Disclaimer

The views expressed by the speaker do not necessarily reflect those of the Bank of Canada's Governing Council.

BANK OF CANADA
BANQUE DU CANADA

JUNE 15, 2021

PRESENTED TO THE FINANCIAL INCLUSION GLOBAL INITIATIVE SYMPOSIUM

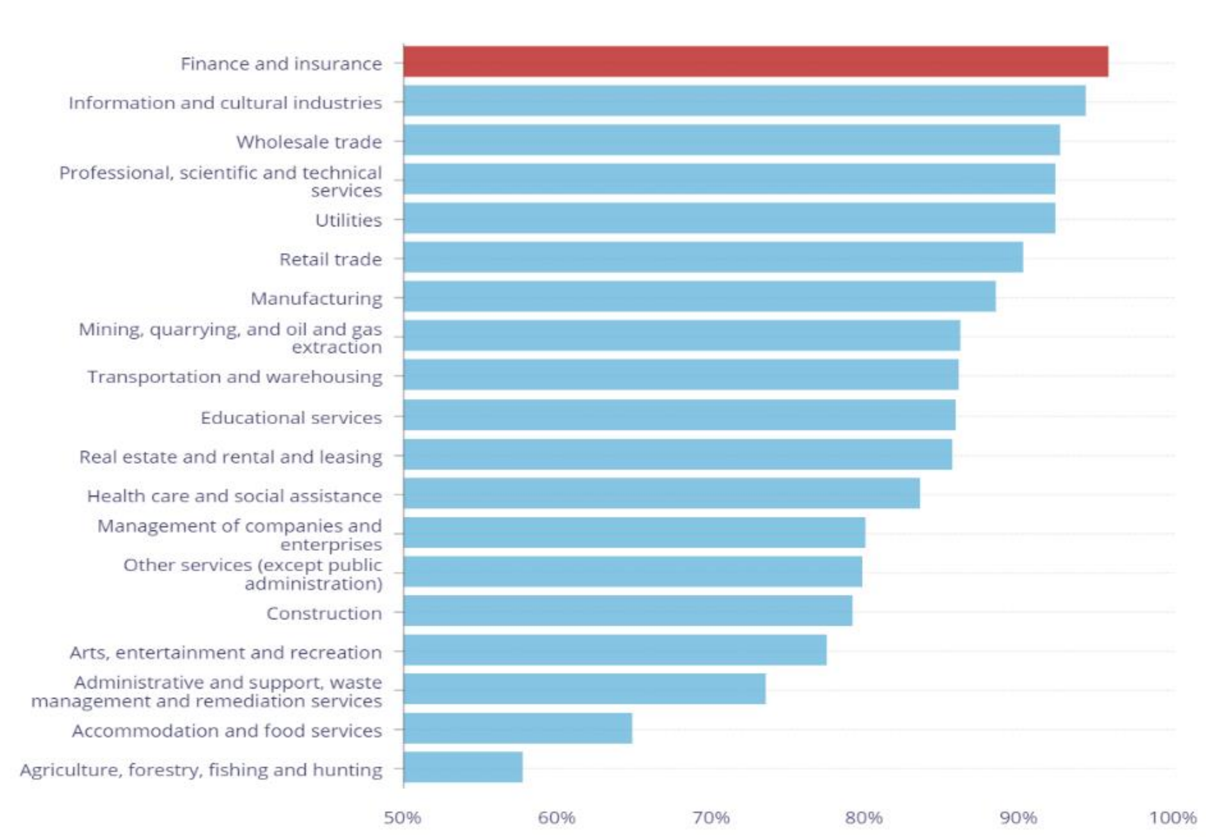
Bank of Canada – Cyber Strategy & Industry Resilience

Reduce Risk, Promote Resilience

Hisham El-Bihbety, Chief Information Security Officer
Nikil Chande, Director, Financial Stability Department

Cyber threats remain an important vulnerability to the financial system

Chart 15: Among firms in the finance and insurance industry, 95 percent use at least one cyber risk management arrangement—more than in any other industry



BoC's 2021 Financial System Review -- Vulnerability 5

- The Bank of Canada's latest Financial System Review continues to identify cyber threats a key vulnerability
- Respondents to the Bank's spring 2021 Financial System Survey continue to identify a cyber incident as one of the top three risks facing the financial system.
- They also view cyber threats as the top risk to their own institutions.
- Financial institutions and authorities continue to invest in improving cyber resilience

Cyber Strategy 2019-2021 Themes

Cyber Security Vision:

To strengthen the cyber resilience of the Canadian financial system against an evolving threat environment

Cyber Security Mission:

To promote the efficiency and stability of the Canadian financial system through robust cyber security capabilities and expertise, collaboration and information sharing, and comprehensive oversight.

Theme:

2019–2021

Cyber Security Strategy

Reducing Risk
Promoting Resilience

Category/Catégorie: Non-Sensitive/Non-Délicat

Cyber Security Strategy Goals 2019-2021

Goal 1

Strengthen cyber team and capabilities to enable secure and innovative Bank operations.

Goal 2

Collaborate with key partners to promote resilience and reduce the incidence and severity of cyber security breaches.

Goal 3

Regulate and promote leading cyber security standards through the Bank’s oversight roles.

Strengthen Cyber team and capabilities
Collaborate with partners to promote Cyber resilience
Regulate and promote leading Cyber standards

Focus on External Strategy – 2019-2021

OBJECTIVES	OUTCOMES	ACTIVITIES ROADMAP 2019-2021
Strengthen financial system resilience	Cyber security regulatory requirements are defined in alignment with Bank's oversight objectives Designated FMI's are resilient against major cyber incidents	Resilience of Wholesale Payments Systems (RWPS) Critical cyber system planning Federal cyber security regime implementation
Enhance Collaboration & Partnerships	Domestic system-wide cyber resilience initiatives are in place Information sharing protocols in place with international forums and peers	Cyber accreditation program External cyber program implementation Crisis management coordination and toolkit
Mature Cyber Security Practices among FMI's	FMIs have clear guidance on cyber regulatory expectations FMI cyber security maturity and threat landscape is well understood FMIs have effective cyber security response and recovery plans	Cyber guidance for FMIs Incident response and recovery exercises System threat scenarios identification
Evolve Cyber Security Oversight	BoC cyber oversight role is integrated with PCSA obligations Cyber resources are in place to support oversight role	FMI Oversight Planning Training and development plan for financial system and FSD/cyber

Strengthen Financial System Resilience

Intended Outcomes 2019-2021

- Cyber security regulatory requirements are defined in alignment with Bank's oversight objectives
- Designated FMI's are resilient against major cyber incidents

Key activities undertaken

- Resilience of the Wholesale Payments System (RWPS) initiative
- Federal government initiative to strengthen cyber resilience of critical cyber systems

Enhance Collaboration & Partnership

Intended Outcomes 2019-2021

- Domestic system-wide cyber resilience initiatives are in place
- Information sharing protocols are in place with international forums

Key activities undertaken

- G7 Cyber incident response exercise and protocol
- Established Canadian Financial Sector Resilience (CFRG) and playbook for systemic operational incident
- Cyber exercise to test CFRG cooperation and info sharing

Mature Cyber Security Practices among FMIs

Intended Outcomes 2019-2021

- FMIs have clear guidance on cyber regulatory expectations
- FMI cyber security maturity and threat landscape is well understood
- FMIs have effective cyber security response and recovery plans

Key activities undertaken

- Undertook cyber core assurance reviews for designated FMIs
- Developed *Expectations for Cyber Resilience of Designated FMIs* to complement CPMI-IOSCO Cyber Guidance
- Developed security requirements for modernized payments systems

Evolve Cyber Security Oversight

Intended Outcomes 2019-2021

- BoC cyber oversight role is integrated with PCSA obligations
- Cyber resources are in place to support oversight role

Key activities undertaken

- Implemented program of strong dedicated support from IT for FSD's oversight activities
- Hired technical expert directly in Oversight function
- Received training related to operational resilience

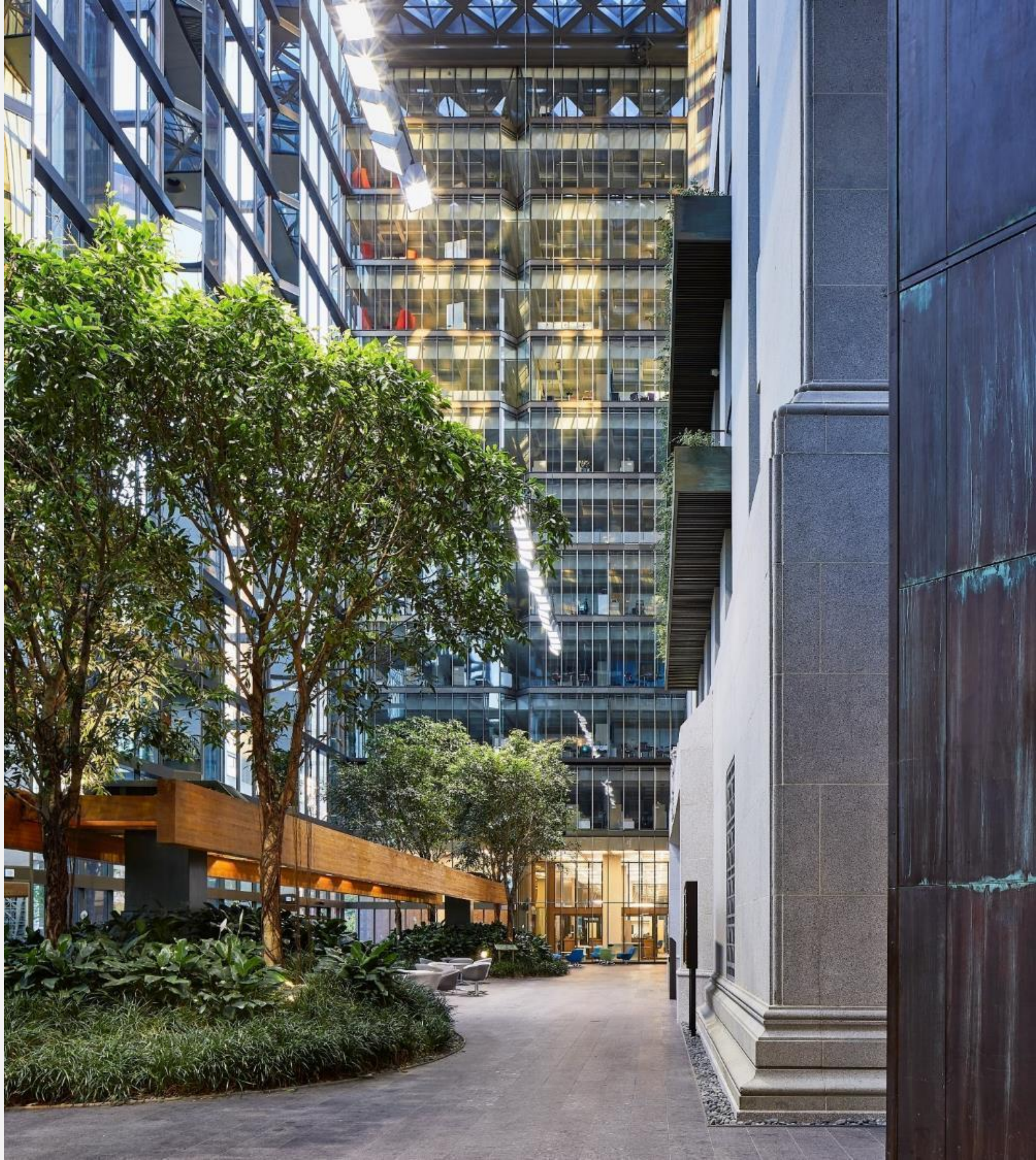
Developing the next strategy

- Internal and external components will remain prominent
- Updating based on new threats and challenges
- Collaboration and partnerships are even more important
- Public and private sector linkages stronger

APPENDIX

BANK OF CANADA
BANQUE DU CANADA

Resilience of Wholesale Payments System (RWPS) initiative



Resiliency of the Wholesale Payment Systems

In Q3'18, the Bank of Canada formalized ongoing discussions with the six large Canadian Banks (SIBs) and Payments Canada to strengthen the resiliency of wholesale payments ecosystem against cyber-attacks and data corruption. The Bank of Canada initiated the **Resiliency of the Wholesale Payments Systems (RWPS) program** consisting of several workstreams tasked to enhance cyber resiliency capabilities and decrease systemic risk. These workstreams support the continuity of Canada's wholesale payments ecosystem should a cyber event occur at one or more of the big six Canadian banks, Payments Canada, or the supporting Bank of Canada's operations. Participants are leading and actively contributing to the workstreams. The following are the workstreams objectives and accomplishments:

Objective

A **Prevention & Detection of Payment Data Corruption:** Improve the prevention, and detection controls through benchmarking, information sharing and remediation of gaps

B **Canadian Financial-sector Resiliency Group (CFRG) and Outage Playbook:** To refine the mandate of BoC's industry wide crisis coordination group and to enhance the industry wide crisis management playbooks. *Note: This workstream is now maintained separately from the RWPS program*

C **Cyber Resiliency Testing:** To improve the maturity and effectiveness of resiliency testing cycles and enhance the scope to cover a range of cyber related test scenarios

D **Payments Processing Resiliency:** To assess and increase the capabilities to recover the wholesale payment service in case of severe cyber event

E **Systemic Cyber Risk Scenarios:** Identify and maintain a catalogue of cyber risk scenarios with systemic impact on the wholesale payments environment to ensure proper overall prioritization across work streams

Accomplishments

A The SIBs completed a self-assessment of prevention and detection controls and updated their payment escalation playbooks to include early engagement of cyber teams. The SIBs, in collaboration with the Bank, prepared their individual plans to improve their cyber controls maturity. The Industry continues to hold quarterly bilateral meetings with the Bank to track and monitor progress. Planning has commenced for the second round of controls benchmarking

B The Canadian Financial-sector Resiliency Group has been officially operationalized as a public-private crisis management group

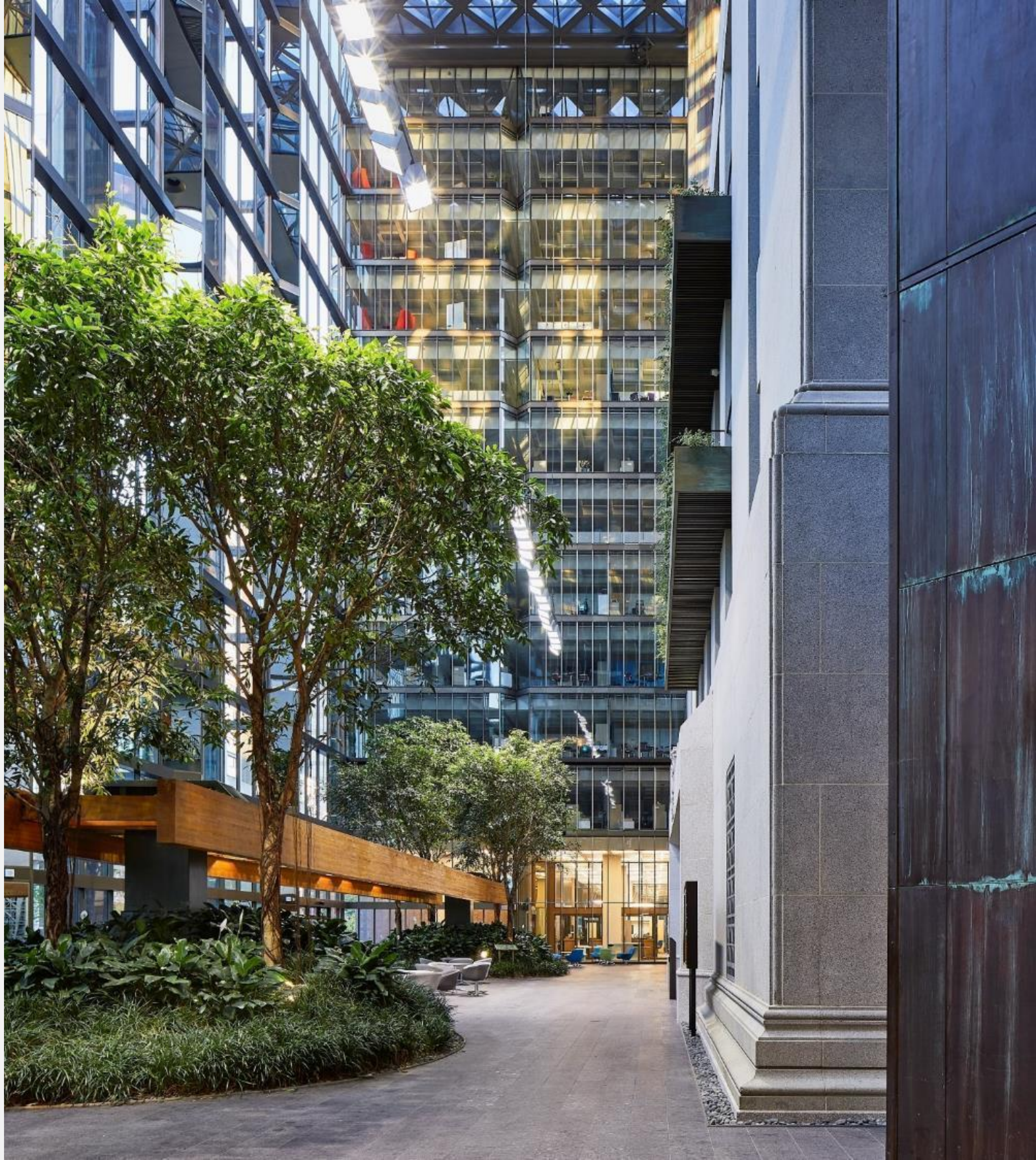
C Several Cyber Resiliency simulation exercises have been conducted since the start of the program. Actions or gaps identified by the exercises are prioritized and remediated. The last exercise focused on the SWIFT By-pass contingency option and volume throughputs

D The SIBs have completed a self-assessment of their ability to restore mission critical data. Aggregation of this data has been completed by the Bank of Canada. The results indicated two focus areas: Backup Network Segregation and Backup Restoration Testing

E The Industry has completed the systemic cyber risk assessment.

BANK OF CANADA
BANQUE DU CANADA

Canadian Financial Sector Resilience Group (CFRG)



CANADIAN FINANCIAL SECTOR RESILIENCY GROUP (CFRG)

The **Canadian Financial Sector Resiliency Group (CFRG)** is a public-private partnership launched by the Bank in 2019. It brings together Canada's systemically important institutions, financial market infrastructures, government departments, and key regulators.

The principal mandate of the CFRG is to coordinate responses to systemic-level operational incidents within the financial sector. The CFRG has developed and put in a place an incident response protocol to respond in a coordinated manner to operational events including cyber incidents.

COVID-19 Response: The CFRG was convened on March 20, 2020 to share updates and experiences on managing impacts of COVID-19. During the first several months of the crisis, members held weekly meetings to share operational status updates and discuss emerging issues such as essential services designations and cyber threats. CFRG also facilitated interactions with government bodies such as Public Safety, Public Health Agency of Canada, and other critical infrastructure sectors during the COVID-19 crisis.

Current Initiatives

- **Developing a crisis coordination playbook:** Outlines the process for coordination. Can be activated at the request of any member when a disruption could threaten the operations of the critical financial system. The scope of incidents that could qualify under the Playbook includes industry-wide incidents related to operations, cyber, and physical security.
- **Resiliency Testing:** To improve the industry response capabilities to incidents with systemic impacts to the financial sector.
- **Information-sharing protocols:** Establish and adhere to Non-Disclosure Agreements or Memorandum of Understanding to facilitate the sharing of information amongst CFRG's private sector members

Accomplishments

- Developed first version of the crisis coordination playbook.
- Updated the playbook based on COVID-19 lessons learned.
- Next steps will include further training for CFRG members.

- The sector held a simulation exercise in March 2021 that focused on the industry's reaction to a cyber impact on one of the critical sector participants.
- This gave CFRG members a chance to practice how they would share information, coordinate their decisions and communicate with each other.

- A working group has been established.
- Documenting key challenges and establishing a target state.