2019–2021

Cyber Security Strategy

Reducing Risk
Promoting Resilience

BANK OF CANADA
BANQUE DU CANADA

MESSAGE FROM THE CHIEF OPERATING OFFICER

Modern technology is helping the Bank of Canada embrace innovation in everything we do.

But this requires a strong, ongoing commitment to cyber security.

Our Cyber Security Strategy outlines the Bank's approach to cyber security for the medium term: ***reducing risk and promoting resilience***.

While it is important to prevent cyber attacks where possible, we must be prepared to respond and recover quickly if a breach does occur.

We are investing in system-wide defences to ensure the Bank's operations are secure.

And we intend to work closely with our financial system partners to promote cyber security in Canada and around the world.

Filipe Dinis, COO

INTRODUCTION

The Bank of Canada is committed to fostering a stable and efficient financial system. Given the worldwide increase in the frequency and severity of cyber attacks, cyber security will be a priority for the Bank for many years to come.

The 2019–2021 Cyber Security Strategy articulates the Bank's plan to reduce risk and promote resilience in its own operations and the domestic and international financial system.

The Bank's Cyber Security Vision:

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

The Bank's 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

The Bank's Cyber Security goals:

1. **Strengthen** cyber team and capabilities to enable secure and innovative Bank operations
2. **Collaborate** with key partners to promote resilience and reduce the incidence and severity of cyber security breaches
3. **Regulate** and promote leading cyber security standards through the Bank's oversight roles

THE CYBER SECURITY ENVIRONMENT

The financial industry in Canada and around the world is using innovative new technologies to improve services, automate work and drive costs down. The "cloud," quantum computing, artificial intelligence, the Internet of Things, fintech and other tools facilitate the efficient electronic transmission of financial transactions between and among clients, vendors, institutions, and payment systems.

While this interconnectedness has many benefits, it has become a vulnerability in today's world of frequent and sophisticated cyber attacks. A breach compromising the data and operations of even one financial institution has the potential to spread to its external partners and ultimately disrupt important national and international financial systems.

With daily transaction values in the billions of dollars—and hackers motivated in many cases by financial gain—it's not surprising that financial institutions and systems are experiencing more cyber attacks. The Bank and other sector participants have been making ongoing, significant investments in the protection of internal systems and cyber detection, response, and recovery capabilities.

However, an inward focus is not sufficient. The Bank and its partners are also concerned about the potential for a successful attack to undermine confidence in the financial system. Increasingly, there is a need for integration of response and recovery strategies across all sector participants—and particularly large financial institutions and crucial financial market infrastructures (FMIs).

As a central player in Canada's economy, the Bank aims to reduce the potential for cyber incidents to "disrupt financial services crucial to both national and international financial systems, undermine security and confidence, and endanger financial stability."[1]

The Bank recognizes its responsibility to work with external partners to promote and facilitate the resiliency of the financial system. Effective collaboration between public and private participants is required.

Similarly, through its oversight role, the Bank requires FMIs to use appropriate cyber security tools and practices. This contributes not only to their individual protection but also to reducing risk and promoting resilience of the financial system as a whole.

INCREASINGLY, THERE IS A NEED FOR INTEGRATION OF RESPONSE AND RECOVERY STRATEGIES

THE BANK'S CYBER SECURITY JOURNEY

In 2014, the Bank of Canada published research highlighting the profound significance of cyber attacks for the operational resilience of Canada's financial institutions and financial market infrastructures.[2] And for the first time, based on an internal assessment, cyber security was rated as a Tier 1 risk for the Bank's own operations.

The Bank has since made cyber security a top priority. The 2016–2018 Medium Term Plan (MTP) included investments in new technologies, processes, and people to address existing and emerging cyber security risks. A proactive approach to cyber defence was adopted to limit or contain the impact of a potential cyber security event.

The Bank focused on understanding cyber security impacts to financial stability

The Bank has been collaborating for many years with the Government of Canada and other public and private sector partners both nationally and internationally to reduce or mitigate cyber security risks to the financial system. A key example of this work is the Bank's participation in the development of the CPMI-IOSCO Cyber Guidance for FMIs[3], which forms the basis for the Bank's cyber oversight requirements.

The Joint Operational Resilience Management Committee (JORM) was created as a forum for major banks, FMIs and public authorities to share information on operational risk events and test resiliency protocols. The forum is evolving into the Canadian Financial-sector Resiliency Group (CFRG) to reflect an updated mandate to explicitly include cyber events, with increasingly complex coordination needs.

While protecting against cyber attacks remains a goal, the focus is shifting to building readiness to respond to and recover from cyber incidents that do occur. This reflects a better understanding of the nature of cyber threats; risk proofing the financial system against all attacks is not a realistic expectation.

In line with this, in 2018 the Bank entered a more formal business-continuity partnership with Payments Canada and the six largest Canadian banks. This is intended to improve domestic coordination and make the wholesale payments system more resilient to a cyber attack.

The Bank invested in the foundational elements of cyber security

Building a strong cyber security posture has been a primary focus. The Bank developed cyber security directives and standards to establish a baseline for its cyber posture. This led to the refinement of its governance model to support the larger size and scope of its cyber programs and shared roles and responsibilities among several departments.

The Bank adopted a cyber security risk management framework to guide posture assessments and evaluate progress. In addition, a "people strategy" was developed to attract, retain and grow cyber talent, including recent graduates and students.

In 2018, a Chief Information Security Officer was appointed to promote alignment and coordination of cyber programs and activities both within the Bank and externally. Under the CISO, a risk-based approach to priority setting is used, informed by results of testing, audits, assessment, and operational experience.

The Bank prioritized protecting critical operations and assets

The Bank has carefully examined its most critical operations and assets, known as "crown jewels", to understand how they might be targeted by cyber attackers. To protect the Bank and detect threats, controls specific to each asset have been added or enhanced to mitigate the highest likelihood risks.

In particular, the Bank enhanced the controls related to its SWIFT[4] payment system environment, through which it communicates with financial institutions around the world.

The systems that support the critical banking operations in the Funds Management and Banking department were also a key area of focus.

In addition, an integrated security testing program was implemented to identify and remediate system, people, and process vulnerabilities. Testing results are used to improve key processes and response plans for cyber incident such as ransomware.

The Bank took a people focused approach to security services

As most successful cyber attacks occur through people, the Bank has enhanced its capabilities to mitigate people-based lines of cyber attack.

A user awareness program was developed to educate regular and privileged users of the Bank's systems about the risks related to their work—such as phishing and credential theft.

Measures were introduced to ensure the security and management of Bank passwords, in particular for people who have privileged access to mission-critical and critical systems. Furthermore, software was deployed on Bank laptops and servers to detect and rapidly respond to malicious activity.

The Bank invested in key initiatives to increase resilience

Building a stronger recovery infrastructure to promote operational resilience was a major priority for the Bank in the last MTP.

Programs like Business Recovery Enhancements (BRE) and Resilience for Market and Banking Operations (RMBO) enhanced the Bank's ability to recover from or avoid potential harm if capabilities or services are impaired for any reason. These initiatives have laid the foundation for improved cyber resilience.

Moving beyond protecting: Ready to respond and recover from an attack

While the Bank has enhanced its overall cyber security and resilience capabilities, more is needed. The Bank will continue to adapt its internal and external operations to the rapidly evolving cyber environment

The 2019–2021 Cyber Security Strategy builds on past accomplishments, is aligned with the Bank's Medium-Term Plan[5] and risk appetite (see Appendix) and reflects the challenges of our financial ecosystem.

THE CYBER JOURNEY CONTINUES – 2019–2021

The 2019–2021 Cyber Security Strategy defines the Bank of Canada's new, holistic approach to cyber security. The Bank's critical role within the financial system is now integrated with its internal cyber security operations.

Based on the assumption that cyber breaches are inevitable, the strategy emphasizes the need to detect, respond and recover from cyber intrusions that may occur.

The strategy also articulates the Bank's contribution to the overall cyber resilience of the Canadian financial system. This includes important collaborative activities with public- and private-sector partners and its legislated mandate for oversight of financial market infrastructures (FMIs).

Leaders across the Bank were consulted in the development of the strategic vision, mission, and goals. These reflect the broad scope of the Bank's cyber security interests and alignment with its risk appetite statement.

The Bank's Cyber Security Vision:
To strengthen the cyber resilience of the Canadian financial system against an evolving threat environment

The Bank's 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

The following sections outline the strategic goals, objectives and intended outcomes that will contribute to the achievement of the Bank's vision and mission.

2019–2021 GOALS

GOAL 1 Strengthen cyber team and capabilities to enable secure and innovative Bank operations.

What success looks like

- The Bank is able to attract and retain top cyber talent that are enabled and innovative.
- The Bank's diverse business lines understand their own cyber risks, which are proactively managed within the cyber risk appetite.
- Cyber security at the Bank is best in class and stays ahead of the threat landscape, enabling secure, innovative solutions for the Bank.

GOAL 2 Collaborate with key partners to promote resilience and reduce the incidence and severity of cyber security breaches.

What success looks like

- The Bank regularly exercises its response and recovery abilities with partners, improving the effectiveness of cyber defences and enhancing the sector's overall cyber resilience.
- The Bank collaborates and shares information effectively with external parties, including other central banks, peer organizations, and the Government of Canada security and intelligence community.
- The Bank helps shape the design and implementation of cyber security strategies for Canadian and international financial systems.

GOAL 3 Regulate and promote leading cyber security standards through the Bank's oversight roles.

What success looks like

- FMIs manage their cyber security risks in alignment with Bank guidance, which is based on international best practices.
- The Bank works effectively with domestic and international partners to enhance legislative, regulatory and supervisory initiatives related to cyber security.
- The Bank provides robust regulatory oversight of the risk management undertaken by Financial Market Infrastructures, including their cyber security risks.

THE JOURNEY AHEAD – INTERNAL OBJECTIVES, OUTCOMES AND ACTIONS

While the Bank has enhanced its overall cyber security and resilience capabilities through the previous MTP, a more significant effort is required to prepare for and respond to the cyber security risks anticipated in the years ahead.

The size and scope of the cyber security program has been increased to achieve the Bank's strategic goals. In addition to the important projects and operating systems that will carry over from the last MTP, new initiatives will be undertaken over the next three years to address emerging priorities. This includes the Bank's expanded focus on detection, response, and recovery activities.

The program roadmap, objectives and intended outcomes have been grouped by NIST function. (See Appendix) This framework facilitates the monitoring and evaluation of the Bank's efforts to implement cyber security controls and reduce risk.

IDENTIFY **PROTECT** **DETECT** **RESPOND** **RECOVER**

Effectively Manage People, Risk, Resources and Governance to address cyber security risks

The Bank will have the governance and information needed to manage and oversee cyber security risk.

Intended Outcomes

- Governance and risk management processes enable effective management and oversight of cyber security risks and risk-based decision-making
- Cyber security risks to critical operations, including those from third parties, are understood and effectively assessed
- The Bank has access to the right cyber skills and talent at the right time

Strategic Actions 2019–2021

To achieve these intended outcomes, the Bank will continue to develop its governance and risk management framework to include:

- an updated risk appetite and metrics to support risk-based decision making, e.g. Key Risk Indicators, Key Performance Indicators, and Maturity Targets;
- enhanced reporting tools to support effective program oversight;
- clear roles and responsibilities across the three lines of defence;
- consistent and rigorous risk assessments of third parties throughout the lifecycle;
- workforce planning for cyber resources to meet future cyber security skills and talent needs.

Establish a proactive posture against cyber attacks

How do we protect the mission-critical and critical digital assets, also known as the crown jewels?

Intended Outcomes

- Access to assets and systems is effectively managed and limited to authorized users and usage
- Vulnerabilities are rapidly identified, impact is understood, and appropriate mitigations are applied
- Data is appropriately categorized and safeguarded
- Employees' cyber security awareness exceeds peer organizations
- Cyber security services are updated and security is built-in to system designs

Strategic Actions 2019–2021

To achieve these intended outcomes, the Bank will:

- mature Identity and Access Management capabilities to include effective, centralized control of privileged identities and a secure application to manage the access of external partners to Bank systems;
- continue to develop the security testing program to support more systematic assessments of the effectiveness of cyber defences (people, processes, and technology) and identification of vulnerabilities and exposure to malware;
- enhance processes and tools to categorize sensitive data and measures to prevent and detect data loss, to reduce data security risks;
- mature the Bank's cyber security awareness program, including training and testing on preventive measures (e.g. effective password management) and new capabilities to detect and respond to cyber attacks (i.e. through malicious emails);
- implement next-generation cyber security services—such as centralized firewall management—to improve the resilience and security of all Business Recovery Enhancement (BRE) environments.

Strengthen systems to identify a cyber security event

The Bank will expand cyber defence capabilities to find a problem when it does occur.

Intended Outcomes

- Cyber attacks are rapidly detected and appropriately managed
- Security configurations are consistently applied and monitored
- Timely threat intelligence supports effective cyber incident management

Strategic Actions 2019–2021

To achieve these intended outcomes, the Bank will:

- implement next generation security monitoring tools and processes, such as real-time analysis and behaviour analytics, to rapidly detect malicious activities and understand the potential impact of events;
- conduct regular cyber security tests to exercise cyber defences, detection and assessment capabilities;
- augment detection processes and procedures, such as expanded end-point detection and data mining capabilities;
- implement strong standards for security configuration and continuously monitor for configuration changes;
- improve processes to handle threat intelligence information and develop threat hunting activities to detect malicious activities.

Enhance measures to limit the impact of a potential cyber security incident

The Bank will ensure it has what it needs to respond effectively when an incident occurs.

Intended Outcomes

- Cyber defence and response plans and processes are regularly exercised
- Incident response actions are consistently handled 24 x 7 and automated when appropriate
- Forensic investigation is performed effectively
- Response activities are effectively coordinated with internal and external stakeholders

Strategic Actions 2019–2021

To achieve these intended outcomes, the Bank will:

- further increase the frequency and coverage of cyber security tests to exercise the Bank's cyber defence capabilities to respond to an event. This includes expanding response plans and testing activities using a coordinated approach with external stakeholders, such as financial system participants and the federal government. This is consistent with External Objectives outlined in the next section;
- enhance tools and processes to enable the Bank to contain or limit the impact of a cyber security incident, in an automated fashion;
- implement enhanced processes and tools, and retain cyber forensic and technical experts, to conduct effective investigations. This includes creating awareness of the information required to investigate cyber incidents.

Build resilience to recover from a cyber event

The Bank will ensure it can restore normal business operations.

Intended Outcomes

- Recovery from a cyber attack is exercised regularly and plans are continuously improved
- Recovery from cyber incidents occurs within an appropriate timeframe including proper communications with both external and internal parties

Strategic Actions 2019–2021

To achieve these intended outcomes, the Bank will:

- test cyber security incident recovery capabilities with internal and external stakeholders (financial system participants, federal government, etc.) to ensure approaches are consistently used in all scenarios. This is an important focus of our external objectives outlined below. Incident response processes will be developed or updated;
- manage cyber security issues efficiently through co-ordination and communication with all stakeholders affected. Cyber recovery playbooks and tabletop exercises will be used to test recovery preparation and speed. In particular, the Bank's ability to respond and recover from a ransomware attack will be enhanced and tested.

THE JOURNEY AHEAD – EXTERNAL OBJECTIVES, OUTCOMES AND ACTIONS

The Bank works with government partners, regulatory authorities and financial institutions to develop and implement policies and standards that contribute to Canada's financial stability and provide a sound foundation for Canada's economic growth.

Collaboration and coordination between the public and private sectors in Canada and abroad are essential to cyber security. Sharing information contributes to the development of effective detection, response and recovery strategies.

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

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.

In 2018 the Bank entered a partnership with large Canadian banks and Payments Canada to improve the resilience of the wholesale payments system. This includes joint tabletop exercises, coordinated communications protocols, improved cyber detection, and joint resiliency and recovery alternatives. Going forward, these will be managed by the new CFRG forum.

The Bank oversees designated FMIs whose responsibilities to clear and settle payments are important to the stability of the financial system. The Bank performs risk assessments of FMIs against its own standards, which are based on the Principles for Financial Market Infrastructures (PFMIs) developed by CPMI-IOSCO. These standards cover financial, business, and operational risk, among others.

The Bank's external cyber program activities have been grouped into four themes:

Strengthen financial system resilience

The Bank will continue to enhance the cyber resilience of the Canadian financial system.

Intended Outcomes

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

Strategic Actions 2019–2021

To achieve these intended outcomes, the Bank will:

- work with government and regulatory partners to define cyber security requirements for critical Canadian cyber security systems, consistent with the Government of Canada's National Cyber Security Strategy;[6]
- continue joint initiatives with Payments Canada and Canadian financial institutions to modernize and promote the resiliency of Canada's wholesale payments systems;
- enhance the tools and data used to analyse, assess and communicate cyber security threats and vulnerabilities to increase understanding of financial system cyber security vulnerabilities.

Enhance Collaboration & Partnerships

The Bank will work closely with key public- and private-sector partners to develop expertise, share best practices, and collaborate on cyber security risk mitigation strategies, policies and regulations initiatives.

Intended Outcomes

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

Strategic Actions 2019–2021

To achieve these intended outcomes, the Bank will:

- work with partners to explore measures to enhance the quality of cyber security services used in the Canadian marketplace;
- enhance information sharing and co-ordination with domestic and international cyber security forums and peer organizations.

Mature Cyber Security Practices among FMIs

The Bank will fulfill its legislated mandate to promote a stable financial system through its oversight of FMIs.

Intended Outcomes

- 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

Strategic Actions 2019–2021

To achieve these intended outcomes, the Bank will:

- set out more detailed expectations for how FMIs could meet the Bank's cyber risk management standards.
- work with subject matter experts and external partners to assess cyber security risks and threats facing FMIs;
- work with partners to strengthen the ability of FMIs to respond to and recover from a cyber event. Cyber recovery playbooks and tabletop exercises will be used to test recovery preparation and speed.

Evolve Cyber Security Oversight

The Bank will work with the Government of Canada and its agencies to enhance legislative, regulatory and supervisory initiatives related to cyber security.

Intended Outcomes

- BoC cyber oversight is integrated with Payment Clearing and Settlement Act (PCSA) obligations.
- Cyber resources are in place to support oversight role

Strategic Actions 2019–2021

To achieve these intended outcomes, the Bank will:

- develop plans to satisfy its new legislative obligations for critical Canadian cyber systems;
- implement a cyber security training and development plan for people involved in oversight of the Canadian financial system.

Cyber Security Strategy 2019–2021 – Internal Plan

OBJECTIVES	IDENTIFY & MANAGE	PROTECT	DETECT	RESPOND	RECOVER
OUTCOMES	Governance and risk management processes enable effective management and oversight of cyber security risks and risk-based decision-making Cyber security risks to critical operations, including those from third parties, are understood and effectively assessed The Bank has access to the right cyber skills and talent at the right time	Access to assets and systems is effectively managed and limited to authorized users and usage Vulnerabilities are rapidly identified, impact is understood, and appropriate mitigations applied Data is appropriately categorized and safeguarded Employees' cyber security awareness exceeds peer organizations Cyber security services are updated and security is built-in to systems designs	Cyber attacks are rapidly detected and appropriately managed Security configurations are consistently applied and monitored Timely threat intelligence supports effective cyber incident management	Cyber defence and response plans and processes are regularly exercised Incident response actions are consistently handled 24 x 7 and automated when appropriate Forensic investigation is performed effectively Response activities are effectively coordinated with internal and external stakeholders	Recovery from a cyber attack is exercised regularly and plans are continuously improved Recovery from cyber incidents occurs within an appropriate timeframe including proper communications to both external and internal parties
ACTIVITIES ROADMAP 2019–2021	Risk Appetite, Thresholds, Targets Refined Standards, Policies, Processes People Strategy	Categorizing and Safeguarding of Data and Information Expanded Vulnerability Management Enhanced Cyber Awareness Identity and Access Management Program	Enhanced Security Tools Security Configuration Management Security Monitoring Evolution Program Enhanced Threat Intelligence	Cyber Security Testing Program Enhanced Forensic Investigations	Cyber Recovery exercises Recovery Planning and Remediation, Playbook Development and Incident Response Exercises

Cyber Security Strategy 2019–2021 – External Plan

EXTERNAL OBJECTIVES	STRENGTHEN FINANCIAL SYSTEM RESILIENCE	ENHANCE COLLABORATION & PARTNERSHIPS	MATURE CYBER SECURITY PRACTICES AMONG FMI'S	EVOLVE CYBER SECURITY OVERSIGHT
OUTCOMES	Cyber security regulatory requirements are defined in alignment with Bank's oversight objectives Designated FMI's are resilient against major cyber incidents	Domestic system-wide cyber resilience initiatives are in place Information sharing protocols in place with international forums and peers	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	BoC cyber oversight role is integrated with PCSA obligations Cyber resources are in place to support oversight role
ACTIVITIES ROADMAP 2019–2021	Resilience of Wholesale Payments Systems (RWPS) Critical cyber system planning Federal cyber security regime implementation	Cyber accreditation program External cyber program implementation Crisis management coordination and toolkit	Cyber guidance for FMIs Incident response and recovery exercises System threat scenarios identification	FMI Oversight Planning Training and development plan for financial system and FSD/cyber

CONCLUSION – REALIZING THE CYBER SECURITY VISION

"Reducing risk and promoting resilience" is the Bank of Canada's cyber security theme for the medium term.

The Bank will promote resilience in its own operations and contribute to stronger domestic and international financial systems.

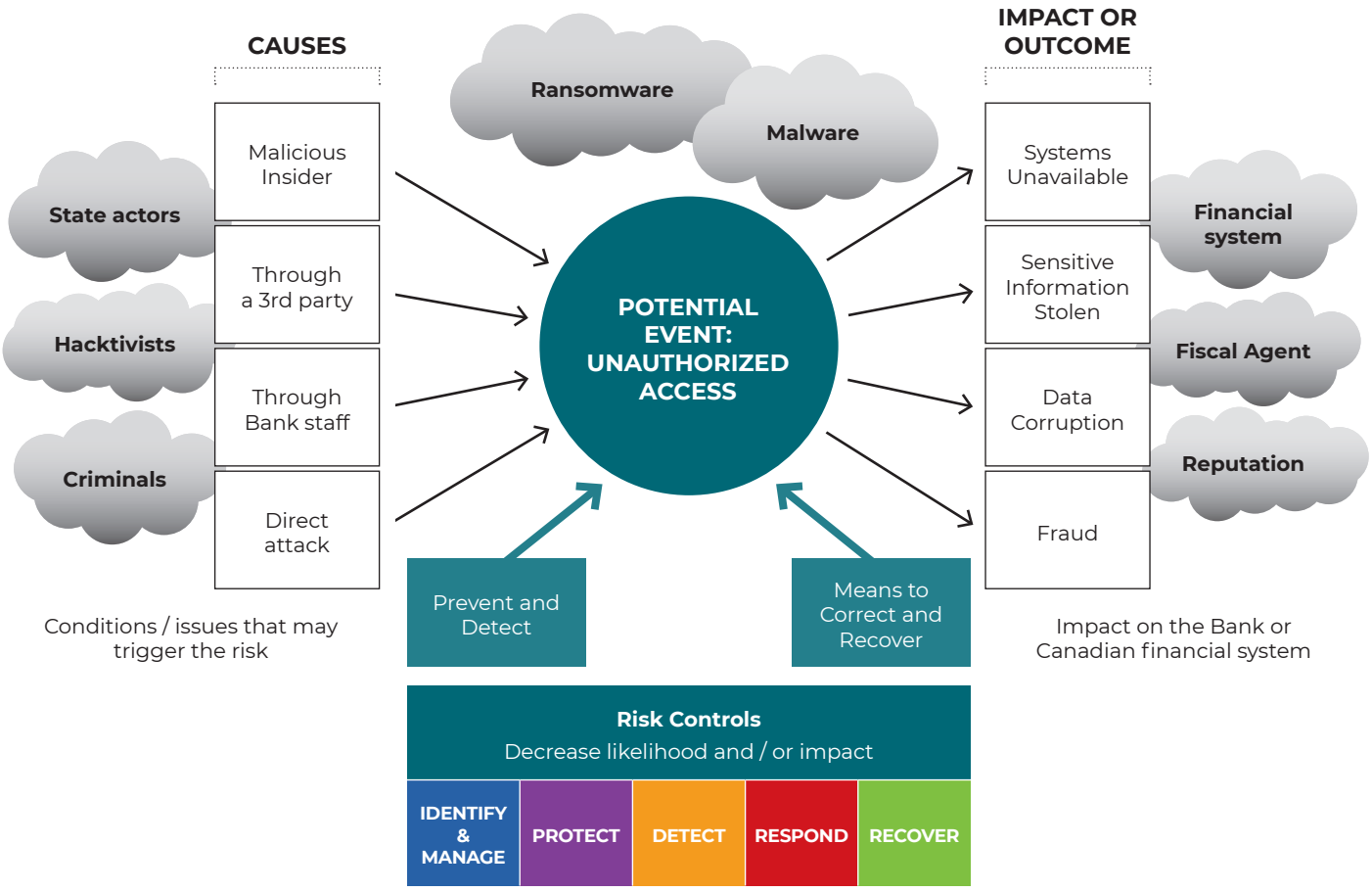
To achieve this, internal and external cyber efforts will be tightly integrated through collaboration with private- and public-sector financial system partners and stakeholders.

The vision, mission, goals and intended outcomes are deliberately ambitious, given the critical nature of cyber security. Building on the Bank's strong cyber security foundation, the strategy defines how the Bank will respond to the challenging threat environment ahead.

A measurement framework will be developed to track and report progress, including cyber security testing and posture assessments.

The Cyber Security Strategy will help the Bank realize its cyber security vision, mission, and goals.

APPENDIX – RISK MANAGEMENT AND NIST



The Bank of Canada's Enterprise Risk Management (ERM) policy and framework are the foundation for the assessment of the effectiveness and resilience of cyber security programs and infrastructure.

The Cyber Security Strategy is aligned with the two main principles of the Bank's Risk Appetite Statement:

1. To minimize and manage the impact of risks that could undermine the Bank's ability to fulfill its mandate.
2. To take informed risks to foster innovation, advance our research and policy development, and to improve our operations and business practices.

The cyber security strategic vision, mission and goals reflect the Bank's intent to minimize cyber security risks while fostering innovation through information sharing and collaboration. Behaviours supporting the risk appetite are integrated into the strategy's definitions of success.

Cyber Security Risk Management Framework

The Bank has developed a risk management framework to guide the assessment of cyber security risks. This is based on National Institute of Standards and Technology (NIST), a set of standards, guidelines, and best practices focused on managing cyber security-related risk.

The five NIST functions—Identify, Protect, Detect, Respond, Recover—were used to guide discussions and analysis of the cyber threat environment and define appropriate controls to manage key risks.

The Cyber Security Strategy outlines the approach and actions the Bank will take to address current and emerging risks, ultimately to prevent cyber attacks and promote resilience to respond and recover to incidents of unauthorized access, should they occur.

NOTES

1. See Communiqué of the G20 Finance Ministers and Central Bank Governors Meeting, Germany, March 2017. As quoted in the Bank for International Settlements, Basel Committee on Banking Supervision report: *Cyber-resilience: range of practices* https://www.bis.org/bcbs/publ/d454.htm

2. Bank of Canada, Financial System Review, 2014. *Cyber Security: Protecting the Resilience of Canada's Financial System*. https://www.bankofcanada.ca/wp-content/uploads/2014/12/fsr-december14-morrow.pdf

3. Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions, *Guidance on cyber resilience for financial market infrastructures*, June 2016 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

4. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is the principal payment messaging service provider for financial institutions around the world. https://www.swift.com/

5. Bank of Canada *2019–21 Medium-Term Plan: Leading in the New Era* https://www.bankofcanada.ca/about/governance-documents/2019-21-medium-term-plan-leading-new-era/

6. Government of Canada, *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age* https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx