POWERED BY
Institute for
Citizen-Centred
Service

Citizen FIRST

Cybersecurity

A look at the Canadian landscape

JOINT COUNCIL'S EXECUTIVE MONTHLY REPORT

(Product of the Research Committee)

June 2020

Image Source: Pikist

1. Introduction

Cybersecurity must be an agenda-topping issue in order for governments to effectively combat cybercrime. That being said, maintaining best practices whilst managing vulnerabilities and patching the most critical public-facing systems is no simple feat when jurisdictions are working alone. There are many benefits of jurisdictions and organizations within them working together to identify and solve cyber security problems, and mutually beneficial security regulations are recommended by experts.

In this Executive Report, we will take you through some key cybersecurity organizations and initiatives, outline 'top of mind' opportunities and challenges in the cybersecurity space, and identify where governments should be focusing their efforts.

Global annual cybercrime will cost the world in excess of $6 trillion annually by 2021, an increase from $3 trillion in 2015. This is the single greatest transfer of economic wealth in history and is more profitable than the global trade of all major illegal drugs combined.

2. Key National Cybersecurity Organizations and Initiatives

There are many organizations and departments across governments that play a role with respect to cyber security in Canada. Here are some to be aware of:

Canadian Centre for Cybersecurity

- The single unified source of expert advice, guidance, services and support on cybersecurity for government, critical infrastructure owners and operations, the private sector and the Canadian public.

Canadian Antifraud Centre

- Collects information on fraud and identity theft and provides information on past and current scams affecting Canadians.

Treasury Board of Canada Secretariat

- Establishes and oversees a whole-of-government approach to cyber security, including setting government-wide direction and establishing priorities for securing government IT systems and networks.

Public Safety Canada

- The department works closely with domestic and international partners as part of the global effort to protect critical assets and information and combat cyber crime.

Read more about the Cyber Security in the Canadian Federal Government here.

Jurisdictions to take note of

- Canada
  - New Brunswick
  - British Columbia
- International
  - United Kingdom (The National Cyber Security Centre)
  - United States (Department of Homeland Security, National Institute of Standards and Technology)

3. Cybersecurity themes that are 'Top of Mind" for governments

Cyberattacks on government systems are increasing, public service technologies are becoming a key part of value-based services, and outside disruptors are making moves into the public sphere. These are some of the themes that public sector sources say the industry is currently focused on.

Ransomware

"Ransomware is a type of malware that locks a computer system down until the victim pays the extortioner for the key code to unlock the device.[1]"

Cyber Insurance

"Cyber insurance is an insurance product designed to help businesses hedge against the potentially devastating effects of cybercrimes[2]."

Extortionware

"Extortionware is to demand a good, service, or payment to prevent violence or destruction of property. Some cyber criminals … demand money **before** they hurt you.[1]"

Security Risks in Work From Home

As many organizations have instituted work-from-home procedures, the risk of cyber attacks and security breaches is elevated.

Zero-Trust Security

"Zero trust posits that anyone logging into a network -- whether outsiders or insiders -- poses a possible threat. This approach replaces the "castle and moat" approach to security, where organizations protect their perimeters and assume everything inside is, therefore, safe.[3]"

Risk-Based Security Strategy

While governments move towards a risk-based approach to information security, security and user needs must be balanced.

1. "Cyber Extortion: Ransomware vs. Extortionware" 2018, alpinesecurity.com
2. "What is Cyber Insurance? 2020. cisco.com
3. "How governments can trust IT security: It's all about identity" 2020, gcn.com

4. Case Study: The Canadian Centre for Cyber Security (CCCS)

The public sector is providing a commitment to advancing bilateral collaboration on cybersecurity in Canada. Some organizations, such as the Canadian Centre for Cyber Security (CCCS), offer cross-jurisdiction support that can facilitate collaboration in the cybersecurity sphere.

What is the CCCS?

Under the Communications Security Establishment (CSE) Act, funding was approved for the new Canadian Centre for Cyber Security (CCCS) which consolidated federal efforts under one umbrella. CSE is Canada's national lead for foreign signals intelligence and cyber operations, and the technical authority for cybersecurity.[1]

CSE was born from WWII code-breaking efforts at the National Research Council, and its initial focus was a cryptologic agency helping to decrypt intelligence from foreign adversaries. The CCCS, also known as the "Cyber Centre", opened October 1st 2018, to support leadership and collaboration between different levels of government as well as national and international partners, while providing a clear and trusted single resource for Canadian citizens and businesses. It is Canada's authority on cyber security and single source of expert advice, guidance, services and support from the Government of Canada.[2]

Read more about the CCCS here.

CCCS Guidance, Tools and Services

CCCS support can help foster collaboration within the Canadian cybersecurity ecosystem, through:

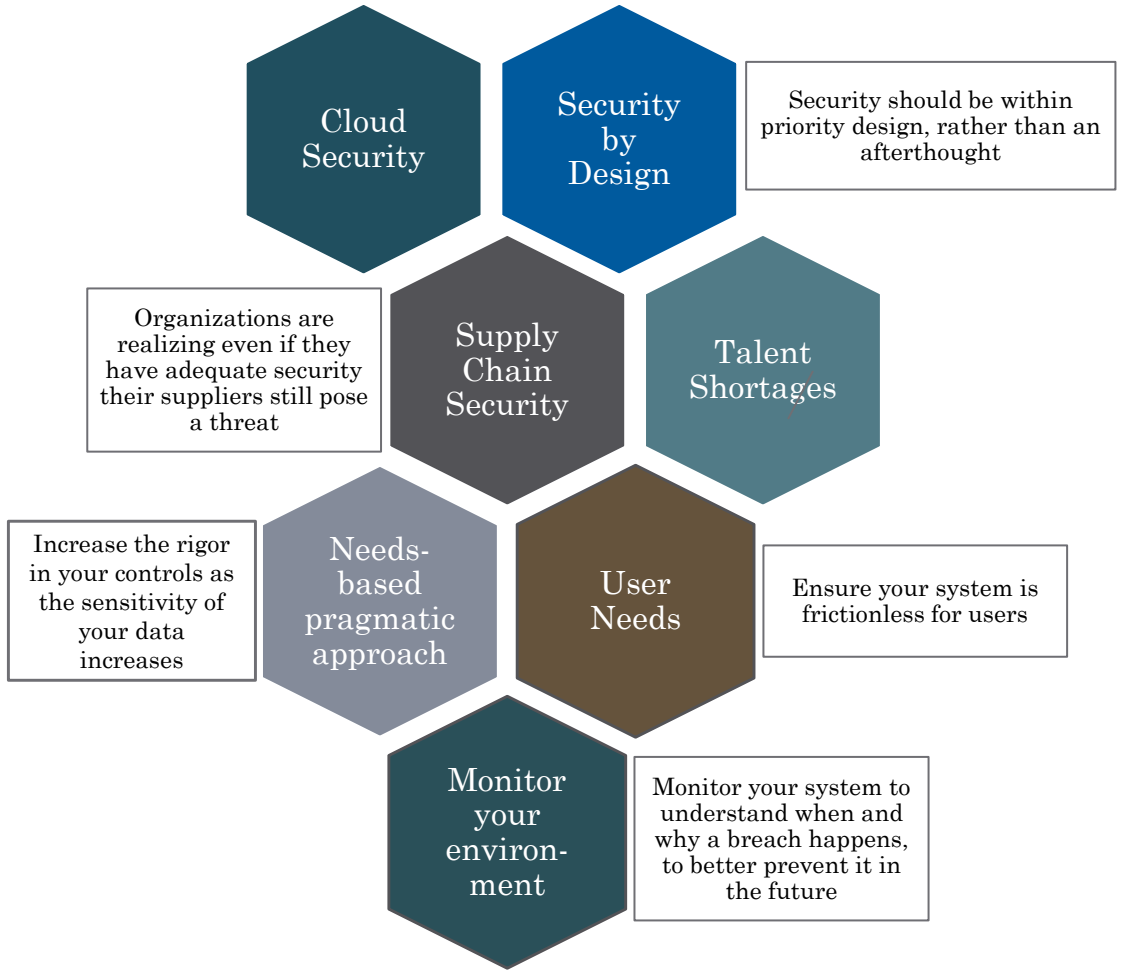
- Sharing cyber security incidents (phishing email reports, etc.)
- Providing advice and guidance on multitude of topics, such as video teleconferencing guidance, Email Domain Protection, Benefits and Risks of Adopting Cloud-Based Services in Your Organization and more available at (https://cyber.gc.ca)
- Services such as Alert (time-sensitive email relating to a high-impact cyber issue)
- Sharing resources, such as the recently published 'Configurations for Microsoft 0ffice 365 Services: On-Premises to Public Cloud Deployment Model'. This document needs to be tracked and therefore can be provided upon request at contact@cyber.gc.ca.

Contact CCCS for a full list of available tools and services.

1. "Inside CSE" 2020, cse-cst.gc.ca
2. "About the Cyber Centre" 2020, cyber.gc.ca

5. Where governments should focus their cybersecurity efforts?

More measures need to be put in place to safeguard cybersecurity in Canada. According to experts, some key areas of focus to enable government cybersecurity collaboration should include:



6. COVID-19 resulting in an increase in cyber threats

Amid the COVID-19 pandemic, Canadians and Canadian organizations have embraced technology to stay better connected, adopt alternative work arrangements, and move business activities online. The crisis has, however, proved opportune for increased cyber criminal activity.

For instance, the CCCS has noted an increase in healthcare related phishing and malware scams. The threats apply to more than just healthcare, as there is also an increase in online criminal activity.

COVID-19 Cyber Threat Activity Bulletin:

This bulletin warns that threat actors likely will target organizations conducting COVID-19-related research in order to steal intellectual property linked to the pandemic. Foreign interests are also likely after other intelligence, such as gaining advanced warning of public health responses (e.g., travel restrictions) under consideration by foreign states.

Daily Newsletter: Trends This Month
June 2020

Digital Transformation

COVID-19 crisis has meant a leap in the move to digital transformation. Read more here.

As the pandemic takes a toll, it is important to keep momentum going. Read more here.

User-centred public services

In the last few weeks, some government departments have accelerated change and launched new services at record-speed, standing up public services in days rather than months. Read more here.

Facial Recognition Tech

Amazon is halting police use of its controversial facial-recognition technology for a year as it awaits federal legislation to regulate it. Read more here.

IBM is altogether getting out of the facial recognition business. Read more here.

Other noteworthy articles this month:

COVID-19 Proves the Essential Nature of Government

IT modernization in the time of COVID-19: How government investment in critical IT systems can enhance citizen services

Foreign cyberthreats to Canada persist: spy agency

Designing public services in a user-centred way in a time of crisis

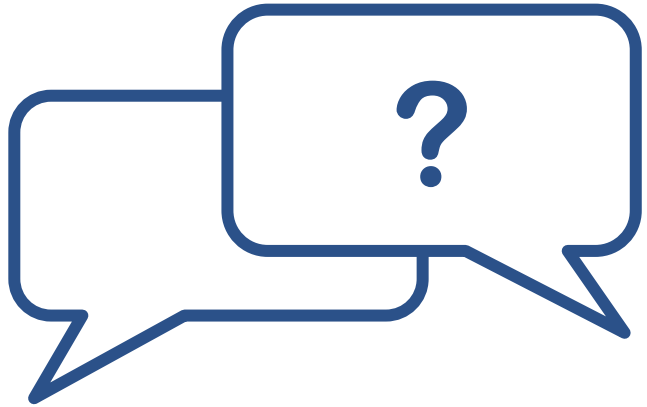
Is a 'Cyber Pandemic' Coming?

Research Repository

Access the Citizen First Research Repository here.

For further reading

- Cyber Security Today – A look at the future of work
- Five post-pandemic pivots in Canadian security and intelligence
- Taking a people-centric approach to federal cybersecurity
- Cyber Security Today- Take the time to find ransomware, how a ransomware gang recruits partners and a Norwegian fund victimized for $10 million
- How Security Leaders Can Manage Cyber-Risk During COVID-19
- Reconnaissance faciale: “Un risqué grave de surveillance de masse”



We would love to hear from you!

Do you know someone who may be interested in the Joint Councils Executive Report? Please share a copy of this report.

If you are not already a subscriber, you can now subscribe to receive the Executive Report by signing up here. Send your questions or suggestions to info@iccs-isac.org.