

# CANADIAN CENTRE<sup>FOR</sup> **CYBER** SECURITY

Nuhad Zoght  
Partnerships - Canadian Critical  
Infrastructure

27 February 2020

© 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.



cyber theft  
anonymity  
disruption  
cybercrime  
ubiquitous  
vulnerabilities  
asymmetric warfare  
malicious code  
censorship  
pervasive connectivity  
A WORLD GONE DIGITAL  
job losses  
hackable homes  
Internet of Things  
non-attribution  
fake news  
pervasive risks  
vulnerable control systems  
self-replicating botnets  
Insufficient data privacy  
hackable transportation

# CIO's Top 10 Priorities

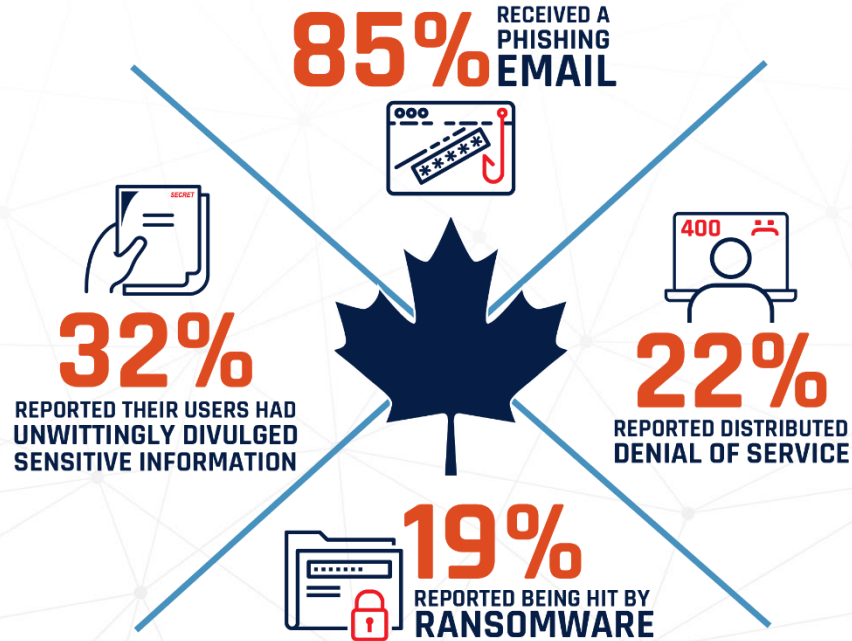
2020 Survey says...

- 1 Cybersecurity and Risk Management
- 2 Digital Government
- 3 Cloud Services
- 4 Consolidation/Optimization
- 5 Customer Relationship Management
- 6 Budget, Cost Control, Fiscal Management
- 7 Legacy Modernization
- 8 Data Management and Analytics
- 9 Broadband/Wireless Connectivity
- 10 Innovation and Transformation through Technology

Source: NASCIO.org



# Canadian Context – Cyber Security



75% of small businesses store corporate confidential information on externally hosted web-services while 48% of large businesses

21% of Canadian businesses reported that a cyber security incident affected their

66% of Canadian businesses have employees using personally-owned devices to conduct

76% of incidents attributed to an external perpetrator had monetary or ransom payment

Between 80% and 90% of all businesses currently hold insurance coverage for direct losses due to attack or intrusion.

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

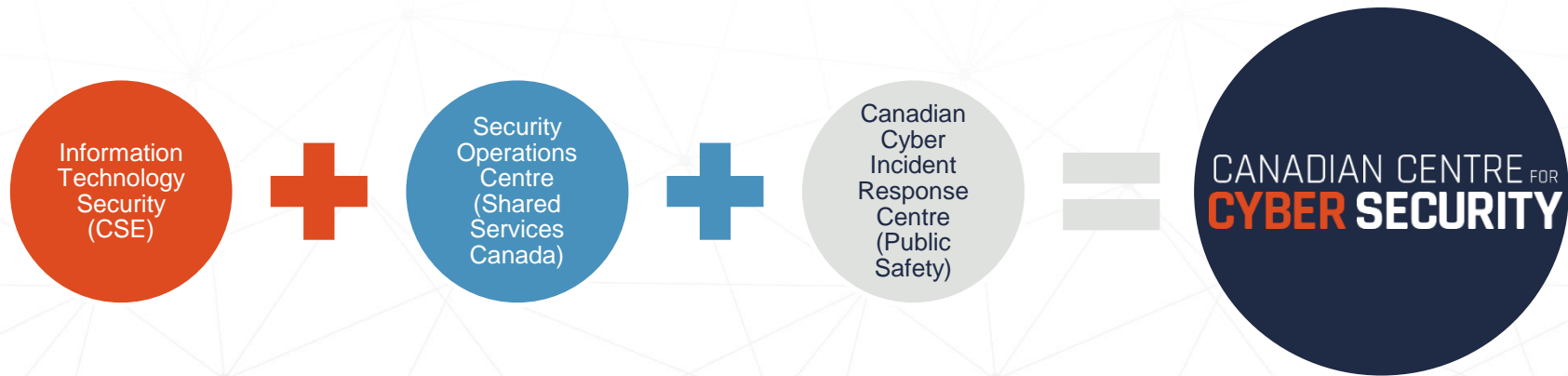


### Effective Leadership, Governance, and Collaboration

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



# Centralizing Cyber Security Expertise



*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.*



# CSE's Role in Cyber Security



CYBER SECURITY  
LEAD IN CANADA



ACCESS TO UNIQUE  
FOREIGN INTELLIGENCE



AHEAD OF  
EMERGING THREATS



MONITOR GC SYSTEMS  
24/7 FOR CYBER THREATS



SAFEGUARDS CANADA'S  
MOST IMPORTANT INFORMATION



CANADIAN CENTRE FOR  
**CYBER SECURITY** | CENTRE CANADIEN POUR  
**CYBER SÉCURITÉ**

# The CSE Act: Authorities and Capabilities

In Force: August 1, 2019

## FOREIGN SIGNALS INTELLIGENCE



**MAINTAIN CSE'S ABILITY TO COLLECT FOREIGN SIGNALS INTELLIGENCE**  
Use advanced techniques to access foreign networks to collect intelligence in support of government priorities

## CYBERSECURITY & INFORMATION ASSURANCE



**DEFEND IMPORTANT NON-GOVERNMENT OF CANADA NETWORKS**  
Upon request, deploy CSE's cybersecurity tools on non-government systems  
Remove legal barriers to sharing cyber threat information and mitigation advice

## ASSISTANCE TO FEDERAL SECURITY & INTELLIGENCE PARTNERS



**ASSISTANCE TO DND/CAF INCLUDING CYBER OPERATIONS FOR GOVERNMENT-AUTHORIZED MILITARY MISSIONS**  
Use advanced techniques to support military campaigns and protect military personnel

## FOREIGN CYBER OPERATIONS



**DEFENSIVE CYBER OPERATIONS**  
Disrupting foreign cyber threats targeting important Canadian networks  
**ACTIVE CYBER OPERATIONS**  
Interfere with foreign online efforts that threaten Canada



## INCREASED ACCOUNTABILITY MEASURES



# Increased Cyber Security Service Scope

*National  
Defence Act  
(NDA)*

CSE could provide advice, guidance and services to protect information infrastructures of importance to the GC.

*CSE Act*

CSE is now authorized to provide more robust cyber defense services by deploying its cyber defence tools to critical non-Government networks designated as being of importance to Canada.

## CYBERSECURITY AND INFORMATION ASSURANCE



### DEFEND IMPORTANT NON-GOVERNMENT OF CANADA NETWORKS

Upon request, deploy CSE's cybersecurity tools on non-government systems

Remove legal barriers to sharing cyber threat information and mitigation advice

# How does the Cyber Centre help?



*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

# Who Do 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.*

## Government

- We are the centralized voice and resource for senior leadership in government on cyber security operational matters.

## External Partners

- We are the primary federal government point of contact on cyber security operational matters for external partners, including incident response and coordination.

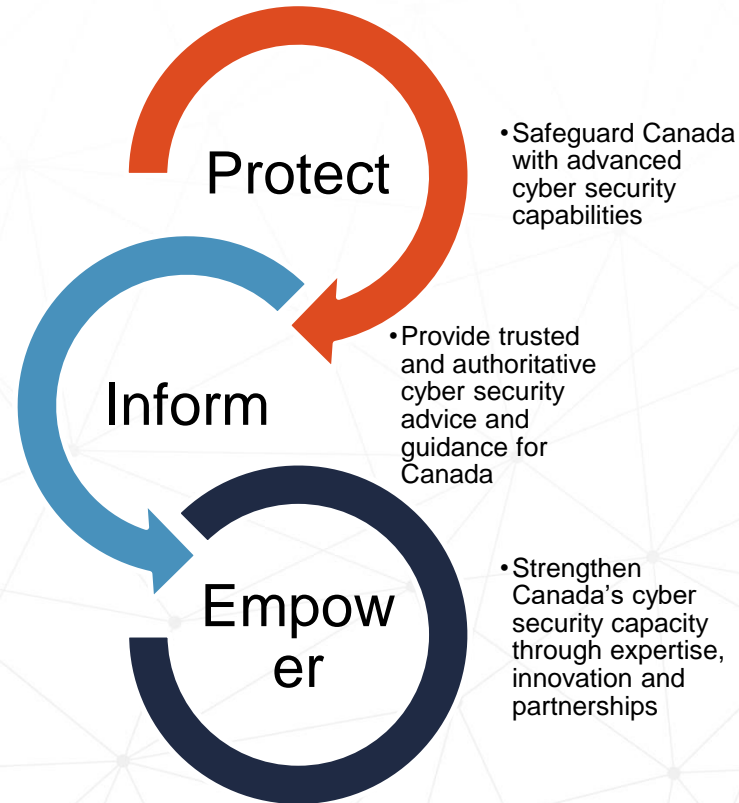
## Law Enforcement

- We are the single authoritative source of technical cyber security expertise to support lead agencies in their policing, security and intelligence work.

## Canadians

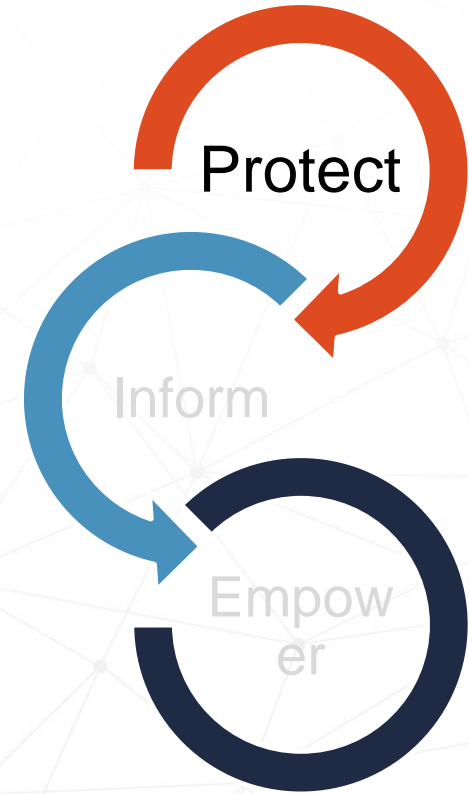
- We inform, communicate, and educate Canadians about cyber security issues by providing clear, practical advice backed up by unique expertise and insight.

# Enabling a Cyber Secure Digital Canada



# Protect

- Risk Mitigation Programs
- Incident Management Support
- Automated Information Sharing Services
- Network Defence
- Cryptographic Services
- Collaborative Cyber Defence Projects



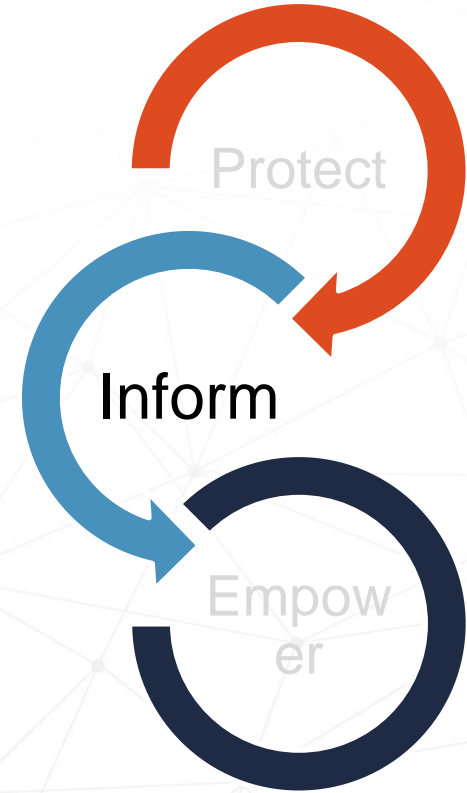
# Protecting Government of Canada Networks

- 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 an open-source Cyber Centre tool that was used to detect and analyze the malware during the compromise.

# 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

UNCLASSIFIED



## 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



25%  
SMART TV'S



25%  
GAMING SYSTEMS



74%  
SMARTPHONES

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.



Communications  
Security Establishment

Centre de la sécurité  
des télécommunications

# 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



# Controls Recommended

Develop an Incident Response Plan

Provide Employee Awareness Training

Implement Access Control and Authorization

Automatically Patch Operating Systems and Applications

Establish Basic Perimeter Defenses

Secure Cloud and Outsourced IT Services

Securely Configure Devices

Enable Security Software

Use Strong User Authentication

Secure Mobility

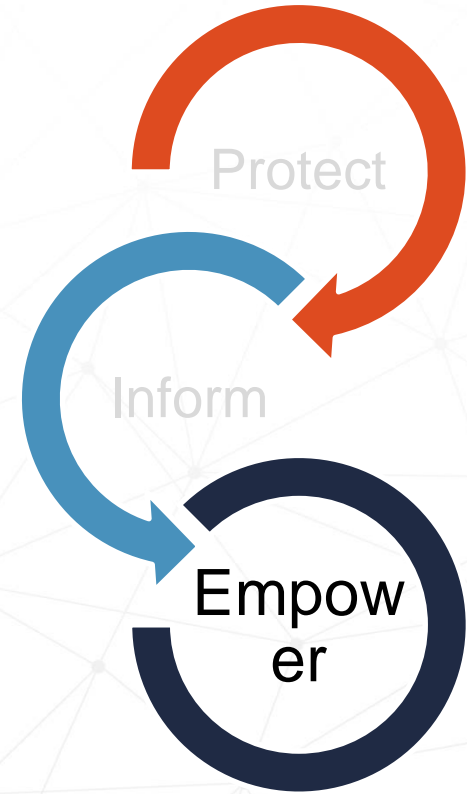
Backup and Encrypt Data

Secure Portable Media

Secure Websites

# Empower

- Partnerships (CI Sectors)
- Learning and Innovation Hub
- GeekWeek Collaboration Event
- Academic Outreach
- Research and Development



- Electronic delivery (free), including:
  - *601-Introduction to IT Security Management*
  - *604-Overview of IT Security Risk Management ITSG-33 Exec Summary*
  - *606-IT Security Fundamentals for IT Practitioners*
  
- Classroom, including:
  - 104 - IT Security Risk Management: A Lifecycle Approach (ITSG-33)
  - 105 - Information System Security Implementation Process (ISSIP)
  - 107 - Cyber Security in the GC for non-IT Employees
  - 109 - Cyber Security in the GC for IT Practitioners
  - 110 - Cyber Security in the GC and Online Exposure
  - 111 - Cyber Security in the GC for Home and Telework
  - 115 - Introduction to Cloud Computing in the GC
  - 345 - Cybersecurity for Wireless Communications
  - 701 - IT Risk Management and Security Control Profiles
  
- WebEx Sessions available (max. 25)

# What Do We Do

## SINGLE SERVICE WINDOW



## INCLUSIVE LEARNING AND INNOVATION HUB



## INTEGRATED INCIDENT RESPONSE



## EXPERT ADVICE AND GUIDANCE



## CRITICAL INFRASTRUCTURE ENGAGEMENT PROGRAM



## COMMERCIAL AND GOVERNMENT CRYPTOGRAPHIC EQUIPMENT ASSURANCE



## DEFENDING GOVERNMENT NETWORKS AND SYSTEMS FROM CYBER THREATS



## INFORMATION AND TECHNOLOGY SHARING WITH THE PRIVATE SECTOR

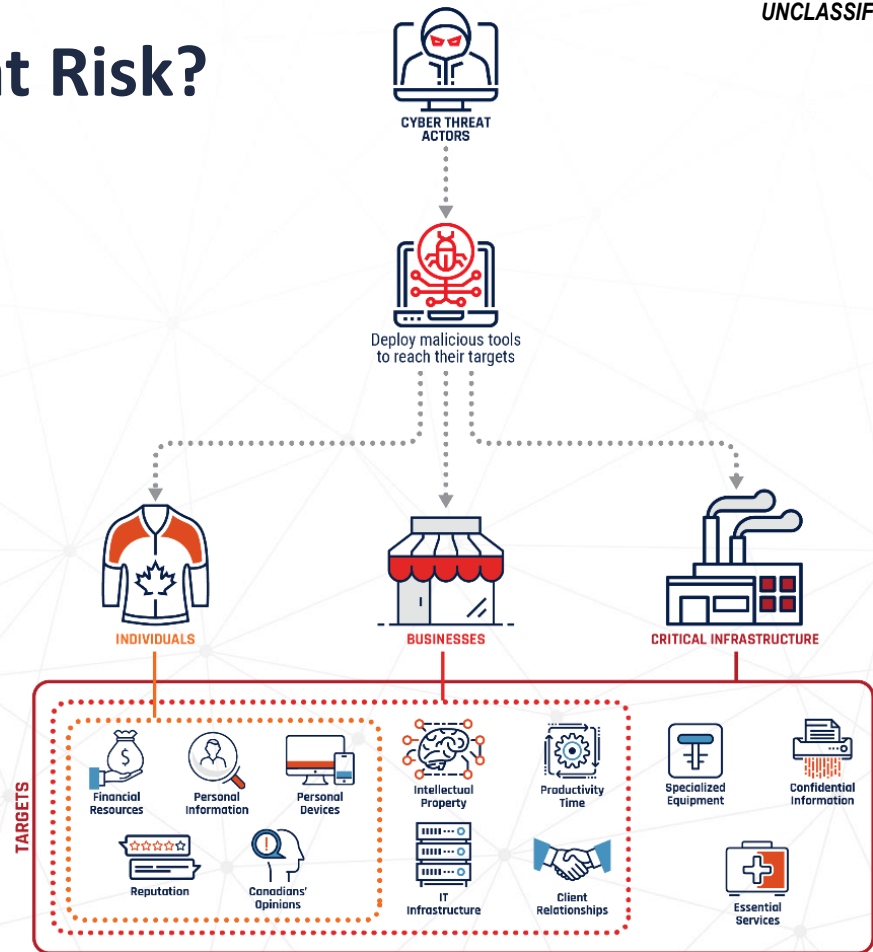
 PTM services leveraged today



# How are Canadian Networks at Risk?

- Foreign states
- Hacktivists
- Criminals
- Terrorists

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.

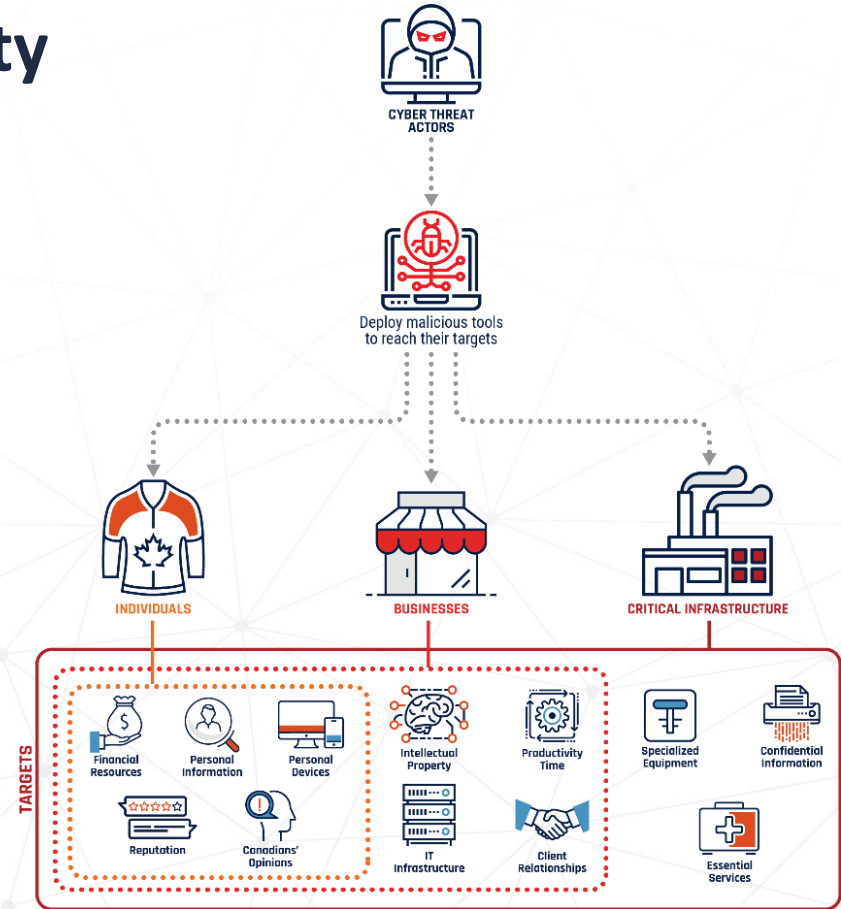




# Targets of cyber threat activity

## Focus on things that have value

- To people
- To organizations
- To governments



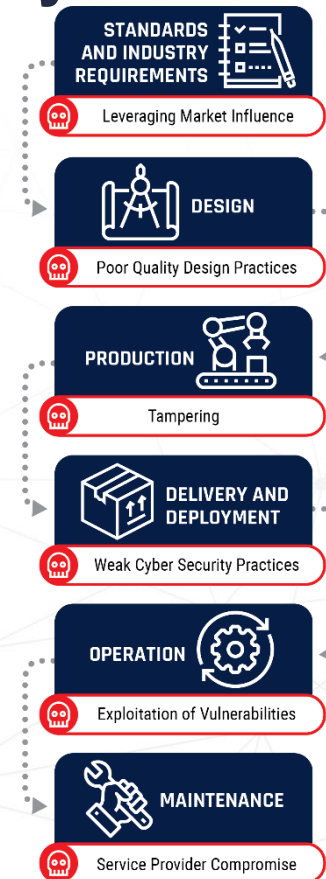
# State-Sponsored Cyber Threats

- State-sponsored cyber threat actors will continue to conduct cyber espionage against Canadian businesses and critical infrastructure to advance their national strategic objectives
- More nation-states are developing cyber tools designed to conduct cyber espionage
- Nation states will use what works
- Attribution remains difficult



# Supply Chain Threats Throughout a System's Lifecycle

- Every link in a global supply chain can pose a threat to cyber security
- The earlier a threat occurs in the development lifecycle, the more significant the potential impact
- Supply chain weaknesses are a valuable avenue for malicious activity for cyber threat actors



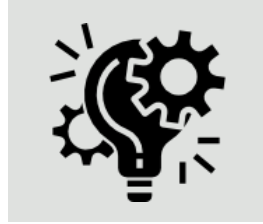
# RANSOMWARE IN NUMBERS (Ref. Deloitte, 2019)

- Average ransom payment of \$50,000
- A new business targeted every 40 seconds worldwide
- Above 50% ransomware infections originate from Remote Connections (RDP) compromise
- 40% of Canadian companies opted to pay for ransom
- Data recovery rate of 80%

# Business Value



**Economic  
Loss**



**Innovative  
Edge**



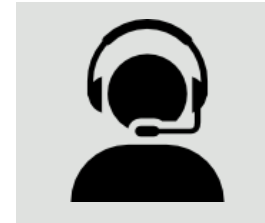
**Damage to  
Reputation**



**IP Theft**



**Availability of  
systems**



**Service  
Delivery**

# What to focus on:

## ○ 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, coordinate community efforts and leverage GC advice and guidance

# What should you do?

- Focus on the essentials (Planning, Policy, Process)
- Special treatment for high-value information
- Build cybersecurity into institutional governance
- Have a recovery plan
- Increase people's resiliency



# IN CYBER SECURITY, COLLABORATION IS THE KEY TO SUCCESS

The Centre's new facility will allow private and public sector organizations to work side-by-side on Canada's most complex cyber issues

- ▶ Open and accessible
- ▶ Large unclassified footprint
- ▶ Innovation spaces for collaborative work
- ▶ Co-development opportunities

# How the Canadian Centre for Cyber Security helps

## What can you get from the Cyber Centre?

①



**Awareness Reports  
and Notifications**

Access Actionable  
Cyber Threat  
Intelligence

②



**Tools to Assist Cyber  
Defence Teams**

Strengthen Your  
Defence Capabilities

③



**Report a Threat to  
the Cyber Centre**

Leverage the Cyber  
Centre's Expertise

④



**Community  
Building**

Further Cyber  
Security Together

# Who to Contact and When?

Cybertip.ca

- Child exploitation, trafficking of child porn, sextortion etc.



Royal Canadian Mounted Police  
Gendarmerie royale du Canada

- Cybercrime
- Ransomware, Money Laundering, Identity Theft, Cyberbullying, etc.

Canadian Anti-Fraud Centre



C A F C

Centre antip fraude du Canada

- Personal phishing email, telemarketing, tax scam.

CENTRE CANADIEN POUR LA  
CYBERSÉCURITÉ

- Cyber incidents, to report on malware and share malware samples, to request Advice and Guidance.

# Engaging the Cyber Centre

**Register** with the Cyber Centre for non-public alerts and information

Leverage publicly and commercially available **expertise** in improving your capabilities and resilience

## Contact Us

- When you experience a cyber incident
- If you have cyber security-related questions

Have an idea or project that could greatly **benefit** the ecosystem? We want to hear from you!

# CONNECT WITH US

Call 613-949-7048 or 1-833-CYBER-88

 @cse\_cst

 [contact@cyber.gc.ca](mailto:contact@cyber.gc.ca)

 [www.cyber.gc.ca](http://www.cyber.gc.ca)

 @cybercentre\_ca