Ontario Broader Public Sector Cyber Security Strategy Report

Cyber Security Division,
Ministry of Public and Business Service Delivery and Procurement

ontario.ca/cybersecurity

Ontario

Table of Contents

Messages

Message from Todd McCarthy

Minister of Public and Business Service Delivery and Procurement

Delivering simpler, faster and better government services comes with a duty to protect the people of Ontario. And as technology continues to advance, so do the threats to our residents online. Our government is helping ensure we have the right protections in place for the people and businesses in Ontario to safely participate and thrive in an increasingly digital world, especially for our most vulnerable populations such as our children and seniors.

In alignment with this commitment, I am proud to share with you the Broader Public Sector Cyber Security Strategy Report, completed in response to the Cyber Security Expert Panel Report (2022). Ontario is one of the first jurisdictions in Canada to adopt an enterprise-wide and public sector wide strategy regarding regulating privacy, cyber security, and the use of artificial intelligence. The intersection of these three pieces is of critical importance in our modern digital economy.

Establishing digital trust for the people of Ontario to interact with government requires ongoing efforts. My ministry will continue to innovate and be agile so that we can adapt to new threats and technologies as they emerge. Through consultations with key government and public sector partners, we will work together to bolster cyber security, protect personal data, and safeguard the use of artificial intelligence in the public sector.

Message from Sarah Harrison

Deputy Minister of Public and Business Service Delivery and Procurement

The broader public sector (BPS) provides services essential to the people of Ontario and the data collected by these organizations, including children's aid societies and school boards, must remain protected from cyber threats. As public services continue to undergo digital transformation, we recognize that by combining our expertise and perspectives we are stronger. As Ontario looks to build potential regulatory guidance for the public sector related to cyber security and artificial intelligence, we look forward to growing these existing partnerships. This work ensures that cyber security programs build resiliency to address the evolving threat landscape and provide Ontario with secure digital services across the public sector.

Introduction

The cyber security landscape is rapidly changing and as a result, the level of risk that exists when organizations are not prepared is increasing. Cyber attacks targeting government and public sector organizations, such as health care and educational institutions, are increasing in frequency and sophistication. The increase in cyber attacks is disruptive and negatively impacts the people of Ontario, bringing heightened risks, distrust and fear. As technologies, such as artificial intelligence (AI), continue to advance, our ability to distinguish trusted sources from deep fakes will become more challenging.

This report highlights the journey and actions that Ontario's Ministry of Public and Business Service Delivery and Procurement has taken to improve cyber resiliency in Ontario's broader public sector (BPS). Ontario's commitment advanced with the introduction of the Cyber Security Strategy 2019-2022 and appointment of the Cyber Security Expert Panel in October 2020. The Expert Panel was tasked to identify cyber security challenges in the BPS and to develop recommendations to improve our cyber resilience across the province, notably in education, child welfare, health, and municipal environments.

The Cyber Security Expert Panel's final report (2022) highlighted four key themes to improve digital resilience across government and the BPS:

1. Reinforce governance and operating models
2. Improve education and training
3. Embrace cross-sector shared services to better mitigate future cyber attacks
4. Expand communication between organizations.

The panel's recommendations informed the development of the activities described below. In addition, the report helped inform the cyber security components in *Bill 194, Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*, that received Royal Assent on November 25, 2024.

Ontario is constantly working to strengthen our cyber security practices and protect the data entrusted to us by our people and businesses. Ontario is committed to providing the right tools to quickly respond to cyber attacks and emerging threats, keeping people safe from data, cyber and AI-related harms while supporting the growth of a safe and prosperous digital economy.

Cyber security is a collective responsibility — not the responsibility of one individual or one organization. We all have a part to play in building cyber maturity and resiliency to better protect the people of Ontario.

Background

Safeguarding data entrusted to the government and the broader public sector (BPS) by the people and businesses of Ontario is of utmost importance. Ontario uses a defence-in-depth approach to cyber security which includes multiple layers of security controls, firewalls, continuous vulnerability scanning, 24 hour/365 days a year monitoring, endpoint detection and response, and routine cyber security assessments, such as penetration tests and threat risk assessments.

The Ontario Broader Public Sector Cyber Security Strategy was designed to deliver the right tools to the Ontario Public Service (OPS) and the BPS to better predict, identify, avert, monitor, defend against and resolve cyber attacks, while also reducing duplication of effort. This strategy further enhances the OPS defence-in-depth approach to secure and modernize digital public services. Cyber security is evolving, and with it the supports, policies, and tools described below will continue to grow and mature as they are adopted by our BPS partners.

Building resiliency for the OPS

The Cyber Security Strategy activities between 2019 and 2022 focused on significantly expanding the number of cyber technology platforms across the OPS to enhance monitoring and threat intelligence. These systems proactively manage cyber risk and improve online experiences for OPS and BPS customers.

To further enhance these learnings, the Ministry of Public and Business Service Delivery and Procurement routinely evaluates its cyber security maturity across the OPS using recognized industry guidance. The cyber security maturity of the organization is evaluated holistically and includes people, processes and technology, such as operational processes and safeguards. These are refreshed though life-cycle operational and product changes to reflect changes to legislation, regulations, policies, standards and business processes and in response to the needs of people in Ontario.

The ministry refined the recommendations from the cyber maturity assessments and the 2022 Cyber Security Expert Panel Report, in consultation with ministry partners, to form a set of strategic priorities leading into 2023 through to 2026. These priorities further strengthen cyber protection for the OPS and the means to provide cyber protection across critical sectors by empowering BPS organizations to build greater cyber resilience.

No strategy can prevent all cyber risks facing Ontario. However, the Cyber Security Strategy provides the BPS with the necessary education and resources required to better predict and avert cyber threats and monitor and resolve incidents — minimizing service disruptions to ensure these organizations can continue to operate even when breaches occur.

Milestones toward BPS resiliency

In addition to the recommendations outlined in the Cyber Security Expert Panel report, the approach of **Ontario's Cyber Security Strategy** (past and present) yielded several achievements on the path to build cyber security resiliency in the BPS.

2017

In 2017, the ministry established the **Cyber Security Centre of Excellence** to help educate Ontario government ministries and BPS organizations about cyber security and best practices to keep Ontario's information safe and secure.

2019

To further enhance BPS support and education, the **Cyber Security Community of Practice (CoP)** was formed in 2019. It began with a total of 63 members from six sectors. The CoP provides members from across government, the BPS and municipalities with guidance, information and services to strengthen cyber security resilience while meeting digital service delivery expectations.

2020

The Cyber Security Centre of Excellence launched an **online Cyber Security Ontario portal** in 2020 for the BPS and municipalities to provide cyber security education and learning at any skill level.

2019 to 2023

The ministry's Cyber Security Division started working in partnership with the Ministry of Health and Ontario Health, along with health sector partners, in 2019, to help support cyber security maturity in the health sector. Together, they developed the **Provincial Cyber Security Model for Healthcare** and began scaling the Cyber Security Model in 2023.

The ministry, with Supply Ontario, established IT security product and service arrangements with over 70 vendors available to both OPS and BPS.

2024

Ontario introduced ***Bill 194, Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024***, and it received Royal Assent on November 25, 2024. The bill introduced new legislation, the *Enhancing Digital Security and Trust Act, 2024*, that once in force, would set a framework to bolster cyber security, better protect personal data, including children's, and support the responsible use of AI across the BPS. This milestone was achieved through the united support of the ministry's Cyber Security Division and Strategic Policy Division.

With its passage, Ontario became one of the first jurisdictions in Canada to regulate three key pieces of digital security in the public sector: cyber security, data protections and the use of artificial intelligence. Through adopting robust security measures, enhancing accountability, and fostering innovation, this legislation positions Ontario as a leader in digital trust and resilience.

Strategic Initiatives

The activities outlined in this next section advanced Ontario's Cyber Security Strategy, and operationalized a government-wide approach to respond to cyber incidents. Operational activities were developed, piloted, evaluated and improved upon to ensure effectiveness. BPS organizations have unique challenges and continuous improvement is built into the government's approach to responding to cyber incidents.

Reinforce Governance & Operating Models 1

The governance, oversight and effective risk management of cyber security across the OPS and BPS remains a key focus for government.

Update to Policy and Standards

- Together with key partners across the OPS, the Cyber Security Division created frameworks, consulted with experts, and developed supports to integrate the following into business areas:
    - Bill 194 introduced new legislation that, once in force, would establish a framework to build modern and responsive safeguards that help keep data secure, while ensuring responsible use of emerging technologies like AI systems.
    - Announced the creation of the Artificial Intelligence Expert Working Group to provide the Ontario government with advice and recommendations on the development of Ontario's Trustworthy AI Framework and policies related to the responsible use of AI within the public sector.

- Key cyber security policies and information technology standards have been refreshed based on emerging opportunities/threats, adopted industry changes, organization priorities and disruptive technologies.

Operational models

- The ministry worked in partnership with Ontario Health and the Ministry of Health to develop, pilot, and evaluate the Provincial Cyber Security Model for health care.

- During a two-year period (2021-2023), six regional pilots occurred that reached 44 per cent of acute care hospitals in Ontario. Building on the success of the pilot, in 2023, Ontario Health formalized and began scaling out the Cyber Security Model through ten cyber security shared service partnerships across the province with 100 per cent of the acute hospitals now engaged.
- The model for healthcare defines roles and responsibilities for governance and service delivery to increase cyber resiliency and the protection of sensitive data and services.
- To learn more about the Ontario Health Cyber Security Model pilot and operational plans, please refer to:
  - Participating in the Provincial Cyber Security Operating Model [PDF]
  - 2022/23 Ontario Health Annual Privacy and Security Report [PDF]

- Through the recommendations provided by the Cyber Security Expert Panel, the Cyber Security Division was able to extend the Provincial Cyber Security Model to select BPS organizations in partnership with the Ministry of Children, Community and Social Services, Ministry of Education and Ministry of Colleges and Universities.

- The Provincial Cyber Security Model for healthcare will be used as the foundation for additional sector cyber security operating models. The models will assist the BPS to strategically drive investments and protect provincial digital assets and services.

Education & Training 2

The ministry is committed to empowering diverse communities across Ontario to grow their cyber awareness through education and training.

Enhance education and training for diverse audiences

- One of the most effective strategies against cyber attacks is cyber security education and awareness. Ontario's Cyber Security Centre of Excellence develops practical materials and courses for the OPS and BPS to support cyber workforce development.
  - The Cyber Security Centre of Excellence helps educate government ministries, BPS organizations and municipal partners about cyber security and best practices to keep information safe and secure for the people of Ontario. They offer advice, guidance, information, courses, and services to strengthen digital resilience while meeting digital service delivery expectations.
  - The Cyber Security Centre of Excellence offers cyber security tabletop exercises in partnership with Emergency Management Ontario for groups managing critical value assets. These exercises ensure continuity of operations planning is current and can be quickly acted upon.

- In addition, the Cyber Security Centre of Excellence develops and promotes diverse and inclusive cyber security awareness and OPS training initiatives across all stages of learning, supported by a variety of common and tailored content and hands-on activities available at cybersecurityontario.ca, including:
  - The online course catalogue is continually evolving and currently has 18 training modules on topics such as vulnerability management, incident management planning, and governance and risk management.
  - The Knowledge Library holds introductory information on a range of cyber security topics, including cyber hygiene, identifying and responding to social engineering attacks, and cyber attacks.
  - The K-12 zone, launched in 2023, provides an online resource for students, teachers and parents to learn about the importance of online safety.
- Bill 194 introduced new legislation that, once in force, would enable regulations to be made governing cyber security for public sector organizations, including cyber security programs, as well as education and awareness measures.

Shared Resources & Services 3

Stopping cyber attacks requires proactivity, not just to detect threats but to eliminate or mitigate potential cyber-related risks within systems, applications and processes.

Evolve and Sustain Core Services

- One of the keys to managing cyber-related risk is to identify the most critical value assets (CVA). The ministry provides guidance to help identify CVAs containing sensitive data which may be protected, private, or confidential. In addition, the guidelines for Identity and Credential Assurance were strengthened, clarifying access management controls for systems and services. Together, these guidelines help target investments and updates that protect what is most critical to Ontario's citizens and businesses.

- A government-wide approach was applied to enhance the Incident Response Playbook, streamlining procedures and communications during a cyber incident. It simplified the incident reporting to help with quick decision-making, communications and follow-through of decisions. In addition, this approach promotes ongoing relationship building with Emergency Management Ontario and their reach across the BPS.

- On-going product management practices are used to balance the evolving needs in cyber security services with user experience, lifecycle management, business and fiscal responsibilities.

Extend Cyber Protection Across Critical Sectors

- Pooled resources and shared services help to reduce cyber risk to areas that protect our vulnerable citizens — education, health and social services.

- In collaboration with Supply Ontario, supply advice is provided to the OPS and BPS when leveraging existing procurement supports and resources.

Extend Communications 4

Operational collaboration is increased across the OPS and BPS by providing awareness of cyber threats to these partners.

Expand and improve cross-sector cyber knowledge sharing

- An information sharing channel was implemented that encourages the OPS and BPS organizations to easily and securely share information related to cyber security.
  - The Cyber Security Centre of Excellence delivers cyber awareness campaigns, including hosting interactive events and activities for BPS organizations, such as hack-a-thon and tabletop exercises.
  - The Community of Practice provides members with insights on the latest cyber security news and developments to help keep public service delivery systems secure at a practical level. This community has grown to over 1,600 participants from over 600 organizations.

Expand tactical and operational threat intelligence sharing

- Cyber threat notices and incident response advisories are shared quickly to assist government and BPS partners in defending themselves and Ontarians' data.

Enhancing Digital Security and Trust – Bill 194

Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*, introduced a new statute — the *Enhancing Digital Security and Trust Act, 2024 (EDSTA)*. Once in force, this legislation would set a framework for modern and responsive safeguards for cyber security, AI, and children's data protections.

The *Enhancing Digital Security and Trust Act, 2024 (EDSTA)* enables the government to set regulation requirements and directives governing cyber security in public sector organizations. Regulations may be made respecting the cyber security of public sector organizations, including regulations requiring them to develop and implement cyber security programs. Regulations may also set technical standards respecting cyber security.

Regulation requirements under EDSTA would be developed with key partners, including those impacted by potential regulations. All regulations developed under EDSTA would involve public consultation through the Ontario Regulatory Registry.

The province is continuously consulting with key public sector stakeholders, including Indigenous partners, academia, civil society, technology experts, the Ontario Human Rights Commission, the Information and Privacy Commissioner of Ontario and the public as it considers what future regulations could come forward for approval under EDSTA.

Regulations may be phased in over time to support improving cyber resilience in public sector organizations as cyber maturity increases. This approach helps improve cyber security resilience and cyber security maturity within specific BPS organizations.

This legislation was developed using recommendations from the Cyber Security Expert Panel and consultation feedback from ministry and sector partners, particularly the health, education and child and family well-being sectors. By enhancing cyber resilience, Ontario is ensuring these essential sectors remain secure and operational, protecting the safety and privacy of the people of Ontario, while providing them with more connected and convenient services across government.

Conclusion

The government will continue to enhance safeguards and supports needed to be resilient and better at repelling, responding and recovering from cyber incidents. This includes leading security enhancements and improvements across the OPS and within key public sectors. The ministry will continue to work toward developing regulations under the *Enhancing Digital Security and Trust Act, 2024*, including public consultation and engagement with the sectors.

Building digital resiliency across the government and the BPS requires an ecosystem of allies. In addition to partners mentioned earlier in this report, the ministry consulted with the federal government, academia, industry security and intelligence partners, including Public Safety Canada, Canadian Security Intelligence Service, the Royal Canadian Mounted Police, Communications Security Establishment Canada and the Canadian Centre for Cyber Security.

By working together, government, BPS organizations and allies can ensure a more resilient digital future for Ontario, where the opportunities of technology are harnessed, and Ontarians are protected from risk.