



Réponse du SNDPI aux demandes du CDPISP

Réunion du mois de septembre 2018

Préparé pour le compte du SNDPI avec la contribution des membres du Comité par
Robert Samuel, président du SNDPI et dirigeant principal de la cybersécurité (DPC) de la Nouvelle-Écosse
Mohammad Qureshi, vice-président du SNDPI et dirigeant principal de la sécurité de l'information (DPSI) de
l'Ontario

Gary Perkins, secrétaire du SNDPI et dirigeant principal de la sécurité de l'information (DPSI) de la
Colombie-Britannique

Le 28 août 2018

OBJECTIF

Les membres du Conseil des dirigeants principaux de l'information du secteur public (CDPISP) ont cerné plusieurs sujets d'intérêt et ont réservé 45 minutes pour étudier sommairement les sujets suivants et en discuter au cours de la réunion du mois de septembre à Whitehorse :

- *Compte rendu de la réunion de juin 2018 du SNDPI à Halifax.*
- *Rapport d'étape sur les mesures à prendre (matrice de cybersécurité).*
- *Confirmer le mandat et le plan de travail du SNDPI.*

Le document qui suit résume ces sujets.



1. COMPTE RENDU DE LA RÉUNION DU SNDPI AU PRINTEMPS 2018 – DU 5 AU 8 JUIN 2018 – HALIFAX (N.-É.)

Organisations participantes

La réunion a attiré beaucoup de participants, dont les suivants :

- DPSI provinciaux (10)
- Secrétariat du Conseil du Trésor du Canada (SCT)
- Sécurité publique Canada (SPC)
- ASIM (Est, Ouest, Prairies)

Mises à jour des secteurs de compétence

Chaque organisation participante a présenté au groupe une mise à jour des secteurs de compétence, qui a donné lieu à une discussion en table ronde, à un échange d'information et aux points saillants des mesures possibles et des points du plan de travail que le SNDPI pourrait examiner collectivement. La majeure partie de la discussion a porté sur les priorités, les enjeux, les défis, les menaces et les stratégies tactiques pour prévenir, détecter et réagir aux cyberattaques et gérer adéquatement les risques opérationnels liés à la cybersécurité.

Au cours des mises à jour, il y avait plusieurs thèmes communs pour tous les secteurs de compétence, notamment :

Attirer et maintenir en poste les talents en sécurité.

Ressources nécessaires pour exécuter les fonctions de sécurité.

- Elles augmentent en fonction des services professionnels.

Adoption de l'informatique en nuage, préparation et implications en matière de sécurité.

- Il est essentiel d'éduquer les utilisateurs sur la sécurisation des configurations et l'utilisation du nuage.

Vitesse de commercialisation et commodité pour l'utilisateur.

- Tendance à présenter des risques plus élevés pour la sécurité.

Le SNDPI tire parti d'instruments d'approvisionnement conjoints (réduction du double emploi, des coûts et du temps de livraison).

Thèmes stratégiques communs

Les mises à jour des secteurs de compétence ont fourni des occasions de collaboration entre les secteurs de compétence dans les secteurs suivants :

- éducation et sensibilisation en matière de cybersécurité;
- établissement d'une hygiène de base en matière de sécurité avec des mesures critiques;
- politique et gouvernance en matière de sécurité de l'information;
- Stratégie en matière de sécurité de l'information;
- pratiques techniques exemplaires (p. ex., HTTPS Everywhere);
- mesures d'atténuation nécessaires (p. ex., visibilité des logiciels malveillants);
- modernisation de l'infrastructure (p. ex., authentification à facteurs multiples);
- identification des actifs, gestion et correction des vulnérabilités.



Collaboration du SNDPI avec les intervenants et les partenaires de l'industrie

Amazon Web Services (AWS) (Cloud)

Grant Streeter, chef de la sécurité d'AWS au Canada, a fait une présentation sur AWS et a décrit les capacités de sécurité offertes par la société ainsi que plusieurs caractéristiques qui seront mises à la disposition des organisations qui collaboreront avec AWS au Canada. La rigueur en matière de sécurité d'AWS, sa transparence, ses caractéristiques, son leadership en matière de nuage et son modèle « sans contrat » avec paiement à l'utilisation en font une option attrayante et viable pour le CDPISP.

SERENE-RISC (Réseau intégré sur la cybersécurité) (Mobilisation des connaissances)

Michael Joyce du « Réseau intégré sur la cybersécurité » a présenté SERENE-RISC dont l'objectif est d'être un réseau d'échange d'information sur la cybersécurité reconnu comme un forum ouvert, inclusif et impartial pour tous les Canadiens. La discussion a permis de cerner des défis en matière de sécurité auxquels font face les organisations partout au Canada et Michael a invité les participants à participer au forum et à aider à cerner les défis et les solutions qui pourraient être abordés collectivement.

Groupe CSA (sécurité de l'Internet des objets)

Stephen Michell de l'Association canadienne de normalisation (CSA) a fait un exposé sur l'Internet des objets (IdO) et la nécessité de mesures de sécurité adéquates pour protéger les citoyens. Les dispositifs de l'IdO dotés de mesures de sécurité insuffisantes représentent une menace importante, surtout dans le monde des soins de santé où les patients dépendent de dispositifs médicaux avec des systèmes intégrés.

Centre canadien de cybersécurité

Le gouvernement fédéral a communiqué son rapport intitulé « Cybermenaces contre le processus démocratique du Canada » ou une séance d'information connexe à la haute direction afin de la sensibiliser aux attaques et aux risques contre le processus démocratique du Canada.

Le gouvernement fédéral a également fait le point sur le Centre canadien pour la cybersécurité (CCC) et des renseignements supplémentaires sont attendus en octobre 2018. Il y a encore beaucoup d'incertitude quant à la façon dont les changements organisationnels au sein du gouvernement fédéral et le mandat et la vision du CCC se répercuteront sur les provinces, les territoires et les municipalités.



DEMANDE 2 : RAPPORT D'ÉTAPE SUR LES MESURES DE SUIVI

Plusieurs mesures de suivi ont été déposées à la réunion du CDPISP du 22 février 2018. La section ci-dessous présente un aperçu de chacune des mesures de suivi du SNDPI et une mise à jour de chacune d'entre elles :

2.A. METTRE À JOUR ET TENIR À JOUR LA MATRICE DE CYBERSÉCURITÉ

La matrice de cybersécurité a été créée pour assurer le suivi des mesures pour toutes les entités participantes du SNDPI, notamment :

- capacités des services de cybersécurité (p. ex., protection, détection, intervention, etc.);
- intervenants appuyés par des secteurs de compétence (p. ex., ministères, éducation, services publics, infrastructures essentielles, etc.);
- disponibilité des artéfacts de cybersécurité (p. ex., lois, règlements, politiques, normes, etc.).

Les intervenants n'ont signalé aucun changement notable à la matrice de cybersécurité.
Le document sera mis à jour à mesure de l'évolution du projet.

2.B. FAIRE RAPPORT AU CDPISP SUR LA FAÇON DONT LE GOUVERNEMENT PEUT INCITER LES ÉCOLES À INCLURE LA CYBERSÉCURITÉ DANS LEUR PROGRAMME D'ENSEIGNEMENT.

Le SNDPI prévoit présenter les exposés de position suivants dans le cadre de cette mise à jour :

- Développement de ressources spécialisées en cybersécurité (participation des gouvernements aux programmes d'enseignement postsecondaire afin de développer davantage de talents et de ressources spécialisées en cybersécurité).
- Sensibilisation à la cybersécurité dans le système scolaire de la maternelle à la 12^e année (participation du gouvernement à la formation sur la cybermenace et la sensibilisation à la cybersécurité pour les élèves de la maternelle à la 12^e année).

Ces exposés de position ont été reportés en raison de problèmes de capacité parmi les participants.

2.D. EXAMINER DE PLUS PRÈS LES RÉALISATIONS RÉCENTES DU SNDPI ET LES EXIGENCES NATIONALES EN MATIÈRE DE CYBERSÉCURITÉ QUI POURRAIENT NE PAS ÊTRE RESPECTÉES À L'HEURE ACTUELLE AFIN DE RÉVISER LE MANDAT DU COMITÉ D'ICI L'AUTOMNE 2018 DANS LE BUT D'AMÉLIORER LA POSITION GLOBALE DU CANADA EN MATIÈRE DE CYBERSÉCURITÉ.

Le CDPISP se concentre sur les questions intergouvernementales de technologie de l'information et de gestion de l'information. En tant que forum pancanadien des dirigeants et des représentants du secteur public en matière de cybersécurité, le SNDPI a fourni et continue d'offrir un soutien et une valeur à ce conseil et il est mutuellement avantageux pour les organismes participants, les représentants et les conseils mixtes.

Il est aussi reconnu que la cybersécurité est devenue un enjeu important dans tous les secteurs d'activités et pour toutes les industries puisque la convergence de l'information, de la technologie de l'information, des techniques

DPI national
Sous-comité sur la
protection de l'information



d'exploitation et tous les autres appareils numériquement connectés peuvent avoir des répercussions considérables comme : des pertes de productivité (infections virales), des pertes financières (fraudes financières par voie électronique), des événements commerciaux néfastes (violations de données), des urgences nationales (pannes de courant) et même des effets sur la santé et la sécurité personnelle (prestation de soins et de services médicaux aux patients ou changes non autorisés à l'équipement hydroélectrique).

Le SNDPI a discuté de ces questions et a réfléchi aux objectifs stipulés par le comité :

1. Échanger de l'information et des pratiques exemplaires et recommander des priorités, des objectifs et des programmes nationaux et provinciaux en matière de protection de l'information.
2. Créer, élaborer et appuyer conjointement des procédures opérationnelles et des outils automatisés pour veiller à ce que tous les secteurs de compétence au Canada respectent les normes les plus élevées en matière de protection de l'infrastructure de l'information.

Le groupe s'est posé les questions suivantes :

- Le SNDPI devrait-il poursuivre sur sa voie actuelle?
- A-t-il déjà évolué pour devenir une tribune plus large (p. ex., au-delà de la protection de l'information)?
 - Le travail du SNDPI pour étudier et recommander des stratégies pour les programmes postsecondaires de cybersécurité et l'éducation de la maternelle à la 12^e année constituent un bon exemple de cette évolution.
- Si le SNDPI a déjà évolué, a-t-il dépassé son mandat prévu?
- Doit-il évoluer davantage?
- Quelle sera l'incidence de l'établissement du Centre canadien de cybersécurité (CCC) sur les structures existantes?

Compte tenu de l'annonce de la création du CCC et de l'échéancier connexe, le SNDPI préparera un exposé de position à ce sujet.



DEMANDE 3 : CONFIRMER LE MANDAT ET LE PLAN DE TRAVAIL DU SNDPI.

Confirmer le mandat du SNDPI

Tous les membres du SNDPI conviennent qu'appuyer le CDPISP dans ses domaines d'intérêt en matière de technologie de l'information et de mandat d'information est une exigence et un avantage continu. Le SNDPI examinera le mandat afin de veiller à ce qu'il reflète fidèlement les besoins du CDPISP, déterminer s'il y a des lacunes et proposer des recommandations. Cela coïncidera avec un dialogue entre le CST et le CCC pour collaborer à la vision pancanadienne de la cybersécurité et à une approche globale et simplifiée.

Plan de travail

Le plan de travail du SNDPI comprend les éléments suivants :

- Inviter le CST et le CCC à participer activement au SNDPI et à établir un dialogue de collaboration à l'avenir;
- Examiner et mettre à jour le mandat du SNDPI afin de veiller à ce qu'il reflète fidèlement les besoins du CDPISP;
- Exposé de position du SNDPI à paraître :
 - Développement de ressources spécialisées en cybersécurité (participation des gouvernements aux programmes d'enseignement postsecondaire afin de développer davantage de talents et de ressources spécialisées en cybersécurité).
 - Sensibilisation à la cybersécurité dans le système scolaire de la maternelle à la 12^e année (participation du gouvernement à la formation sur la cybermenace et la sensibilisation à la cybersécurité pour les élèves de la maternelle à la 12^e année).
- Nouveaux énoncés de position (candidats) :
 - HTTPS partout
 - Modernisation de l'authentification des utilisateurs (passage des mots de passe aux phrases de passe)
 - Adoption de l'authentification à facteurs multiples
 - Intelligence artificielle
 - Possibilités de sécurité
 - Considérations liées à la sécurité
 - Préparation à l'adoption de l'informatique en nuage
 - Un énoncé de position sur le nuage
 - Exposés de positions complémentaires pour différents domaines :
 - Classification des données
 - Éducation des utilisateurs sur l'utilisation et la configuration sécurisées du nuage
 - Surveillance des services d'informatique en nuage
 - Règlement général sur la protection des données
- Plateforme pancanadienne (exercice dirigé par Sécurité publique Canada)
 - P. ex. : un scénario de propagation du logiciel malveillant Wannacry

DPI national
Sous-comité sur la
protection de l'information



Le SNDPI a besoin de l'aide du CDPISP :

« Utiliser plus efficacement les ressources publiques limitées par la mise en commun de fonds pour des initiatives; permettre aux administrations plus petites de profiter de l'expertise et des ressources du gouvernement fédéral et des provinces plus importantes »

- Éliminer les obstacles (approvisionnement, outils, capacités et services communs (p. ex., tirer parti des économies de SPC et du GC).



EN CONCLUSION

Si vous avez d'autres questions ou préoccupations, veuillez communiquer avec l'un des agents du SNDPI :

- **Président du SNDPI** : Robert Samuel, DPC de la Nouvelle-Écosse Robert.Samuel@novascotia.ca Téléphone : 902-222-6685.
- **Vice-président du SNDPI** : Mohammad Qureshi, DPSI de l'Ontario Mohammad.Qureshi@ontario.ca Téléphone : 416-327-0413.
- **Secrétaire du SNDPI** : Gary Perkins, DPSI de la Colombie-Britannique Gary.Perkins@gov.bc.ca Téléphone : 250-387-7590.