

CANADIAN CENTRE FOR **CYBER SECURITY**

**ISACA Annual General Meeting
Cyber Threat Assessment 2018
June 13th, 2019**

© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.



censorship
 pervasive connectivity
 cyber theft
 anonymity
 disruption
 cybercrime
 ubiquitous
 vulnerabilities
 asymmetric warfare
 malicious code

A WORLD GONE DIGITAL

job losses
 hackable homes
 self-replicating botnets
 Internet of Things
 data privacy
 fake news
 non-attribution
 pervasive risks
 vulnerable control systems
 hackable transportation



67% of CIRA survey respondents in Canada outsource at least a portion of their cyber security footprint to external vendors (CIRA)

Cyber Security contributes \$1.7 billion to Canada's GDP and consists of over 11,000 well-paying jobs (CIRA)

Canadian Cyber Security Ecosystem

30% of organizations deploy an e-commerce platform (CIRA)

Canadian organizations will need to hire approximately **8,000** additional cyber security professionals between 2016-2021 (Deloitte)

The 2018 National Cyber Security Strategy: *Canada's Vision for Security and Prosperity in the Digital Age*, introduces a new strategic direction for cyber security in Canada.

National Cyber Security Strategy

Secure and Resilient Canadian Systems

Protect Canadians from cybercrime, respond to evolving threats, and help defend critical government and private sector systems



An Innovative and Adaptive Cyber Ecosystem

Support advanced research, foster digital innovation, and develop cyber skills and knowledge



Effective Leadership, Governance, and Collaboration


Collaborate with provinces, territories, the private sector, as well as international allies, to take a leadership role in advancing cyber security





CANADIAN CENTRE FOR **CYBER SECURITY** | CENTRE CANADIEN POUR LA **CYBERSÉCURITÉ**

We are the single unified source of expert advice, guidance, services and support on cyber security for government, critical infrastructure owners and operations, the private sector and the Canadian public.



National-level
outcomes

Information and
information systems of
importance

Complement public &
commercial capability

Communications Security Establishment

- The Cyber Centre is part of the Communications Security Establishment (CSE)
- CSE operates in accordance with all Canadian laws, including the **Privacy Act**, the **Criminal Code**, and the **Canadian Charter of Rights and Freedoms**
- CSE's mandate and authorities are defined in the **National Defence Act**:

A dark blue hexagon with a white letter 'A' inside.

Provide **foreign intelligence**, in accordance with Government of Canada intelligence priorities

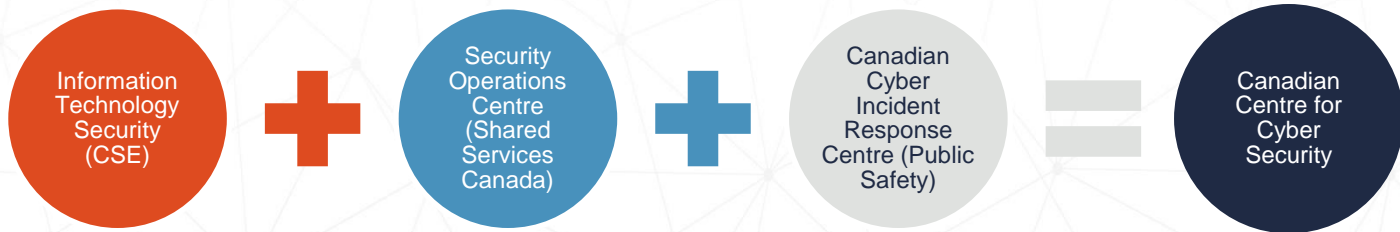
A dark blue hexagon with a white letter 'B' inside.

Provide **advice, guidance and services** to help ensure the protection of electronic information and of information infrastructures of importance to the GC

A dark blue hexagon with a white letter 'C' inside.

Provide **technical and operational assistance** to federal law enforcement and security agencies

Centralizing Cyber Security Expertise

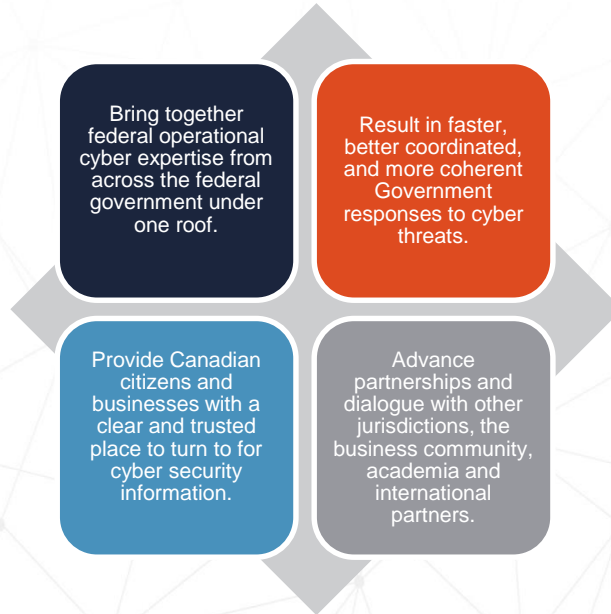


Who We Serve

We welcome partnerships that help build a stronger, more resilient cyber space in Canada. We hold unclassified, multi-purpose spaces for the joint use of government, private industry and academia.



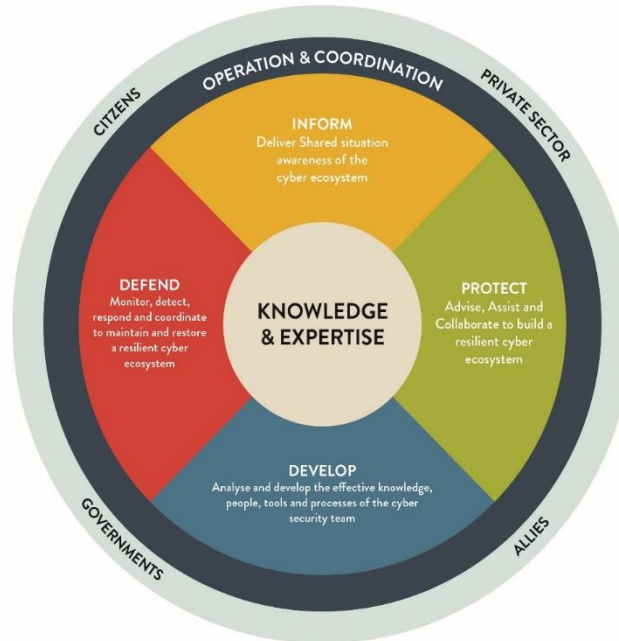
The Cyber Centre's Vital Role in Protecting Canada and Canadians



FUNCTIONS

Inform Canada and Canadians about cyber security matters, including about cyber security threats.

Defend networks and systems that are within its purview.



Protect Canadian interests through advice, assistance, and collaboration with partners across the country and abroad.

Develop and enrich the knowledge, personnel, and skills needed to continually improve cyber security for Canadians.

Inform

- GetCyberSafe Public Awareness Campaign
- Technical Advice and Guidance
- Strategic Cyber Threat Assessments
- Cyber Health and Trends Reporting
- Cyber Event Notifications and Reports



GetCyberSafe Campaign

HOW CYBER SAFE ARE YOU IN THE DIGITAL AGE?



Canadians spend an average of
6 hours a day online

WHAT DEVICES DO CANADIANS USE TO ACCESS THE INTERNET?



94%
LAPTOP OR
DESKTOP
COMPUTER



58%
TABLETS



74%
SMARTPHONES



25%
SMART TVS



25%
GAMING SYSTEMS

Canadians protect their
computers from online threats,
but **only 50% know** of the
risks to their other devices



5 WAYS TO RUN A #CYBERSAFEBUSINESS

For any business, employees are both the biggest risk
AND the best defence against cybercrime.

Knowledge and training make all the difference.

Get Cyber Safe Blog



Protect yourself and report scams

At Get Cyber Safe, we offer tips on how to protect yourself from cyber threats. But what should you do when it does happen? The type of recourse depends on the type of cyber incident



5 ways to protect your privacy on a new smart device

While connected devices (also known as "smart devices") are fun and make our lives easier, they also provide opportunities for hackers to access personal and private information. Take steps to protect yourself, and your family, by following these tips.



3 Things to Look for Before You Buy a Smart Device

Smart home assistants, virtual reality headsets, smartwatches - these are some of the hottest gifts flying off the shelves this holiday season. Before you buy a device that connects to the Internet, do your research to help protect yourself, and your gift's recipient, from falling victim to cybercrime.

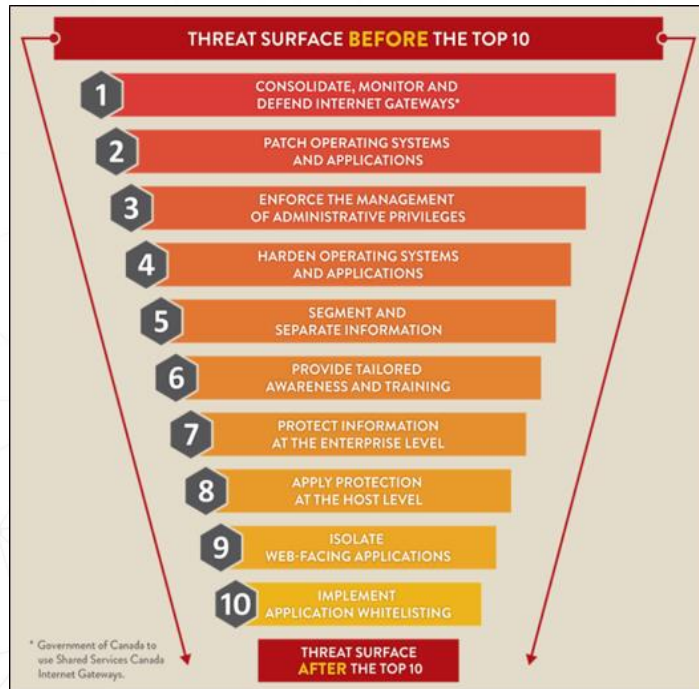
Baseline Cyber Security Controls

- Intended for small and medium organizations (<499 employees)
- Provides advice and guidance on accessible cyber security practices
- Tailored to balance investment costs and cyber security outcomes



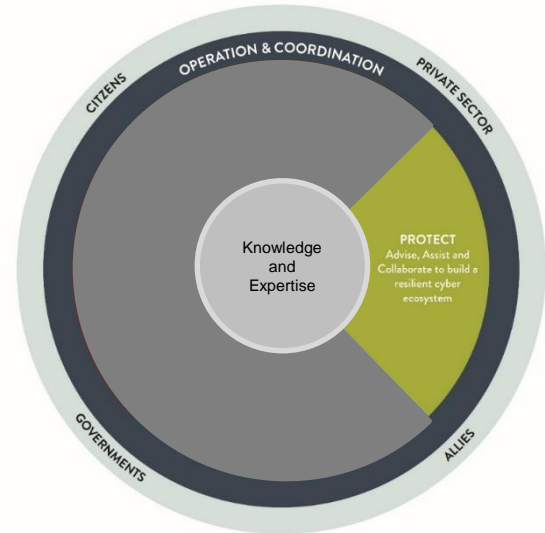
CSE Top 10

- Full set of cyber threat mitigation measures for any size organization
- Based on analysis of cyber threat activity trends to counter most current cyber threats



Protect

- Product Assurance
- Risk Mitigation Programs
- Incident Management Support
- Automated Information Sharing Services



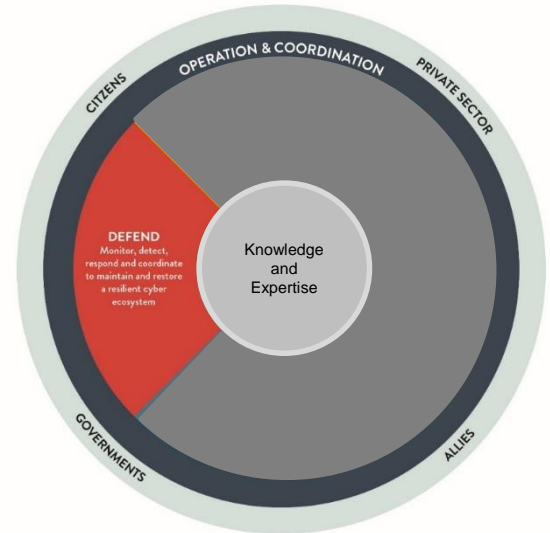
Common Criteria Program

- International program in which accredited laboratories test IT products against standard cyber security specifications called Protection Profiles (PPs)
 - These PPs represent the security assurance requirements for technology classes
- The Cyber Centre operates the Canadian Common Criteria program to certify products tested by Canadian Common Criteria testing laboratories.
 - Evaluation services are conducted by commercial facilities



Defend

- Security Operations Management for the Federal Government
- Network Defence
- Cryptographic Services
- Secure Communications Solutions
- Collaborative Cyber Defence Project



Protecting Government of Canada Networks

- We detected and confirmed a cyber-intrusion by a highly sophisticated Chinese state-sponsored actor on the computer networks of the National Research Council (NRC)
- This involved collaboration between NRC, SSC and other Government of Canada IT security partners
- Many cyber defence methods were used in the tracking and mitigation of this cyber intrusion against NRC
 - The lessons learned from this incident helped improve and perfect these tools and techniques

Assembly Line is a Cyber Centre open-source tool that was used during the compromise of the NRC.

Good Crypto is the front line in Cyber Defence

Protect Confidentiality



Protection from Cyber Attack



By the 2030s, quantum computers could break the crypto used today – The Cyber Centre is doing the following:

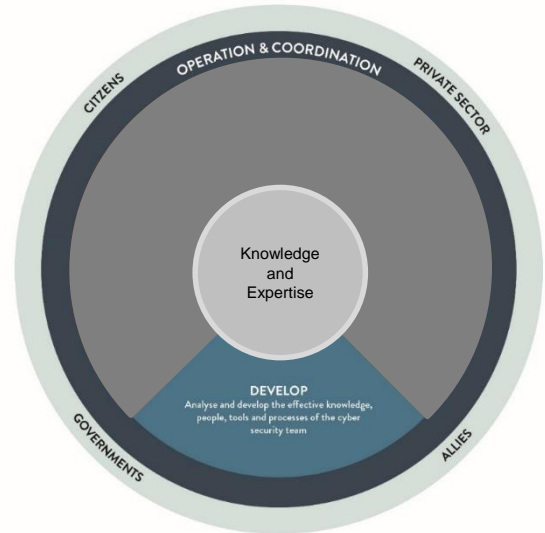
- Conducting research to evaluate replacement crypto components
- Actively participating in the development of new crypto standards
- Working with the Government of Canada to update the crypto used to protect its most sensitive information
- Reaching out to industry and academia to develop a plan to ensure Canada's cyber safety

Collaborative Partnership with the Independent Electricity System Operator (IESO)

- In addition to information and technology sharing, the Cyber Centre will provide support with threat prediction, identification and response on an as-needed basis, as well as guidance on threat assessment and reporting
- This partnership reflects the importance of managing cyber risk and encouraging collaboration within the industry
- Our collaborative efforts will help the IESO manage the risks associated with cyber threats

Develop

- Learning and Innovation Hub
- GeekWeek Collaboration Event
- Academic Outreach
- Research and Development



Learning Hub

- Trusted source for leading-edge learning activities and programs for cyber security and COMSEC professionals working in government, industry and academia
 - This includes services, guidance and advice on cyber security training and education
- Over 30 courses offered in two streams:
 - COMSEC
 - Cyber Security



GeekWeek

- GeekWeek is a one-of-a-kind event where government, industry, academia and international cyber security partners come together to improve and protect the cyberspace
- This collaborative event focuses on the importance of information sharing between partners to achieve success in innovation



- In 2018, GeekWeek hosted more than 200 participants
 - This led to more than 80 new open-source tools and major innovations in many fields such as network traffic and log analysis, malware detection and automated malware analysis



CANADIAN CENTRE ^{FOR}
CYBER SECURITY

NATIONAL CYBER THREAT ASSESSMENT 2018



Communications
Security Establishment

Centre de la sécurité
des télécommunications

Canada



Communications
Security Establishment

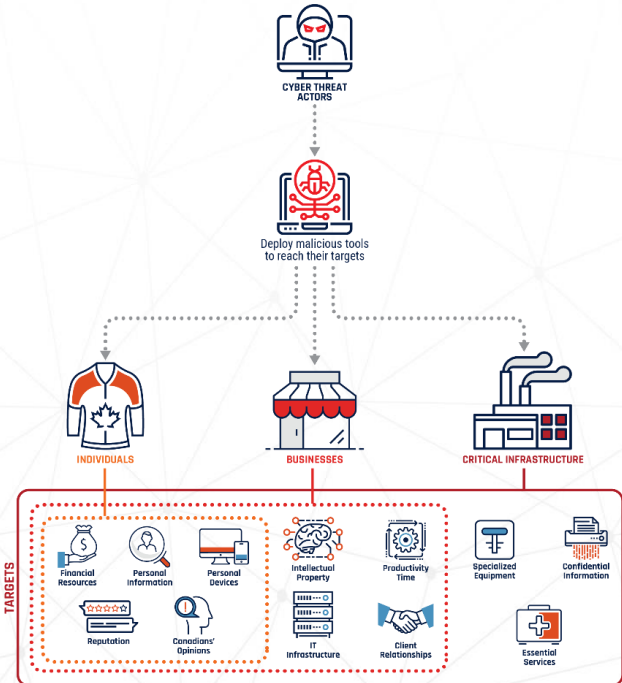
Centre de la sécurité
des télécommunications

Canada

How are Canadian networks at risk?

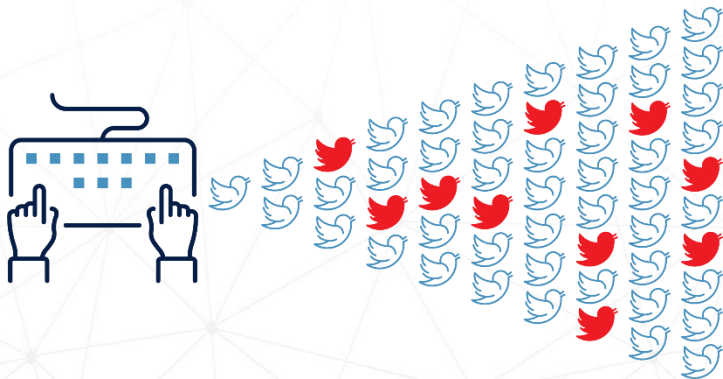
- Cyber threats — including foreign states, hackers, criminals, and terrorists — continually probe systems, looking for vulnerabilities in order to gain access to a computer.

With access, threat actors can steal or distort information, corrupt operations or program the computer to exploit other computers and the systems to which it is connected.



Cyber Threats to Canadians

Key Judgements



Cybercrime is the cyber threat most likely to affect Canadians and Canadian businesses in 2019.

Canadians are very likely to encounter malicious online influence activity in 2019.

Cyber Threats to Canadian Businesses

Key Judgements

Sophisticated cyber threat actors will likely continue to exploit the trusted relationships between businesses and their suppliers and service providers.

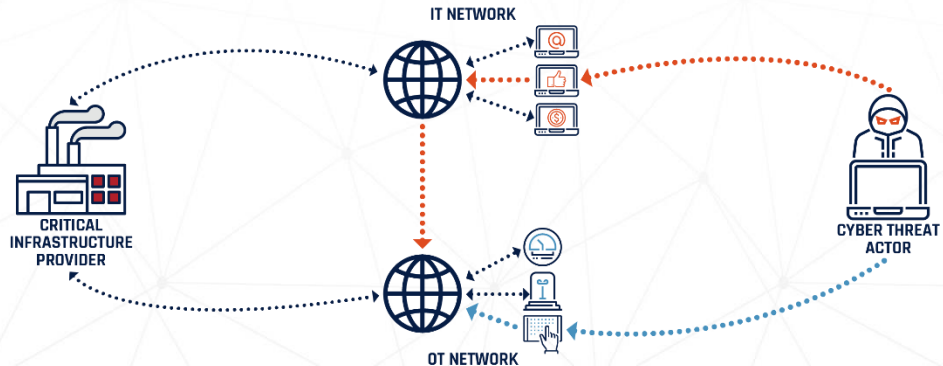
Cyber threat actors — of all sophistication levels — will increase the scale of their activities to steal vast troves of personal and commercial data.

As cyber security improves, cyber threat actors are adopting more advanced methods, such as compromising hardware and software supply chains, making detection and attribution more difficult for defenders.



Cyber Threats to Canadian Critical Infrastructure

Key Judgements



It is very unlikely that, absent international hostilities, state-sponsored cyber threat actors would intentionally disrupt Canadian critical infrastructure.

State-sponsored cyber threat actors will continue to conduct cyber espionage against Canadian businesses and critical infrastructure to advance their national strategic objectives.

Energy Sector Compromise

Example Case Study



- In 2017, CSE alerted partners in the United States to an energy sector ICS cyber compromise.
- According to officials at DHS, Russian cyber threat actors reached secure systems and isolated networks, advancing to the point where they could have disrupted power flows in North America.
- The cyber threat actors exploited the supply chain using relatively simple techniques, such as spear-phishing emails.

What to look at next for your organization

○ Internal Governance

- Is cyber security a maintained priority?

○ Investment

- How much are you focusing resources on cyber security?

○ Resilience


- How prepared are you for a cyber attack?

○ Supply Chain

- Do all components of your supply chain have adequate cyber protection?

○ Collaboration

- Work with commercial cyber experts and leverage GC advice and guidance



**Adopting even basic cyber security practices
can help thwart cyber threat actors and reduce
the threats to Canadians and Canadian businesses.**

CONNECT WITH

US



@cse_cst



contact@cyber.gc.ca



www.cyber.gc.ca



@cybercentre_ca