Groupe d'experts en cybersécurité du ministère des Services au public et aux entreprises (MSPE) de l'Ontario

Cybersécurité dans le secteur parapublic de l'Ontario

RAPPORT

au ministre des Services au public et aux entreprises de l'Ontario

2022

Ontario

Table des matières

Message du Groupe d'experts en cybersécurité dans le secteur parapublic

L'intérêt pour les enjeux de cybersécurité n'a cessé de croître au cours des dernières années. Le secteur public et l'ensemble de la population de l'Ontario sont confrontés à toute une gamme de cyberrisques, qu'il s'agisse de rançongiciel restreignant l'accès à des données critiques ou de logiciels malveillants perturbant les activités d'infrastructures essentielles. En plus de l'interruption de services critiques, les cyberrisques entraînent des conséquences financières importantes qui incluent, entre autres, la perte de données critiques, l'inaccessibilité à des systèmes essentiels et les coûts associés à la réponse à un événement majeur et la restauration des systèmes qui s'en suit. En cette période où la prestation des services publics repose de plus en plus sur des systèmes numériques, il est indispensable que le gouvernement de l'Ontario, les organismes du secteur parapublic et les experts en cybersécurité travaillent de concert pour aborder les enjeux de cybersécurité.

Le Groupe d'experts en cybersécurité (« le Groupe d'experts ») a réuni des experts reconnus en technologies de l'information (TI), en technologie opérationnelle (TO), en gestion des risques, en éducation à la cybersécurité et en application des règlements pour analyser la situation actuelle en Ontario. Dans le cadre de son mandat d'identification des enjeux de sécurité rencontrés par les organismes du secteur parapublic et de formulation de recommandations pour améliorer la cyberrésilience globale en Ontario, le Groupe d'experts a animé au cours des dernières années une variété de conférences, d'ateliers et d'entretiens, recueillant au passage des données requises à ses analyses. Le présent rapport est rendu possible par les efforts conjoints et l'engagement de divers professionnels et intervenants du secteur parapublic et public.

Nous avons pu observer au cours de notre recherche que, peu importe le profil de risque et les capacités des organismes, trop peu d'entre eux ont développé une forte gouvernance en matière de cybersécurité. Par conséquent, nous estimons que les organismes devraient accorder à la gouvernance une place de choix dans l'élaboration de leurs stratégies de cybersécurité. Un plan complet de gouvernance devrait définir des normes de cybersécurité, une politique et un cadre de travail, des niveaux de maturité et des pratiques exemplaires; élaborer une feuille de route et un guide numérique; mettre sur pied un service consultatif et une chaîne de communication des risques; et organiser un milieu favorisant la capacité des organismes à intervenir et à se relever plus rapidement à la suite de cyberincidents.

Étant donné que de nombreux organismes du secteur parapublic éprouvent des difficultés à gérer les cyberrisques en raison du manque de ressources, nous recommandons en outre que des mandats d'évaluation des risques soient coordonnés selon les directives du cadre de cybersécurité du National Institute of Standards and Technology (NIST). L'évaluation des risques peut être complétée en interne ou par l'intermédiaire de services partagés régionaux, selon la disponibilité des ressources et des compétences en cybersécurité des organismes. L'adoption collective d'un cadre de cybersécurité favorise des politiques et un suivi cohérents; un avantage dont profitera l'ensemble du secteur parapublic.

Le présent rapport inclut en outre des constats et recommandations supplémentaires qui ont pour objet de donner au gouvernement de l'Ontario les moyens d'optimiser son encadrement des organismes du secteur parapublic et de ses partenaires de prestation de services. Au nom du Groupe d'experts en cybersécurité, je tiens à exprimer notre sincère reconnaissance envers toutes les personnes qui ont pris le temps de partager leur

expérience et leurs points de vue avec le Groupe d'experts. Votre contribution est d'une valeur inestimable, tant dans la formulation des présentes recommandations que dans la création d'un environnement numérique sûr pour l'Ontario de demain.

Cordialement,

Robert Wong

Président du Groupe d'experts en cybersécurité dans le secteur parapublic

Sommaire

Le ministère des Services gouvernementaux et des Services aux consommateurs, désormais nommé ministère des Services au public et aux entreprises (MSPE), a mis sur pied le Groupe d'experts en cybersécurité dans le secteur parapublic en 2020 pour aider les communautés, les organismes et les entreprises de l'Ontario à améliorer leur cyberrésilience. Il s'agit notamment de sensibiliser et d'aider la population de l'Ontario à mieux comprendre les changements numériques qui propulsent les entreprises et leurs activités au quotidien, et à s'y adapter. Le renforcement de la cyberrésilience est vital aux succès de demain en Ontario.

Le mandat du Groupe d'experts consiste à :

- Identifier et évaluer les thèmes et les enjeux qui touchent les organismes du secteur parapublic et les partenaires de prestation de services de l'Ontario, dans son ensemble et par secteurs;

- Examiner les mesures de cybersécurité du gouvernement et les efforts de réduction des risques dans les divers secteurs parapublics et formuler des recommandations connexes; et

- Fournir des conseils au ministère des Services au public et aux entreprises sur des sujets précis par l'intermédiaire de rapports officiels afin d'améliorer la posture de cybersécurité du secteur parapublic.

Au cours de ce mandat, le Groupe d'experts vise le renforcement de la cybersécurité au sein du secteur parapublic. Le Groupe d'experts a déterminé cinq principes directeurs pour s'assurer que ses recommandations et stratégies répondent aux besoins du secteur parapublic de façon durable et efficace. Les principes directeurs englobent des questions d'intérêt public, de gouvernance, de soutien à l'éducation, de responsabilisation des intervenants et de facilitation d'améliorations continues de la cybersécurité au sein de divers organismes.

Guidé par ces principes directeurs, le Groupe d'experts a examiné la situation actuelle en matière de cybersécurité de l'Ontario dans les secteurs de l'éducation, des services de bien-être de l'enfance, de la santé, des espaces municipaux et dégagé des enjeux communs et spécifiques aux secteurs.

Afin d'améliorer la cyberrésilience au sein du secteur parapublic, le Groupe d'experts a fondé ses recommandations sur quatre des principaux enjeux identifiés, lesquels reflètent les besoins particuliers de la province de l'Ontario et orientent les efforts conjoints des intervenants de son écosystème pour y répondre. Les observations du Groupe d'experts ont été regroupés en quatre thèmes principaux, assortis de recommandations :

1 Gouvernance et modèle opérationnel

Enjeu : Il n'y a actuellement aucune cohérence à l'égard des politiques, des procédures et de la responsabilisation au sein des structures de gouvernance du secteur parapublic. Les

initiatives en matière de cybersécurité sont déployées simultanément dans les différents secteurs, sans toutefois répondre à un modèle commun ou à une coordination centralisée. Bien que plusieurs grands organismes soient activement engagés dans l'évaluation des risques et de la maturité, d'autres organismes, plus petits, souffrent disproportionnellement d'un accès limité aux ressources et aux compétences communes en gestion des cyberrisques.

Recommandation : Le gouvernement de l'Ontario devrait renforcer la structure de gouvernance existante pour favoriser une gestion efficace des cyberrisques dans l'ensemble du secteur parapublic.

2 Éducation et formation

Enjeu : Une lacune en matière de ressources éducatives sur la cybersécurité adaptées aux divers risques et aux groupes d'âge a été observée à l'échelle de la province. Le programme scolaire de la maternelle à la 12e année (K-12) ne comprend pas suffisamment d'objectifs relatifs aux environnements numériques, tandis que les programmes d'éducation supérieure offrent des formations spécialisées, mais limitées en possibilités d'expérience pratique. Des programmes de formation intégrée sont en cours de développement en réponse à la demande croissante de contenus relatifs aux environnements numériques; il convient cependant qu'un large auditoire puisse profiter de l'accès à ces ressources.

Recommandation : Le gouvernement de l'Ontario devrait poursuivre l'élaboration d'initiatives diversifiées en matière de sensibilisation à la cybersécurité adaptées à tous les niveaux d'éducation et assortir ces initiatives d'une variété de contenus généraux et spécialisés et d'activités pratiques.

3 Communications

Enjeu : Les communications sont limitées au sein du secteur parapublic en raison de composants de cybersécurité mal définis et de la méconnaissance des plateformes communes. Des protocoles de partage des renseignements existent actuellement pour informer le gouvernement en cas d'incident, mais ces protocoles ne servent pas l'ensemble du secteur parapublic. Il convient que toute entité au sein du secteur parapublic soit mise au courant des canaux de communication au sein de son réseau pour favoriser et améliorer la cyberrésilience actuelle.

Recommandation : Le gouvernement de l'Ontario devrait mettre en œuvre un cadre qui favorise le partage des protocoles de cybersécurité dans l'ensemble du secteur parapublic.

4 Services partagés

Enjeu : Les niveaux de sensibilisation à la cybersécurité et les normes et cadres de cybersécurité des organismes du secteur parapublic sont inégaux. Comparativement aux grands organismes, la gestion des cyberrisques des entités de plus petite taille est insuffisante, notamment à l'égard des plans d'intervention et de rétablissement en cas d'incident. Il s'agit pourtant de compétences devenues aujourd'hui fondamentales et qui

sont en outre requises pour souscrire à une police d'assurance cyberrisque. Par conséquent, l'acquisition d'une police d'assurance cyberrisque devient de plus en plus difficile et coûteuse pour les petits organismes en raison des exigences grandissantes en matière de cybersécurité et du manque de personnel qualifié qui s'y consacre.

Recommandation : Le gouvernement de l'Ontario devrait poursuivre l'élaboration et l'optimisation des services partagés et des contrats en matière de cyberrésilience et étendre leur portée à l'ensemble du secteur parapublic en tenant compte des besoins sectoriels distincts.

Le gouvernement de l'Ontario reconnaît que l'écosystème numérique est en constante évolution et que des efforts continus sont requis de sa part pour identifier et établir ses priorités et pour faire face à de nouveaux défis de sécurité tout en embrassant les nouvelles possibilités. Les recommandations émises par le Groupe d'experts visent à mettre en place de nouvelles stratégies tout en apportant des améliorations aux initiatives de cybersécurité déjà en cours en Ontario. La province est en mesure d'atteindre ces objectifs en rationalisant les procédures existantes et les responsabilités, en optimisant les ressources éducationnelles, en favorisant le partage des protocoles de cybersécurité dans les réseaux et en guidant l'établissement d'une norme acceptable et atteignable de cybersécurité dans l'ensemble du secteur parapublic.

Les améliorations, fondées sur de solides connaissances et des compétences en cybersécurité ciblées, seront progressivement et stratégiquement mises en œuvre au moyen de ressources issues de partenariats stratégiques. Les intervenants provenant des principaux secteurs travailleront de concert pour étendre la portée des réseaux existants et mettre en place un mécanisme unifié de cyberdéfense plus fort, plus adaptatif, mieux informé, à la fois abordable et durable.

L'avenir de la cybersécurité passe par l'engagement intersectoriel, la participation et la collaboration des organismes du secteur parapublic. Ce tout, bien plus grand et résilient que la somme de ses parties, résultera en une cohérence en matière de prestation de services publics accessibles partout en Ontario.

Introduction

L'évolution rapide des technologies et leur récente intégration accélérée ont changé notre vision de l'avenir du travail. Les entreprises, et la société en général, sont plus que jamais dépendantes des systèmes numériques, tant pour leurs interactions que pour leurs transactions. La transition numérique actuelle a engendré des avantages remarquables, tout en introduisant de nouveaux risques dans l'économie. Les environnements numériques sont en constante évolution et les besoins en ressources pour prévenir les cyberrisques ne font que grandir.

Le ministère des Services au public et aux entreprises (MSPE) a créé le Groupe d'experts en cybersécurité (« le Groupe d'experts ») en 2020 dans le cadre de la *Stratégie ontarienne de cybersécurité de 2019-2020 à 2022-2023*. Depuis sa création, le Groupe d'experts a dirigé des initiatives collaboratives pour déterminer les enjeux communs et sectoriels, pour fournir des conseils pour améliorer la cyberrésilience et pour forger un avenir numériquement sûr pour le secteur parapublic de l'Ontario.

Dans le cadre du présent rapport, le Groupe d'experts a évalué l'état actuel de la cybersécurité de quatre (4) secteurs parapublics (programme scolaire K-12, programmes d'éducation supérieure, services de bien-être de l'enfance, et municipalités). Les recommandations qui y sont émises font appel à de nouvelles et d'actuelles compétences au sein du secteur parapublic. Les recommandations s'appliquent aux divers secteurs parapublics et visent les objectifs suivants :

- Accroître les connaissances et les compétences des organismes du secteur parapublic afin que les contrôles appropriés soient mis en place pour réduire les risques et les menaces sur l'écosystème numérique;
- Améliorer la cyberrésilience et la posture de cybersécurité des organismes du secteur parapublic;
- Éviter la fermeture et l'interruption des activités des entreprises causées par des failles de cybersécurité;
- Améliorer la préparation aux situations d'urgences pour accélérer la récupération de données et la reprise des services dans le cas d'une faille de cybersécurité.

Définition du secteur parapublic

Le secteur parapublic est composé de divers organismes partenaires du gouvernement participant à la prestation de services dans divers secteurs à l'échelle de la province. Chacun de ces secteurs est caractérisé par des organismes de tailles et de capacité différentes et dont l'accès à diverses ressources est varié.

La *Loi de 2010 sur la responsabilisation du secteur parapublic* désigne comme faisant partie du secteur parapublic les organismes suivants :

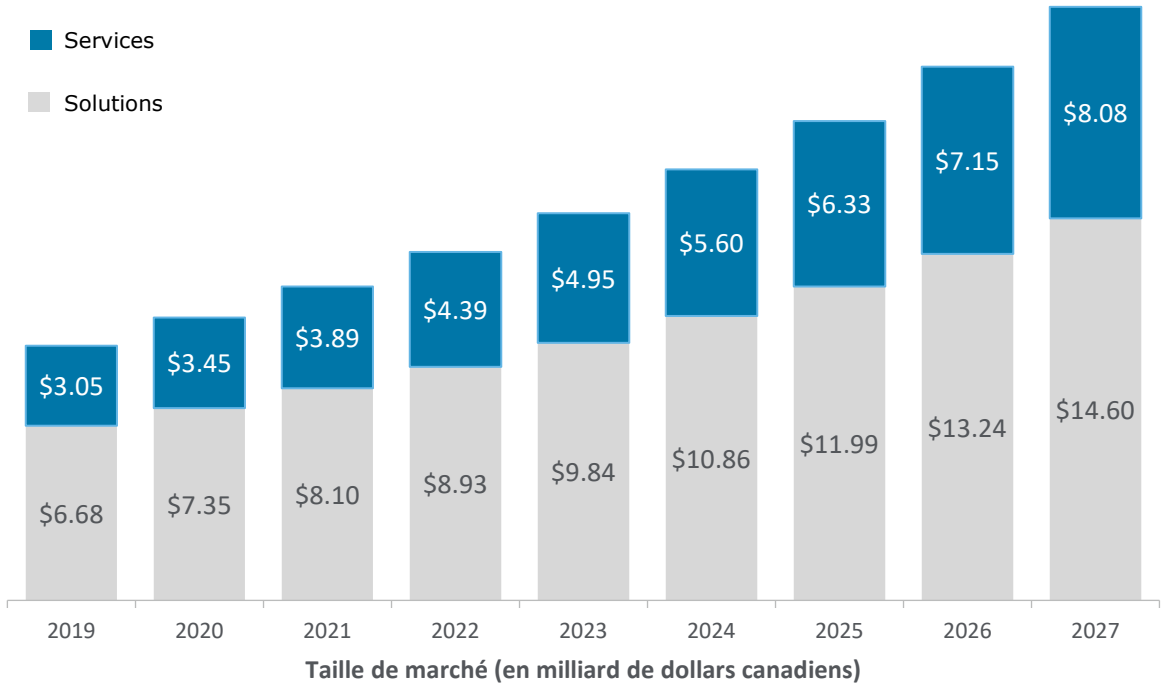
- les hôpitaux;
- les conseils scolaires;
- les universités de l'Ontario, les collèges d'arts appliqués et de technologie et les établissements postsecondaires de l'Ontario;

- les sociétés d'aide à l'enfance;
- les sociétés d'accès aux soins communautaires;
- les personnes morales contrôlées par un ou plusieurs organismes désignés du secteur parapublic dont la mission exclusive ou principale consiste à acheter des biens ou des services pour le compte d'un ou de plusieurs organismes désignés du secteur parapublic; et
- les organismes financés par des fonds publics qui ont reçu des fonds publics totalisant au moins 10 millions de dollars du gouvernement de l'Ontario.

Rôle critique de la cybersécurité dans le programme du secteur parapublic

Compte tenu de la sophistication grandissante des cyberattaques et de la hausse des dépenses en services et solutions de cybersécurité, il est prévu que la demande en la matière continue de croître de manière significative au cours de la prochaine décennie, et qu'elle dépasse l'offre. Comme illustré à la figure 1, une croissance composée annuelle de 12 % est anticipée sur le marché de la cybersécurité au Canada, atteignant une taille de marché de 22,68 milliards de dollars canadiens d'ici 2027 (*Allied Market Research Analysis – en anglais*). Toutefois, bien que la transition numérique ait généré de nombreux avantages pour les organismes, l'étendue et le niveau de maturité des compétences des organismes ont posé des défis de gestion des cyberrisques et l'adoption de solutions de cybersécurité.

Figure 1 : Projections du marché de la cybersécurité au Canada, de 2019 à 2027 (milliard)



Source : AMR Analysis

Le gouvernement de l'Ontario accorde une grande valeur à la cybersécurité dans le cadre de son engagement en matière de prestation de services. Compte tenu de la variété de la taille

des organismes du secteur parapublic et des secteurs qu'ils représentent, l'approche en matière de cybersécurité doit être concertée tout en restant adaptative afin de protéger, soutenir, connecter et équiper l'ensemble de ces organismes et d'assurer leur succès dans notre monde numérique. Le renforcement de la cyberrésilience crée un environnement favorable aux affaires dans la province de l'Ontario et prévient d'éventuelles perturbations tout en protégeant les données et en gardant la confiance du public. De plus, des capacités robustes en cybersécurité profitent à toute la population de l'Ontario en assurant la continuité des services publics essentiels, dont les services d'urgence, les programmes scolaires et d'éducation supérieure, les services gouvernementaux et les soins de santé.

Présentation du Groupe d'experts en cybersécurité dans le secteur parapublic

Mandat et position du Groupe d'experts concernant la cybersécurité

La cybersécurité est de plus en plus considérée comme un enjeu stratégique qui touche l'ensemble de la société. Elle constitue en outre un aspect essentiel à la réalisation de la *Stratégie ontarienne pour le numérique et les données*. Le Groupe d'experts a pour objet d'aider les communautés, les organismes et les entreprises à s'adapter et à réussir dans une ère numérique en mouvance. Pour renforcer la cyberrésilience du secteur parapublic, le Groupe d'experts a reçu le mandat de :

- Identifier et évaluer les thèmes et les enjeux rencontrés par les organismes du secteur parapublic et les partenaires de prestation de services de l'Ontario, dans son ensemble et par secteurs;
- Évaluer les efforts déployés par le gouvernement pour la gestion des cyberrisques au sein du secteur parapublic et de formuler ses recommandations;
- Fournir son conseil au ministère des Services au public et aux entreprises par l'intermédiaire de rapports officiels sur des sujets déterminés et la production d'un rapport final présentant ses conclusions, ses analyses, ses recommandations au gouvernement, une stratégie détaillée de cybersécurité dans le secteur parapublic et des options pour améliorer la posture de cybersécurité du secteur parapublic.

Principes directeurs du Groupe d'experts

Le mandat du Groupe d'experts en cybersécurité consistant à analyser, à conseiller et à émettre ses recommandations au ministère des Services au public et aux entreprises sur les moyens à mettre en œuvre pour améliorer la cybersécurité au sein du secteur parapublic est d'une importance vitale, tout particulièrement dans un contexte où les cyberattaques ciblent sans distinction tous les secteurs d'activités.

Les principes directeurs ont été fournis pour s'assurer que les stratégies et les recommandations émises par le Groupe d'experts sont efficaces et ont une portée à long terme. Les cinq principes directeurs auxquels le Groupe d'experts a fait appel pour déterminer ses stratégies numériques dans le secteur parapublic sont les suivants :

- Être d'intérêt public;
- Stimuler le leadership;
- Soutenir l'éducation;
- Favoriser la responsabilisation individuelle des intervenants;
- Faciliter des améliorations continues en matière de cybersécurité; et
- Adopter une approche rentable pour accroître les capacités en cybersécurité.

Adoption d’une méthodologie

La Stratégie ontarienne de cybersécurité (« la Stratégie ») fournit un cadre stratégique pour guider le renforcement de la cybersécurité, l’optimisation des capacités et l’atteinte des niveaux de maturités requis du secteur parapublic. Il s’agit notamment de former un Groupe d’experts en cybersécurité, d’accroître les collaborations entre le gouvernement et le secteur parapublic et d’assurer une protection continue des applications gouvernementales.

Au cours de son mandat, le Groupe d’experts a adopté l’approche mise de l’avant dans la Stratégie pour recueillir les données, élaborer ses plans de recherche, consulter les diverses agences du secteur parapublic, impliquer les intervenants du secteur parapublic et publier ses résultats et autres rapports connexes. Le Groupe d’experts a rapporté divers constats en analysant l’état actuel de la cybersécurité — en tenant compte des programmes et des infrastructures de cybersécurité existants du gouvernement — et a soumis ses recommandations au Ministère pour leur acceptation.

Le Groupe d’experts et les sous-comités ont travaillé en étroite collaboration avec la Division de la cybersécurité relevant du ministère des Services au public et aux entreprises (MSPE) pour recueillir divers points de vue et formuler ses recommandations. Les approches, les activités, les rôles et les responsabilités de chacun sont décrits en détail ci-dessous.

Le Groupe

Le Ministère a réuni un groupe d’experts pour identifier les enjeux communs et spécifiques aux secteurs en matière de cybersécurité dans le secteur parapublic et pour développer différentes approches de prévention des cyberrisques compilées dans une stratégie de cybersécurité du secteur parapublic. Les membres du Groupe d’experts (voir l’*annexe B*) représentent le Groupe d’experts lors d’événements publics, fournissent une expertise pour le développement de plans de recherche et des recommandations pour orienter les décisions concernant les politiques de cybersécurité du gouvernement, conformément au mandat confié par le ministère des Services au public et aux entreprises.

Le rôle du Groupe d’experts consiste à établir des priorités pour faciliter la prise de décision relative aux enjeux déterminés et de partager ses constats et des recommandations avec le Ministère.

Au cours du processus de production des rapports, le Groupe d’experts a pris les mesures immédiates suivantes :

- Accueil de deux conférences sur la cybersécurité avec la participation d’intervenants du secteur parapublic pour évaluer les lacunes en cybersécurité du secteur et proposer des solutions potentielles;
- Animation de nombreux ateliers sur la cybersécurité pour les sociétés d’aide à l’enfance et le secteur de la santé et soutien de Santé Ontario pour accélérer son intégration au modèle opérationnel régional;
- Consultation auprès du centre d’innovation Rogers Cybersecure Catalyst de l’Université métropolitaine de Toronto pour établir un partenariat pour le soutien des professionnels à la mi-carrière effectuant une transition vers une profession du secteur numérique; et

- Analyse des pratiques numériques adoptées par les autorités administratives dans divers pays et régions du monde pour orienter les recommandations du Groupe d'experts.

Sous-comités

La présidence du Groupe d'experts a établi les sous-comités suivants pour porter ses travaux :

- Gouvernance et modèle opérationnel;
- Éducation et formation;
- Communications et intervenants; et
- Services partagés et ressources.

Chacun des sous-comités est chargé d'effectuer une étude approfondie de la cybersécurité au sein de leurs domaines respectifs et de produire un rapport présentant leurs constats, les lacunes observées et leurs recommandations au Groupe d'experts. Les travaux des sous-comités ont contribué à la production du rapport final de Stratégie de cybersécurité dans le secteur parapublic.

Identification des risques associés au secteur parapublic

Les organismes du secteur parapublic fournissent des services à diverses populations. L'ensemble des services du secteur parapublic, qu'ils soient destinés au public ou en interne, sont caractérisés par des profils de risques variés. Ces profils de risque sont mesurés selon le degré de numérisation du service et le type de données traitées. Pour maintenir son intégrité, le secteur parapublic doit protéger les données critiques recueillies par ses systèmes et offrir une prestation habile et continue de services à la population de l'Ontario.

Une prise de conscience des cyberrisques communs qui guettent le secteur parapublic est essentielle pour comprendre l'importance d'une forte cybersécurité. Voici quelques exemples de conséquences défavorables :

1. **Interruption des activités**

La fiabilité et l'accès continu aux infrastructures essentielles encadrées par des organismes du secteur parapublic (p. ex., routes, édifices, établissements de soins de santé, systèmes d'aqueduc, etc.) constituent un aspect fondamental de la prestation de service réussie. La défaillance de telles infrastructures est susceptible de causer une interruption d'activités portant atteinte à la sécurité de la population.

2. **Brèche de données critiques**

De nombreux organismes du secteur parapublic recueillent des données critiques, notamment de l'information gouvernementale et des renseignements personnels (p. ex., nom, NAS, passeport, adresse). Une brèche de ce type de renseignements est associée au risque de vol d'identité ou à d'autres activités frauduleuses.

3. **Atteinte à la sécurité publique et confiance**

Le secteur parapublic fournit de nombreux services sur lesquels la population compte (p. ex., programme d'éducation et d'aide à l'enfance, soutien à l'accessibilité et services d'aide à l'emploi). L'interruption ou la perte de tels services ébranle la confiance que la population accorde au secteur parapublic et compromet la sécurité publique.

4. **Atteinte à la propriété intellectuelle**

Les organismes du secteur parapublic tels que les universités et les collèges conservent des dossiers de recherches confidentielles, des secrets industriels et divers documents détenant des droits de propriété intellectuelle, lesquels sont susceptibles de faire l'objet d'un vol ou d'être perdus s'ils ne sont pas consignés et protégés de manière adéquate.

5. **Pertes financières**

De nombreux organismes et services du secteur parapublic conservent des données financières (p ex., paiements de frais de service, subventions). Une brèche de ce type de données confidentielles est susceptible d'engager des pertes financières pour les organismes et les individus.

Analyse de la situation actuelle

Le Groupe d'experts a examiné les pratiques en matière de cybersécurité dans le secteur parapublic et des administrations de premier plan pour identifier les possibilités de renforcement des pratiques actuelles. Cette analyse a aidé à déterminer la posture de cybersécurité actuelle en Ontario et à formuler les recommandations appropriées.

Pour caractériser la posture de cybersécurité actuelle du secteur parapublic, le Groupe d'experts a consulté divers organismes et intervenants des secteurs de l'éducation (scolaire et postsecondaire), d'aide à l'enfance, de la santé et des espaces municipaux. Le Groupe d'expert a partagé dans son rapport les enjeux communs et sectoriels identifiés au sein du secteur parapublic pour favoriser une meilleure compréhension de ses perspectives à cet égard.

Évaluation des principales pratiques en cours

De nombreux organismes du secteur parapublic ont lancé des initiatives pour renforcer leur cybersécurité. Plusieurs de ces initiatives pluriannuelles centralisent l'offre de services généraux et spécialisés en matière de cybersécurité. L'évaluation des principales pratiques a repris les quatre thèmes du Groupe d'experts :

Thème 1 : Gouvernance et modèle opérationnel

- Santé Ontario a mis en place un projet pilote mettant en place six centres régionaux d'opérations de sécurité et des mécanismes de gouvernance à l'échelle régionale. Ce projet a pour but de mobiliser le secteur de la santé vers une vision concertée de la sécurité et de mettre en évidence les aspects de la responsabilisation à différentes échelles, soit la gouvernance, les services, les processus, l'octroi des contrats, les communications, l'écosystème des fournisseurs. Il détermine en outre les résultats attendus.
- Le Canadian Shared Security Operating Center (CanSSOC) centralise les opérations de sécurité d'établissement d'enseignement supérieur, s'attaquant aux cybermenaces d'un seul front uni.
- L'Association ontarienne des sociétés d'aide à l'enfance (AOSAE) a recours aux services de l'Information Technology Network Group pour assurer la coordination technologique et la cybersécurité des organismes d'aide à l'enfance.
- Simcoe County travaille auprès du MSPE pour adapter le modèle de centre régional d'opérations de sécurité de Santé Ontario à son contexte régional.

Thème 2 : Éducation et formation

- Le ministère de l'Éducation a lancé un programme pilote de cybersécurité (K-12 Cyber Protection Strategy) pour aborder le besoin grandissant de protéger davantage les personnes mineures et les jeunes enfants contre les menaces provenant d'environnements numériques. Ce programme inclut un champ de travail entièrement dédié à l'élaboration de ressources d'éducation au numérique pour le secteur.

- Santé Ontario a mis en place un programme d'activités prioritaires et rapidement réalisables de sensibilisation et d'évaluation, notamment d'un centre de formation pour le secteur de la santé (Health Sector Training Hub) qui fournit une sélection d'outils et de ressources éducatives.
- Divers établissements offrent des programmes professionnels en lien avec le numérique de premier et deuxième cycles (p. ex., des programmes de premier et deuxième cycle de l'Université de Toronto avec concentration en protection de l'identité, des renseignements personnels et de la sécurité, un diplôme en cybersécurité au Collège Seneca, et le centre d'innovations Rogers Cybersecure Catalyst de l'Université métropolitaine de Toronto).
- Le MSPE, entre autres, a établi un partenariat avec le centre d'innovations Rogers Cybersecure Catalyst de l'Université métropolitaine de Toronto pour soutenir l'éducation et la formation (incluant des exercices pratiques) du secteur parapublic.
- Le MSPE a déjà rendu accessibles plusieurs modules sur le Portail de l'Ontario pour l'apprentissage pour la cybersécurité qui couvrent une variété de sujets concernant la cybersécurité et qui ont pour objectif de prépare les organismes aux défis d'un avenir de plus plus numérique.
- Le MSPE organise une conférence annuelle sur la cybersécurité pour le secteur parapublic (depuis 2020), accueillie par le Centre d'excellence en cybersécurité de l'Ontario.

Thème 3 : Communications

- Le MSPE a lancé le Portail de l'Ontario pour l'apprentissage pour la cybersécurité; le secteur parapublic peut y partager ses défis, ses ressources et son expertise.
- CanSSOC encourage la mise à profit des renseignements en matière de cybermenace entre les établissements d'enseignement supérieur et leurs partenaires à l'échelle locale, provinciale et nationale afin de les aider à prévenir des cyberattaques et des brèches de données tout en améliorant l'efficacité de la sécurité et en réduisant les coûts qui y sont associés.
- Les sociétés d'aide à l'enfance ont mis sur pied un réseau d'échange de renseignements pour optimiser la détection de cybermenaces nuisant à des organismes similaires.
- Le secteur de la santé, de l'éducation et les municipalités favorisent des communications intersectorielles proactives dans leurs stratégies numériques respectives.
- Le MSPE a initié des pratiques communes et établi un système de notification des menaces pour promouvoir la sensibilisation à la cybersécurité au sein du secteur parapublic.

Thème 4 : Services partagés

- Les centres régionaux d'opérations de sécurité de Santé Ontario et du MSPE servent de modèles pour la conception de services partagés de gestion des cyberrisques au

sein des différents secteurs du parapublic tout en menant le secteur de la santé vers une approche mature en matière de cybersécurité.

- Le programme pilote de cybersécurité du ministère de l'Éducation propose une stratégie pour le partage des ressources en gestion des cyberrisques spécifiques au secteur de l'éducation. De plus, un projet de centre régional de cybersécurité (K-12 Regional Cyber Hubs) prévoit offrir des services de sécurité axés sur le secteur de l'éducation au cours de l'année qui vient.
- L'Ontario Cybersecurity Higher Education Consortium (ON-CHEC) offre des conseils pour une approche rentable de la cybersécurité, des programmes de formation et des services, notamment en établissant des normes de références à atteindre en matière de cybersécurité générale et de préparation en cas d'incident numérique dans les collèges et les universités de l'Ontario.
- En plus d'avoir établi une chaîne de communication des risques, CanSSOC a élaboré une suite d'outils de détection et de préparation aux incidents numériques pour ses établissements universitaires membres partout au Canada.
- Les sociétés d'aide à l'enfance ont mis sur pied un mécanisme d'approvisionnement pour soutenir les organismes pour leurs évaluations annuelles de sécurité, de vérification de la vulnérabilité et de simulation d'intrusion des systèmes. De plus, certains organismes d'aide à l'enfance ayant des ressources humaines et budgétaires dédiées à la cybersécurité partagent de façon informelle ces avantages dans leur région.
- Le comté de Grey explore actuellement la possibilité de partager les ressources en cybersécurité de 30 municipalités entre elles.
- Le Programme de gestion des contrats du MSPE détermine des modalités en matière de cybersécurité pour l'approvisionnement de services d'un ou de plusieurs fournisseurs qualifiés.

Enjeux identifiés

L'avenir de l'Ontario en ce qui concerne les opérations de cybersécurité repose sur une série d'entités provenant de divers secteurs, mais chargés de la prestation de services similaires au moyen de ressources comparables. Plusieurs secteurs et organismes parapublics se dirigent déjà dans la bonne direction, comme le témoignent leurs activités en cours. Toutefois, de nombreux enjeux doivent être abordés afin de répondre au besoin toujours prépondérant en Ontario de créer une culture de la cybersécurité et une sensibilisation aux cyberrisques au sein du secteur parapublic.

Thème 1 : Gouvernance et modèle opérationnel

La gouvernance et les modèles opérationnels existants ne sont généralement pas suffisants relativement aux risques associés à la cybersécurité dans le secteur parapublic. Dans la plupart des cas, les cybermenaces sont considérées comme un risque important, mais les ressources allouées ne suffisent pas à les prévenir.

Les enjeux identifiés sont :

- Une lacune en matière de normes, de politiques et de procédures pour soulever des enjeux de cybersécurité ou trop peu de sensibilisation à l'égard d'une gouvernance polyvalente dans le secteur parapublic.
- Les stratégies numériques et les notions de responsabilisation sont diversifiées ou très centrées sur leur propre secteur; elles ne correspondent pas à l'objectif d'une stratégie ou d'une vision commune au sein du secteur parapublic.
- Bien que des organismes de plus grande taille effectuent de façon proactive des évaluations du risque et de maturité, il manque de cohésion à cet égard entre les secteurs et les organismes. Les plus petits organismes ont rarement mis en place de telles procédures en raison du manque de mise en commun des ressources pour les aider à comprendre et aborder les risques associés au numérique.
- Les organismes ne sont pas tous dotés de ressources humaines en cybersécurité, de procédures ou de politiques.
- Ils emploient des normes et des cadres de gestion de la cybersécurité plutôt variés. Par conséquent, il convient que les organismes collaborent pour mettre en place des indicateurs communs et une plus grande cohérence entre eux.

Thème 2 : Éducation et formation

Les programmes d'éducation et de formation existants ne suffisent pas ou sont trop peu diversifiés pour répondre à la demande en sensibilisation à la cybersécurité auprès de populations diversifiées. En outre, plusieurs programmes sont dispensés de façon disparate, ce qui entraîne en une sous-utilisation des ressources disponibles.

Les enjeux identifiés sont :

- Les programmes d'éducation et de formation sur des risques et des comportements spécifiques tels que les procédures en cas de rançongiciel, d'hameçonnage par courriel ou par appel téléphonique sont limités.
- Les contenus de sensibilisation à la cybersécurité pour des groupes d'âge spécifiques sont limités.
- Le programme scolaire n'inclut pas d'objectifs clairs à propos de l'éducation numérique.
- Plusieurs programmes collégiaux et universitaires offrent une formation spécialisée en cybersécurité, mais peu de possibilités d'acquérir une expérience pratique.
- L'accès aux programmes de formation continue comme ceux du centre d'innovations Rogers Cybersecure Catalyst est limité, en raison de la forte demande.
- Le secteur parapublic profiterait certainement de la mise en commun de ressources d'éducation et de formation de divers organismes de toute taille.
- Le secteur parapublic requiert une approche intégrée plus cohérente et accessible en matière de prestation de programmes d'éducation et de formation.

Thème 3 : Communications

Le gouvernement de l'Ontario n'a pas établi de cadre pour les communications électroniques de catégorie de sécurité élevée et pour réglementer le partage des renseignements entre ses plateformes et ses organismes. Les communications ainsi limitées ont pour résultat un manque de cohérence dans la gestion des cyberrisques et dans la préparation et la réponse aux incidents.

Les enjeux identifiés sont :

- Les agences individuelles du secteur parapublic ont accès à des conseils en cybersécurité par l'intermédiaire d'un service d'assistance téléphonique, mais peu d'organismes du secteur parapublic sont au courant de l'accessibilité à de nombreuses ressources centralisées du Centre d'excellence en cybersécurité.
- Les ressources en cybersécurité sont éparses sur diverses plateformes et sont souvent difficiles à repérer.
- La gestion numérique des divers intervenants du secteur est fragmentée; il est difficile d'avoir une vue d'ensemble du secteur parapublic à cet égard.
- Les protocoles de partage des renseignements critiques sont actuellement unidirectionnels, c'est-à-dire qu'ils ne servent qu'à informer le gouvernement des cyberincidents. Ces renseignements, dont la diffusion entre les organismes du secteur parapublic établirait un réseau d'entraide concret, sont cependant peu partagés.

Thème 4 : Services partagés

De nombreux services partagés spécifiques aux secteurs sont planifiés ou en cours d'élaboration pour déterminer des modalités de partage des renseignements, d'approvisionnement, de réponse aux incidents et de cyberrésilience. Encore une fois, ces initiatives ne couvrent pas l'ensemble du secteur parapublic. Par conséquent, il conviendrait qu'une source centralisée émette des normes et des procédures communes et fournisse un modèle de prestation de services partagés qui soit adapté aux besoins communs du secteur parapublic.

Les enjeux identifiés sont :

- Les ressources dont disposent les organismes sont inégales. Plusieurs petits organismes ont peu de ressources de gestion des cyberrisques qui sont requises en cas d'incident, comme des outils d'investigation, des services d'expert-conseil en cybersécurité et des procédures de rétablissement.
- La plupart des grands organismes sont munis de plans de protection et de rétablissement des données. Ce n'est pas le cas pour plusieurs petits organismes.
- L'acquisition d'une police d'assurance cyberrisque devient de plus en plus difficile et coûteuse pour les petits organismes en raison des exigences grandissantes de cybersécurité.

Analyse des pratiques numériques dans le monde

De nombreuses administrations homologues dans le monde ont répondu à la transition numérique en intégrant à leur programme la cybersécurité en tant qu'élément critique et en exigeant la responsabilisation et la conformité de organismes à cet égard. Le gouvernement de l'Ontario devrait tirer profit des pratiques exemplaires observées chez ses homologues pour renforcer sa posture de cybersécurité. Une telle démarche contribuerait à faire progresser le secteur parapublic et à soutenir l'écosystème numérique grandissant de l'Ontario.

Thème 1 : Gouvernance et modèle opérationnel

Des administrations de premier plan ont fait appel à des services et des ressources centralisés qui tiennent compte des caractéristiques sectorielles pour stimuler des avantages économiques tout en offrant des services publics sûrs.

Voici quelques exemples de pratiques exemplaires :

- Le gouvernement d'Israël a officiellement intégré les efforts de cybersécurité dans ses objectifs gouvernementaux et sollicité une implication étroite des organismes individuels. Un centre des opérations de sécurité a été intégré à l'infrastructure technologique et opérationnelle de l'équipe d'intervention en cas d'urgence informatique du gouvernement central, ce qui offre une meilleure vue d'ensemble et un suivi optimal des opérations de sécurité sectorielles.
- En Australie, un centre de cybersécurité est responsable de la cybersécurité nationale et collabore avec les centres des opérations de sécurité nationaux qui fournissent des services adaptés dans chaque État et territoire.

Thème 2 : Éducation et formation

L'établissement d'objectifs fondamentaux d'éducation et de sensibilisation des citoyens à la cybersécurité, soutenus par des pratiques exemplaires, est à même de favoriser une citoyenneté numérique responsable.

Voici quelques exemples de pratiques exemplaires :

- Les programmes du centre d'innovations Rogers Cybersecure Catalyst de l'Université métropolitaine de Toronto ont été conçus pour répondre aux besoins des secteurs publics et privés au Canada. Cette initiative offre aux particuliers et aux entreprises canadiens les outils pour s'attaquer aux défis de sécurité numérique. Le lancement de nouvelles initiatives semblables au centre d'innovations Rogers Cybesecure Catalyst élargirait l'offre en matière de formation sur la cybersécurité et les possibilités locales d'acquérir les compétences requises afin de remédier au manque de ressources humaines dans le domaine de la cybersécurité.
- Le gouvernement d'Israël a adopté une approche globale de la cybersécurité tant dans l'éducation que pour l'identification, les alertes et les investigations relatives aux cybermenaces. Des services, des opérations et une gestion partagés sont au cœur d'une citoyenneté numérique exemplaire. L'intégration d'un centre des opérations de cybersécurité au gouvernement central oriente la planification des

opérations sectorielles, tout en offrant une meilleure vue d'ensemble et un suivi optimal de ces opérations. Une stratégie similaire en Ontario favoriserait des partenariats fructueux et optimiserait les communications entre les secteurs publics et privés, le milieu universitaire et la population à l'échelle de la province.

Thème 3 : Communications

Le développement et la promotion de pratiques exemplaires par l'intermédiaire de centres d'excellence marquent un point en faveur de la maturité numérique du secteur public en Amérique du Nord et à l'international.

Voici quelques exemples de pratiques de premier plan en Amérique du Nord :

- Le Centre canadien pour la cybersécurité propose aux secteurs publics et privés canadiens un forum où diffuser des pratiques exemplaires et de l'information concernant des menaces émergentes. Cette source nationale fournit aux organismes de toutes les tailles un accès à des renseignements critiques en matière de protection.
- Le Multi-State Information Sharing and Analysis Center (MS-ISAC) est un organisme sans but lucratif chargé par le Département de la sécurité intérieure des États-Unis de fournir divers niveaux de soutien au gouvernement des États-Unis. En échange du signalement d'activités suspectes, le MS-ISAC offre un soutien en temps réel aux membres du gouvernement pour assurer un échange d'information sans failles.

Voici quelques exemples de pratiques de premier plan à l'international :

- Les organismes d'État en Israël travaillent en collaboration avec des représentants individuels d'organismes des secteurs publics et privés, du milieu universitaire et des citoyens. Ils ont ainsi réussi à mobiliser de significatives ressources nationales en cybersécurité, notamment de chaînes de communication des risques, des solutions d'investigations et de mitigation des cybermenaces et des services de sécurité centralisés.
- Le gouvernement de Singapour a mandaté des organismes de contrôle sectoriels de renseigner les organismes du secteur parapublic sur les cyberincidents. Un réseau qui englobe ces organismes est quant à lui chargé de coordonner ce mandat et d'offrir l'assistance requise.

Thème 4 : Services partagés

Les services partagés, tels que les chaînes de communication des risques, les services d'évaluation des risques et d'intervention en cas d'incident, sont des outils qui stimulent l'amélioration continue de la maturité organisationnelle tout en promouvant une culture de prise en compte du risque.

Voici quelques exemples de pratiques de premier plan au Canada :

- En 2019, Santé Ontario a mis en place une structure partagée de gouvernance du système de santé et des programmes d'activités visant une expertise globale en matière de cybersécurité au sein du secteur de la santé. Cette nouvelle structure fait la promotion du partage de renseignements afin que l'ensemble du réseau des

fournisseurs de soins soit en mesure d'aborder les menaces informatiques à partir de renseignements opportuns, précis et exploitables. La mise en place de centre des opérations de sécurités partenaires et de comités locaux de gouvernance de la cybersécurité dans le cadre de cette initiative stimule des collaborations régionales en matière d'opérations de sécurité, permet de rationaliser les efforts et les coûts et de partager les ressources en cybersécurité au profit de tous, tout en assumant les responsabilités à l'échelle locale.

Voici quelques exemples de pratiques de premier plan à l'international :

- L'initiative Cyber Spark Industry en Israël centralise la coordination des mesures de cybersécurité employées dans les divers organismes gouvernementaux, l'armée, le milieu universitaire, l'entreprise en développement, les fonds de capital de risque et les groupes étrangers. Il découle de cette initiative un écosystème numérique sûr qui stimule le développement économique.

- Le gouvernement de Singapour a centralisé les efforts en matière de cybersécurité sous le seul mandat de son agence de cybersécurité, laquelle relève du Cabinet du premier ministre. Cette agence est chargée de la protection des infrastructures critiques de renseignements et de services essentiels, de la coordination des activités de prévention des risques informatiques à grande échelle, du développement et du renforcement de règlements, de politiques et de pratiques en matière de cybersécurité.

Prise en compte des facteurs et considérations communs

Le secteur parapublic englobe tout un éventail d'organismes et de services qui ont des besoins en cybersécurité distincts. Nous avons cependant dégagé certains facteurs qui sont communs à l'ensemble du secteur parapublic et qui ont servi à la formulation de nos recommandations. Les voici :

- **Une approche de prise en compte des risques**

Il convient que le secteur parapublic adopte une approche de prise en compte des risques pour acquérir une meilleure compréhension des risques et pour favoriser l'adoption de politiques et de pratiques durables et résilientes.

- **Un environnement vaste et diversifié**

Le secteur parapublic forme un groupe diversifié d'organismes et des services offerts partout dans la province, ce qui requiert des solutions efficaces qui peuvent être personnalisées et adaptées à divers contextes.

- **Des approches communes et sectorielles**

Les menaces auxquelles font face les organismes sont souvent les mêmes; cependant, certaines menaces ciblant un secteur distinct requièrent des approches nuancées. Par conséquent, il convient que le secteur parapublic dispose d'un espace de diffusion de stratégies communes et sectorielles adoptées pour régler des problématiques communes.

- **Des structures communes intentionnellement sûres**

La sécurité devrait être un élément fondamental de la transition numérique afin de prévenir les cyberrisques de demain. L'établissement de politiques et de procédures cohérentes au sein des structures communes et la promotion de contrôles technologiques dans le secteur parapublic sont à même de réduire les risques partagés dès aujourd'hui.

- **La pénurie de talents en cybersécurité**

La pénurie de main-d'œuvre qualifiée en cybersécurité partout au Canada se chiffre à un nombre estimé d'emplois à combler de 37 100 d'ici 2027 *[Source : (ISC)2: A Resilient Cybersecurity Profession Charts the Path Forward. Disponible à : https://www.isc2.org/]*. Par conséquent, il convient que toute stratégie de développement de main-d'œuvre tienne compte de cet enjeu.

- **Un sous-investissement systémique dans les technologies**

Les exigences concurrentielles d'investissements à la fois dans la cybersécurité et dans le remplacement des systèmes hérités ont généré un sous-investissement dans ces deux domaines.

- **L'impact économique potentiel**

Les incidents informatiques qui perturbent le secteur parapublic posent un risque significatif d'impact économique défavorable. Toutefois, l'adoption de solutions adaptées à l'ensemble

du secteur parapublic est susceptible de générer des avantages considérables tout en réduisant le risque d'impact défavorable.

- **Des investissements continus pour stimuler les améliorations**

Les modèles de financement des améliorations des technologies et de l'écosystème numériques sont de plus en plus catégorisés comme une dépense opérationnelle annuelle plutôt que comme un investissement ponctuel en capitaux. Par conséquent, les approches de financement et d'approvisionnement devraient s'aligner à une telle conception du financement des améliorations.

Recommandations du Groupe d'experts

Les ressources en cybersécurité et les niveaux de maturité des organismes du secteur parapublic sont inégaux, il est donc raisonnable de s'attendre à ce que les petits organismes n'atteignent pas les mêmes résultats que les grands organismes du jour au lendemain. Les organismes les plus avancés ont déjà parcouru une bonne partie du chemin, mais divers petits organismes moins matures ont désespérément besoin d'un encadrement, d'un soutien et d'une assistance externe. Dans la plupart des cas, l'atteinte des objectifs requiert une transformation majeure, et d'importantes ressources intégrées sur plusieurs années.

Compte tenu de cette situation, le Groupe d'experts a émis des recommandations fondées sur les thèmes abordés par ses sous-comités, c'est-à-dire la gouvernance et le modèle opérationnel, l'éducation et la formation, les communications et les services partagés.

Gouvernance et modèle opérationnel

Recommandation fondamentale du Groupe d'experts :

Le gouvernement de l'Ontario devrait renforcer la structure de gouvernance existante pour favoriser une gestion efficace des cyberrisques dans l'ensemble du secteur parapublic.

L'objectif du Centre d'excellence en cybersécurité est d'optimiser la cybersécurité au sein des ministères et des organismes du secteur parapublic par la prestation de conseils, d'encadrement et de renseignement. Le manque de centralisation et de cadre de gestion normalisée des risques rend l'élaboration de solutions de cybersécurité conformes à la stratégie provinciale difficile pour les organismes d'envergure variée au sein du secteur parapublic. Il convient de développer une vision globale proposée par un organisme de contrôle unique présentant un modèle opérationnel commun, établissant les responsabilités et faisant appel à divers ressources et partenariats.

Par conséquent, le Groupe d'experts recommande de :

1. **Fournir un encadrement supervisé des programmes de cybersécurité dans le secteur parapublic**

Le gouvernement de l'Ontario devrait nommer un organisme unique responsable de la supervision des programmes de cybersécurité afin de renforcer les structures de gouvernance actuellement responsables de la gestion sectorielle des cyberrisques. Cet organisme unique serait responsable de la coordination centralisée, des ressources et de l'intégration d'approches de prise en compte des cyberrisques au moyen de consultations, d'application de la loi, de rapports et de collaborations au sein du secteur parapublic. Une telle approche contribuerait à aligner les programmes de cybersécurité aux besoins du secteur parapublic et à augmenter la participation aux dits programmes.

2. **Adopter un modèle opérationnel commun**

Le gouvernement devrait intégrer un modèle opérationnel relatif au cyberrisque à son cadre de gestion globale des risques pour promouvoir des améliorations continues. Il convient

d'élaborer un cadre de cybersécurité fondé sur les normes du National Institute of Standards and Technology (NIST) qui inclue des ressources partagées, telles que des politiques, des normes, des outils de contrôle et d'auto-évaluation pour promouvoir un langage commun et une meilleure compréhension des cyberrisques au sein du secteur parapublic. Il convient en outre qu'un tel cadre puisse être adapté aux différentes tailles des organismes pour aborder leurs enjeux et leurs besoins uniques, qu'il leur fournisse les ressources pour mesurer les risques, pour établir les fondements de pratiques en gestion des risques et pour élaborer et mettre en œuvre des programmes de cybersécurité personnalisés de manière rentable.

3. Déterminer clairement les responsabilités en matière de cybersécurité

Le gouvernement de l'Ontario doit renforcer les rôles et les responsabilités des intervenants en matière de cybersécurité pour habiliter les dirigeants à proposer des mesures communes qui s'harmonisent aux programmes et aux initiatives du secteur parapublic. Chacun des organismes du secteur parapublic devrait nommer un responsable principal à la cybersécurité, afin de déterminer clairement les attentes du secteur et de promouvoir l'expertise au sein des organismes.

4. Promouvoir la résilience et la préparation aux incidents informatiques

Le gouvernement de l'Ontario devrait accorder la priorité aux ressources d'intervention en cas en cas d'incident informatique pour faciliter les communications et la collaboration dans de telles situations. La sélection, la validation et l'utilisation d'outils cruciaux, notamment de guides d'intervention en cas d'incident et de restauration de données, d'assurances et des procédures de communications entre les intervenants du secteur parapublic sont essentiels à la mitigation des pertes et à un rétablissement rapide à la suite de failles dans la cybersécurité.

5. Évaluer le développement économique régional

Le gouvernement de l'Ontario devrait évaluer les retombées économiques potentielles du regroupement des ressources intersectorielles de cybersécurité dans les collectivités de la province. Une telle démarche favoriserait le leadership en matière d'innovations et stimulerait la croissance d'une main-d'œuvre spécialisée en cybersécurité.

Quels sont les impacts de la mise en œuvre de cette recommandation sur la cybersécurité en l'Ontario?

La mise en œuvre de cette recommandation fondamentale du Groupe d'experts dans ce domaine favorisera une croissance économique graduelle en Ontario. Une adhésion accrue des organismes du secteur parapublic à des programmes intersectoriels et à des principes directeurs unifiés de cybersécurité offrira une meilleure vue d'ensemble de l'écosystème numérique en Ontario, facilitant du même coup sa supervision. Une meilleure vue d'ensemble signifie davantage d'analyses et une capacité accrue à identifier et à promouvoir les possibilités d'innovation, avec pour résultat une croissance saine du marché du travail et des entreprises partout en Ontario.

Les collaborations et le partage des ressources entre les secteurs favorisent des innovations aux applications multiples. La province de l'Ontario ainsi propulsée au premier plan dans ce domaine et attirant les meilleurs talents dans un marché en expansion continue assure son avenir avec une solide main-d'œuvre en cybersécurité.

Éducation et formation

Recommandation fondamentale du Group d'experts :

Le gouvernement de l'Ontario devrait poursuivre l'élaboration d'initiatives diversifiées en matière de sensibilisation à la cybersécurité adaptées à tous les niveaux d'éducation et assortir ces initiatives d'une variété de contenus généraux et spécialisés et d'activités pratiques.

La tribune accordée à la cybersécurité grandit avec le nombre croissant de menaces auxquelles font face les organismes du secteur parapublic. Cependant, les programmes d'éducation actuels manquent de contenus de formation axés sur les risques adaptés aux groupes d'âge; le manque d'activités pratiques limite en outre la portée des apprentissages. Les besoins en matière d'éducation au numérique sont multiples : initiation aux environnements numériques dans le programme scolaire, optimisation des programmes spécialisés supérieurs, formation continue de la main-d'œuvre ontarienne et promotion de l'accès à divers contenus d'apprentissage et outils pour le public ontarien.

Par conséquent, le Groupe d'experts recommande de :

1. **Normaliser l'apprentissage de la citoyenneté numérique et de l'initiation à la cybersécurité dans le programme scolaire**

Le gouvernement de l'Ontario devrait organiser et intégrer des contenus adaptés aux groupes d'âge du programme scolaire, à l'instar de la province de la Saskatchewan. Le personnel enseignant devrait en outre recevoir une formation pour être sensibilisé à des pratiques numériques sûres et préparé aux nouveaux objectifs d'apprentissage du programme. Une telle approche favoriserait une citoyenneté numérique responsable en plus de promouvoir des pratiques numériques fondamentales auprès de tous les intervenants impliqués dans le programme scolaire.

2. **Former des professionnels de la cybersécurité aux cycles d'éducation supérieure**

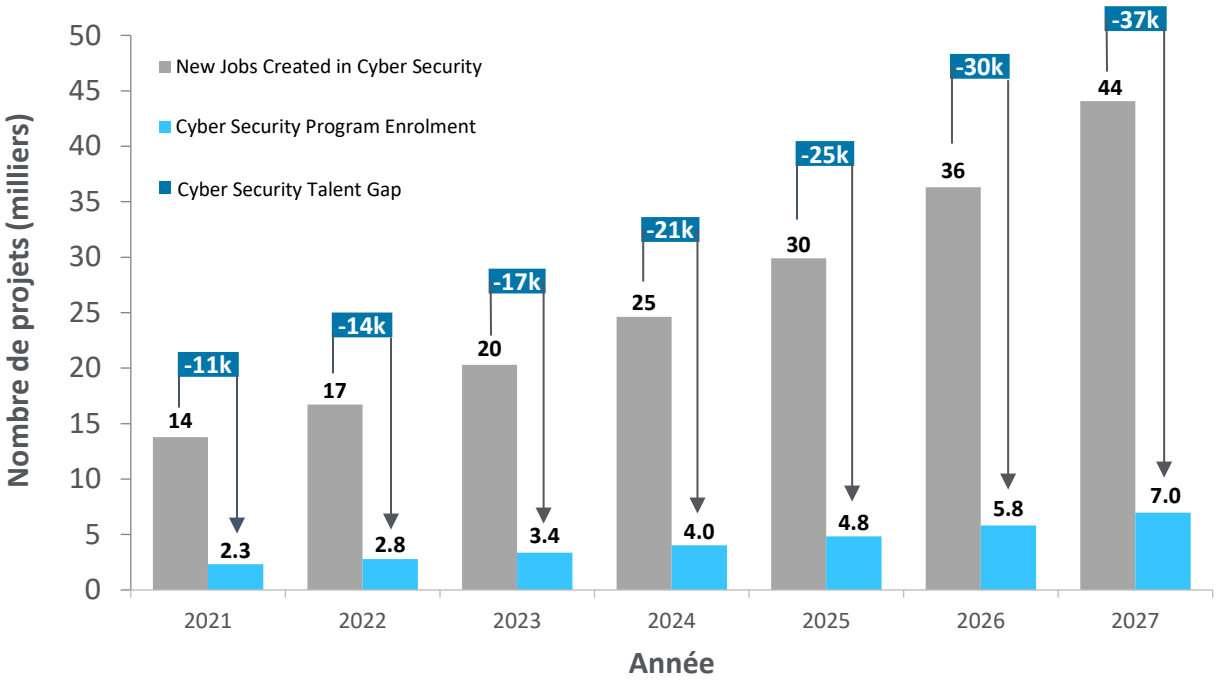
Le gouvernement de l'Ontario devrait mettre en place des programmes d'éducation et de formation sur les fondements de la cybersécurité pour les étudiants des niveaux postsecondaires et élaborer des programmes spécialisés prévoyant un volet pratique. Ces programmes devraient prévoir un développement équilibré des connaissances et des savoir-faire en établissant des partenariats pour promouvoir l'acquisition de compétences requises. Une telle approche répond au besoin de sensibilisation accrue du personnel à la cybersécurité et à la préparation aux incidents dans tous les secteurs en plus d'accélérer la formation d'une main-d'œuvre qualifiée.

3. **Mettre en place un programme de développement de la main-d'œuvre en cybersécurité**

Le gouvernement de l'Ontario devrait mettre en place un programme de développement de la main-d'œuvre qui promeut les avantages d'une carrière en cybersécurité. L'étude du marché de l'emploi en cybersécurité de l'Ontario illustré à la figure 2 (*(ISC)²: A Resilient Cyber Security Profession Charts the Path Forward – en anglais*) suggère qu'il serait

avantageux de combler le manque de talents en cybersécurité en promouvant la formation continue de la main-d'œuvre ontarienne. Un programme de développement de la main-d'œuvre favoriserait en outre l'accroissement des ressources de cybersécurité en Ontario.

Figure 2 : Projection du marché de l'emploi en cybersécurité (Ontario)



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

4. Poursuivre les améliorations et étendre la portée des initiatives d'éducation et de sensibilisation continues, diversifiées et inclusives

Le gouvernement de l'Ontario devrait soutenir des campagnes d'éducation et de sensibilisation inclusives et diversifiées par l'intermédiaire de différents médias. La direction de ces campagnes devrait tenir compte de la diversité de la population ontarienne en adaptant ses contenus pour tenir compte des besoins des personnes, de l'ensemble des secteurs et des organismes (et de leur rôle). Une telle approche favoriserait une cyberrésilience accrue des individus et des organismes sur l'ensemble de la province.

5. Poursuivre le développement et l'amélioration d'outils pratiques pour une promotion continue de la cybersécurité

Le gouvernement de l'Ontario devrait poursuivre ses investissements dans le développement et l'amélioration des ressources et des outils d'éducation et de sensibilisation offerts sur son portail de cybersécurité en tenant compte des changements démographiques en Ontario. Il devrait en outre prévoir un répertoire d'exercices pratiques et de cas de figure adaptés aux secteurs et des campagnes de sensibilisation à l'hameçonnage; réduire les obstacles nuisant à la cyberrésilience des organismes du secteur parapublic; promouvoir l'évaluation périodique de la cybersécurité et des apprentissages

continus. Une telle approche réduirait l'incertitude et renforcerait la résilience et la cybersécurité des organismes.

Quels sont les impacts de la mise en œuvre de cette recommandation sur la cybersécurité en l'Ontario?

L'avenir de l'Ontario repose entre les mains et les esprits de sa jeunesse. Investir dans la sensibilisation à la cybersécurité et développer des savoirs et des comportements numériques sûrs dès le jeune âge favorise une citoyenneté numérique responsable et l'adoption de pratiques numériques sûres et responsables chez les dirigeants de demain.

La main-d'œuvre de l'Ontario profiterait également d'une accessibilité accrue à des programmes de formation et de sensibilisation inclusifs et diversifiés à tous les stades d'apprentissage. Des programmes professionnels intensifs axés sur les compétences et une éducation au numérique continue, facilités par le développement et l'accessibilité à des contenus et des outils pratiques, renforceraient la prestation des services numériques en Ontario, assurant un accès sûr et continu aux services publics essentiels aujourd'hui et demain.

Communications

Recommandation fondamentale du Groupe d'experts :

Le gouvernement de l'Ontario devrait mettre en œuvre un cadre qui favorise le partage sécurisé et simplifié des protocoles de cybersécurité entre les entités au sein du secteur parapublic.

Les communications entre les organismes du secteur parapublic sont extrêmement limitées, avec pour résultats des approches cloisonnées et une méconnaissance des tendances du secteur. Des communications efficaces et cybersécures ne seront atteintes que par une meilleure présentation des intervenants, le recours unanime à une plateforme commune, des collaborations intersectorielles et des protocoles simplifiés de partage des renseignements critiques.

Pour aborder les lacunes de communications observées, le Groupe d'experts a émis les recommandations suivantes :

1. **Identifier les responsables principaux de la cybersécurité**

Le gouvernement de l'Ontario devrait publier un répertoire des responsables principaux nommés à la cybersécurité des organismes du secteur parapublic mis à jour annuellement. Une telle approche favoriserait l'identification et la gestion des responsables de la cybersécurité et les relations entre les organismes du secteur parapublic.

2. **Poursuivre les améliorations des plateformes de mise en commun des ressources existantes et étendre leur portée**

Le gouvernement de l'Ontario devrait poursuivre les améliorations des plateformes de signalement, de promotion et de mise en commun des ressources (formation, éducation, sensibilisation). Des renseignements adaptés aux secteurs devraient être intégrés pour favoriser un guichet d'accès unique aux ressources dans le secteur parapublic. Une telle approche fournirait un répertoire centralisé des ressources adaptées au secteur parapublic et à ses sous-secteurs et favoriserait la promotion des ressources en cybersécurité, tout en rassemblant une communauté d'intervenants partageant des intérêts semblables.

3. **Établir un cadre de communications intersectorielles proactives**

Le gouvernement de l'Ontario devrait établir un cadre convivial qui stimule le partage actif des ressources et les collaborations entre les intervenants principaux du secteur parapublic et du gouvernement. Ce cadre devrait tenir compte de l'éventail d'intervenants (p. ex., les dirigeants, le personnel, la population) et la nature diversifiée des exigences de communications (p. ex., générale, technique ou confidentielle). Une telle approche stimulerait le partage de renseignements liés à la cybersécurité entre les organismes du secteur parapublic et renforcerait la confiance du public concernant le traitement de données confidentielles.

4. **Simplifier les communications d'intervention en cas d'incident informatique**

Le gouvernement de l'Ontario devrait définir un protocole standard de partage de renseignements critiques pour s'assurer de communications rapides d'incidents informatiques, de renseignements sur des cybermenaces et de vulnérabilités dans la

cybersécurité entre les organismes du secteur parapublic. Des chaînes de communications primaires et alternatives (p. ex. courriel et téléphone) devraient être consignées dans un répertoire maintenu à jour pour faciliter les communications en cas d'incident ou d'interruption majeurs. Une telle approche améliorait le partage efficace et opportun des renseignements, particulièrement en situation d'intervention.

Quels sont les impacts de la mise en œuvre de cette recommandation sur la cybersécurité en l'Ontario?

Si les infrastructures, les connaissances, la sensibilisation et les ressources constituent la fondation d'un programme de cybersécurité efficace, les communications sont le ciment qui le solidifie et qui assure sa résistance à l'épreuve du temps. Une plateforme unique de partage des renseignements constituerait un ensemble cohérent de données d'incidents informatiques auquel les organismes du secteur parapublic contribuent et ont accès, peu importe leur rôle ou leur taille. L'accès à un répertoire de données ce type et de ce calibre favoriserait une compréhension accrue des menaces, des incidents et des interventions ayant eu lieu sur l'ensemble de la province pour tout le secteur parapublic. La visibilité et la transparence favorisées par l'application de cette recommandation renforceraient la résilience et la préparation aux incidents d'un secteur parapublic. Les organismes seraient ainsi en mesure de tirer des apprentissages des expériences de leurs homologues et d'adopter des mesures de prévention des incidents appropriées.

L'avenir des communications au sein du secteur parapublic y gagnerait des pratiques communes solides et un réseau intersectoriel de soutien, en plus d'habiliter les organismes à reconnaître les cybermenaces, à les prévenir et à y réagir avec assurance.

Services partagés

Recommandation fondamentale du Groupe d'experts :

Le gouvernement de l'Ontario devrait investir dans des services partagés cyberrésilients au sein du secteur parapublic tout en tenant compte des besoins sectoriels distincts.

L'accès inégal au financement et aux ressources a généré des niveaux de compétences en cybersécurité divers parmi les intervenants du secteur parapublic. Les petits organismes souffrent généralement d'un manque d'accès aux technologies, à l'expertise et aux assurances cyberrisques. Il est possible de mettre à profit les connaissances et les procédures existantes en créant des ressources d'assistance communes et sectorielles. Les écarts en matière de cybersécurité entre les organismes du secteur parapublic pourraient être réduits grâce à des investissements partagés. Une telle approche renforcerait la cyberrésilience du secteur parapublic de façon significative.

Par conséquent, le Groupe d'experts recommande de :

1. **Établir des normes de gestion des risques**

Le gouvernement de l'Ontario devrait développer des ressources de gestion des cyberrisques pour aider les organismes du secteur parapublic à aborder des risques identifiés dans un cadre d'évaluation commun. Les organismes seraient alors en mesure d'adopter ou d'adapter des ressources modèles, comme des politiques organisationnelles, des objectifs de contrôle, des guides de mise en œuvre et des indicateurs communs d'évaluation de la cybersécurité. Une telle approche optimiserait les ressources organisationnelles allouées et réduirait la vulnérabilité du secteur parapublic.

2. **Investir dans des centres d'opérations de sécurité partagés dans le secteur parapublic**

Le gouvernement de l'Ontario devrait considérer l'adoption d'une approche des opérations de sécurité numérique qui favorise le partage et la collaboration entre les organismes, les secteurs et la province, optimisant ainsi les investissements en capacité, en talents et en ressources. Une telle approche est en mesure d'accroître l'efficacité et la rentabilité des ressources actuellement limitées.

3. **Établir une procédure d'évaluation de la cybersécurité**

Le gouvernement de l'Ontario devrait mettre en place des ressources ou un véhicule d'approvisionnement pour effectuer un contrôle ou une évaluation indépendante des risques à intervalles réguliers dans un cadre de gestion des cyberrisques. Une telle approche faciliterait la normalisation des évaluations de la cybersécurité avec pour résultat une gestion améliorée des risques et une réduction de la vulnérabilité.

4. **Explorer la possibilité d'établir un programme d'assurances cyberrisques**

Le gouvernement de l'Ontario devrait explorer la possibilité d'établir un programme autofinancé d'assurances cyberrisques auxquelles les organismes du secteur parapublic pourraient souscrire, notamment pour des services d'experts-conseils en cybersécurité et

d’assistance à l’intervention et au rétablissement en cas de brèche ou d’incident. Une telle approche procurerait un filet de sécurité stable et abordable pour l’intervention et le rétablissement en cas d’incident informatique.

5. **Optimiser les services partagés**

Le gouvernement de l’Ontario devrait poursuivre les améliorations et le développement des ressources du volet sécurité du Programme de gestion des contrats. Une telle approche favoriserait une accessibilité directe à des ressources de cybersécurité, permettant ainsi aux organismes de concentrer leurs ressources limitées dans leurs champs d’activités les plus critiques.

6. **Renforcer la cyberrésilience et les capacités**

Le gouvernement de l’Ontario devrait considérer les enjeux sectoriels découlant du « déficit technologique » et élaborer des stratégies pour remédier aux écarts au moyen d’investissements partagés. Une telle approche permettrait d’ériger une infrastructure numérique robuste qui soutient la prestation des services publics et favorise une économie numérique sûre.

Quels sont les impacts de la mise en œuvre de cette recommandation sur la cybersécurité en l’Ontario?

Le secteur parapublic de l’Ontario est représenté par un large éventail d’organismes de tailles diverses profitant d’un accès inégal aux ressources et dotés de capacités de cybersécurité assorties à leur fonction et aux exigences réglementaires. À cet égard, le gouvernement de l’Ontario reconnaît qu’une approche passe-partout de la cybersécurité dans secteur parapublic n’est ni raisonnable ni inclusive.

L’avenir des services et des ressources partagées de cybersécurité dans le secteur parapublic en Ontario doit tenir compte des besoins et des contraintes de tous les organismes du secteur et offrir diverses options qui favorisent des services et des ressources de sécurité de base normalisées qui sont abordables et adaptables afin de répondre aux besoins sectoriels distincts. Les organismes seront ainsi en mesure de choisir d’acquérir des services de sécurité supplémentaires sur la base d’exigences individuelles et d’élaborer des programmes de cybersécurité personnalisés qui conviennent à leurs besoins et leur budget.

La mise en place de services et de ressources partagés au sein du secteur parapublic améliore la posture de l’Ontario en matière de cybersécurité; elle élève le niveau de maturité des maillons plus faibles et renforce la cyberrésilience collective en installant un filet de sécurité qui assure les interventions et le rétablissement en cas d’incident informatique majeur.

L’avenir de la cybersécurité dans le secteur parapublic de l’Ontario

Le gouvernement de l’Ontario reconnaît que l’écosystème numérique est en constante évolution et que des efforts continus sont requis de sa part pour identifier et établir ses priorités et pour faire face à de nouveaux défis de sécurité tout en embrassant les nouvelles possibilités. Les recommandations émises par le Groupe d’experts du MSPE visent à mettre en place de nouvelles stratégies tout en apportant des améliorations aux initiatives de cybersécurité déjà en cours en Ontario. La province est en mesure d’atteindre ces objectifs en rationalisant les procédures existantes et les responsabilités, en optimisant les ressources éducationnelles, en favorisant le partage des protocoles de cybersécurité dans les réseaux et en guidant l’établissement d’une norme acceptable et atteignable de cybersécurité dans l’ensemble du secteur parapublic.

Les améliorations, fondées sur de solides connaissances et des compétences en cybersécurité ciblées, devraient être progressivement et stratégiquement mises en œuvre au moyen de ressources issues de partenariats stratégiques. Les intervenants provenant des principaux secteurs devraient travailler de concert pour étendre la portée des réseaux existants et mettre en place un mécanisme unifié de cyberdéfense plus fort, plus adaptatif, mieux informé, à la fois abordable et durable.

L’avenir de la cybersécurité passe par l’engagement intersectoriel, la participation et la collaboration des organismes du secteur parapublic. Ce tout, bien plus grand et résilient que la somme de ses parties, résultera en une cohérence en matière de prestation de services publics accessibles partout en Ontario.

Conclusion

Dans un monde de plus en plus axé sur les données, la cybersécurité devient un aspect central de la conception de services gouvernementaux accessibles, pratiques et fiables. Au fil de l'intégration des technologies numériques à ses services, le gouvernement de l'Ontario a lancé diverses initiatives pour promouvoir la sensibilisation à la cybersécurité et la cyberrésilience dans le secteur parapublic. Bien que ces efforts aient contribué à augmenter le niveau de maturité de la cybersécurité du secteur parapublic, ses organismes bénéficieraient d'approches sur mesure plus facilement adaptables pour atteindre les objectifs communs de cybersécurité. Peu importe leur taille ou leur mandat, les organismes s'entendent pour dire que davantage de ressources, d'investissements et d'expertise en cybersécurité sont nécessaires.

Le Groupe d'experts est d'avis que la mise en place d'un écosystème numérique sûr dans le secteur parapublic requiert une gouvernance forte, une éducation continue, des communications efficaces et une collaboration intersectorielle. Une mise en œuvre réussie des recommandations émises dans le présent rapport favorisera le maintien d'un écosystème numérique sûr favorable à la prestation de services publics pratiques et à la croissance économique dans un avenir prospère pour tous les Ontariennes et Ontariens.

En raison de l'apport croissant des technologies numériques dans la prestation des services gouvernementaux en Ontario, la cybersécurité devrait demeurer une priorité absolue du Ministère afin de prévenir toute perturbation de l'écosystème numérique d'aujourd'hui et de demain.

Annexe A : Termes et définitions

Australian Cyber Security Centre (ACSC) : L'Australien Cyber Security Centre est un centre qui dirige les efforts du gouvernement de l'Australie pour le renforcement de la cybersécurité et la surveillance des cybermenaces, la protection des infrastructures de données critiques, la collaboration entre les entreprises, le gouvernement et les partenaires du milieu universitaire et le développement de solutions de cybersécurité.

Secteur parapublic : De façon générale, on entend par secteur parapublic l'ensemble formé par les organismes qui reçoivent un financement du gouvernement de l'Ontario, mais qui n'en font pas partie. Les organismes considérés comme faisant partie du secteur parapublic sont définis dans la *Loi loi de 2010 sur la responsabilisation du secteur parapublic*.

Canadian Shared Security Operations Centre (CanSSOC) : Le Canadian Shared Security Operations Centre est un réseau d'analyse de la fréquence et de la complexité des cybermenaces qui pèsent sur les établissements d'éducation supérieure. Des projets pilotes sont en cours pour maximiser les compétences et les outils de cybersécurité du réseau de l'éducation supérieure au Canada.

Israeli Cyber Emergency Response Team (CERT) : Il s'agit d'une équipe nationale israélienne d'intervention aux incidents informatiques dans la sphère civile. Elle relève de la Direction numérique nationale d'Israël — une entité dédiée à la protection technologique et numérique dirigée par l'État.

Ministère des Services au public et aux entreprises (MSPE) : Le ministère des Services au public et aux entreprises rassemble les leviers du secteur de l'entreprise pour transformer et améliorer les services gouvernementaux à l'intention des ministères et du public. Le mandat à long terme du Ministère est de fournir une prestation des services gouvernementaux toujours plus simples et rapides.

Multi-State Information Sharing & Analysis Center (MS-ISAC) : Le MS-ISAC est un organisme sans but lucratif chargé par le Département de la sécurité intérieure des États-Unis de fournir divers niveaux de soutien de prévention et de protection des cybermenaces et d'intervention en cas d'incident au gouvernement des États-Unis. La portée de ses travaux inclut l'analyse et le partage continu (24/7) des données de cybermenaces, l'évaluation de la cybersécurité nationale, les services de rétablissement, et la sensibilisation à la cybersécurité.

National Institute for Standards & Technology (NIST) : Le NIST est un laboratoire de sciences physiques et une agence non réglementaire du Département du Commerce des États-Unis. Il est chargé du développement des technologies, des normes et des indicateurs appliqués aux sciences et au secteur des technologies. Le cadre de cybersécurité du NIST propose aux organismes une série de mesures de gestion et de réduction des cyberrisques et des résultats attendus; il a été adopté par de nombreux secteurs d'activités et gouvernements partout dans le monde.

Association ontarienne des sociétés d'aide à l'enfance/sociétés d'aide à l'enfance : Les sociétés d'aide à l'enfance sont des organismes autonomes mandatés par le ministère des Services à l'enfance et des Services sociaux et communautaires du gouvernement de

l'Ontario de fournir des services de protection de l'enfance. Leur objet est de promouvoir les intérêts, la protection et le bien-être des enfants.

Ontario Cyber Security Higher Education Consortium (ON-CHEC) : ON-CHEC aborde les enjeux de cybersécurité et travaille pour le maintien d'une posture favorable de l'Ontario en matière de recherche et d'éducation dans le domaine. Le consortium fournit des conseils pour rentabiliser la gestion des risques numériques, des programmes et des services qui répondent aux besoins en recherche, en éducation et en innovations de l'écosystème numérique.

Rogers Cybersecure Catalyst : Le Rogers Cybersecure Catalyst est un centre national privé d'innovations et de collaboration en cybersécurité dirigé par l'Université métropolitaine de Toronto. Le centre travaille avec l'industrie, les gouvernements, des partenaires du milieu universitaire pour aider le public et les entreprises canadiennes à s'attaquer aux défis de la cybersécurité et à maintenir un écosystème numérique sûr.

Centre des opérations de sécurité : Un centre des opérations de sécurité est un service centralisé qui emploie des ressources humaines, des processus et les technologies pour surveiller et améliorer la posture des organismes en matière de sécurité tout en prévenant, en détectant, en analysant les cybermenaces et en intervenant en cas d'incidents.

Hameçonnage téléphonique : Il s'agit d'un type de fraude semblable à l'hameçonnage par courriel qui consiste en une attaque par piratage psychologique pour convaincre une victime de partager des renseignements personnels par téléphone.

Annexe B : biographies des membres du Groupe d’experts en cybersécurité

Robert Wong, Président

M. Wong est membre du conseil d’administration de la Société indépendante d’exploitation du réseau d’électricité, siégeant à son conseil organisationnel et à son comité de vérification, ainsi que directeur de Hesketh Sloane Advisory, qui offre des services de consultation en gestion. Il a pris sa retraite après avoir été vice-président directeur et directeur de l’information à Toronto Hydro. Il était responsable, entre autres, des technologies de l’information, des technologies opérationnelles, de la cybersécurité et des télécommunications. M. Wong a siégé au conseil d’administration, au comité des finances et de la vérification, ainsi qu’au comité de recherche de l’Échange canadien de menaces cybernétiques, et a exercé les fonctions de cadre responsable du Projet des protégées de l’organisme Les femmes en communications et technologie. Il détient un baccalauréat en sciences appliquées en génie électrique de l’Université de Toronto, une maîtrise en administration des affaires de la Schulich School of Business de l’Université York, et le titre de directeur agréé du Directors College, une collaboration entre l’Université McMaster et Le Conference Board du Canada.

Adam Evans, Vice-président

Monsieur Evans est vice-président des cyberopérations et directeur général de la sécurité de l’information à la Banque Royale du Canada. Ses responsabilités comprennent les cyberopérations mondiales, la cyberstratégie, la gestion des cybercrises, la conformité réglementaire en matière de cybersécurité, les partenariats industriels et la gouvernance. Monsieur Evans détient les certifications professionnelles CISSP (Certified Information System Security Professional), CISA (Certified Information System Auditor) et CISM (Certified Information System Manager).

Derek Bowers, Membre

Monsieur Bowers est directeur général des technologies de l'information à la ville de Wasaga Beach. Titulaire d'un diplôme spécialisé en programmation informatique du Georgian College, il possède plus de 25 années d'expérience dans le domaine de l'informatique. Avant d'entrer au service de la ville de Wasaga Beach, Monsieur Bowers a fourni une expertise informatique à l'Association canadienne pour la santé mentale à Barrie et au ministère canadien de la Défense nationale à la base des Forces canadiennes Borden. Monsieur Bowers siège au Groupe de travail gouvernemental sur le numérique de l'Association des municipalités de l'Ontario et est un membre actif de l'ASIM.

Marc Coyle, Membre

M. Coyle est chef de la technologie de l'information à la Ville de Bellville depuis 30 ans. Il est trésorier de l'Association des systèmes d'information municipale (MISA) du Canada et ancien directeur des communications et directeur de la région de l'Est de l'ASIM Ontario. M. Coyle est titulaire d'un diplôme en science informatique du Collège Loyalist.

Scott Currie, Membre

Monsieur Currie a occupé le rôle de premier directeur de la sécurité de l'information à l'hôpital pour enfants malades SickKids depuis 2016. En 2011, il se joignait à au réseau public d'hôpitaux de recherche et d'enseignement de Toronto (University Health Network) dans son rôle conjoint. Il possède 20 ans d'expérience en cybersécurité, en gouvernance et en opérations des TI, ainsi qu'en audit de cybersécurité auprès d'organisations de consultation, de sociétés du Fortune 100, et de jeunes pousses du secteur des technologies. Monsieur Currie est titulaire d'un baccalauréat ès arts en économie de l'Université Laurentienne et d'une maîtrise en gestion des systèmes d'information de l'Université Carnegie Mellon.

Hélène Fournier, Membre

Madame Fournier est directrice générale du centre Valoris pour enfants et adultes de Prescott-Russell. Elle est membre de l'Ordre des travailleurs sociaux et des techniciens en travail social de l'Ontario. Madame Fournier est titulaire d'une maîtrise en service social de l'Université Laval, d'un baccalauréat en travail social de l'Université du Québec en Outaouais, à Gatineau, et d'un baccalauréat en service social avec mineure en criminologie de l'Université d'Ottawa.

Carolyn Glaser, Membre

Madame Glaser est directrice générale des services de technologie de l'information du Thames Valley District School Board. Elle est actuellement membre du conseil d'administration et secrétaire du Réseau informatique éducationnel de l'Ontario, membre du Comité directeur de la Stratégie pour la cyberprotection, présidente du Comité de gestion stratégique d'Aspen et chef de projet professionnelle au sein du Project Management Institute. Madame Glaser détient un diplôme de premier cycle de l'Université de Waterloo, un diplôme de deuxième cycle de l'Université de Guelph et possède plus de 20 années d'expérience en leadership stratégique dans le secteur des technologies de l'information.

Antoine Haroun, Membre

Monsieur Haroun est directeur général de l'information du Peel District School Board. Il était auparavant directeur des technologies de l'information pour la municipalité régionale de Halton, directeur général de l'information au Mohawk College et directeur au sein de la fonction publique de l'Ontario. Monsieur Haroun a siégé au conseil d'administration de l'Association canadienne des CIO (section de Toronto). Il est titulaire d'un baccalauréat et d'une maîtrise en sciences appliquées et en génie civil de l'Université de Toronto.

Andrew Kirsch, Membre

M. Kirsch a été agent du renseignement au sein du Service canadien du renseignement de sécurité pendant un peu moins de 10 ans. Il a exercé les rôles d'analyste des politiques et d'enquêteur sur le terrain, et a par la suite dirigé l'équipe de sécurité des opérations spéciales chargée de diriger les opérations secrètes justifiées de surveillance technique. Aujourd'hui, il dirige une société d'experts-conseils en sécurité qui aide les organisations et les particuliers à déterminer les menaces et les vulnérabilités, de même qu'à mettre en œuvre des stratégies pour atténuer les risques. Avant de démarrer son entreprise, M. Kirsch exerçait les fonctions de premier agent ministériel de la sécurité au Bureau du conseiller provincial en matière de sécurité de l'Ontario, ayant pour mandat de renforcer la sécurité matérielle, du personnel, de l'information et des réseaux dans l'ensemble de la fonction publique de l'Ontario.

Isaac Straley, Membre

Monsieur Straley est directeur général de la sécurité de l'information à l'Université de Toronto. M. Straley occupe ce poste inaugural à l'Université de Toronto depuis décembre 2018. Auparavant, il a occupé le double poste de directeur général de la sécurité de l'information et de directeur de la protection de la vie privée à l'Université de Californie à Irvine, où il a travaillé pendant 13 ans. Dans le cadre de son rôle actuel, M. Straley supervise le programme de sécurité de l'information, où il est appelé à veiller à ce que les réseaux, les systèmes et l'information de l'Université de Toronto soient protégés et respectent les exigences réglementaires et stratégiques. Il est également chargé de déterminer et d'évaluer les risques pour la sécurité de l'information, ainsi que de les signaler au Information Security Council et à l'équipe administrative principale de l'Université. M. Straley a été nommé directeur général de la sécurité de l'information de l'année lors du CISO Forum Canada en 2021.