

# Cyber Security Centre.



Cyber security incidents and issues dominate headlines globally, creating persistent and pressing challenges for both the public and private sectors. Cyber-attacks have victimized major retailers, financial institutions, and government departments and agencies. Experts argue that intellectual property loss from cyber attacks is reaching catastrophic levels, as well as damaging brand and stakeholder trust.

In this costly and rapidly evolving cyber-security environment, exchanging information and best practices is vital. The Conference Board of Canada created the Cyber Security Centre (CSC) to serve as a confidential, multi-sectoral forum where leaders from industry and government can exchange strategic information and insights, identify emerging threats, and establish shared research priorities.



In spring 2014, the Conference Board brought together a range of senior executives to identify their strategic needs for cyber security. While many forums exist, they tend to be sector-specific and/or highly technical, leaving a critical gap in the current cyber security environment. The Conference Board's Cyber Security Centre fills this gap by providing a multi-sector, non-partisan forum that focuses on the strategic and policy implications of cyber security and informs and empowers senior executives responsible for these issues.

The Centre also provides a confidential, collaborative venue for executives to build relationships and knowledge across sectors and industries, with the ultimate goal of making Canada a safer, more prosperous place in which to live and work.

## Key Objectives

- Identify emerging cyber security trends and threats that cut across industries and sectors.
- Develop independent, evidence-based research and provide a foundation for informed decision-making about critical cyber security issues and how they impact organizations and Canadians.
- Provide a trusted forum for candid dialogue on cyber security issues with business, government, and academic representatives.

## Who should join?

The Cyber Security Centre is for senior-level representatives, thought leaders, and key stakeholders from private sector organizations, government, and academia who require new knowledge to help their organizations cope with the strategic and policy challenges of cyber security. This includes: chief information security officers, chief security officers, and other senior employees who wrestle with cyber security on a regular basis.

## Exclusive Benefits of Participation

- Keep your finger on the pulse of key developments and debates in cyber security that can only come from a secure, confidential setting for public-private information exchange.
- Gain new insights and better inform your decision-making on cyber issues by networking with senior-level representatives, thought leaders, and key stakeholders in a multi-industry platform.
- Participate in frank and open dialogue aimed at improving the quality of your policy-making and decision-making, while at the same time gain access to a broad range of security experts from academia, government, and business.
- You will have the opportunity to inform the research agenda and support, review, and access rigorous, balanced research in this area.
- Access research findings before they are publicly released.
- Benefit from ongoing engagement and updates between meetings through webinars, blogs, bulletins, and social media.
- Access to the private members-only website, which features meeting notes, agendas, and presentations, as well your peer network.



## Looking Forward

The Cyber Security Centre, together with its advisory committee and members, has developed a forward-looking, operationally relevant agenda and research program for the coming years. It reflects the thought-leadership and collaborative approach of members who are committed to helping each other take on the strategic and policy challenges of cyber security. The following themes and topics have been identified as priority areas for the Centre to advance research and thinking:

### **Policy and Governance**

- Building working relationships with senior leaders
- Improving cyber security governance and leadership
- Crisis communications best practices and considerations
- Risk assessment
- Aligning reporting in Canada across critical infrastructure

### **Talent and Education**

- Finding and managing cyber security talent
- Educating and accommodating a new generation
- Talent development and training

### **The Human Side of Cyber Security**

- Influencing employee behaviour through cultural change
- Insider threat: remaining secure without impacting productivity
- Workforce transformation
- Implementing cyber security practices in light of organizational vulnerability
- Making decisions with limited information

### **A Sustainable Cyber Security Market**

- Keeping pace with technology adoption
- Understanding the implications of new and emerging technologies
- Building productive, candid relationships with the cyber security industry
- Implementing successful cyber security initiatives
- Planning, directing, and assessing investment on cyber security controls and technologies
- Understanding jurisdictional differences
- Developing solutions-based cyber security procurement

## Research Highlights

As a Centre member, you help to set the research agenda and can request additional custom research on demand. In its first year, the Cyber Security Centre's research focused on foundational public policy issues of concern to Canadians and Canadian businesses, such as privacy in the online world, cyber security governance, and cyber security in Smart Cities. Other highlights included:

- **Data Privacy:** In May 2016, our research team published a comprehensive survey of data privacy regimes in Canada, the EU, and U.S., comparing their implementation and pointing to six critical future trends that will affect Canadians.
- **Improving Executive Performance in Cyber Security:** Ongoing Center research focuses on promising practices to improve corporate governance of cyber security through executive education and performance reporting to boards of directors.
- **Information and Intelligence Sharing:** In spring 2016, the Conference Board surveyed security stakeholders across Canada on their information and intelligence-sharing practices, and in particular the relationship between public and private organizations. Centre for National Security members convened in Montreal in June 2016 to hear preliminary insights and discuss the issue.
- **National Security and Cyber Security Blog:** Conference Board researchers and experts continue to publish blogs on current events and ongoing research, providing insights on the latest developments in national security and the cyber domain.

The Cyber Security Centre is an integral component of Conference Board's National Security and Public Safety (NSPS) knowledge area. It is one of the four security-related executive networks run by NSPS, along with the Centre for National Security, the Council on Emergency Management, and a strategic foresight practice. This rich collection of networks allows the Cyber Security Centre to draw together insights and connections from a diverse array of stakeholders and experts in the private sector, academia, and every level of government.

## Member Organizations

Bell Canada

Business Development Bank of Canada

City of Calgary

Emera Inc.

Enbridge

Export Development Canada

J.D. Irving Limited

Ontario Provincial Police

Payments Canada

Public Safety Canada

Royal College of Physicians and Surgeons of Canada

Transat A.T. Inc.

### CONTACT

**Deborah Fleck**

Senior Manager,

Executive Networks

National Security and Public Safety

The Conference Board of Canada

613-526-3090 ext. 362

fleck@conferenceboard.ca

[www.conferenceboard.ca/networks/csc](http://www.conferenceboard.ca/networks/csc)