Ministry of Public and Business Service Delivery of Ontario (MPBSD)
Cyber Security Expert Panel

Cyber Security in the Ontario Broader Public Sector

REPORT

to the Minister of Public and Business Service Delivery of Ontario

2022

Ontario

Table of Contents

Message from the Chair of the Broader Public Sector Cyber Security Expert Panel

Cyber security has become a topic of increasing interest in recent years, affecting the Broader Public Sector (BPS) and all Ontarians. We face a wide range of cyber risks, from ransomware that restricts access to sensitive information to malware that disrupts the operations of critical infrastructure. In addition to the disruption of critical services, these risks carry serious financial implications that may include, but are not limited to, the loss of critical or sensitive data, inavailibility of essential systems, and the costs associated with incident response and restoring systems following a major cyber event. As public service delivery becomes increasingly dependent upon digital systems, the Ontario Government, BPS organizations, and cyber security practitioners need to work closely to address cyber security challenges.

The Expert Panel on Cyber Security brought together recognized Information Technology (IT) and Operational Technology (OT) security, risk management, cyber awareness education, and regulatory compliance experts to analyze the current state of cyber security in Ontario. As part of its mandate to identify cyber security challenges encountered by BPS organizations and provide recommendations to improve overall cyber resilience in Ontario, the Expert Panel conducted several conferences, workshops, and interviews during the past year as a means of gathering data. This report would not be possible without the joint effort of dedicated professionals, government staff, and BPS stakeholders.

We identified through our research that a lack of strong cyber security governance is common among BPS organizations, despite differing cyber capabilities and risk profiles. Thus, prioritizing improvements in governance should be a key consideration when developing an organization’s overall cyber strategy. A comprehensive governance model involves cyber security standards, policies, frameworks, maturity models, best practices, roadmaps, playbooks, advisory services, threat intelligence sharing platforms and empowers organizations to respond and recover more quickly when faced with cyber incidents.

Considering that many BPS organizations have difficulty effectively managing cyber security risks due to resource constraints, it is also recommended that risk assessments be mandated based on the National Institute of Standards and Technology (NIST) Cyber Security Framework. Risk assessments can be completed internally or through the regional shared services depending on the organization’s available resources and cyber capabilities. A commonly adopted cyber security framework can benefit practitioners by offering consistent oversight and policies.

There are additional findings and recommendations in this report aimed to enable Ontario to better support BPS organizations and service delivery partners. On behalf of the Expert Panel on Cyber Security, I would like to express a sincere thank you to everyone who took time to share their experiences and perspectives with the Panel. Your contributions were critical to developing these recommendations and shaping the future of Ontario’s cyber security landscape.

Sincerely,

Robert Wong

Chair – Broader Public Sector Cyber Security Expert Panel

Executive Summary

The Minister of Government and Consumer Services, now the Ministry of Public and Business Service Delivery (MPBSD), created the Broader Public Sector Expert (BPS) Panel on Cyber Security in 2020 to support Ontario communities, organizations, and businesses in becoming more cyber resilient. Building better cyber resilience means educating and helping Ontario citizens better understand and adapt to the changes in digital technology that drive everyday business interactions. Increased cyber resilience will play an essential role in Ontario's future success.

The Expert Panel's mandate aimed to:

- Identify and assess common and sector-specific cyber security themes and challenges affecting BPS organizations and service delivery partners in Ontario;
- Review and advise on the government's cyber security measures and risk mitigation efforts across multiple sectors of the BPS; and
- Provide advice to the Minister of Public and Business Service Delivery on specific topics through formal reports to improve the cyber security posture of BPS partners.

Through its mandate, the Expert Panel aimed to improve the BPS's cyber security posture. The Panel has provided five guiding principles to ensure the recommendations and strategies it offers are sustainable and effective across the BPS over time. The guiding principles encompass public interest, leadership, learning support, stakeholder accountability and the facilitation of continuous improvement in cyber security across a variety of diverse organizations.

Following these guiding principles, the Expert Panel reviewed Ontario's current cyber security landscape in the education, child welfare, health, and municipal environments and identified common and sector-specific challenges.

To improve cyber resilience within the BPS, the Expert Panel provides recommendations aligned with the four key challenges identified, reflective of the specific needs of the Province of Ontario and requiring joint effort from all stakeholders within the ecosystem. The four key observations and corresponding recommendations from the Expert Panel include:

1 Governance and Operating Model

Challenge: Policies, procedures, and accountabilities within current BPS governance structures for cyber security are disparate. Cyber-related initiatives are happening in parallel across different sectors without a centrally coordinated strategy or model. While many larger organizations are proactively engaged in risk and maturity assessments, smaller organizations suffer disproportionately from limited access to common cyber security risk management resources and expertise.

Recommendation: Ontario should reinforce existing governance structures to enable effective cyber security risk management across the BPS.

2 Education and Training

Challenge: The province lacks risk- and age-specific content and diversity in cyber security education. K-12 education does not have a sufficient cyber-featured curriculum; higher education offers specialized training but limited opportunities for hands-on experience. Integrated training programs are being developed in response to the growing demand for more robust cyber-related content, however, better access to these resources is required to benefit a wider audience.

Recommendation: Ontario should continue to develop diverse and inclusive cyber security awareness and training initiatives across all age-levels of learning, supported by a variety of common and tailored content and hands-on activities.

3 Communication

Challenge: Communication is limited amongst BPS organizations due to unclear cyber security constituents and a lack of awareness of common platforms. Current information-sharing protocols exist to inform the government in the event of an incident, but these protocols do not serve to support the overall cyber security of the sector. BPS entities require a comprehensive view of communication channels within their network to facilitate and enhance existing cyber resilience.

Recommendation: Ontario should implement a framework that encourages BPS entities to share information related to cyber security securely amongst each other with ease.

4 Shared Services

Challenge: BPS organizations have varying levels of cyber security awareness and employ a variety of standards and frameworks. Compared to their larger counterparts, smaller entities lack critical cyber risk management capabilities such as incident response and backup and recovery plans. These capabilities are now considered fundamental and are often required to qualify for cyber insurance policies. Therefore, acquisition of commercial cyber security insurance is becoming more difficult and expensive for smaller organizations due to lack of dedicated, qualified cyber security personnel and increasing cyber security maturity expectations.

Recommendation: Ontario should continue to develop, improve, and expand shared services and contracts for cyber resiliency across the BPS, considering sector-specific needs where required.

Ontario recognizes that the digital landscape is continuously evolving and that ongoing effort is required on the part of the government to identify, prioritize and address new security challenges and enhancement opportunities. The recommendations provided by the Expert Panel aim to implement new strategies while improving upon the province's existing and ongoing cyber initiatives. The province can achieve these objectives by streamlining existing processes to create clear accountabilities, enhancing existing educational resources, encouraging critical cyber information sharing, and facilitating an acceptable and achievable baseline of cyber security for all organizations across the BPS.

Improvements will be implemented strategically over time, built on a solid foundation of cyber expertise and sector-specific knowledge and resources created through strategic partnerships. Key stakeholders will work together across sectors to expand their existing networks and generate a unified cyber defence mechanism that is stronger, more adaptable, better informed, affordable, and sustainable.

The future of cyber security in Ontario will see cross-sector engagement, participation, and collaboration among all BPS organizations, ensuring consistency in the continuous delivery and accessibility of public service and culminating in a whole that is greater and more resilient than the sum of its parts.

Introduction

The rapid evolution and pervasive integration of technology are disrupting the future of work. Businesses, and society in general, are more reliant than ever on digital systems to interact and conduct transactions. The ongoing digital transformation has delivered significant benefits while introducing new risks to the economy. As the cyber environment steadily evolves, the need for additional resources to combat cyber security risks continues to increase.

The Minister of Government and Consumer Services established a Cyber Security Expert Panel ("Expert Panel") in 2020 as part of *Ontario's Cyber Security Strategy 2019/20 - 2022/23*. Since its inception, the Panel has led collaborative initiatives to identify common and sector-specific challenges and provided advice to improve cyber resilience and create a more cyber-secure future for the Ontario Broader Public Sector (BPS).

In this report, the Panel assesses the current state of cyber security across four (4) BPS sectors (K-12 and higher education, children's aid services, and municipalities). It provides recommendations to incorporate new and enhance existing capabilities within the BPS. The recommendations apply to a broad range of BPS sectors and aim to achieve the following objectives:

- Enhance the knowledge and expertise of BPS organizations so appropriate controls can be put in place to reduce the risk of cyber threats
- Improve digital resilience and security posture of BPS organizations
- Avoid operational shutdowns and disruption to business continuity due to cyber security breaches
- Improve emergency preparedness to enable expedient recovery of data and restoration of services in the event of a cyber security breach.

Defining the Broader Public Sector (BPS)

The BPS is composed of various provincial government-affiliated organizations serving multiple sectors. Each sector is characterized by organizations of different sizes and capabilities with varying access to resources.

According to the *Broader Public Sector Accountability Act, 2010*, designated broader public sector organizations include every:

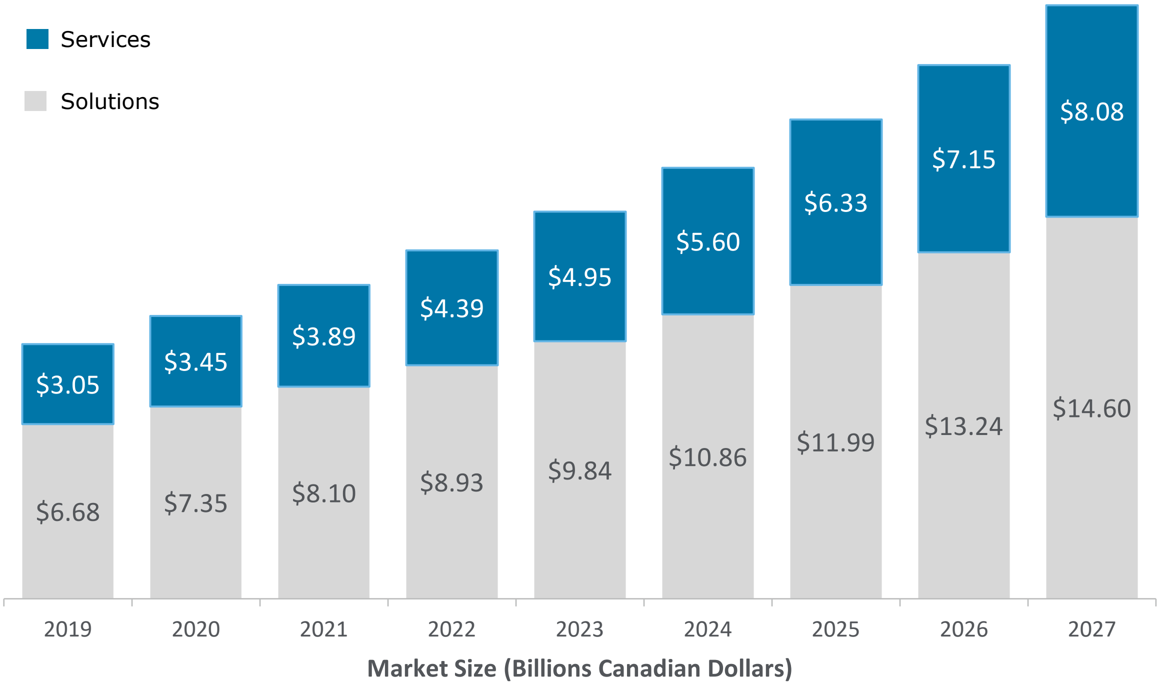
- Hospital
- School board
- University, college of applied arts and technology and post-secondary institution in Ontario
- Children's aid society
- Community care access corporation

- Corporation controlled by one or more designated public service organization that exists solely or primarily for the purpose of purchasing goods or services for said organizations
- Publicly funded organization that receives $10 million or more from the Government of Ontario.

Highlighting the Critical Role of Cyber Security in the BPS Agenda

Given the sophistication of cyberattacks and increased spending on cyber security services and solutions, the global cyber security market demand is expected to grow significantly over the next decade, outpacing the available supply. As shown in Figure 1, the Canadian cyber security market is estimated to experience a compounded annual growth of 11.2% to reach a market size of $22.68 billion Canadian by 2027 (*Allied Market Research Analysis*). However, even though digital transformations have brought considerable benefits to organizations, the range of cyber capabilities and maturity levels across organizations have led to challenges in managing cyber risks and adopting cyber security solutions.

Figure 1: Canadian Cyber Security Market Projection, 2019–2027 ($Billion)



Source: AMR Analysis

Ontario places a high value on cyber security through its digital service commitments. Considering the varying sizes and sectors represented by BPS organizations, a coordinated yet adaptable cyber security approach is critical to protect, support, connect and equip all organizations to succeed in the digital world. Improvement of digital resilience would sustain the overall business environment in the Province of Ontario and avoid any potential disruptions while safeguarding critical data and retaining public trust. Moreover, robust cyber security capabilities will benefit all Ontario citizens by ensuring the continuity of essential public services, including emergency services, K-12 education, higher education, government services, and healthcare.

Introducing the Expert Advisory Panel on BPS Cyber Security

Establishing the Panel’s Mandate and View on Cyber Security

Cyber security is increasingly regarded as a strategic issue affecting all levels of society and a critical element supporting *Ontario’s Digital and Data Strategy*. This Expert Panel aims to help communities, organizations, and businesses adapt and succeed in the changing digital world. To improve the cyber resiliency in the BPS, the Panel’s mandate was to:

- Assess and identify common and sector-specific cyber security themes and challenges encountered by BPS organizations and service delivery partners in Ontario.
- Review and provide advice on the government’s efforts to address cyber security risk across multiple sectors in the BPS.
- Provide advice to the Minister of Public and Business Service Delivery through formal reports on specific topics, culminating in a final report containing findings, analysis, and recommendations to the government detailing a BPS Cyber Security Strategy and options to improve the cyber security posture of our BPS partners.

Sharing our Guiding Principles

The mandate of the Expert Panel to analyze, advise, and make recommendations to the Minister of Public and Business Service Delivery on how best to improve the cyber security posture of Broader Public Sector partners is of critical importance, especially given the rising levels of cyberattacks across all business sectors.

The guiding principles were provided to ensure the strategies and recommendations put forward by the Expert Panel will be effective and sustainable in the long term. The five guiding principles used by the Expert Panel to determine the recommended cyber strategies for the broader public sectors include:

- Generate public interest
- Encourage leadership
- Support learning
- Increase individual stakeholder accountability
- Facilitate continuous improvement when it comes to cyber security
- Adopt a cost-effective approach to enhancing cyber security capabilities

Adopting a Methodology

Ontario's Cyber Security Strategy provides a strategic framework to guide the BPS in improving cyber security, enhancing capabilities, and raising maturity levels. It includes convening the Cyber Security Expert Panel, increasing collaboration across government and the BPS, and ensuring the continued protection of government applications.

Through its mandate, the Expert Panel adopted the approach promoted in the Cyber Security Strategy to gather information, develop research plans, consult with BPS agencies, engage broader stakeholder groups and publish progress and ad-hoc reports. The Panel then reported various findings by analyzing the current state of cyber security – noting Ontario's existing cyber security programs and infrastructure - and provided recommendations to the Minister for the province to adopt.

The Expert Panel and its sub-committees worked closely with the Cyber Security Division under the Ministry of Public and Business Service Delivery to gather insights and develop recommendations. Approaches and activities, roles and responsibilities are detailed below.

Expert Panel

The Minister convened the Expert Panel to identify sector-specific and common cyber risks to the BPS and develop options on how to mitigate BPS risks through a BPS Cyber Security Strategy. Expert Panel members (See *Appendix B*) represent the Expert Panel at public events, provide expert input into research plans, and provide recommendations that affect government policies in cyber security-related matters, as requested by the Minister of Public and Business Service Delivery.

The Expert Panel's role involves setting priorities facilitating decisions on relevant issues discussed, and delivering all findings and recommendations to the Minister.

Through the process of developing reports, the Expert Panel took the following actions:

- Hosted two cyber security conferences that included the attendance of the BPS to investigate cyber security gaps within the sector and propose potential solutions
- Facilitated multiple cyber risk workshops for children's aid societies and health sectors and accelerated a push for Ontario Health to integrate with the regional operating model
- Consulted with Rogers Cybersecure Catalyst at Toronto Metropolitan University to establish a partnership in helping mid-career professionals transition into cyber-based careers
- Conducted a jurisdictional scan of various countries and regions to understand their leading cyber practices and inform the Expert Panel's recommendations.

Sub-Committees

The Chair established the following sub-committees to carry out the Expert Panel's scope of work:

- Governance and Operating Model
- Education and Training
- Communications and Stakeholder
- Shared Services and Resources

The individual sub-committees were responsible for conducting an in-depth study for their respective areas of cyber security and reporting all findings, gaps, and recommendations to the chair of the Expert Panel. The work of the sub-committees contributed to the development of the BPS Cyber Strategy final report.

Identifying Risks Facing the Broader Public Sector

Organizations across the BPS provide services to diverse populations. All BPS services, whether public-facing or internal, are characterized by varying risk profiles. Each service's risk profile is based upon the degree of digitization and the type of information it processes. To maintain integrity, the BPS must protect sensitive data within its systems and provide smooth service delivery to the citizens of Ontario.

An awareness of some of the common cyber risks facing BPS organizations is critical to understanding the importance of strong cyber security. Some examples and potential adverse outcomes are:

1. **Disruption of Operations**

The reliability and availability of critical infrastructure managed by some BPS organizations (e.g., roads and buildings, health care facilities, wastewater systems, etc.) is essential to successful service delivery. Failure of these infrastructures could disrupt operations and adversely affect public safety.

2. **Breach of Sensitive Data**

Many BPS organizations utilize sensitive data including government information or personal information (e.g., name, SIN, passport, address). A breach of such information could result in identity theft and/or other fraudulent activities.

3. **Damage to Public Safety and Trust**

The BPS provides several services that the public relies on (e.g., student learning, child welfare, disability support and employment services). Disruption or loss of these services could uproot public trust in the BPS or compromise public safety.

4. **Loss of Intellectual Property**

BPS organizations such as universities and colleges store confidential research, trade secrets and intellectual property, which could be stolen or lost if not adequately protected and monitored.

5. **Financial Losses**

Many organizations and services store financial data (e.g., payment of service fees, grants). A breach of such confidential information could cause steep financial losses to organizations and individuals.

Analyzing the Current Landscape

The Expert Panel looked at cyber security practices across BPS organizations and other leading jurisdictions to identify potential opportunities to strengthen cyber security practices. This scan helped the Expert Panel understand Ontario’s cyber security landscape and informed the corresponding recommendations.

To characterize the current state of cyber security across the Ontario BPS, the Expert Panel consulted various organizations and stakeholders from education (K-12 and higher education), child welfare, health, and municipal environments. The Panel has shared the challenges identified in this report across the BPS to help foster insights into common and sector-specific issues of concern.

Observing our Leading Practices

Several BPS organizations have launched initiatives to enhance their cyber security. Many of these multi-year efforts are focused on sharing the burden of efficient delivery of common and specialized cyber security services. This assessment observes the following leading practices aligned with the Expert Panel’s four themes:

Theme 1: Governance and Operating Model

- Ontario Health has established six Regional Security Operation Center (RSOC) pilots and regional governance mechanisms. These serve to mobilize a province-wide vision in the health sector and outline key accountabilities at each level related to governance, services, processes, contracting, communication, vendor ecosystem, and expected outcomes.
- The Canadian Shared Security Operating Center (CanSSOC) is a centralized security operating center for the higher education sector, tackling cyber security threats as a single united entity.
- The Information Technology Network Group is endorsed by the Ontario Association of Children’s Aid Societies (OACAS) as the primary body responsible for coordinating technology and cyber security amongst Children’s Aid Society (CAS) organizations.
- Simcoe County is working with MPBSD to adopt the RSOC model from health to the municipal context in their region.

Theme 2: Education and Training

- The Ministry of Education has launched a K-12 Cyber Protection Strategy pilot to address the growing needs for increased cyber protection in the K-12 population, specifically among minors. The Cyber Protection Strategy includes an entire workstream dedicated to developing cyber security education resources for the sector.
- Ontario Health has initiated quick-wins and priority activities around training, awareness and assessments, including the launch of a Health Sector Training Hub that includes an inventory of curated material and tools.

- Various institutions offer cyber-related programs at the undergraduate, graduate, college and professional levels (e.g., University of Toronto's undergraduate and graduate degrees with concentration on Identity, Privacy and Security, Seneca College's cybersecurity diploma programs, and Rogers Cybersecure Catalyst).
- MPBSD and others are developing partnerships with Rogers Cybersecure Catalyst to support BPS awareness, training, and exercises.
- MPBSD has released several modules on the Cyber Security Ontario Learning Portal, covering a variety of cyber security topics aimed to prepare organizations for the challenges of an increasingly digital future.
- MPBSD organizes an annual cyber security conference for the BPS (established in 2020), hosted by Ontario's Cyber Security Centre of Excellence.

Theme 3: Communications

- MPBSD has established a Cyber Security Ontario Learning Portal, where BPS organizations can share their issues, resources, and expertise.
- CanSSOC fosters collaboration amongst institutional and sector partners across the local, provincial, and national levels to provide the higher education sector with threat intelligence that will help them prevent potential cyber security attacks and breaches while improving efficiency and reducing costs.
- Children's aid societies have established information-sharing arrangements to support the detection of cyber threats affecting similar organizations.
- Health, K-12 and municipalities encourage proactive cross-sector communication through their cyber strategies.
- MPBSD has initiated a community of practice and a threat notification service to promote cyber awareness among BPS organizations.

Theme 4: Shared Services

- The Health Sector Cyber Security Operating Model developed by Ontario Health and MPBSD provides a conceptual design for moving the sector towards a shared service approach to managing cyber risks and improving health system cyber security maturity.
- K-12 Cyber Protection Strategy outlines a plan to share cyber risk management resources tailored to the sector. In addition, a planned pilot of K-12 Regional Cyber Hubs delivering sector-focused security services will take place over the next year.
- The Ontario Cyber Security Higher Education Consortium (ON-CHEC) offers cost-effective cyber security guidance, programs, and services such as maturity benchmarking to improve the overall cyber security capabilities and readiness for colleges and universities in Ontario.
- In addition to their threat intelligence feed, the CanSSOC is developing a suite of advanced detection and response capabilities for their member Universities across Canada.

- Children's aid societies have established a shared procurement vehicle to support organizations with annual security awareness testing, vulnerability assessment and penetration testing. In addition, some children's aid society organizations have dedicated cyber security talent and capabilities that are shared informally across regions.
- Grey County is exploring shared cyber capabilities for municipalities on behalf of 30+ municipalities.
- MPBSD has a Vendor of Record Program in place for the BPS to procure cyber security services from one or more qualified vendors.

Identifying Challenges

Ontario's future cyber security operations landscape will rely on a series of sector-specific entities delivering similar services with similar resources. Many BPS sectors and organizations are already headed in the right direction through their ongoing activities. However, several challenges must still be addressed to meet the ongoing needs of most Ontarians and create a cyber-secure and risk-informed culture across the BPS.

Theme 1: Governance and Operating Model

The existing governance and operating models are generally not commensurate with the level of risk associated with cyber security across the BPS. In many cases, the risk is ranked high on risk registers, but the allocation of resources is insufficient for mitigation.

Identified challenges include:

- A lack of coordinated standards, policies, and procedures for raising cyber security-related issues or awareness impair comprehensive governance across the BPS.
- Cyber security strategies and accountabilities are disparate or sector-focused, with limited alignment to a common strategy or vision for the BPS.
- Larger organizations proactively conduct risk and maturity assessments, but there is a lack of consistency across sectors and organizations. Smaller organizations often struggle in this area because limited common resources are available to help them understand and address potential cyber security risks.
- Not all organizations have dedicated cyber security personnel, processes, policies, or procedures.
- Organizations employ a variety of standards and frameworks when managing cyber security. As a result, there is a need for collaboration, attestation, and consistency among organizations.

Theme 2: Education and Training

The existing education and training programs are not sufficient or diversified enough to address the broader audience's growing cyber awareness needs. In addition, many programs are delivered in a dispersed manner, resulting in the underutilization of available resources.

Identified challenges include:

- Limited education and training to address specific risks and behaviors such as ransomware defences, phishing, and vishing.
- Limited age-specific content for cyber security awareness training.
- Cyber security does not feature prominently in the K-12 education curriculum.
- Many university and college programs offer specialized training in cyber security; however, there are limited opportunities for hands-on experience.
- Limited availability of existing programs for re-training, such as Rogers Catalyst, due to significant demand.
- BPS could benefit from a unified cyber security education and training resource across organizations of various sizes.
- BPS requires a more cohesive, accessible and integrated approach for education and training delivery.

Theme 3: Communications

Ontario has no high-level cyber security communication framework to regulate information sharing across platforms and organizations. Limited communication results in a lack of consistency in cyber risk management and incident response.

Identified challenges include:

- Individual BPS agencies have access to cyber security advice through a central helpline, but many BPS organizations are unaware of the significant number of centralized resources available through the Cyber Security Centre of Excellence.
- Cyber security resources are spread across several platforms and are often challenging to locate.
- Cyber stakeholder management is fragmented, without a complete view across all BPS entities.
- Critical information-sharing protocols are currently unidirectional, serving only to inform the government when an incident occurs. However, this information is not broadly shared across the BPS to promote awareness and support other organizations.

Theme 4: Shared Services

Multiple sector-specific shared services are being developed and planned to establish a baseline of threat intelligence, procurement, incident response, and digital resiliency. Still, they do not cover all BPS sectors. Therefore, a central source with defined standards and procedures and a shared delivery model are required to sufficiently support more BPS organizations.

Identified challenges include:

- Organizations have varying levels of cyber security capacities. Many smaller organizations lack cyber incident management capabilities required to respond to an incident, such as investigation tools, data breach coaching, and response processes.
- Most larger organizations are equipped with an appropriate backup or recovery plan. However, many smaller organizations do not have the same capability in place.
- Acquisition of commercial cyber security insurance is becoming more difficult and expensive due to increasing cyber security maturity expectations.

Performing a Jurisdictional Scan

Many global counterparts have responded to digital transformation by integrating cyber security as a critical agenda item, requiring constituents' accountability and compliance. Ontario can enhance its cyber security posture by reflecting on opportunities to incorporate best practices from global leaders. Leveraging these could also help mature BPS cyber capabilities and support Ontario's growing digital ecosystem.

Theme 1: Governance and Operating Model

Leading jurisdictions have used centrally delivered services and resources that consider sector-specific nuances to drive economic benefits while securing public services.

Leading practices include:

- In Israel, cyber security efforts are explicit national objectives of the government, with close involvement of individual organizations. A central governmental Security Operations Centre (SOC) is integrated into the Cyber Emergency Response Team (CERT) technological and operational infrastructure, facilitating the unified visibility and oversight of sector based SOCs.
- The Australian Cyber Security Centre (ACSC) leads the Australian Government's efforts to protect national cyber security, working with the CERT state-based centres that provide contextualized services to each state.

Theme 2: Education and Training

Establishing education and awareness standards for educating citizens with foundational and specific cyber security best practices can promote good digital citizenship at every level.

Leading practices include:

- The Rogers Cybersecure Catalyst Program's design meets demonstrated needs in the Canadian public and private sectors. It empowers Canadian citizens and businesses to seize opportunities and tackle cyber security challenges. Launching additional educational initiatives, such as the Rogers Cybersecure Catalyst Program, will provide Ontarians with more access to cyber security training; enhancing local opportunities to build the skills required to address the gap in cyber talent.

- Israel has adopted a holistic approach to cyber security education covering risk identification, alerts, and attack investigation. Shared services, operations, and management are the core of good cyber digital citizenship. Integration of a central governmental SOC helps inform the operations of sector-based SOCs – providing unified visibility and oversight. A similar strategy within Ontario would facilitate beneficial partnerships and better communication between both public and private sector entities, academia, and Ontarians.

Theme 3: Communications

Developing and sharing best practices through Centers of Excellence has been effective at kick-starting cyber maturity across the public sector in North America and abroad.

Leading North American practices include:

- The Canadian Centre for Cyber Security provides forums for Canadian public and private sector organizations to share best practices and information regarding emerging threats. This National view provides organizations of all sizes with access to critical information they need to defend themselves.
- Multi-State Information Sharing & Analysis Center (MS-ISAC) is a non-profit organization designated by the U.S Department of Homeland Security (DHS) to provide various levels of support for the United States government. It allows members to seamlessly share information by reporting suspicious activities in exchange for live support from MS-ISAC.

International examples of leading practices include:

- In Israel, government bodies work with individual, organizational representatives from public and private sector entities, academia, and citizens. As a result, they have built advanced national cyberspace capabilities such as information sharing platforms, solutions to investigate and contain cyber threats, and centralized security services.
- Singapore relies on their national sector-specific regulators to inform broader public sector organizations of cyber incidents. A network comprised of sector-focused Security Operations is responsible for coordinating and helping to enable this function.

Theme 4: Shared Services

Shared services such as threat intelligence, risk assessment, and incident response are practical tools to motivate the continued improvement of organizational maturity as they help create a risk-informed culture.

Leading Canadian practice:

- Ontario Health launched a shared health system governance structure and program of activities in 2019 to improve the overall cybersecurity maturity of the health system. The new system promotes the sharing of cyber intelligence across the entire sector so health care providers (HCPs) have timely, accurate and actionable cybersecurity information to manage cybersecurity threats and incidents. The establishment of Regional Security Operation Centres (RSOCs) partners and local Cybersecurity Governance Committees as part of this initiative enables regional collaborations within security operations and allows for streamlining of effort, cost efficiency and leveraging of shared cybersecurity expertise while maintaining local accountability.

International examples of leading practices include:

- Israel's Cyber Spark Industry Initiative coordinates joint cyber industry activities across government agencies, military, academia, start-ups, venture capital funds, and foreign groups. It fosters a cyber security ecosystem that drives economic development.
- Singapore has centralized cyber security efforts under a Cyber Security Agency (CSA) housed within the Prime Minister's Office. It provides protection of critical information infrastructures and essential services, coordinates efforts against large-scale cyber incidents, develop and enforce cyber security regulations, policies, and practices.

Applying Key Factors and Considerations

The Broader Public Sector encompasses an array of organizations and services, each with its own unique cyber security requirements. Common factors considered to be applicable across the BPS and relevant to many of the Panel's recommendations include:

- **A risk-informed approach**

The BPS should use a risk-informed approach to allow decision-makers to understand the risks and form more sustainable and resilient policies and practices.

- **A vast and diverse environment**

The BPS represents a diverse group of constituents and services distributed across the province, necessitating adaptable and customizable solutions for various contexts to achieve success.

- **Common and sector-specific approaches**

Organizations face many common threats; however, sector-specific and unique threats may require a nuanced approach. Therefore, the BPS should create space to enable community or sector-specific strategies to solve common problems.

- **Security by design with common architectures**

Security should be considered a foundational element of digital transformation to reduce future cyber risks. Defining consistent policies and procedures with common architectures and promoting technical controls across sectors can help to reduce shared risks today.

- **Cyber security skills shortage**

The cyber security workforce lacks qualified professionals across Canada, resulting in an estimated gap of over 37,100 jobs by 2027 *[Source: (ISC)2: A Resilient Cybersecurity Profession Charts the Path Forward. Source link: https://www.isc2.org/]*. Therefore, any plan to significantly expand current capacity will need to address this challenge.

- **Systemic underinvestment in technology**

Competing requirements for investment in both cyber security and legacy technology replacement have resulted in systemic underinvestment in both areas.

- **Potential economic impacts**

Cyber security incidents affecting BPS organizations pose a risk of significant adverse economic impacts. However, effective BPS-wide solutions can create considerable benefits while reducing the risk of adverse outcomes.

- **Continuous investments to drive improvement**

Funding models for cyber and technology improvements are increasingly categorized as annual operational expenses instead of one-time capital investments. As a result, procurement and funding approaches should align with this new model.

Providing Expert Panel Recommendations

There is a wide range of baseline cyber security capabilities and maturity levels amongst BPS organizations, so it is unreasonable to expect less advanced organizations to catch up to the leaders overnight. The more advanced players are already well into this journey, but smaller and less mature practitioners desperately need external guidance, support, and assistance. In most cases, the journey to achieving this objective requires transformational-level efforts, necessary resources, and several years.

Considering this, the Expert Panel provides recommendations that align with the four sub-committee themes of Governance and Operating Model, Education and Training, Communications, and Shared Services.

Governance and Operating Model

Expert Panel Core Recommendation:

Ontario should reinforce the existing governance structure to enable effective cyber security risk management across the Broader Public Sector (BPS).

The objective of the Cyber Security Centre of Excellence is to help strengthen cyber security across ministries and BPS organizations through the provision of advice, guidance, and information. A lack of central governance and standardized risk management frameworks makes it difficult for BPS organizations of various sizes to develop cyber security solutions that align with the province’s strategy. A holistic view needs to be developed through a single oversight body, employing a common operating model, clearly establishing accountabilities, shared resources and partnerships.

Therefore, the Expert Panel recommends the following:

1. Provide Cyber Security Program Oversight for the BPS

Ontario should align BPS cyber security program responsibilities and oversight to a single body to augment the current governance structures responsible for sector-specific cyber security risks. This body would be responsible for centrally coordinating, resourcing and instilling a risk-informed approach to cyber security across the BPS through consultation, compliance, reporting and collaboration. This approach will enhance cyber security program participation and help the program evolve to meet the BPS’ needs.

2. Adopt a Common Operating Model

Building on the Enterprise Risk Management Framework, Ontario should establish a cyber security risk operating model for continuous improvement. A National Institute of Standards and Technology (NIST)-based Cyber Security Framework (CSF) supported by shared resources such as policies, standards, controls and self-assessment tools will promote a common language and understanding of cyber risk across the BPS. The flexibility of the NIST CSF provides a cost-effective way for organizations of varying sizes to measure risks and establish a foundation of risk management practices to meet their unique needs and challenges by building and implementing a customized cyber security program.

3. Establish Clear Accountabilities for Cyber Security

Ontario must reinforce the cyber security accountabilities that empower leaders to act while ensuring alignment with central and regional BPS programs and initiatives. Each BPS organization should appoint a senior official responsible for cyber security. Establishing designated responsible individuals will build clear expectations and foster informed executives.

4. Advance Cyber Resilience and Preparedness

Ontario should prioritize emergency preparedness resources that facilitate communications and collaboration in the face of adverse events. The curation, validation, and use of critical resources such as incident response playbooks, data recovery, insurance, and communications procedures across BPS stakeholders will be essential to reduce loss and accelerate recovery from cyber security breaches.

5. Evaluate Regional Economic Development

Ontario should evaluate the potential economic impact of concentrating cross-sector cyber security capabilities in communities across the province, building tomorrow’s cyber workforce and spurring innovation in cyber security technologies. This will encourage leadership innovation and cyber security workforce enrichment.

How will the implementation of this core recommendation impact the future of cyber security in Ontario?

Implementing the Expert Panel’s core recommendation in this area will positively benefit Ontario’s economic growth over time. As more BPS organizations participate in cross-sector cyber security programs with a unified set of guiding principles, it will be possible to achieve greater oversight and visibility into Ontario’s cyber landscape. Better visibility means more effective analysis and an enhanced ability to identify and promote new and innovative opportunities, resulting in healthy market growth and entrepreneurship across Ontario’s digital workforce.

Cross-sector collaboration and sharing of resources will foster multifaceted innovation, making Ontario a leader in this space and perpetuating the allure of a steadily growing market to attract top talent—ensuring a robust cyber workforce for the future.

Education and Training

Expert Panel Core Recommendation:

Ontario should continue to develop diverse and inclusive cyber security awareness and training initiatives across all stages of learning, supported by a variety of common and tailored content and hands-on activities.

There is growing popularity of general cyber security awareness in response to the increasing number of threats facing BPS organizations. However, the current programs lack a specific focus on risks and age-specific training, and hands-on experiences tend to reach limited audiences. Cyber security awareness requires further improvement by building foundations in K-12 education, reinforcing specialized programs in higher education, up-skilling the made-in-Ontario workforce, and promoting the availability of continuous learning content and tools to all Ontarians.

Therefore, the Expert Panel recommends the following:

1. Formalize Digital Citizenship and Cyber Security Awareness Foundations for K–12 Students

Ontario should curate age-specific content for K–12 students and embed this in the learning curriculum as provinces like Saskatchewan have done. Educational staff should also receive specific training to improve their awareness of cyber-safe practices to prepare for the delivery and implementation of the curriculum. This approach will promote good digital citizenship and build foundational cyber safe practices for all practitioners involved in K-12 education.

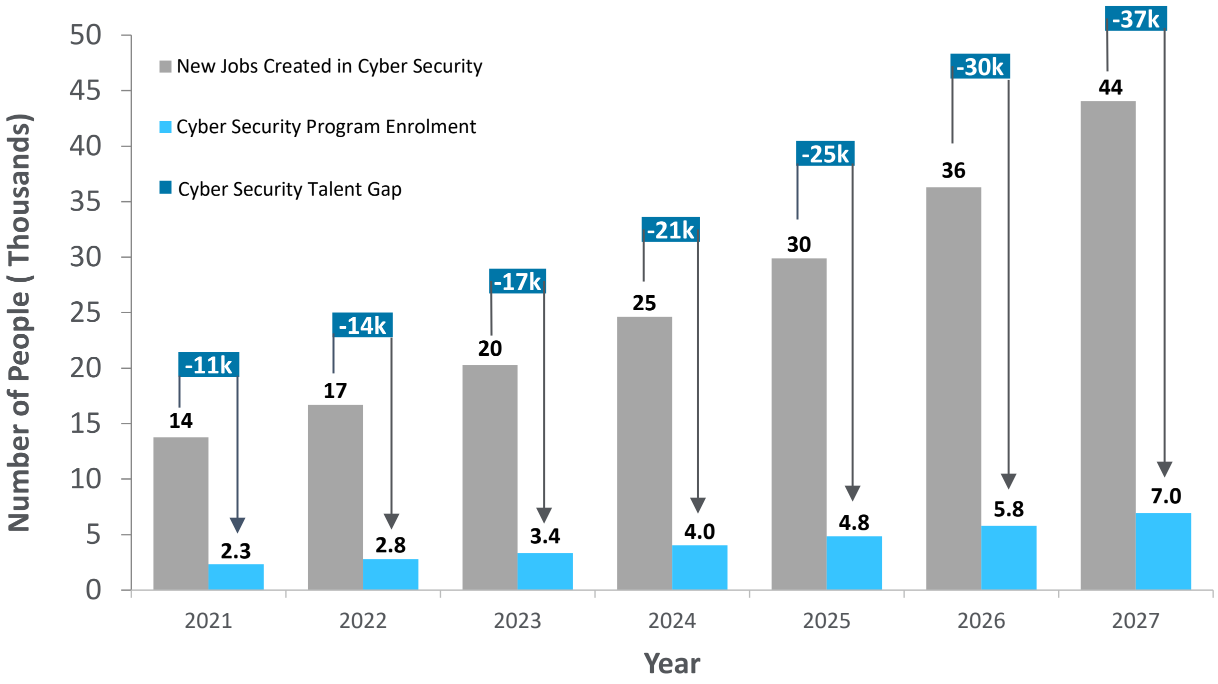
2. Develop Cyber Security Professionals Through Higher Education

Ontario should develop foundational cyber security training and education for all post-secondary students and develop specialized post-secondary programs with integrated experiential pathways. The programming should balance academic learning with hands-on experience facilitated via key partnerships that promote the necessary skill development. This approach will address the growing need for increased employee cyber awareness across all sectors while accelerating training and workforce readiness.

3. Establish a Cyber Workforce Development Program

Ontario should establish a workforce development program that promotes the benefits of careers in cyber security. The recommended focus is on up-skilling a made-in-Ontario workforce through a program designed to address the cyber security talent gap, as evidenced by research on Ontario’s cyber security job market shown in Figure 2 (*(ISC)²: A Resilient Cyber Security Profession Charts the Path Forward*). In addition, a cyber workforce development program will increase Ontario’s overall cyber security capabilities.

Figure 2: Cyber Security Job Market Gap Projections (Ontario)



Source: (ISC)²: A Resilient Cyber Security Profession Charts the Path Forward

4. Continue to Improve and Expand Consistent, Diverse and Inclusive Education and Awareness Initiatives

Ontario should endorse continuous education and awareness campaigns, utilizing various media platforms to be inclusive and diverse-aware. The direction of these campaigns should consider all Ontarians, with customized components to address the diversity of individual (citizen), sector, and organizational (role-based) needs. This approach will empower all Ontarians (individuals and organizations) with increased cyber resiliency.

5. Continue to Develop and Improve Practical Tools for Continuous Cyber Learning

Ontario should continue investing in the development and improvement of the education and awareness content and tools within its cyber portal to align with the changing demographic of Ontarians. This approach includes repositories of sector-specific practical exercises, scenarios for tabletop exercises and phishing campaigns; to reduce barriers and increase cyber resiliency for BPS organizations, encourage re-evaluation of cyber security maturity and promote continuous learning. This plan will reduce uncertainty, encourage resiliency, and enhance maturity in cyber security.

How will the implementation of this core recommendation impact the future of cyber security in Ontario?

Ontario’s future lies in the hands and minds of the province’s youth. Investing in early cyber security awareness, safe digital behaviours, and foundational cyber literacy will promote good digital citizenship and help develop secure cyber practices and digital responsibility among the leaders of tomorrow.

Ontario’s growing cyber workforce will also benefit from increasingly diverse and inclusive cyber security training and awareness initiatives across all stages of learning. Accelerated, hands-on certification programming and provision of continuous cyber education via the development and promotion of practical tools will bolster Ontario’s delivery of digital services, ensuring that citizens have secure and consistent access to critical public services today and into the future.

Communications

Expert Panel Core Recommendation:

Ontario should implement a framework that encourages BPS entities to share information related to cyber security securely and with ease.

Communication amongst BPS organizations is extremely limited, which leads to a siloed, independent approach and a lack of awareness of sector trends. Effective cyber security communication can only be realized with well-defined stakeholders, a commonly recognized platform, cross-sector collaborations, and simplified information sharing processes for the most critical information.

To address the existing communication gap, the Expert Panel recommends the following:

1. Identify Cyber Security Constituents

Ontario should develop and maintain a consolidated list of cyber security stakeholders across the BPS, including an authoritative index of each organization's senior cyber security official, updated annually. This approach will assist identification and management of key stakeholders and foster relationships amongst BPS entities.

2. Continue to Improve and Expand the Existing Common Resource Platform

Ontario should continue to improve and expand the existing platform for BPS organizations to promote and share various common resources such as notifications, training, education, and awareness. Sector-specific information should be integrated to promote a 'one-stop-shop' for cyber security resources across the BPS. This approach will provide a central repository of resources relevant to the BPS and sub-sectors and increase awareness of available cyber security resources and foster a community of like-minded practicioners.

3. Implement a Framework that Promotes Proactive Cross-Sector Communication

Ontario should create a simple structure that promotes the active communication of resources and collaboration amongst the BPS and key government stakeholders. The framework should account for the range of stakeholders (e.g., leaders, employees and citizens) and diverse communication requirements (e.g., general, technical, or sensitive). This approach will drive the sharing of cyber security-related information across the BPS and improve public trust in the handling of sensitive information.

4. Simplify Incident Response Communications

Ontario should establish a unified critical information sharing protocol to ensure quick communication of cyber incidents, threat intelligence, and vulnerabilities amongst BPS organizations. Primary and alternate communication channels (e.g., email and telephone) should be maintained to provide the ability to communicate in the event of a significant incident or outage. This approach will increase the efficiency of information sharing, especially for time-sensitive information and incident response.

How will the implementation of this core recommendation impact the future of cyber security in Ontario?

If structure, knowledge, awareness, and resources are the building blocks of an effective cyber program, communication is the glue that will bring it together and ensure its stability over time. A single-source information sharing platform will generate a robust pool of cyber security incident data, contributed by and accessible to all BPS organizations and sub-sector entities, regardless of size or function. An accessible repository of this type and calibre of cyber data will promote cross-sector understanding of relevant threats, incidents and responses occurring across the province. As such, this level of visibility and transparency will promote enhanced cyber resiliency and preparedness across all sectors of the BPS, where organizations can learn from the experiences of others and take the necessary proactive measures to mitigate potential risks before an incident occurs.

The future of communications within the BPS will see a stronger community of practice and cross-sector support network, empowering all organizations to recognize, defend against, and respond to relevant cyber threats with confidence.

Shared Services

Expert Panel Core Recommendation

Ontario should invest in shared services for cyber resiliency across the broader public sector, considering sector-specific needs where required.

Varying access to funding and resources has resulted in differing levels of cyber capabilities across BPS partners. Small organizations usually suffer more from a lack of technology, expertise, and cyber security insurance. Common and sector-specific supporting resources need to be created or developed to maximize the benefits of existing knowledge and procedures. Current cyber security gaps amongst BPS members can be narrowed through shared investments. This approach will significantly improve overall cyber resiliency across the BPS.

Therefore, the Expert Panel recommends the following:

1. **Standardize Risk Management Resources**

Ontario should develop cyber security risk management resources to help BPS organizations address the risks identified through the assessment framework. Organizations could then adopt or adapt available templated resources such as organizational policies, controls objectives, implementation guides, and assessment metrics aligned to common cyber security standards. This approach will optimize organizational resource allocation and lower BPS vulnerability.

2. **Invest in Shared Security Operations for the BPS**

Ontario should consider how a tiered approach to cyber security operations that builds on organization, sector, and provincial-level capabilities could be adopted to promote collaboration and maximize investment in shared capabilities, talent, and resources. This approach could increase the effectiveness and efficiency of the limited available resources.

3. **Establish Cyber Security Assurance**

Ontario should establish a shared resource or contract vehicle to conduct or independently validate risk and control assessments at regular intervals as part of the cyber security risk management framework. This approach will facilitate the standardization of assessments that will improve risk management and vulnerabilities remediation.

4. **Investigate Options for a Cyber Insurance Program**

Ontario should investigate options for establishing a self-funded cyber insurance program to support the delivery of services such as breach coaching, incident response, and recovery to which all BPS organizations can subscribe. This approach will create a stable and affordable backstop for response and recovery activities in the event of a significant incident.

5. **Shared Procurement**

Ontario should continue improving, expanding, and communicating the capabilities of the Security Vendor of Record Program. This approach will create ready access to cyber security support to allow organizations to focus their limited resources in the most critical areas.

6. **Enhance Digital Resilience and Capabilities**

Ontario should study the 'technical deficit' issue across all sectors and develop creative strategies to close the gap through shared investments. This approach will build a robust digital infrastructure that underpins provincial service delivery to citizens and enables a secure digital economy.

How will the implementation of this core recommendation impact the future of cyber security in Ontario?

Ontario's Broader Public Sector is comprised of a diverse set of organizations representing various sizes, differing access to resources, and assorted cyber capabilities based on function and regulatory requirements. As such, the province recognizes that a one-size-fits-all approach to enhancing the cyber security across the larger BPS is unreasonable and exclusionary.

The future of shared cyber services and resources within Ontario's BPS considers the needs and constraints of organizations across all sectors and offers diverse options that will promote an affordable, standardized level of basic security services and resources across the province that can be nuanced to address sector-specific concerns. Organizations will then have the option to acquire additional security services based on individual requirements to build a customized cyber security program that best fits their needs and budget.

Implementing shared services and resources across the BPS will enhance Ontario's overall cyber security posture by elevating the least mature weakest and will strengthen cyber resilience across the collective by promoting an affordable backstop for response and recovery activities in the event of a significant incident.

Looking Ahead: The Future of Cyber Security Within Ontario's Broader Public Sector

Ontario recognizes that the digital landscape is continuously evolving and that ongoing effort is required on the part of the government to identify, prioritize, and address new security challenges and enhancement opportunities. The recommendations provided by the MPBSD Expert Panel aim to implement new strategies while improving upon the province's existing and ongoing cyber initiatives. The province can achieve these objectives by streamlining existing processes to create clear accountabilities, enhancing existing educational resources, encouraging critical cyber information sharing, and facilitating an acceptable and achievable baseline of cyber security for all organizations across the BPS.

Improvements should be implemented strategically over time, built on a solid foundation of cyber expertise and sector-specific knowledge and resources created through strategic partnerships. Key stakeholders should work together across sectors to expand their existing networks and generate a unified cyber defence mechanism that is stronger, more adaptable, better informed, affordable, and sustainable.

The future of cyber security in Ontario will see cross-sector engagement, participation, and collaboration among all BPS organizations, ensuring consistency in the continuous delivery and accessibility of public service and culminating in a whole that is greater and more resilient than the sum of its parts.

Conclusion

Cyber security is becoming increasingly critical for building convenient, reliable, and accessible government services in a data-driven world. As more and more services incorporate digital technology, the Government of Ontario has launched several initiatives to enhance cyber awareness and cyber resilience across the Broader Public Sector (BPS). While these efforts have helped increase BPS organization's cyber maturity, BPS organizations still require a tailored and flexible approach to achieve the overall cyber security goal. Regardless of the size or mandate of the BPS organization, there is a general desire for more cyber security resources, investments, and expertise.

The Expert Panel believes that building a secure cyber environment to protect Ontario's BPS requires strong governance, continuous education, effective communication, and cross-sector collaboration. Successful implementation of the recommendations in this report will foster a healthy cyber security ecosystem while delivering more convenient services and supporting economic growth to build a more prosperous future for all Ontarians.

In response to Ontario's steadily increasing uptake of digital technology to deliver essential government services, cyber security should remain a top priority for the Minister to mitigate disruptions for its citizens today and into the future.

Appendix A: Terms and Definitions

Australian Cyber Security Centre (ACSC): The Australian Cyber Security Centre leads the Australian Government's effort to improve cyber security by monitoring cyber threats, protecting critical information infrastructure, and collaborating with business, government, and academic partners to develop cyber security solutions.

Broader Public Sector (BPS): Generally, the Broader Public Sector refers to the organizations that receive funding from the Government of Ontario. They are not, however, a part of the government itself. Designated BPS organizations are defined in the *Broader Public Sector Accountability Act*.

Canadian Shared Security Operations Centre (CanSSOC): The Canadian Shared Security Operations Centre investigates the frequency and complexity of cyber security threats targeting higher education institutions. Pilot initiatives are currently underway to leverage the cyber security skills, resources, and tools within Canada's collective higher education community.

Israeli Cyber Emergency Response Team (CERT): The national CERT handles cyber incidents in the civilian cyber sphere of the State of Israel. It is part of the operational unit of the Israeli National Cyber Directorate – a state-run, defense-technological entity devoted to protecting the Israeli cyberspace.

Ministry of Public and Business Service Delivery (MPBSD): The Ministry of Public and Business Service Delivery is an enterprise ministry bringing together business levers to transform and improve government services, both internally to ministries and externally to the public. The long-term vision of the ministry is to deliver simpler, faster, better government services.

Multi-State Information Sharing & Analysis Center (MS-ISAC): MS-ISAC is a non-profit organization designated by the U.S Department of Homeland Security (DHS) to provide cyber threat prevention, protection and response support for the United States government. Their scope of work includes intelligence analysis, national cyber security review, 24/7 information sharing, remediation services, and cyber awareness initiatives.

National Institute for Standards & Technology (NIST): NIST is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce. It is responsible for establishing technology, standards, and metrics to be applied to the science and technology industries. The NIST Cyber Security Framework provides a set of desired cyber security activities and outcomes for organizations to manage and reduce their cyber security risks which has been adopted across many industries and governments around the world.

Ontario Association of Children's Aid Societies (OACAS)/Children's Aid Societies (CAS): Children's Aid Societies are separate, independent organizations that have each been approved by the Ontario government's Ministry of Children, Community and Social Services to provide child protection services. Their goal is to promote the best interests, protection and wellbeing of children.

Ontario Cyber Security Higher Education Consortium (ON-CHEC): ON-CHEC addresses cyber security challenges and raises the cyber security posture of Ontario's research and education community. It provides cost-effective cyber security guidance, programs, and services to meet the needs of Ontario’s research, education, and innovation ecosystem.

Rogers Cybersecure Catalyst: The Catalyst is a national centre owned and operated by Toronto Metropolitan University for innovation and collaboration in cyber security. It collaborates with industry, governments, and academic partners to help Canadians and Canadian companies tackle cyber security challenges and maintain safety in the digital world.

Security Operations Center (SOC): A Security Operation Center is a centralized function that employs people, processes, and technology to continuously monitor and improve an organization’s security posture while preventing, detecting, analyzing, and responding to cyber security incidents.

Vishing: Vishing or often referred to as voice phishing, is a cyber crime where cyber criminals use social engineering tactics to convince victims to share personal information through the use of a phone.

Appendix B: The Cyber Security Expert Panel Member Biographies

Robert Wong, Chair

Mr. Wong is a Board of Director of the Independent Electricity System Operator (IESO), serving on its corporate board and its audit committee, as well as the Principal of Hesketh Sloane Advisory, providing management consulting services. He retired as Executive Vice-President and Chief Information Officer at Toronto Hydro, where his responsibilities included information technology, operational technology, cyber security, and telecommunications. Mr. Wong served on the board, finance & audit committee, and research committee at the Canadian Cyber Threat Exchange (CCTX), and as an executive sponsor of the Protégé Project for Women in Communications and Technology. He holds a Bachelor of Applied Science degree in electrical engineering from the University of Toronto, a Master of Business Administration degree from the Schulich School of Business at York University, and a Chartered Director designation from the Directors College, which is a collaboration between McMaster University and the Conference Board of Canada.

Adam Evans, Vice Chair

Mr. Evans is Vice-President of Cyber Operations and Chief Information Security Officer at the Royal Bank of Canada. His responsibilities include global cyber operations, cyber strategy, cyber crisis management, regulatory compliance for cyber security, industry partnerships and governance. Mr. Evans is a Certified Information System Security Professional (CISSP), Certified Information System Auditor (CISA) and Certified Information System Manager (CISM).

Derek Bowers, Member

Mr. Bowers is the Chief Information Technology Officer for the town of Wasaga Beach. With an honours diploma in computer programming from Georgian College, Mr. Bowers has over 25 years of computer-related experience. Before joining the town, Mr. Bowers provided IT expertise for the Canadian Mental Health Association in Barrie and the Canadian Department of National Defense at CFB Borden. Mr. Bowers sits on the Association of Municipalities of Ontario

Digital Government Task Force and is an active member of the Municipal Information Systems Association (MISA).

Marc Coyle, Member

Mr. Coyle has been the Manager of information technology at the City of Bellville for 30 years. He is the Treasurer for Municipal Information Systems Association (MISA) Canada and former Communications Director & Eastern Region Director for MISA Ontario. Mr. Coyle holds a diploma in computer science from Loyalist College.

Scott Currie, Member

Mr. Currie has held the inaugural Chief Information Security Officer (CISO) role at the Hospital for Sick Children (SickKids) since 2016, and in 2021 he joined the University Health Network (UHN) in his joint role. He has 20 years of experience in Cyber Security, IT Governance, IT Operations, and IT Audit with global consulting organizations, Fortune 100 companies, and technology start-ups. Mr. Currie holds a Bachelor of Arts degree in Economics from Laurentian University and a Master of Information Systems Management degree from Carnegie Mellon University.

Hélène Fournier, Member

Ms. Fournier is Executive Director of Valoris for Children and Adults of Prescott-Russell. She is a member of the Ontario College of Social Workers and Social Services Workers. Ms. Fournier holds a Master of Social Services from Université Laval, a Bachelor of Social Work from Université du Quebec in Gatineau and a Bachelor of Social Services degree with a minor in criminology from the University of Ottawa.

Carolyn Glaser, Member

Ms. Glaser is the General Manager of Information Technology Services for the Thames Valley District School Board. She presently serves as a board member and secretary for the Educational Computing Network of Ontario, a member of the Cyber Protection Strategy Executive Steering Committee, Chair of the Aspen Strategic Management Committee, and a Project Manager Professional with the Project Management Institute. Ms. Glaser has an Undergraduate degree from the University of Waterloo, a Graduate degree from the University of Guelph, and over 20 years of strategic leadership experience in the information technology sector.

Antoine Haroun, Member

Mr. Haroun is Chief Information Officer with the Peel District School Board. He has previously served as Director of Information Technology for the Regional Municipality of Halton, Chief Information Officer at Mohawk College, and as a director with the Ontario Public Service. Mr. Haroun has served as a board member with the Chief Information Officer Association of Canada (Toronto Chapter). He holds both a bachelor's and master's degree in applied science and civil engineering from the University of Toronto.

Andrew Kirsch, Member

Mr. Kirsch served as an intelligence officer with the Canadian Security Intelligence Service (CSIS) for just under a decade. He held roles as a policy analyst and a field investigator, ultimately leading the special operations security team running covert warranted technical surveillance operations. Today, he runs a security consulting firm, assisting organizations and individuals identify threats and vulnerabilities and implement strategies to mitigate their risk. Prior to starting his firm, Mr. Kirsch was the first Department Security Officer at Ontario's Office of the Provincial Security Advisor, with a mandate to enhance physical, personnel, information and network security across the Ontario Public Service.

Isaac Straley, Member

Mr. Straley is the Chief Information Security Officer (CISO) at the University of Toronto (U of T). Mr. Straley has held this inaugural U of T position since December 2018. Previously, he held the dual post of both CISO and Privacy Officer at the University of California, Irvine, where he was for 13 years. In his current role, Mr. Straley has oversight of the Information Security program, ensuring U of T's networks, systems and information are protected and meeting regulatory and policy requirements. He is also responsible for identifying, evaluating, and reporting information security risks to the Information Security Council and the University's senior administrative team. Mr. Straley was named CISO of the year at the CISO Forum Canada in 2021.