3rd Digital Transformation in Government

"THE CYBER LANDSCAPE IN THE NEW COLD WAR"

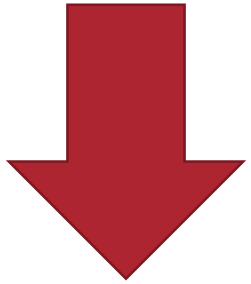
Bob Gordon

Strategic Advisor

2022 06 16

CCTX

DIGITAL TRANSFORMATION



Is your plan prepared for the evolving cyber threat?

CCTX

A changed operating environment

- COVID-19 resulted in a ‘doing it remotely’ lifestyle

Social distancing

Working from home

Shopping from home

} Human element

- Business responded with an accelerated technological transformation
- Challenges

Complex systems needed to be adapted

Legacy systems difficult to update and patch

} Technology

↓

Cyber criminals & nation states seized the opportunity

CCTX

Cybercrime is the "most pervasive threat to Canadians and Canadian businesses"

Shelly Bruce, Chief of the Communications Security Establishment[1]

"Data breaches have impacted virtually everyone in Canada"

Scott Jones, former Head, Canadian Centre for Cyber Security[2]

Cyber-enabled attacks pose significant threats to Canada's national security, its interests and its economic stability.[3]

1. Speaking May 18, 2021, at Centre for International Governance Innovation
2. "The Western Standard", June 1, 2021
3. "Canadian Security Intelligence Service Public Report 2021"

CCTX

Nation States As Cyber Attackers

- Primary motivation: espionage and conducting ‘statecraft’
- Attackers: Russia, China, Iran, North Korea
- Targets:
  - government agencies, inter- and non-governmental organizations, think tanks, critical infrastructure
- Techniques:
  - Interested in maintaining stealth and access
  - Increasing the scale and volume of phishing and password spray campaigns to evade detection and improve likelihood of success across multiple targets[1]
- Enabling cyber criminals to operate:
  - Minimal interference
  - Don’t attack the enabling state
  - Respond when called upon for assistance

1. “Microsoft Digital Defense Report”, October 2021
2. “Cyber Attacks More Likely to Bring Down an F-35 Than Missiles”, Interestingengineering.com, accessed 2021 10 31

CCTX

Commercialization of Cybercrime

- Motivation: 75% of cyber attacks financially motivated[2]
- Cybercrime operating as a business
  - Barriers are coming down
    - many are technically sophisticated but it's not a requirement
  - Chance of getting caught – limited
  - Crypto currencies have facilitated paying criminals
- Ransomware-as-a-Service since 2017 criminals weaponized ransomware
  - Doesn't require technical expertise
  - Specialization by cyber criminals
  - Canada often ranks among the top countries impacted by ransomware[1]

1. "Cyber Threat Bulletin" issued September 18, 2020, by Canadian Centre for Cyber Security
2. Verizon's 2016 Data Breach Investigations Report (DBIR)

CCTX

Insiders & Hacktivists

- Insider Threat
  - Who are they: employees, contractors, vendors
  - Insiders are both part of the first line of defence and a potential threat
  - Working remotely has compounded the security dynamics for insiders
  - Motivation of insiders:
    - Doing the wrong thing for the right reason
    - Errors
    - Malicious – revenge, greed
      - New twist – ransomware attackers offering a reward to an insider to assist the attacker by deliberately clicking on a malicious link
- Hacktivists
  - Sharp decrease in publicly disclosed hacktivist attacks between 2015 and 2019[1]
  - Since 2019, a resurgence of hacktivism motivated by perceived political and social injustice[2]

1. The Decline of Hacktivism: Attacks Drop 95 Percent Since 2015 (securityintelligence.com) accessed 2021 11 02
2. Hacktivism: An overview plus high-profile groups and examples | Norton, The Resurgence of Hacktivism – MBL Technologies and Hacktivists Are on the Rise—but Less Effective Than Ever | WIRED accessed 2021 11 02

CCTX

The Other Attack Vectors Have Not Gone Away

- Distributed Denial of Service attacks (DDoS)
  - Record breaking level of activity - surged in Q1-2021[1]
  - 31% increase over last year
  - Targets:
    - Healthcare
    - Education
    - E-commerce

} Particularly vulnerable as these are pandemic life-line industries

- Business email compromise
  - 100% increase in 2019[2]
  - Targeting finance departments

1. "The Beat Goes On" by Netscout, 2021 05 17
2. "How much does phishing really cost the enterprise? By David Jones in Cybersecurity Dive, 2021 08 17

CCTX

Cold War, Geopolitics, and Cyber

- Did the Cold War really end?
  - Great-power competition experienced a brief lull – but it's back.
  - It's more than just competition with Russia – China, North Korea, Iran and others
- Geopolitics playing out over the Internet is not new
  - Commentators in 2010 suggest a Cold War-style cyber arms race has emerged between the U.S. and China.[1]
  - North Korea's attack in 2014 against the Sony Corporation
  - Russia suspected of launching state sponsored campaigns against Ukraine
    - 2015 suspected of taking down Ukraine's power grid
    - 2017 Russian military intelligence were accused of being behind the widespread and disruptive NotPetya malware attack

1. Study by McAfee and the Center for Strategic and International Studies Simmering Over a 'Cyber Cold War' – Krebs on Security accessed 2022 06 03

CCTX

Cold War, Geopolitics, Cyber – a dangerous mix

- Cyberspace has become an attractive environment to undertake state activity:
  - relative degree of anonymity and a degree of deniability
  - global reach
  - relatively lower cost than traditional forms of conflict
  - manipulation of information and decision making
- Grey zone aggression – nation state activity that falls below the threshold of formal conflict
  - cyber a visible tool that doesn't constitute an existential threat
  - used to intimidate, punish adversaries, affect morale, cohesion and political stability[1]
  - targets and victims are not only governments - private sector frequently targeted

Defence Minister Anita Anand

the world is "growing darker" and "chaotic".[2]

1. Cognitive Effect and State Conflict in Cyberspace | Center for Strategic and International Studies (csis.org) accessed 2022 06 03
2. Canada's defence minister says the world is 'growing darker' and 'more chaotic' - National | Globalnews.ca accessed 2022 06 08

CCTX

Geopolitics playing out in digital space

Cyber threat bulletin: Cyber Centre urges Canadian critical infrastructure operators to raise awareness and take mitigations against kr cyber thre

US, Europe formally blame Russia for data wiper attacks against Ukraine[4]

New Zealand warns of digital collateral dam m Russia-

Russia attacks Ukraine; peace in Europe 'shattered'

Cyberattack hits Ukrainian banks & government websites[5]

Viasat satellite networking service attacked by Russian military intel.[1]

1. NCSC pins Viasat cyber attack on Russia (computerweekly.com) accessed 2022 06 08
2. https://therecord.media/new-zealand-warns-of-digital-collateral-damage-from-russia-ukraine-crisis/accessed 2022 02 20
3. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadian-critical-infrastructure-operators-raise accessed 2022 02 20
4. https://www.theregister.com/2022/05/10/us_eu_russia/ accessed 2022 05 25
5. Cyberattack hits Ukrainian banks and government websites (cnbc.com) accessed 2022 04 13

CCTX

Geopolitics – the players

Nation States

Started with ‘grey zone aggression’ leading up to the invasion. Created “IT Army of Ukraine”

Objectives:
taking down banking websites, disrupting government services and rail lines, and providing intelligence

Hacktivists

Examples:
Anonymous waging a “cyber war”
‘Cyber Partisans’ in Belarus

Criminals

Pledging support to a nation. For example, the Conti criminal organization acting in support of Russia

CCTX

Countries of all sizes suffer cyber attacks

- Ransomware attacks continue to impact government organizations of small states according to Cyber Research Labs
  - 48 government organizations from 21 countries hit by 13 ransomware attacks in 2022[1]
  - The revenue from cyber extortion is now a financial instrument used by some countries.
  - Small states easy targets due to low level of security of their critical infrastructure
    - 2022 April - Conti ransomware gang disrupts government and private sector in Costa Rica.[2]
    - 2021 - attacks government and financial institutions in Peru, Malaysia, Angola and Republic of Philippines.

1. https://securityaffairs.co/wordpress/131816/malware/ransomware-attacks-small-states-q2-2022.html accessed 2022 05 31
2. https://www.csoonline.com/article/3662311/how-costa-rica-found-itself-at-war-over-ransomware.html?huid=0040e68b-4355-4452-91c2-e022ed3b8f4d accessed 2022 05 31

CCTX

Cyber attacks impact the physical world

- In addition to breaching the privacy of patients and employees, and stealing intellectual property and research, cyber attacks on healthcare facilities can result in:
  - Urgent medial care can be delayed as ambulances are diverted
  - Surgeries are rescheduled
  - Receipt of prescriptions and the medical records necessary for treatment are inaccessible
  - Cancer treatment and radiation equipment is disrupted
  - Delivery of vaccines impeded due to supply chain disruptions.
- Attacks on supply chain can disrupt the availability of gas or food and drive-up prices

We can all be impacted

CCTX

Cyber attacks impact the physical world

Single compromised password took down the largest fuel pipeline in the U.S.[1]

Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom[3]

U.S. Department of Justice recovers $2.3 million worth of Bitcoin that Colonial Pipeline paid to extortionists[2]

Storage tanks at a Colonial Pipeline Inc. facility in Avenel, New Jersey.
Photographer: Mark Kauzlarich/Bloomberg

1. Colonial Pipeline Cyber Attack: Hackers Used Compromised Password - Bloomberg accessed 2021 11 02

2. https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside accessed 2021 06 07

3. DarkSide Colonial Hacker Group's Dark Web Site No Longer Accessible – Bloomberg accessed 2021 05 14

CCTX

Canadian victims: Past nine months

Sunwing Says Outage Result of Cyber Attack on Service Provider

Lynn Elmhirst Open Jaw, April 20, 2022

Ontario hospital hit by data breach incident

Lyle Adriano Insurance Business Magazine, 24 May 2022

Newfoundland cyberattack an 'alarm bell' for Canada

COLIN FREEZE GLOBE & MAIL NOVEMBER 1, 2021

Saskatchewan Liquor and Gaming Authority cyberattack

Lyle Adriano Insurance Business Magazine, 06 Apr 2022

Human rights advocates say they're being hit by foreign cyber attacks — and that Canada is doing little to stop it

Jeremy Nuttall, Toronto Star, January 10, 2022

Toronto Transit Commission still recovering from ransomware attack

HOWARD SOLOMON IT WORLD CANADA OCTOBER 30, 2021

Cyberattack on Clarence-Rockland should be warning to others

Joseph Tunney CBC NEWS · Last Updated: November 1, 2021

CCTX

Cyber Threat in Canada – It's Real

Canadian organizations are being hit

Increase in attacks:

- 28% of respondents noticed an increase in reported cyber attacks, insider threats, or data breaches since the pandemic began[2]
  - 67% of cyber security incidents were ransomware[1]
  - 54% of victims paid the ransom[1]

Increase in cost:

- estimated average cost of a data breach in 2021 = $6.35 million[2]
    - Canada third highest average cost of 17 regions surveyed[3]

1. Canadian Cybersecurity Trends Study 2021 – Blakes, accessed 2021 06 06
2. "Cyber threat bulletin: The ransomware threat in 2021", Canadian Centre for Cyber Security
3. IBM Security, *Cost of a Data Breach Report 2021, research conducted by Ponemon Institute*

CCTX

Small Businesses in Canada Vulnerable to Cyber Attacks

- **Critical component of the economy:** SMEs comprise 99.8% of Canadian businesses (≤ 499 employees) and employed almost 68.8% of private sector workers in 2019[1]

- **Underestimate the risk**:
  - "We have nothing of interest"
  - How bad can it be?

- **SMEs are impacted by cyber attacks**:
  - 44% do not have any defences against possible cyber attacks[2]
  - 60% have no insurance to help them recover if an attack occurs
  - 18% have been affected by a cyber attack or data breach in the last two years

1. ISED Blog October 19, 2021
2. Insurance Bureau of Canada: Small Businesses in Canada Vulnerable to Cyber Attacks, September 25, 2019 **(** https://www.newswire.ca/news-releases/ibc-small-businesses-in-canada-vulnerable-to-cyber-attacks-848022450.html) - https://www.ic.gc.ca/eic/site/061.nsf/eng/h_03090.html#point1 January 2019

CCTX

Canada's National Approach

To be updated

Budget 2022
Enhancing cyber security
$892.9m over 5 years

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Royal Canadian Mounted Police National Cybercrime Coordination Unit (NC3)

Innovation, Science and Economic Development Canada

CyberSecure Canada

2021-2023 Action Plan for Critical Infrastructure

Academia

Other levels of government

Private Sector

CCTX

International Collaboration – recent initiatives

- Reduce the financial motivation of cyber criminals
  - U.S. launched a global campaign to combat ransomware with 30 nation summit
  - Objective: disrupt ransomware by building the capacity to rapidly trace and interdict (cryptocurrency payments) around the world[1]
- Name and shame
  - call out countries involved in cyber attacks
  - raise ransomware during summit meetings, e.g., between President Biden and Russian President Putin
  - indict members of state apparatus for their roles in cyber campaigns
- Criminal prosecutions – international law enforcement operations
- World Economic Forum - 18 companies take 'Cyber Resilience Pledge' "to mobilize global commitment towards strengthening cyber resilience across industry ecosystems"[2]
- U.S, Australia, India and Japan announce cyber security initiatives on software supply chain.[3]

1. Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology, on Why No Sanctions Issued Against China Yet(bankinfosecurity.com) accessed 2021 08 05
2. Global CEOs Commit to Collective Action on Cyber Resilience > Press releases | World Economic Forum (weforum.org) accessed 2022 06 07
3. https://therecord.media/us-australia-india-and-japan-announce-cybersecurity-initiatives-on-software-supply-chains/?_hsmi=214220057&_hsenc=p2ANqtz-8ESE6lPJ5wcErM9hDbbh7KVsv9YYkm_7xsEjb9QTWMuNtGjSzfOXB-YPttRpTWLvfuU86SLIUjWz-beavpAacvFuAnhA#9134b4dae1b339861250a6d71923ff74d5ea3081a1793580bc5e5c5f4346343a accessed 2022 05 25

CCTX

Disrupting cyber criminal operations

Disrupt the financial incentive

Call out nation states engaged in cyber operations – Russian, China, North Korea, Iran

International law enforcement action

"Two Arrested for Alleged Conspiracy to Launder $4.5 Bill… in Stolen Cryptocurrency"

U.S. Seized $3.6 Billion in Stolen Cryptocurrency Direc… Linked to 2016 Hack of Virtual Currency Exchange

US seizes $6 million in ransom payments and charges Ukrainian over major cyberattack[1]

Kuwaiti authorities arrested another GandGrab affiliate[3]

South Korea arrests affiliates involved in GandCrab and Sodinokibi/REvil ransomware families,

CCTX

…spiracy to Launder $4.5 Billion in Stolen Cryptocurrency | OPA | Department of Justice U.S. Depart…

…22 02 23

https://www.cnn.com/2021/11/08/politics/revil-ransomware-attack-charges/index.html accessed 2021 11 08

Canadian cyber criminals

Canada Charges Its "Most Prolific Cybercriminal"

OPP – "individual was responsible for numerous ransomware attacks affecting businesses, government agencies and private individuals throughout Canada…[1,2]

Canadian sentenced for his role in Netwalker ransomware attacks[3]

According to the U.S. Department of Justice, he allegedly earned about $27.6 million through ransomware attacks on Canadian companies such as the Northwest Territories Power Corporation, the College of Nurses of Ontario and a Canadian Tire store in B.C.

1. https://krebsonsecurity.com/2021/12/canada-charges-its-most-prolific-cybercriminal/ accessed 2021 12 09
2. https://www.bankinfosecurity.com/canada-busts-suspect-tied-to-multiple-ransomware-attacks-a-18080?rf=2021-12-09_ENEWS_SUB_BIS__Slot6_ART18080&mkt_tok=MDUxLVpYSS0yMzcAAAGBPthYOeYF89JZTPL6c31--81jTUnV6qPotuYQyhdnkS0SV9AJbXv8KPwWtUd-1B9dBx_IMAFcEvGmzNLAxeQJ70ks306Rn9y2pm_aN9giY5C9WfkXlg accessed 2021 12 09
3. Canadian sentenced for his role in Netwalker ransomware attacks | IT World Canada News February 8, 2022

CCTX

Creating a Cyber Resilient Organization

- **Threat sharing works**
  - Research shows - “Threat sharing, and the use of advanced technologies… organizations are better able to **prevent**, **detect**, **contain** and **respond** to attacks”[1]
  - It’s cost effective
- **Threat sharing across sectors provides unique insights**
  - 45% of attacks were not attributed to a sector but the effort could be seen across the entire community[2]
- **Threat sharing becoming recommended best practice**

INCREASE THE COST TO ATTACKERS WHILE REDUCING YOURS

1. 2019 Ponemon Institute *Fourth Annual Study on the Cyber Resilient Organization*, sponsored by IBM Security, April 2019.
2. Harrison, Rutherford, and White. "*The Honey Community:* Use of Combined Organizational Data for Community Protection.“, System Sciences (HICSS), 2015 48th Hawaii International Conference on. IEEE, 2015; and, “*Forum on Mitigating Consumer IoT Cyber Threats*”, 20 February 2020, Ottawa, by Gregory B. White, Ph.D., Center for Infrastructure Assurance and Security, University of Texas at San Antonio.

CCTX

Canadian Organizations Are Engaged

The **CCTX** enables members to collaborate on reducing financial, operational, and reputational risk through access to timely, relevant, and actionable cyber threat information.

We are

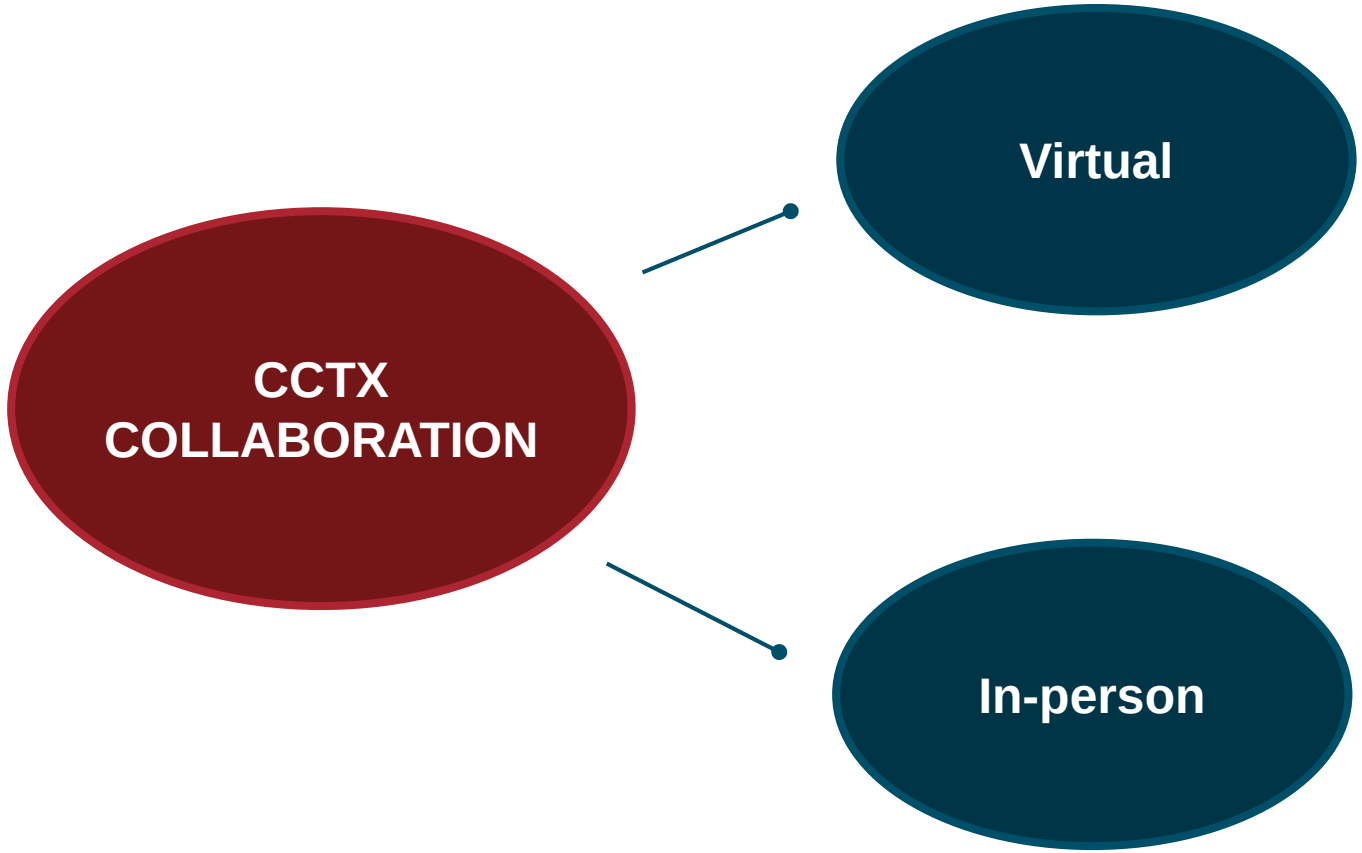
- **Multi-sector / all sizes**
- **Not-for-profit**
- **A private sector initiative**
- **Collaborating & Cyber Threat Sharing**

“You have to beat all of us to beat one of us”[1]

CCTX

1. Chris Inglis, National Cyber Director, Executive Office of the President, remarks to the Atlantic Council, “Cyber9/12 Strategy Challenge”, 2022 03 25

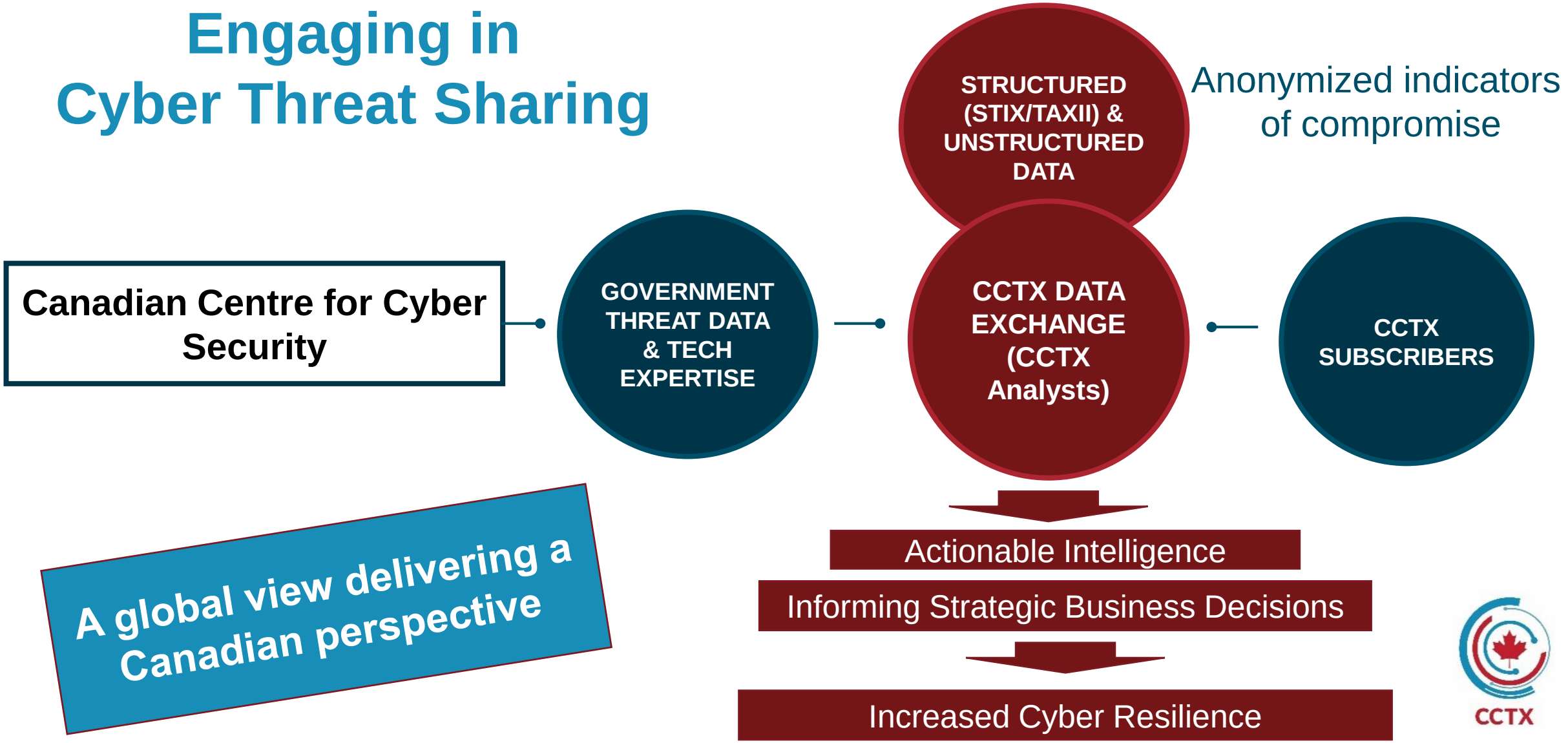
A Community Approach



- Professionals sharing best practices
- Sharing calls
- Technical Webinars with industry experts
- Threat calls weekly
- Collaboration events in person and virtual
- Discussion boards
- Participation in smaller working groups
- Earn education hours to maintain professional certifications

CCTX Facilitated, Member Determined

CCTX Community Engaging in Cyber Threat Sharing



CCTX - your network neighborhood watch.

For Further Information Contact:

Jennifer Quaid, Executive Director

Jennifer.Quaid@cctx.ca

Mobile: 613-292-7016

Bob Gordon, Strategic Advisor

Robert.Gordon@cctx.ca

Mobile: 613-720-2890

Follow us on WWW.CCTX.ca – LinkedIn - Twitter

General Inquiries: info@cctx.ca