2022–24

Cyber Security Strategy

Reducing Risk
Promoting Resilience

BANK OF CANADA
BANQUE DU CANADA

MESSAGE FROM THE CHIEF OPERATING OFFICER

As the nation's central bank, the Bank of Canada has a legislated mandate to promote the stability and operational resilience of our financial system. The Bank's promise is to give Canadians confidence to pursue opportunity. They count on the Bank to:

- foster economic and financial stability
- navigate relentless change with rigour and integrity
- help grow Canada's shared prosperity

Our leadership in cyber security in the financial sector contributes to fulfilling that promise. A strong resilience posture is critical for the security of Canada's financial system as a whole and the participants in it.

Cyber attacks are becoming more sophisticated, more damaging and harder to prevent than ever before. The Bank's survey results[1] show that Canadian firms consider cyber incidents to be among the top risks to individual businesses and the financial system.

While the Bank's cyber security posture has improved overall, the threat from cyber will never go away. The Bank must continue to develop our internal and external cyber resilience initiatives in the years ahead.

The Cyber Security Strategy 2022–24 gives us a plan to do that. The strategy is guided by our cyber security risk appetite and a clear strategic vision: to strengthen the cyber resilience of the Canadian financial system against an evolving threat environment.

Filipe Dinis, Chief Operating Officer

1 Respondents to the Bank's spring 2021 Financial System Survey identified a cyber incident as one of the top three risks facing the financial system.

INTRODUCTION

Cyber resilience is one of the Bank of Canada's highest priorities. A cyber attack on any part of the financial system has the potential to cause a systemic event that could ultimately disrupt Canada's economy.

In 2019, the Bank developed its first Cyber Security Strategy to guide its internal and external cyber security activities and priorities. And considerable progress has been made since then.

The Bank established critical foundational programs such as penetration testing and identity and access management, attracted new talent and developed the expertise of its cyber team, and deployed new cyber technologies and systems. These have become core elements of the Bank's operations.

Operational and cyber resilience were key to the Bank's successful response to and recovery from the COVID-19 pandemic.

At the same time, the Bank developed successful relationships and robust collaborations with external partners in Canada and around the world, promoting cyber security resilience in many jurisdictions.

These efforts contributed to significant improvements in the Bank's overall cyber risk profile from 2019 to 2021.

Operational and cyber resilience were key to the Bank's successful response to and recovery from the COVID-19 pandemic. The Bank's ability to be flexible, nimble and resilient allowed employees to make the transition to secure remote work with minimal or no disruption to the Bank's operations.

Cyber Security Strategy 2022–24 will guide the next phase of work by cyber teams and business functions across the Bank. It will also give external partners clarity on the Bank's intentions.

A new Cyber Security Risk Appetite has been developed to set strategic boundaries and provide overall direction for managing cyber risk.

THE BANK OF CANADA'S CYBER THREAT LANDSCAPE

The complexity of the cyber threat landscape continued to evolve during the COVID-19 pandemic. While some of the attack vectors are not new, cyber attacks are becoming more frequent and sophisticated.

The financial sector was an attractive target for malicious cyber operators during the pandemic.[2] As with other institutions, the Bank's cyber attack surface and risk profile increased as Bank employees and consultants moved to remote work using less secure home networks.

New cyber threats are also linked to changing central banking activities and processes, such as updated payment systems, digital currency, blockchain and digitalization. The Bank continues to be concerned about a higher likelihood of espionage and sabotage that could lead to the theft of intellectual property and proprietary business information or could disable or disrupt critical financial systems.

> **"The financial sector was an attractive target for malicious cyber operators during the pandemic"**

Cyber threats from nation states and state-sponsored groups remain acute, posing a strategic threat to Canada. Nation states have been the source of aggressive cyber attacks around the world, using cyber operations for financial gain or to promote their own national interests.

Financial institutions and governments worldwide are also seeing an increase in the number and complexity of ransomware attacks.[3] Trends include larger ransom payment demands and multifaceted attack tactics.

Major international incidents in 2020 and 2021 have drawn attention to the devastating potential consequences of cyber attacks on critical infrastructure and the need for organizations to manage cyber risks related to third parties.

2 I. Aldasoro, J. Frost, L. Gambacorta and D. Whyte, "COVID-19 and Cyber Risk in the Financial Sector," BIS Bulletin No. 37, Bank for International Settlements (January 2021).

3 S. Lyngaas, "US Financial Institutions Report Major Increase in Ransomware Payments to Cybercriminals," CNN Politics (October 15, 2021.)

EVOLUTION OF CYBER SECURITY AT THE BANK OF CANADA

In recent years, the Bank established a solid cyber security foundation to address existing and emerging cyber security needs. Since its Cyber Security Strategy was published in 2019, the Bank has continued to strengthen its cyber security posture.

Internally, the Bank expanded its cyber security capabilities across the five functions of the US National Institute of Standards and Technology (NIST) Cybersecurity Framework.[4]

The Bank has:

- adopted a risk management approach focused on key Bank assets and cyber scenarios of concern
- applied a lines-of-defence model with a more robust second line of defence
- prioritized training and development for staff in a very competitive cyber security labour market
- augmented protection and detection systems to respond to evolving cyber attack techniques
- put in place a dedicated identity and access management program to enhance controls and reduce the likelihood that privileged accounts could be exploited
- made strategic investments in new tools and monitoring systems that facilitated remote access to data and video conferencing for employees working remotely
- further developed cyber security awareness to include regular Bank-wide phishing and spear-phishing training and exercises

4 The NIST Cybersecurity Framework is a voluntary framework used internationally by industry, academia and government to manage cyber security risk.

Externally, the Bank collaborated with Canadian and international public and private sector partners to strengthen cyber security in domestic and global financial systems.

The Bank:

- promoted cyber security in Canada's payment systems as part of its oversight of designated financial market infrastructures (FMIs)
- introduced new guidelines on Expectations for Cyber Resilience of Designated FMIs
- continued its leadership role in the Canadian Financial Sector Resiliency Group—a forum for Canada's systemically important financial institutions and regulators to coordinate responses to systemic operational issues in the financial sector, including cyber incidents
- continued work on the Resilience of Wholesale Payments Systems initiative—a collaboration with Canada's six largest banks and Payments Canada to share information and enhance the cyber resilience of Canada's wholesale payments systems

---

The Cyber Security Strategy 2022-2024 is the Bank's plan to build on this foundation and continue to strengthen cyber security in the years ahead.

Looking forward

STRATEGIC GOALS FOR 2022–24

The Bank will continue to pursue the cyber security vision and mission articulated in 2019.

Vision

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

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.

Strategic goals, outcomes and actions have been updated to reflect the Bank's evolving requirements in the months and years ahead.

Goals

1. Continue to integrate cyber resilience into all Bank of Canada business operations as the Bank evolves
2. Expand financial sector resilience through collaboration and partnerships
3. Inspire confidence in the financial system through clear cyber security guidance within the Bank's mandate

Cyber Security Risk Appetite

The Cyber Security Strategy has been aligned with the Bank's Cyber Security Risk Appetite. Four risk appetite statements will guide the assessment of cyber security risk in pursuit of the Bank's business objectives.

Acknowledging the Bank of Canada's important role in the financial system and recognizing that cyber events will happen:

1. All Bank employees understand and hold themselves, partners and vendors accountable for their role in protecting Bank systems and information.
2. The Bank has cyber talent and cyber system protection, response and recovery above or on par with those of its peers.
3. The Bank strategically re-evaluates its cyber security exposure to balance risk and opportunity.
4. The Bank collaborates and takes informed risks with verified partners to optimize both its own cyber risk posture and that of the Canadian financial system.

The sections below outline the Bank's internal and external cyber security priorities that will contribute to the achievement of these goals over the next three years.

Internal priorities

The Bank's current resilience capabilities will serve as a strong foundation to manage cyber risks for 2022–24. Cyber security will continue to be an essential part of managing the new technologies and digital platforms that will support the Bank's core functions in the years ahead.

With the increased complexity of business needs, technology and threat landscapes, business units will become fully integrated partners in the management of cyber risks.

The Bank will increase its emphasis on the zero trust[5] model of cyber defence, which assumes that all connected devices bring some risk, even within secure networks. The Bank will also work with public and private sector partners to prepare for the new age of quantum computing.

Responding to the competitive market for cyber security talent remains a priority. In addition to strategies to identify and recruit new people, the Bank will work on retaining experienced employees. Diversity and inclusion, training and skills development will be emphasized.

The Bank will once again group its internal objectives, outcomes and strategic actions into five **NIST categories:** identify and manage, protect, detect, respond and recover. Investments in the identify, protect and detect categories will continue. But, recognizing that cyber attacks cannot be completely prevented, the new strategy puts more emphasis on response and recovery initiatives.

5 Zero trust is the term for an evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to focus on users, assets, and resources. SP 800-207, Zero Trust Architecture | CSRC (nist.gov)

Category 1 **IDENTIFY AND MANAGE**

Build cyber security into Bank of Canada operations

The Bank will ensure that its employees, infrastructure, and assets achieve business objectives in line with the Cyber Security Risk Appetite.

Outcomes

- Cyber risk management processes are well defined, implemented and measured to enable effective risk-based decision making.
- The Bank attracts, retains and develops skilled cyber talent, emphasizing diversity and inclusion.
- The Bank has a defined plan for becoming quantum resilient.

Actions

- Advance development of cyber risk processes and tools
- Implement updated people strategy
- Test quantum readiness framework and assess systems resilience

Category 2 **PROTECT**

Maintain a proactive posture against cyber attacks

The Bank will use its cyber security systems, tools and policies effectively to secure its information and digital assets. More emphasis will be placed on adopting a zero trust architecture.

Outcomes

- Privileged identities at the Bank are rigorously protected and automated through the identity life cycle.
- The cyber security awareness program is responsive to emerging threats.
- The cyber security testing program assures that cyber hygiene remains strong.
- Data loss prevention and application security controls are implemented based on defined risk scenarios.

Actions

- Continue to advance identity and access management controls
- Enhance cyber security awareness initiatives
- Continue to evolve the cyber security testing program
- Evolve measures for data loss prevention and application security

Category 3 **DETECT**

Strengthen systems to detect and identify a cyber security event

The Bank will advance the integration of threat intelligence, detection engineering and cyber security monitoring.

Outcomes

- Advanced detection analytics are leveraged with a focus on priority cyber threats.
- Threat intelligence, detection engineering and cyber security monitoring processes are integrated throughout the Bank.

Actions

- Evolve, automate and integrate cyber security monitoring
- Mature the cyber threat intelligence framework
- Expand detection engineering data analytics

Category 4 **RESPOND**

Enhance measures to limit the impact of a potential cyber incident

The Bank will improve its ability to assess, triage, and respond to cyber events and incidents.

Outcomes

- The actions and processes to respond to cyber incidents are well developed and practised regularly.
- Decision makers and cyber responders have timely access to data on cyber incidents.

Actions

- Conduct regular exercises at all levels of the organization to test cyber defence, response and decision-making
- Continually validate incident response playbooks
- Develop advanced analytics to facilitate early detection and response

Category 5 **RECOVER**

Enhance operational resilience to recover from a cyber incident

The Bank will enhance its capacity to restore key business operations in response to cyber attacks.

Outcomes

- Cyber security, business process, and data recovery protocols are well defined and practised regularly.
- Enhanced data recovery capabilities are integrated in Bank operations.

Actions

- Conduct cyber-driven disaster recovery exercises more frequently
- Continue to enhance recovery planning, playbooks and tools
- Expand data recovery capabilities to include advanced cyber scenarios

Internal priorities

	IDENTIFY & MANAGE	PROTECT	DETECT	RESPOND	RECOVER
OUTCOMES	Cyber risk management processes are well defined, implemented and measured to enable effective risk-based decision making. The Bank attracts, retains and develops skilled cyber talent, emphasizing diversity and inclusion. The Bank has a defined plan for becoming quantum resilient.	Privileged identities at the Bank are rigorously protected and automated through the identity life cycle. The cyber security awareness program is responsive to emerging threats. The cyber security testing program assures that cyber hygiene remains strong. Data loss prevention and application security controls are implemented based on defined risk scenarios.	Advanced detection analytics are leveraged with a focus on priority cyber threats. Threat intelligence, detection engineering and cyber security monitoring processes are integrated throughout the Bank.	The actions and processes to respond to cyber incidents are well developed and practised regularly. Decision makers and cyber responders have timely access to data on cyber incidents.	Cyber security, business process, and data recovery protocols are well defined and practised regularly. Enhanced data recovery capabilities are integrated in Bank operations.
ACTIONS	Advance development of cyber risk processes and tools	Continue to advance identity and access management controls	Evolve, automate and integrate cyber security monitoring	Conduct regular exercises at all levels of the organization to test cyber defence, response and decision-making	Conduct cyber-driven disaster recovery exercises more frequently
	Implement updated people strategy	Enhance cyber security awareness initiatives	Mature the cyber threat intelligence framework	Continually validate incident response playbooks	Continue to enhance recovery planning, playbooks and tools
	Test quantum readiness framework and assess systems resilience	Continue to evolve the cyber security testing program Evolve measures for data loss prevention and application security	Expand detection engineering data analytics	Develop advanced analytics to facilitate early detection and response	Expand data recovery capabilities to include advanced cyber scenarios

External priorities

The Bank's internal and external cyber security activities are increasingly interconnected, particularly around mission-critical and critical systems such as payment clearing and settlement systems, securities auctions and systems that manage foreign exchange reserves.

Coordination between the public and private sectors in Canada and abroad is essential. Information sharing helps all parties define and manage financial system cyber vulnerabilities and risks and jointly prepare to respond and recover from any cyber attack that may affect individual partners or larger systems.

Domestically, the Bank cooperates with federal financial sector partners, other public sector security organizations, the financial industry and provincial securities commissions whose responsibilities include cyber risk. Internationally, the Bank contributes to cyber security work at the G7 and the Committee on Payments and Market Infrastructures, among others.

Work to improve the cyber resilience of FMIs is ongoing. The Bank oversees designated FMIs whose responsibilities to clear and settle payments are important to the stability of the financial system.

The Bank will prepare for a new role in leading the retail payments supervision framework that will take effect around 2024. The Bank will supervise payment service providers' management of operational risks, enforcing regulatory requirements when necessary.

The Bank will also respond to the rapidly evolving external threat environment and trends in information technology and digitalization. This includes potential initiatives such as the introduction of a central bank digital currency and long-term planning for quantum computer security encryption.

STRENGTHEN **ENHANCE** **MATURE** **EVOLVE**

Category 1 **STRENGTHEN**

Strengthen financial system resilience

The Bank will promote stability in Canada's financial system by developing and implementing collaborative measures to increase cyber security resilience.

Outcomes

- Systemically important financial institutions work effectively with the Bank to build financial system resilience.
- Cyber security risks to Canada's financial system are understood, analyzed and documented.
- Financial system stakeholders are able to respond to a system-wide cyber incident.

Actions

- Develop a threat-led penetration testing framework for critical financial sector institutions
- Assess financial system cyber risk using incident data, models and research
- Contribute to Canadian Financial Sector Resiliency Group (CFRG) exercises to promote coordinated incident response

Category 2 **ENHANCE**

Enhance collaboration and partnerships

Collaboration within the Bank and with external partners will ensure that cyber security risks to Canada's financial institutions are understood, communicated and managed effectively.

Outcomes

- The Bank collaborates effectively with partners to develop cyber strategies, policies and regulatory initiatives.
- Domestic and international partners share financial sector information well.

Actions

- Work with partners in the Resilience of Wholesale Payments Systems program to focus on the most critical cyber security scenarios facing Canada's financial sector
- Use CFRG partnerships to identify and bridge any gaps in coordination of a sector-wide response to systemic-level operational incidents
- Contribute to the G7 Cyber Expert Group's work on refining global cyber security

Category 3 **MATURE**

Mature cyber security practices among financial market infrastructures (FMIs)

The Bank will continue to fulfill its legislated mandate to promote a stable financial system through its oversight of FMIs. This includes strengthening and evolving cyber resilience practices for FMIs.

Outcomes

- FMIs meet or exceed the Bank's Expectations for Cyber Resilience of Designated FMIs,[6] including response and recovery plans.
- FMI operators understand and follow requirements for reporting cyber incidents to the Bank.

Actions

- Use the expectations for cyber resilience guidelines in the next core assurance reviews for designated FMIs
- Work with designated FMIs to improve response and recovery from ransomware and compromised data
- Continue to implement guidelines for FMI reporting of cyber incidents

Category 4 **EVOLVE**

Evolve cyber security programs in response to external trends

The Bank will respond to the rapidly evolving external threat environment and trends in information technology and digitalization. This will require collaboration with partner agencies in the Government of Canada and the private sector.

Outcomes

- Cyber security is included in the design of the retail payments system and any potential central bank digital currency.
- The Bank plays a role in developing Canada's long-term preparedness for quantum computing.
- The Bank facilitates the sharing of appropriate cross-border cyber security information in the financial sector.

Actions

- Include cyber security in the Bank's new mandate for retail payments supervision
- Make cyber security part of planning for a central bank digital currency
- Contribute to the research and planning of new encryption technologies through the Government of Canada's National Quantum Strategy and Quantum Working Group
- Explore Canada's role in cross-border cyber intelligence sharing in the financial

6 See the Expectations for Cyber Resilience of Financial Market Infrastructures.

External priorities

	STRENGTHEN FINANCIAL SYSTEM RESILIENCE	ENHANCE COLLABORATION & PARTNERSHIPS	MATURE CYBER SECURITY PRACTICES AMONG FMI'S	EVOLVE CYBER SECURITY IN RESPONSE TO EXTERNAL TRENDS
OUTCOMES	Systemically important financial institutions work effectively with the Bank to build financial system resilience. Cyber security risks to Canada's financial system are understood, analyzed and documented. Financial system stakeholders are able to respond to a system-wide cyber incident.	The Bank collaborates effectively with partners to develop cyber strategies, policies and regulatory initiatives. Domestic and international partners share financial sector information well.	FMIs meet or exceed the Bank's Expectations for Cyber Resilience of Designated FMIs, including response and recovery plans. FMI operators understand and follow requirements for reporting cyber incidents to the Bank.	Cyber security is included in the design of the retail payments system and any potential central bank digital currency. The Bank plays a role in developing Canada's long-term preparedness for quantum computing. The Bank facilitates the sharing of appropriate cross-border cyber security information in the financial sector.
ACTIONS	Develop a threat-led penetration testing framework for critical financial sector institutions	Work with partners in the Resilience of Wholesale Payments Systems program to focus on the most critical cyber security scenarios facing Canada's financial sector	Use the expectations for cyber resilience guidelines in the next core assurance reviews for designated FMIs	Include cyber security in the Bank's new mandate for retail payments supervision
	Assess financial system cyber risk using incident data, models and research	Use CFRG partnerships to identify and bridge any gaps in coordination of a sector-wide response to systemic-level operational incidents	Work with designated FMIs to improve response and recovery from ransomware and compromised data	Make cyber security part of planning for a central bank digital currency
	Contribute to Canadian Financial Sector Resiliency Group (CFRG) exercises to promote coordinated incident response	Contribute to the G7 Cyber Expert Group's work on refining global cyber security	Continue to implement guidelines for FMI reporting of cyber incidents	Contribute to the research and planning of new encryption technologies through the Government of Canada's National Quantum Strategy and Quantum Working Group Explore Canada's role in cross-border cyber intelligence sharing in the financial sector