of government approach

Roles and responsibilities with respect to cyber security



CYBER SECURITY

All CI lead depts – Critical Infrastructure Protection

CSIS – Canadian Security and Intelligence Service – Investigation of Threats to National Security

CSEC – Communications Security Establishment Canada – Cyber Security Tech. Authority & Intel.

DRDC – Defence Research and Development Canada – Cyber S&T

DFATD – Department of Foreign Affairs, Trade and Development – Foreign Policy

DND/CF – Department of National Defence and the Canadian Forces – Military Applications

IC – Industry Canada – Protect Networks & Online Marketplace

JUS – Justice Canada – Legislation

PCO – Privy Council Office – Strategic Guidance

PS – Public Safety Canada – Cyber Leadership and Coordination

PWGSC – Public Works and Government Services Canada – Industrial Security

RCMP – Royal Canadian Mounted Police – Law Enforcement

SSC – Shared Services Canada – Shared Services and IT Security

TBS – Treasury Board Secretariat – Government Security Policies and Directives

Creation of Shared Services Canada

- On August 4, 2011, the Government began to streamline and consolidate its IT architecture in the areas of email, data centres and networks.

- Once complete, this will produce savings and reduce the Government's footprint; strengthen security and the safety of Government data to ensure Canadians are protected; and realize economies of scale and make it more cost-effective to modernize these IT services.

- All resources associated with the delivery of email, data centre and network services are being transferred from 44 of the more IT-intensive departments to a new entity called Shared Services Canada.

Pillar 2: Partner to secure systems outside the Government of Canada

- Strengthened the Canadian Cyber Incident Response Team (CCIRC), Canada's national Computer Emergency Response Team.
  - Extended hours of operation.
  - Hired more staff.
  - Created a malware lab and Industrial Controls System test centre.
- Partner with provinces, territories, and critical infrastructure sectors.
  - Initial focus on three sectors: energy, telecommunications, and finance.
  - Develop and publish a Cyber Incident Management Framework.
- Develop leading edge cyber security science and technology.
  - Leverage existing research networks to strengthen research and development.

Pillar 3: Help Canadians to be secure online

- Promote public awareness, education, and engagement.
  - Launch of the GetCyberSafe.ca campaign.
  - Partnership with Stop.Think.Connect.

- Strengthen legislative framework to address cyber crime.
  - Drafting legislation to permit the ratification of the Budapest Convention.

- Enhance law enforcement capabilities.
  - Established a Cyber Crime Fusion Center at the Royal Canadian Mounted Police to improve cyber crime statistics.

Action Plan 2010-2015 for Canada's Cyber Security Strategy

- Launched in April 2013.

- Outlines progress made across all three pillars and identifies initiatives until 2015.

- Focus on domestic and international efforts:

  - Greater Canadian engagement in international forums

  - Working with cross-border partners to enhance operational collaboration

Government of Canada Gouvernement du Canada

Action Plan 2010-2015
for Canada's Cyber Security Strategy

Canada

What We Learned

- Adopting and implementing a strategy needs to be a whole of government effort.
  - Clarifying the roles and responsibilities of various players is critical.

- Outreach to other levels of government and the private sector in the early stages and throughout the process.

- Cyber is not just a technology issue, it's also about people and policy.

- Early development and promulgation of threat briefs and a simple story to describe the proposed approach.

- International engagement and promoting norms for cyberspace is essential.
  - United Nations Group of Government Experts
  - Meridian Conference on Critical Information Infrastructure Protection
  - Budapest Convention

BUILDING A **SAFE** AND **RESILIENT CANADA**

www.publicsafety.gc.ca/cyber

Canada