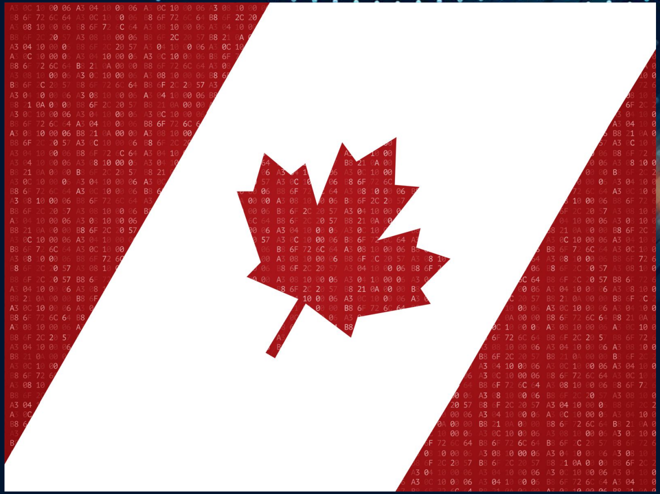
The Digital Front Line

Threats to Canadian Cybersecurity

Lead: Vedant Puthran
Team: Karan Brar, Nicholas Quadrini

Introduction

- Digital technology is everywhere around us.
- From our cell phones, computers, to smart TVs, we are surrounded by powerful tools that can help and hinder us
- These tools are also essential to core parts of our society, from the functioning of government, business payment processing, the operation of critical infrastructure, and national defense activities



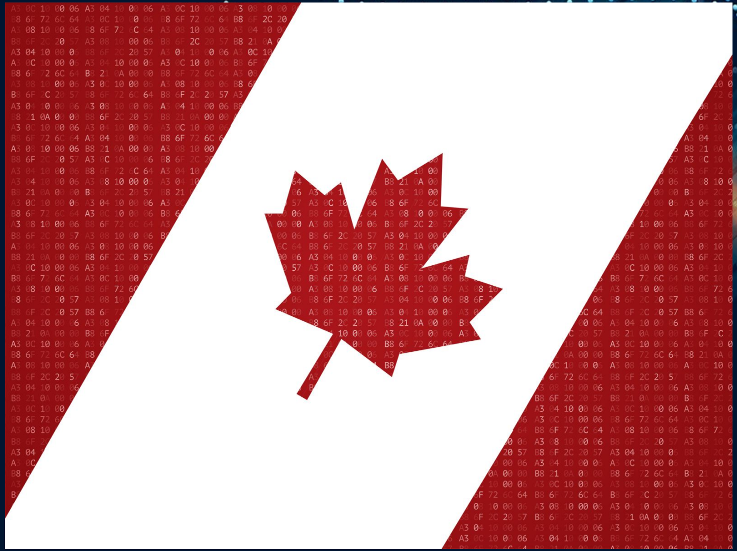
Issue Statement

How can government protect citizens, businesses, and itself from new and emerging cyber threats?

Background

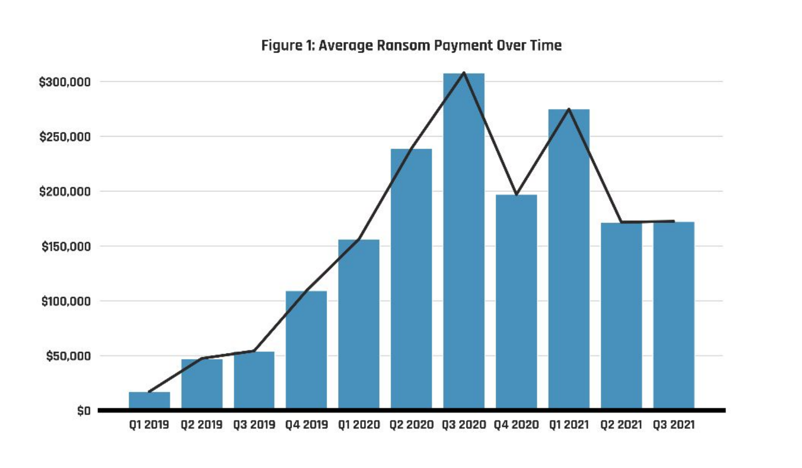
Evolving Nature of Digital Tech

- Canadian reliance on digital technologies continues to grow
- These technologies can be exploited by bad actors impacting the personal security of citizens and national interests



Background
Economic Cost to Cybercrime

- Businesses that experience cyberattacks face immediate costs to recover and secure their data
    - Chapters/Indigo Ransomware Attack
- The estimated average cost of a data breach, a compromise that includes but is not limited to ransomware, is $6.35 million per Statistics Canada

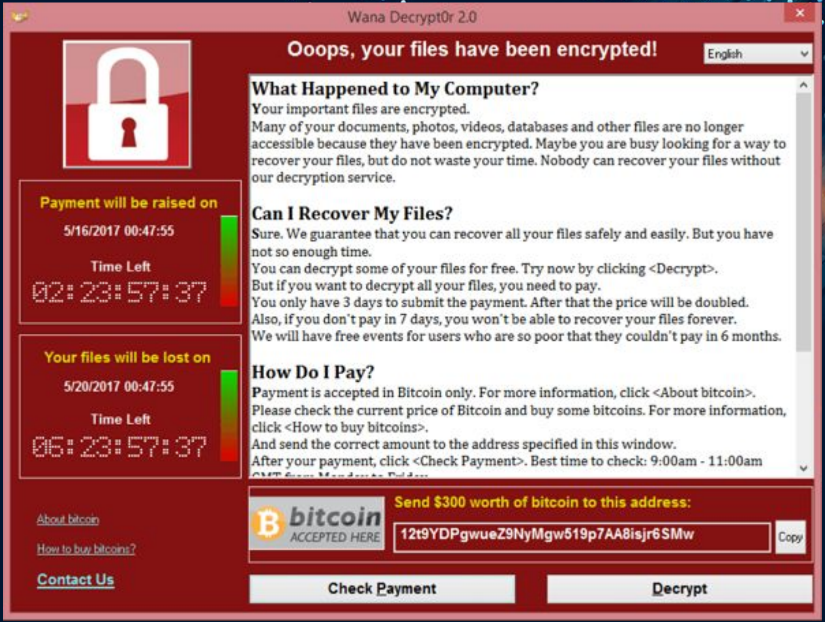


Source: Statistics Canada

Background

Economic Cost to Cybercrime

- Critical infrastructure like healthcare devices, automotive technologies, and nuclear can all be interrupted by complex digital security breaches (i.e. Ransomware, Denial of Service attacks)



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

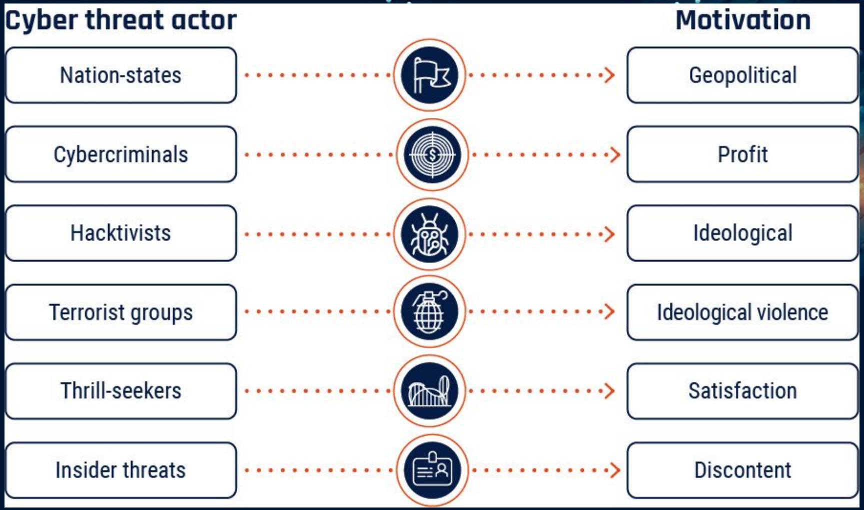
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Background

Threat to National Security

- Nation-states, terrorist groups, and hacktivists harness these new technologies for geopolitical and terrorist activities
- Borders are no longer the final frontier.
- Partners: CSE, Public Safety

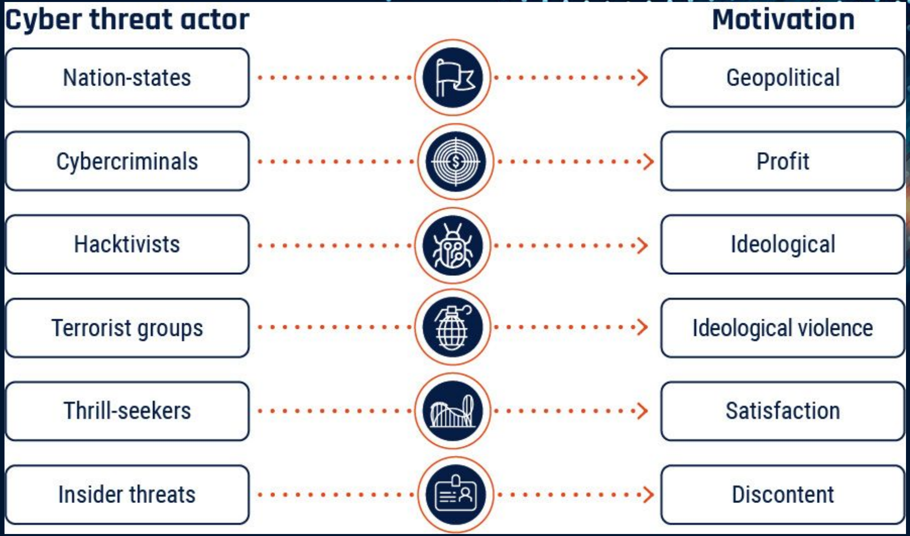


Cyber threat actor	Motivation
Nation-states	Geopolitical
Cybercriminals	Profit
Hacktivists	Ideological
Terrorist groups	Ideological violence
Thrill-seekers	Satisfaction
Insider threats	Discontent

Background

Threat to National Security

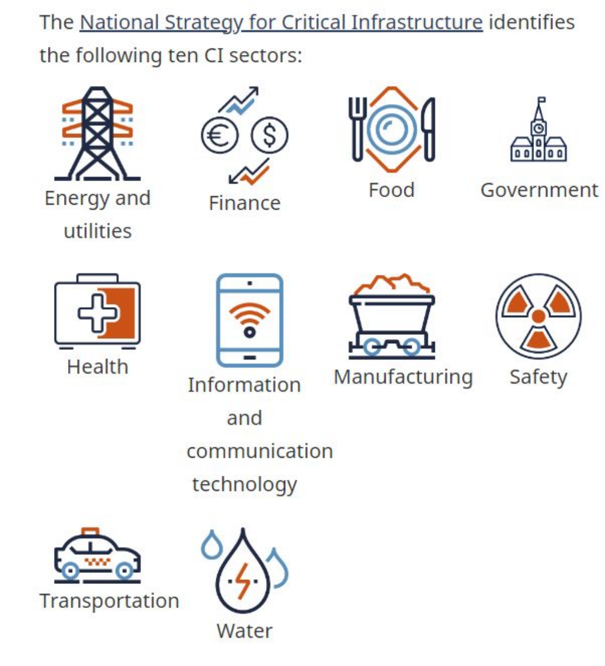
- The Communication Security Establishment defines cyber-threat actors in six categories
  - Nationstates
  - Cybercriminals
  - Hacktivists
  - Terrorists
  - Thrill-seekers
  - Insiders



Cyber threat actor	Motivation
Nation-states	Geopolitical
Cybercriminals	Profit
Hacktivists	Ideological
Terrorist groups	Ideological violence
Thrill-seekers	Satisfaction
Insider threats	Discontent

Key Considerations : Social

- Attack on Critical Infrastructure could lead to loss of vital services harm to public or even loss of life
- Have significant financial resources to pay ransom -> target of attack to collect information



The National Strategy for Critical Infrastructure identifies the following ten CI sectors:

Energy and utilities

Finance

Food

Government

Health

Information and communication technology

Manufacturing

Safety

Transportation

Water

Key Considerations : Economic

- Ransom payments have increased since 2020
- Only 42% of organizations who paid ransom had data restored
- Opportunity costs in addition to ransom value (unrecoverable data, cost of repairing systems, public distrust)

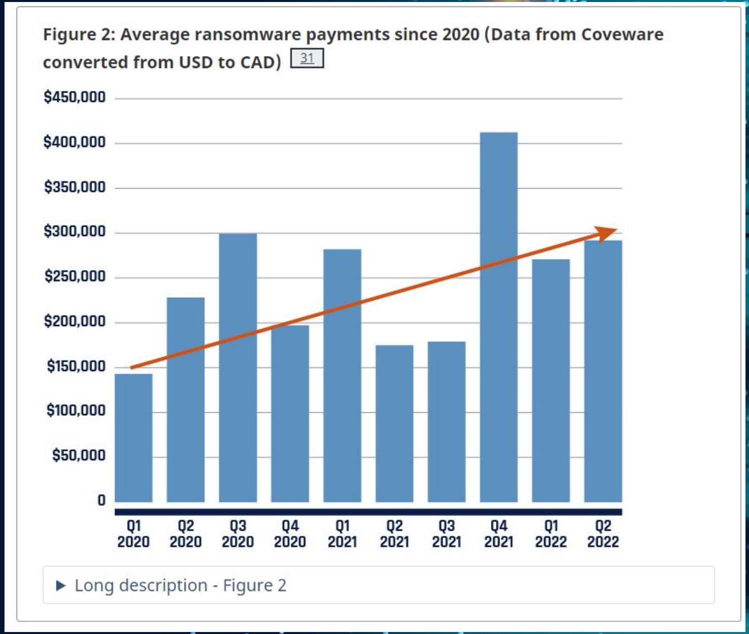


Figure 2: Average ransomware payments since 2020 (Data from Coveware converted from USD to CAD) 31

Key Considerations : Public Reception

- Neglecting Cybersecurity or not addressing framework can result in loss of revenue, service interruptions for customers and staff, loss in customer trust
- Attacks on corporations and government will incite public fear and distrust to use novel systems

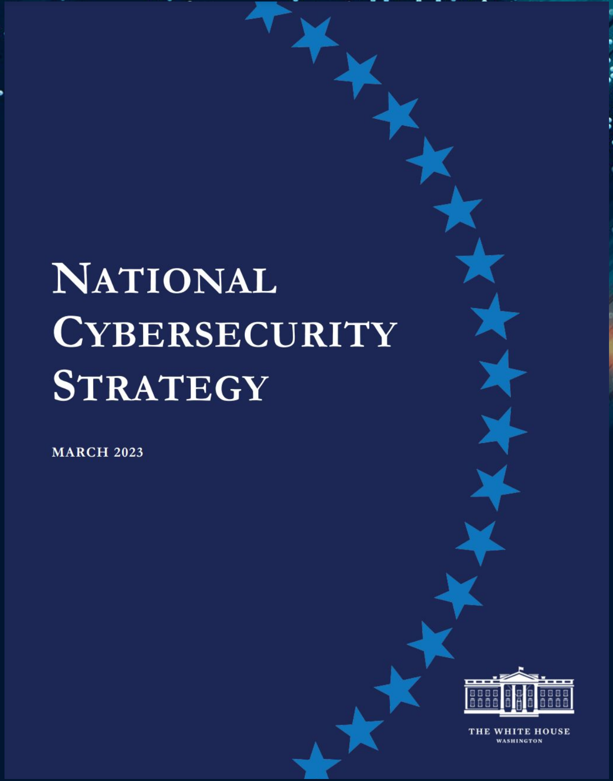
Jurisdictional Scan
Estonia

- Estonian strategy includes:
  - **Investing 50% of technology budget** on cybersecurity to enhance information security
  - **Exchanging intelligence with security agencies** (NATO, U.S CISA) to head off attacks before they start
  - **Inviting private tech firms to invest** in research to develop solutions for public and private firms

Jurisdictional Scan

United States

- National Cybersecurity Strategy released in 2023:
    - Shifting the burden for cybersecurity away from individuals, small businesses, and local governments
    - Favours long-term investments in digital infrastructure to protect citizens/businesses/governments



NATIONAL CYBERSECURITY STRATEGY

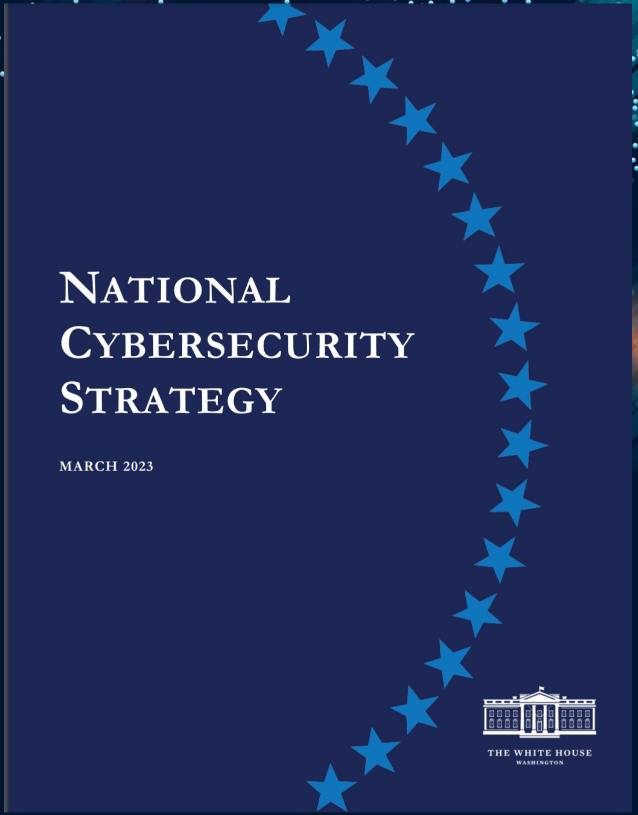
MARCH 2023

THE WHITE HOUSE
WASHINGTON

Jurisdictional Scan

United States

- **Defend Critical Infrastructure**
    - Expanding the use of minimum cybersecurity requirements in critical sectors and modernizing federal tech
- **Disrupt and Dismantle Threat Actors**
    - Create new private sector hubs that work with gov't to share intelligence and stop threats before they start
- **Engage the Market to Drive Security**
    - Legislation to limit use of personal data by private actors, shift liability for insecure software to corporations



NATIONAL CYBERSECURITY STRATEGY

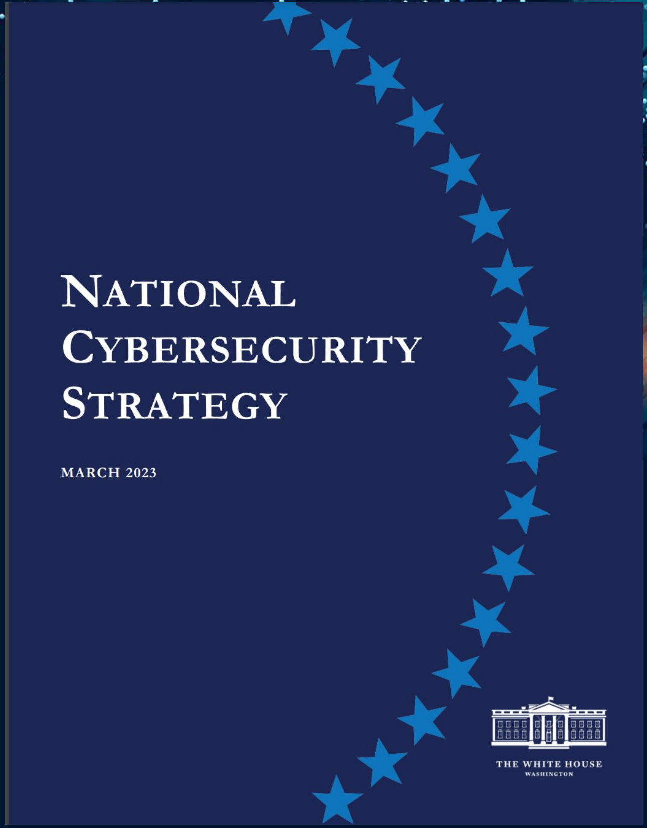
MARCH 2023

THE WHITE HOUSE
WASHINGTON

Jurisdictional Scan

United States

- **Invest in a Resilient Future**
  - Updating internet protocol security, end the use unencrypted domains, implement full adoption of IPv6
  - Develop Digital ID to protect people, business and government against physical ID identity fraud
- **International Partnerships**
  - Building up cyber protections for NATO and other international alliances



NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

THE WHITE HOUSE
WASHINGTON

Options

01

Education

Educate people, business, and broader public sector on how to be cybersafe through a public awareness campaign.

02

Regulation

Regulate minimum cybersecurity protections businesses and government need to achieve.

03

Innovation

Educate the public on cybersafe skills while also providing **fiscal incentives/programs** to encourage businesses to be cybersafe.

Options Table

Recommendation: Innovation	✓ Takes an balanced approach to businesses rather than a forceful one ✓ Encourages innovation, builds labour force capacity, and expands cyber education ✓ **Benefit:** Cost burden is on businesses to implement/train, government only pays for tax credit/subsidy. Regulations can be balanced with business risk/size. ✓ **Risk:** Costs associated with R&D and private sector partners currently unknown.
Education	✓ Expands cyber education to Canadians through established agencies (CSE/PSC) ✓ **Benefit:** hands off approach for Canadians/businesses, internal improvements for the public service ✓ **Risk:** limited regulation increases risk for more sophisticated attacks
Regulation	✓ Direct regulation which would set clear rules for people and businesses to follow ✓ **Benefit:** demands companies and government to future proof gaps in cybersecurity ✓ **Risk:** overregulation puts burden on businesses, increasing costs for companies

Option 3 - Recommendation/Implementation

Incentivize and Innovate

- Expand the mandate of ***Communication Security Establishment (CSE)***:
  - **Consult Canadians/businesses** on cybersecurity limitations and areas where government can support education and skills-development
  - **Communication plan** to introduce CSE's cybersafe campaign to Canadians, offer cybersecurity mini-courses to high schools, post-secondary institutions and small/medium sized businesses

COMMUNICATIONS SECURITY ESTABLISHMENT
CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

Public Safety Canada
Sécurité publique Canada

Option 3 - Recommendation/Implementation

Incentivize and Innovate

- Introduce **tax credit or subsidy** to incentivize businesses to invest in advanced cybersecurity protections and research/development in new Canadian cybersecurity hubs

COMMUNICATIONS
SECURITY ESTABLISHMENT

CENTRE DE LA SÉCURITÉ
DES TÉLÉCOMMUNICATIONS

Public Safety
Canada

Sécurité publique
Canada

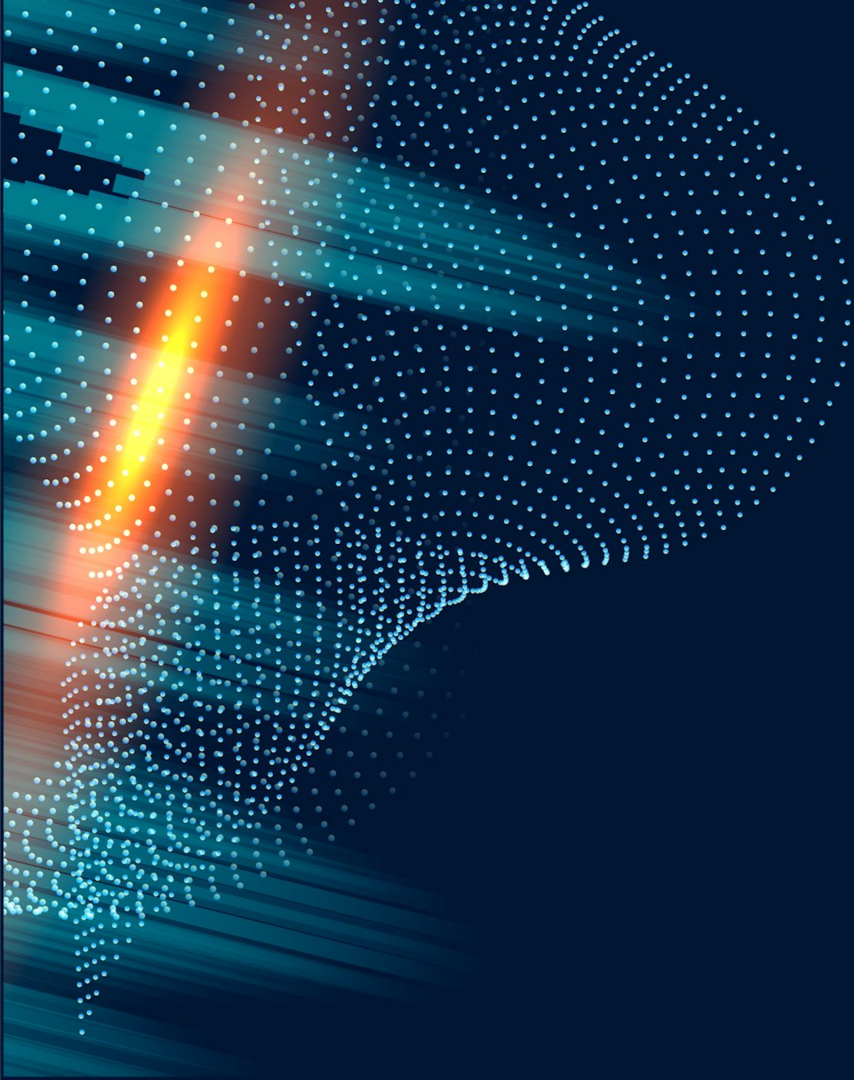
Option 3 - Recommendation/Implementation

Incentivize and Innovate

- Enhance the **Cyber Security Cooperation Program (CSCP)** to help small businesses cover cost of cyber-insurance (2021-24 Budget $4.2 million)
- Implement **regulations** which ensure largest companies with greatest risk have minimum cyber protections as outlined by CSE

COMMUNICATIONS
SECURITY ESTABLISHMENT
CENTRE DE LA SÉCURITÉ
DES TÉLÉCOMMUNICATIONS

Public Safety Canada
Sécurité publique Canada



Thank you!