DIGITAL TRANSFORMATION IN GOVERNMENT

“HAVING A SUCCESSFUL DIGITAL TRANSFORMATION JOURNEY BY THWARTING THE CYBER ATTACKERS”

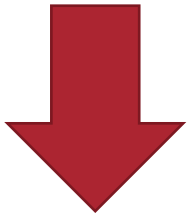
Bob Gordon

Executive Director

2021 06 17

CCTX

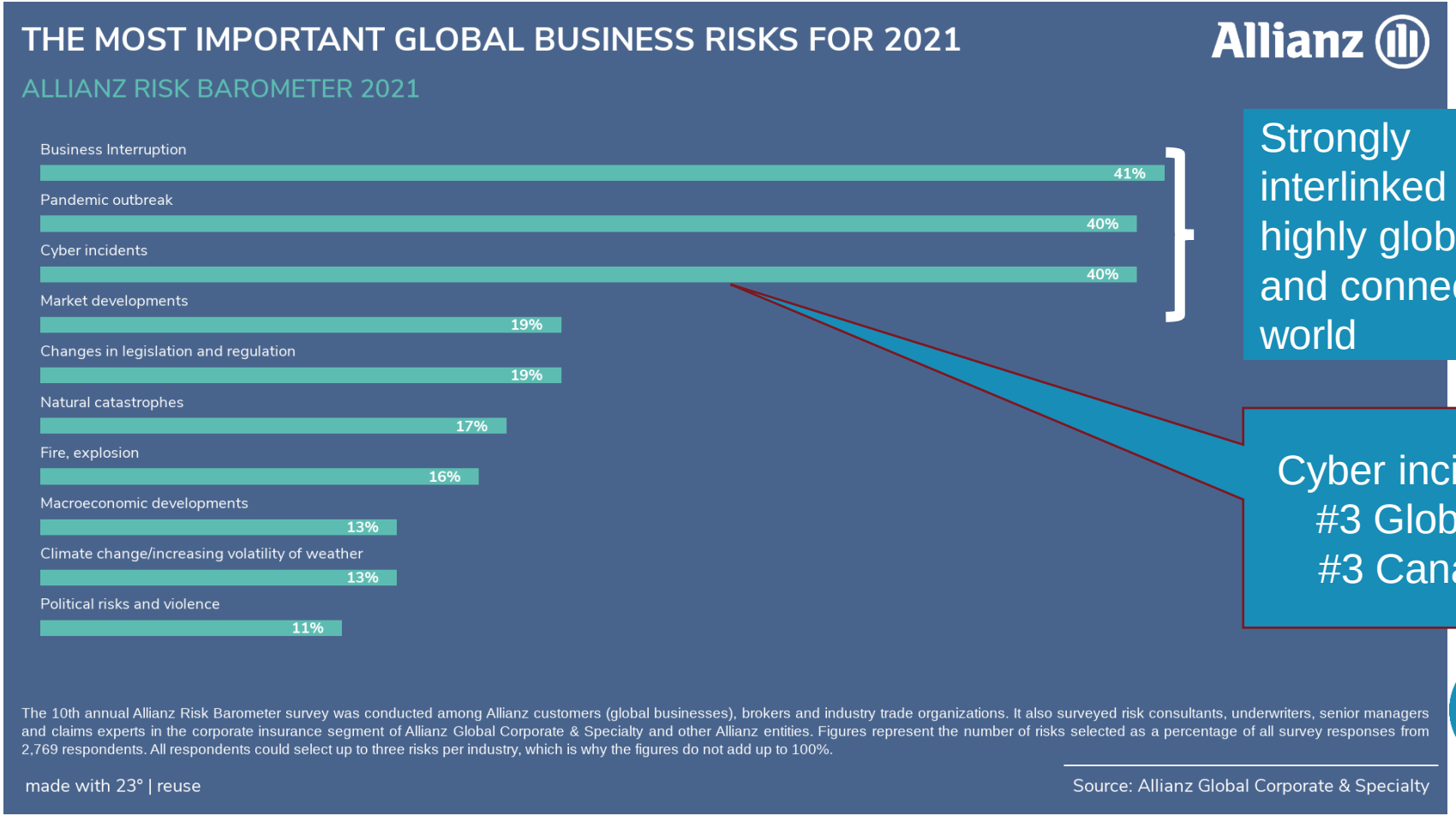
THE DIGITAL TRANSFORMATION JOURNEY



A great plan, but who invited the cyber attackers?

CCTX

Prediction for 2021 Global Business Risks



CCTX

Canadian Perspective
Key Judgements

"Cybercrime continues to be the cyber threat that is most likely to affect Canadians and Canadian organizations"

"We assess that, almost certainly, the most pressing threats to the physical safety of Canadians are to OT and critical infrastructure"

"While cybercrime is the most likely threat, the state-sponsored programs of China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada"

"State-sponsored actors are very likely attempting to develop cyber capabilities to disrupt Canadian critical infrastructure, such as the supply of electricity, to further their goals"

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, Head, Canadian Centre for Cyber Security[2]

1. Speaking May 18, 2021, speaking at Centre for International Governance Innovation
2. In The Western Standard, June 1, 2021

CCTX

TRENDS IN THE CYBER THREAT ENVIRONMENT

Commercialization of Cybercrime

- Cybercrime is operating as a business
- Access to networks and operational systems are being sold on the Internet by cyber criminals.
- Don’t require technical expertise – comes with 24 / 7 x 365 help desk support.
- Some criminal groups are technologically sophisticated
- Specialization by cyber criminals. Cybercrime marketplaces bring together software developers and those with hacking skills, the skills to run email spam campaigns, hosting malicious websites or operating botnets of pre-compromised victims.
- Chances of getting caught – limited.

CCTX

RANSOMWARE – HAS IT BECOME A THREAT TO NATIONAL SECURITY?

- Canadian 2021 cybersecurity trends study[4]:
  - 67% of cyber security incidents were ransomware
  - 54% of victims paid the ransom
  - Only 17% of publicly listed companies indicated they had some form of cyber insurance
- Ransomware-as-a-Service (RaaS) – a whole new business line on the dark web
- Hackers becoming more calculating in targeting and expectations of amount victims will pay
- Drastic increase in extortion demands
  - Average total cost of data breach by industry (U.S.) $3.86million[1]
  - But trend is for fewer companies to pay[2]
- Newest variations not only freeze data but also exfiltrate data before launching ransomware.
  - 70% of attacks involved threat to leak exfiltrated data[2]
  - If you don't pay – your data is published or sold via a leak site

1 -"Market Conditions" by John Farley, Gallagher, February 2021
2 - https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020 accessed 2021 06 06
3 – Palo Alto Networks
4 –Canadian Cybersecurity Trends Study 2021 – Blakes, accessed 2021 06 06

CCTX

Attackers increase the pressure to pay

Ransomware gang urges victims' customers to demand a ransom payment[1]

"Finnish mental health patients blackmailed after suspected data breach"[2]

1. Ransomware gang urges victims' customers to demand a ransom payment (bleepingcomputer.com) accessed 2021 03 29
2. https://portswigger.net/daily-swig/finnish-mental-health-patients-blackmailed-after-suspected-data-breach accessed 2021 06 07

CCTX

RANSOMWARE – TO PAY OR NOT TO PAY

- Can't be guaranteed that:
  - the decryption tool will be provided or that it works effectively
  - stolen data will be destroyed
  - you won't be revictimized

- Ethical matter of paying a criminal

- In U.S., facilitating ransomware payments to sanctioned hacker gangs may be illegal[4]

- Need to have this conversation with your Board **before** it happens

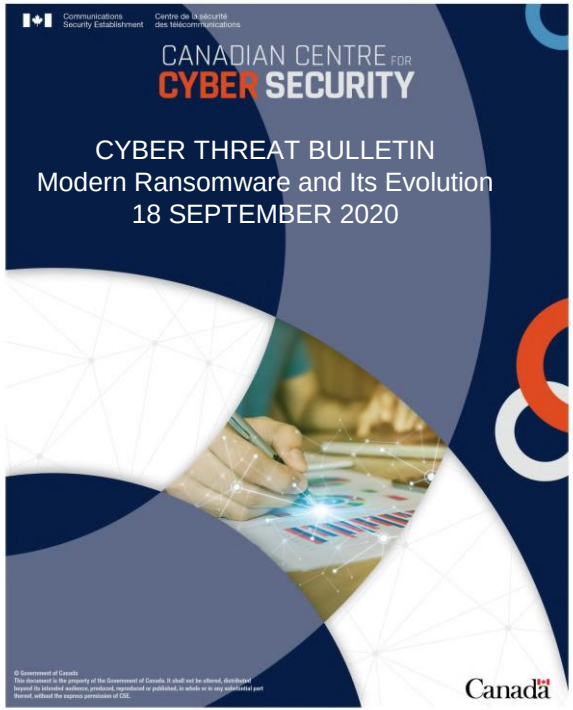
1 -"Market Conditions" by John Farley, Gallagher, February 2021
2 - https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020 accessed 2021 06 06
3 – Palo Alto Networks
4 - https://www.reuters.com/article/us-treasury-cyber-idUSKBN26M77U accessed 2021 06 07

CCTX

Canada Impacted by Ransomware Attacks

Key Judgements

- Canada often ranks among the top countries impacted by ransomware
- Past two years, hundreds of Canadian businesses and critical infrastructure providers impacted
- Almost certain cybercriminals will continue to scale up ransomware operations and coerce larger payments
- Average ransom demand in December 2019 was $257,756. In October 2019, Canadian insurance company paid $1.3 mission to recover 20 servers and 1,000 workstations.



CCTX

IT/OT – OPERATIONAL CONSEQUENCES OF CYBER ATTACK

Convergence of information technology and operational technology

- increases efficiency & supports long term planning
- 2019 survey – 68% of manufacturers plan increasing IT-OT convergence over next two years
- **but** – manifesting into a business risk
- many of the OT systems were never designed to be connected to the corporate IT systems nor to the Internet
- adding cyber security to OT systems can be difficult and, in some instances, impossible
- cyber attack into the IT systems can migrate to the OT environment with potentially physical implications to business operational capability

Cyber attack becomes a matter of business continuity

CCTX

Attack on IT system impacted operational capability

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

BUT

DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized[1]

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

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

1. DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized – Krebs on Security accessed 2021 05 14

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

CCTX

Meat Processing Grinds to Halt After 'Cybersecurity Attack’

World's Largest Meat Supplier Says Servers Hit in North America and Australia

The U.S. headquarters of meat supplier JBS in Greeley, Colorado.

Meat Processing Grinds to Halt After 'Cybersecurity Attack' (bankinfosecurity.com) accessed 2021 06 03

CCTX

IS YOUR SUPPLY CHAIN VULNERABLE?

Types of supply chain:

- **Software**
  - Attack by Russian intelligence agency against Solar Winds
    - very technically sophisticated against the Solar Winds' software
    - attackers were patient, attack executed over many months
    - precision targeting
- **Suppliers of goods and services that keep you operational**
  - Their operational resilience may be the weakest link in your cyber security program.

CCTX

AND THE OTHER ATTACK VECTORS HAVE NOT GONE AWAY

- DDoS
  - Record breaking activity - surged in Q1-2021[1]
  - 31% increase over last year
  - Targets:
    - Healthcare
    - Education
    - E-commerce

} Pandemic life-line industries

1. “The Beat Goes On” by Netscout, 2021 05 17

CCTX

Cyber Threat in Canada – It's Real

- 21% of Canadian businesses reported being impacted by cyber security incidents in 2019[1]
- 28% of respondents noticed an increase in reported cyber attacks, insider threats, or data breaches since the pandemic began[2]
- average cost of a data breach in 2020 was $4.5 million[3]
    - Canada third highest average cost of 17 regions surveyed
    - $148,700 average ransom demand in Q1 up by 33% since Q4 2019[5]
- 36% of organizations are likely to inform a regulatory body of a data breach in 2019 compared to 58% in 2018[4]
- 12% of businesses impacted by incidents reported to police services in 2019[1]
- CIRA 2020 survey report found that 38% of companies did not know whether they had experienced a breach of customer and/or employee data[4]

1. Statistics Canada, results of *2019 Canadian Survey of Cyber Security and Cybercrime*
2. Conference Board of Canada, *Tech Checkup, Dealing with technology change in pandemic recovery*, October 2020
3. IBM Security, *Cost of a Data Breach Report 2020*
4. Canadian Internet Registry Authority, *CIRA Cybersecurity Report 2020*
5. *https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report accessed 2020 11 19*

CCTX

Small Businesses in Canada Vulnerable to Cyber Attacks

- Small & medium size comprise 99.8% of Canadian businesses (≤ 499 employees)
- Poll commissioned by Insurance Bureau of Canada of 300 such owners:
  - 44% of small businesses do not have any defences against possible cyber attacks
  - 60% have no insurance to help them recover if an attack occurs
  - Nearly one in five businesses (18%) polled have been affected by a cyber attack or data breach in the last two years

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

CCTX

Collaboration Increases Cyber Resilience

- Information sharing is cost effective – leverage the knowledge of others – no one can do it alone
- Sharing enriches your existing information making it more actionable
- 59% of organizations said sharing threat intelligence improved cyber resilience[2]
- $213,487 could be saved by threat intelligence sharing when dealing with a data breach[3]
- 39% of all “hacks can be thwarted because the organization engaged in sharing of threat intelligence with peers”[4]

INCREASE THE COST TO ATTACKERS WHILE REDUCING YOURS

1 Conference Board of Canada, Council of Chief Information Security Officers, Cyber Security Centre, “Resiliency in the Face of Cyber Security”, Executive Session Highlights, Ottawa, Ontario, 2-3 October 2018 – Takeaway #3
2 Fifth annual “Cyber Resilient Organization Report 2020” by IBM Security based on research from Ponemon Institute
3 IBM Security, “Cost of a Data Breach Report 2020”
4 Flipping the Economics of Attacks”, Ponemon Institute, sponsored by Palo Alto Networks, January 2016.

CCTX

Creating a Cyber Resilient Organization

- Threat sharing works
  - Research shows - “Threat sharing, and the use of advanced technologies enable organizations to better understand the cybersecurity risks they face, and, as a result, the organizations are better able to **prevent**, **detect**, **contain** and **respond** to attacks”*
- 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**

*2019 Ponemon Institute *Fourth Annual Study on the Cyber Resilient Organization*, sponsored by IBM Security, April 2019.

**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

Threat Sharing Recommended Practice

U.S. Department of Defense – Cybersecurity Maturity Model Certification[1]

- the framework identifies the requirement for defence sector companies to participate in threat information sharing forums as part of situational awareness

Investment Funds Institute of Canada:

- updated Cybersecurity Guide for Canadian firms
- outlines key steps to establishing a cybersecurity program" "steps include:
  - "participating in trusted information sharing" [2]

Canadian Association of Defence and Security Industries

- "The concept of sharing threat information across a diverse array of trusted actors to gain dramatically improved situational awareness is recognized as a critical component to an effective national cyber defence."[3]

Investment Industry Regulatory Organization of Canada

- "information sharing is an essential tool for mitigating cyber threats"[4]

1. https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf
2. https:www.wealthprofessional.ca/news/ific-unveils-updated-cybersecurity-guide-321321.aspx - Article dated 2019 11 04
3. 2020 Report, Canadian Association of Defence and Security Industries, "*The Collaboration Imperative: An Overview of Leading Government-Industry Collaboration Models and Practices in Cyber Defence*
4. https://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf

CCTX

Private Sector in Canada Responds by Creating the CCTX

Mission

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

Vision

- The CCTX is an established leader of cross-sector collaboration, enabling cyber resilience and preparedness in its members.
- The CCTX creates value through the provision of unique data insights with relevant context that are valuable and timely.

CCTX

Canadian Organizations Getting Engaged

CCTX

Canada's cyber threat sharing and collaboration hub
for ALL organizations in Canada

We are

Multi-sector

Not-for-profit

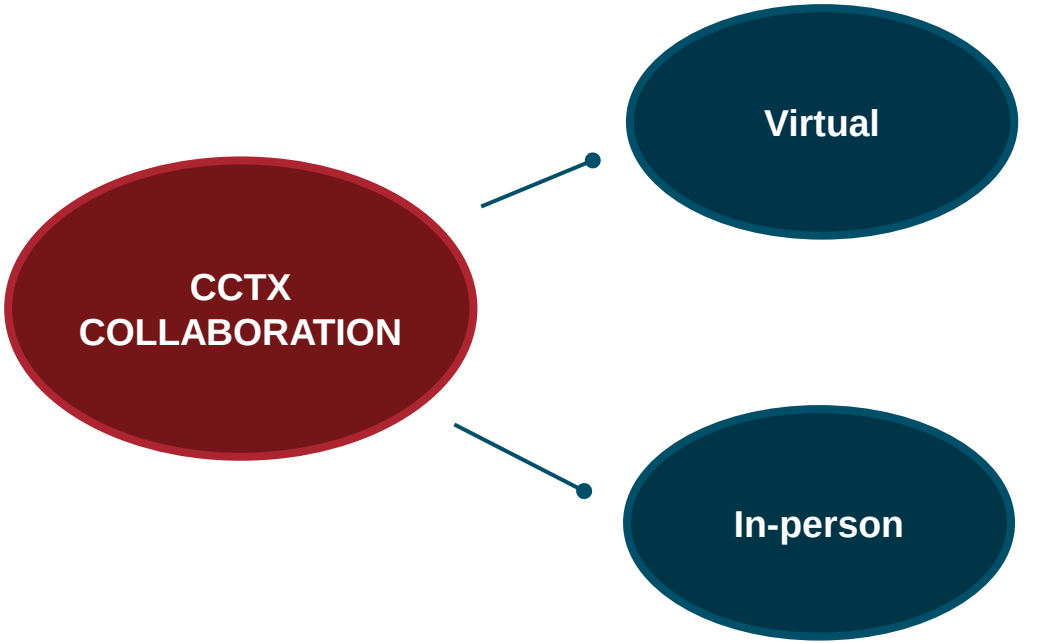
A private sector initiative

Large, medium & small businesses

None of us are as smart as all of us

CCTX

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 Collaboration Events

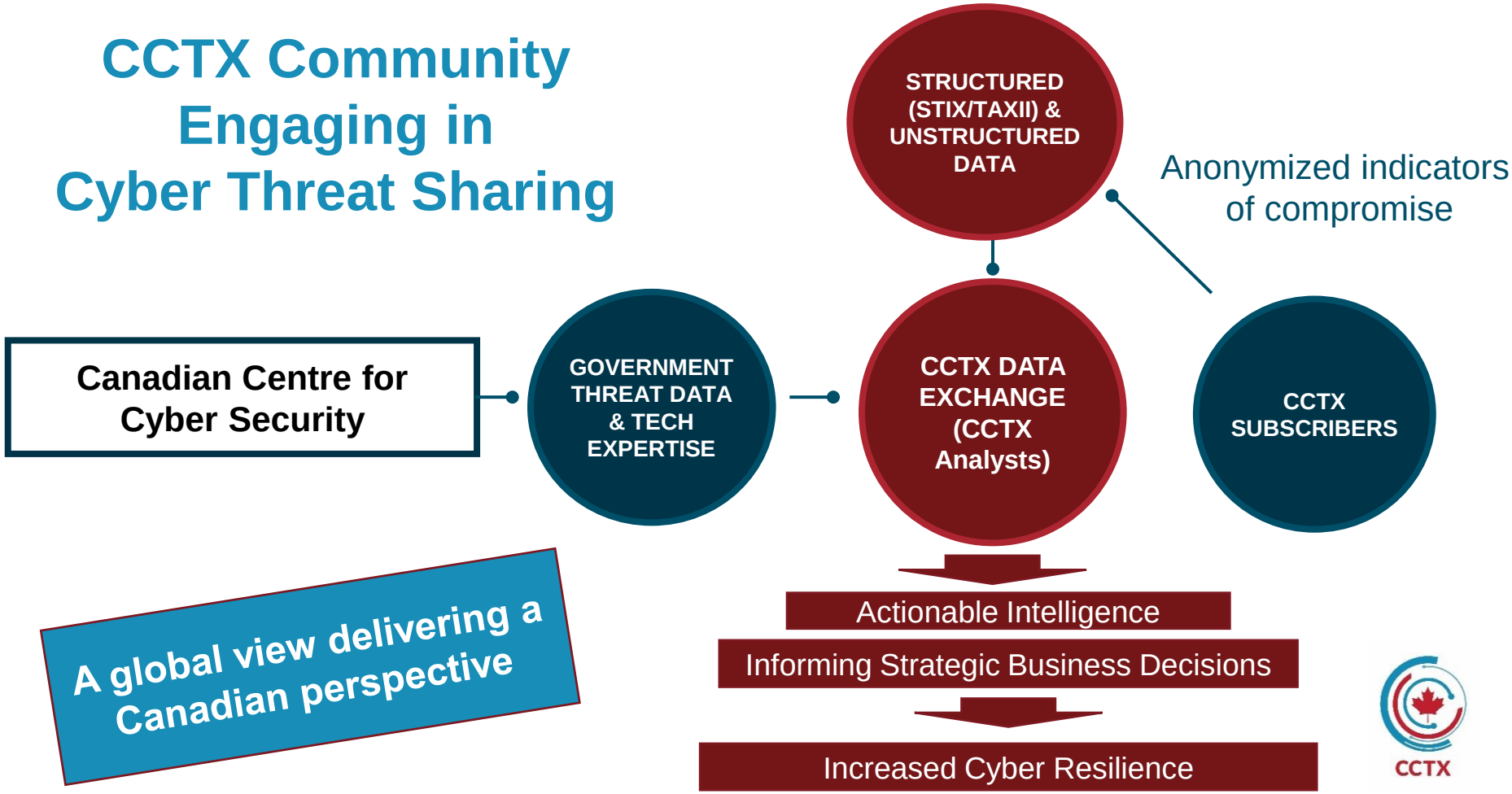
- Members
- Partners
- Sponsors
- Presentations & Workshops
- Infomercial Competition

February: Annual National Event

Throughout year: the CCTX hosts regional events & contributes to other conferences, partner, member & association events/webinars, threat calls, policy discussions, association initiatives

Last Symposium – February 23, 2021
600+ registered to attend

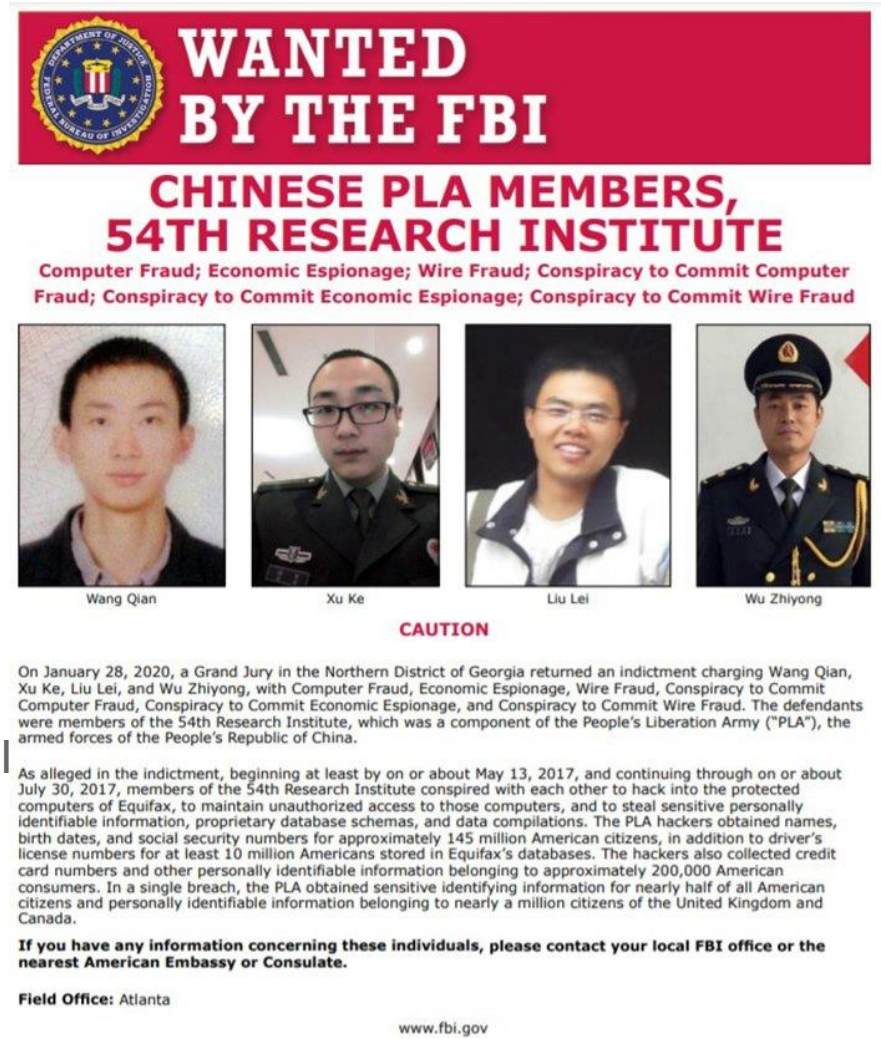
CCTX Community Engaging in Cyber Threat Sharing



Technology is the medium, but it is still people

The U.S. government identified and charged four members of the Chinese People's Liberation Army, who are currently wanted by the FBI for the Equifax hack in 2017.

[Nation-state hacker indictments: Do they help or hinder? (techtarget.com)](#) accessed 2021 04 22



WANTED BY THE FBI

CHINESE PLA MEMBERS, 54TH RESEARCH INSTITUTE

Computer Fraud; Economic Espionage; Wire Fraud; Conspiracy to Commit Computer Fraud; Conspiracy to Commit Economic Espionage; Conspiracy to Commit Wire Fraud

Wang Qian | Xu Ke | Liu Lei | Wu Zhiyong

CAUTION

On January 28, 2020, a Grand Jury in the Northern District of Georgia returned an indictment charging Wang Qian, Xu Ke, Liu Lei, and Wu Zhiyong, with Computer Fraud, Economic Espionage, Wire Fraud, Conspiracy to Commit Computer Fraud, Conspiracy to Commit Economic Espionage, and Conspiracy to Commit Wire Fraud. The defendants were members of the 54th Research Institute, which was a component of the People's Liberation Army ("PLA"), the armed forces of the People's Republic of China.

As alleged in the indictment, beginning at least by on or about May 13, 2017, and continuing through on or about July 30, 2017, members of the 54th Research Institute conspired with each other to hack into the protected computers of Equifax, to maintain unauthorized access to those computers, and to steal sensitive personally identifiable information, proprietary database schemas, and data compilations. The PLA hackers obtained names, birth dates, and social security numbers for approximately 145 million American citizens, in addition to driver's license numbers for at least 10 million Americans stored in Equifax's databases. The hackers also collected credit card numbers and other personally identifiable information belonging to approximately 200,000 American consumers. In a single breach, the PLA obtained sensitive identifying information for nearly half of all American citizens and personally identifiable information belonging to nearly a million citizens of the United Kingdom and Canada.

If you have any information concerning these individuals, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Atlanta

www.fbi.gov

CCTX

CAN YOUR ORGANIZATION AFFORD TO NOT GET INVOLVED?

For further information contact:

Bob Gordon, Executive Director
robert.gordon@cctx.ca

613·720 2890
cctx.ca

General Inquiries:
info@cctx.ca