Comité d'experts pour la cybersécurité dans le secteur parapublic

Rapport provisoire de la présidence – Le 15 décembre 2020

Introduction

Dans le cadre du mandat du Comité d'experts pour la cybersécurité dans le secteur parapublic, qui consiste à « évaluer et à cerner les difficultés et les thèmes communs et particuliers touchant les organismes et les partenaires de prestation de services dans le domaine de la cybersécurité en Ontario », le président a mené des entrevues avec chaque membre du Comité d'experts et avec d'autres intervenants du gouvernement et du secteur parapublic entre le 23 novembre et le 3 décembre 2020.

Des commentaires ont été reçus de la part de représentants des secteurs suivants : municipalités, hôpitaux, établissements d'enseignement supérieur, conseils scolaires publics de districts et un organisme de services sociaux. Ces répondants ont été invités à décrire les principaux problèmes et obstacles qui les empêchent de mieux gérer les risques pour la cybersécurité dans leurs organismes respectifs, et à suggérer des solutions possibles pour améliorer le rendement.

Ce qui suit est un résumé des points saillants qui ont été soulevés pendant les entrevues.

Résumé des conclusions

Degrés de maturité

Dans tous les secteurs, il semble exister une gamme assez large de capacités et de maturité en matière de cybersécurité au sein de chaque secteur. De prime abord, la rétroaction laisse penser que le degré de maturité des organisations varie de faible à moyen. Bien qu'aucune évaluation plus rigoureuse par rapport à un modèle formel d'évaluation de la maturité n'ait encore permis de la confirmer, cette conclusion semble tout à fait raisonnable, d'après les discussions qui ont eu lieu avec les répondants interviewés. Comme preuve à l'appui, mentionnons que dans plusieurs grands organismes du secteur parapublic, la création d'un poste spécialisé en cybersécurité (par exemple, celui de directeur général de la sécurité de l'information ou DGSI) ne date que de quelques années. La cybersécurité figure au second plan des qualifications requises pour le personnel d'infrastructure de technologie de l'information (TI), lequel englobe certains secrétaires municipaux ayant un rôle en TI. En général, les petits organismes se situent au bas du spectre de la capacité et de la maturité.

Contraintes liées aux ressources

Quelle que soit la taille de l'organisation, les répondants expriment généralement le désir de disposer de meilleures ressources en cybersécurité, qu'il s'agisse de financement, de personnel ou de compétences techniques. Dans les plus petits organismes, le service de TI se compose de trois ou quatre employés qui accomplissent avec peine les fonctions essentielles de la TI et n'ont que peu de temps ou de compétences à consacrer à la gestion responsable de la cybersécurité. Tant bien que mal, ils mettent en œuvre des méthodologies très rudimentaires de cybersécurité dans leurs milieux technologiques.

Le manque de professionnels qualifiés en cybersécurité aggrave encore le problème. On constate actuellement sur le marché une forte demande d'experts en sécurité de niveau supérieur. Pour les organismes de petite taille qui ne sont pas situés à proximité ou à l'intérieur d'une des régions densément peuplées de la province, le coût et le manque de personnel talentueux dans leurs localités représentent d'importants obstacles à l'obtention de ces compétences. Un modèle régional de partage de services pourrait être la seule solution viable pour permettre à ces acteurs plus modestes d'accéder à des compétences techniques limitées sur le marché.

Même dans les grands organismes, le financement de la cybersécurité (et de la TI en général) n'est pas priorisé autant qu'il serait opportun ou juste de le faire, en raison de la concurrence acharnée des autres besoins primordiaux pour les budgets. Cela dit, les principaux acteurs sont certainement mieux placés pour répondre aux exigences de la gestion responsable de la cybersécurité, étant donné l'importance de leur personnel et des budgets dont ils disposent. Malgré cela, il serait peut-être possible d'améliorer l'efficience en déployant des outils d'automatisation destinés aux équipes de cybersécurité qui consacrent actuellement une grande partie de leur temps à exécuter des tâches et des procédés manuels.

Systèmes patrimoniaux

Comme le problème des contraintes liées aux ressources, la question des systèmes patrimoniaux est un thème commun parmi tous les représentants des membres du secteur parapublic. L'incapacité de remplacer des systèmes patrimoniaux désuets et non assistés complique énormément la gestion efficace de la cybersécurité. Certains systèmes patrimoniaux sont dépourvus de fonctions de sécurité standards telles que le contrôle de l'accès, l'intégrité des données, l'authentification, le verrouillage de mots de passe et les journaux d'audit. L'utilisation de logiciels commerciaux non assistés signifie que les fournisseurs n'offrent plus de rustines de sécurité permettant de corriger les nouveaux points vulnérables sur le plan de la sécurité. De même, la « dette technique » résultant des logiciels personnalisés mal codés contribue aux risques pour la

cybersécurité lorsque les développeurs de ces logiciels n'ont pas reçu la formation appropriée pour écrire des codes sécurisés. En outre, le développement de logiciels de qualité inférieure crée des complexités, entrave l'amélioration continue et pose un très grand obstacle à la gestion efficace et sécurisée des systèmes de TI.

Le remplacement des systèmes patrimoniaux et l'acquittement de la dette technique ne sont pas des tâches insignifiantes. Cette mesure exige un engagement rigoureux et formel en matière de gestion des biens de TI, de manière à répertorier tous les biens informatiques (logiciels et matériel), à fixer des durées utiles prévues et à prévoir des dates de mise à niveau et/ou de remplacement. L'exécution des activités de mise à niveau ou de remplacement doit aussi s'effectuer en temps utile et selon un cycle vertueux. Il est essentiel de maintenir une bonne hygiène en matière de TI pour réduire les risques liés à la cybersécurité. Cependant, une telle démarche nécessite beaucoup d'efforts, une grande discipline, une feuille de route stratégique bien conçue, un financement régulier et suffisant, des ressources compétentes et la coopération des clients commerciaux qui sont les utilisateurs primaires du système. Néanmoins, cela devrait constituer le but de tout service de TI.

Culture d'entreprise et gouvernance

Un grand nombre de représentants du secteur parapublic se disent mécontents du manque perçu de soutien et de compréhension pour les initiatives de cybersécurité dans leurs organismes respectifs. Lorsqu'ils demandent l'affectation de ressources supplémentaires ou l'augmentation du budget pour les initiatives de cybersécurité, il leur arrive souvent de se heurter au manque de connaissances et de compréhension des principaux décideurs en ce qui concerne les risques et les avantages. Au dire d'un des répondants, « … ils acceptent aveuglément les risques ». Évidemment, la cybersécurité et la TI en général forment des secteurs d'activité qui ne sont traditionnellement pas bien compris par les dirigeants ou les administrateurs, soit les personnes qui sont responsables de la *gouvernance d'entreprise* et qui donnent le ton de la *culture d'entreprise*. De nos jours, la plupart des conseils d'administration se composent en grande partie d'administrateurs formés en comptabilité, en droit et en ressources humaines. Rares sont ceux dont les membres possèdent de l'expérience et une formation en technologie.

Par conséquent, les risques liés à l'accroissement continu de l'empreinte technologique des organismes, ainsi que leur valeur stratégique, ne sont pas reconnus. Cette sous-appréciation de l'importance de la technologie en affaires se manifeste dans des structures organisationnelles où le service de TI (qui englobe habituellement la cybersécurité) relève souvent d'un autre secteur d'activité non pertinent ou avec lequel

il n'y a pas de synergie ou presque. À ce titre, le chef du service de TI (directeur général de l'information ou l'équivalent) n'est pas membre de la direction de l'entreprise et n'a donc pas sa place à table pour soutenir la cause de son service ni exprimer ses préoccupations. Lorsque les dirigeants ne « donnent pas le ton », il s'ensuit un manque d'appui et de coopération de la part des autres dirigeants et du personnel en ce qui a trait aux questions de cybersécurité dans l'entreprise. Frustrés, les membres du personnel de la cybersécurité déplorent leur incapacité à « faire avancer » les programmes de cybersécurité et leur manque d'influence pour obtenir l'appui et l'engagement nécessaires à leurs projets et initiatives dans leurs organismes respectifs.

Une culture d'entreprise qui sous-estime la gravité des risques de cybersécurité est souvent le signe d'un problème lié à la gouvernance d'entreprise. Le conseil d'administration et les cadres de gestion connaissent-ils et comprennent-ils vraiment les principaux risques pour leur entreprise? Ont-ils évalué les répercussions commerciales possibles (continuité des activités, pertes financières, atteinte à la réputation, perte de confiance de la clientèle, perte de moral du personnel, etc.) si et lorsque ces risques critiques se manifestent? Comprennent-ils vraiment les implications? Existe-t-il un programme officiel de gestion globale des risques qui permet de définir et d'évaluer tous les risques pertinents de l'entreprise, de désigner les responsables et d'agir de façon proactive afin de gérer continuellement les risques selon les niveaux de tolérance prévus? La cybersécurité figure-t-elle parmi les dix principaux risques de l'organisation et en discute-t-on régulièrement lors des réunions du conseil et de la direction?

Les systèmes de gestion sont des outils qui favorisent une bonne gouvernance d'entreprise. Ils aident l'équipe de gestion à évaluer le rendement de l'entreprise, à communiquer des rapports et à transmettre des renseignements sur la réalisation des objectifs de rendement définis. Les systèmes de gestion efficaces intègrent généralement divers outils de rendement qui stimulent la réalisation d'objectifs stratégiques clés et qui permettent de veiller à ce que chaque employé sache clairement quels sont ces objectifs et comment contribuer à leur réalisation. Parmi ces outils de gestion, on trouve par exemple les indicateurs de rendement clés (IRC), les cartes de pointage équilibrées, les tableaux de bord, les rapports d'exploitation, les politiques et les normes, les audits internes des contrôles, les méthodologies de gestion du changement, les systèmes de gestion des risques d'entreprise, les buts et objectifs stratégiques et les modèles de rémunération axés sur le rendement.

Lors des entrevues, il est devenu évident que la gouvernance d'entreprise et les systèmes de gestion sont absents dans un grand nombre d'organismes du secteur parapublic. Les professionnels de la cybersécurité doivent donc tâcher de faire de leur

mieux malgré le manque d'outils efficaces. On constate un vif désir d'obtenir des conseils et du soutien, par exemple des normes de cybersécurité, des politiques, des cadres de travail, des modèles de maturité, des pratiques exemplaires, des feuilles de route, des livres de jeux, des services consultatifs, des plateformes d'échange de renseignements sur les menaces et, surtout, l'autonomisation. Certains membres trouvent également que le gouvernement de l'Ontario devrait mieux les appuyer, soit par des services consultatifs, soit par une directive gouvernementale qui rendrait obligatoire la conformité en matière de cybersécurité.

Même dans les institutions où les pratiques de gouvernance d'entreprise sont relativement solides et matures, il reste encore d'importants défis à relever pour gérer efficacement les risques liés à la cybersécurité qui résultent de priorités concurrentes et de l'application incohérente de la surveillance et des politiques. À titre d'exemple, dans l'enseignement supérieur, le financement provient de diverses sources et est attribué en fonction de divers critères. Certains groupes de recherche universitaire qui ont réussi à obtenir des subventions ou des commandites privées considèrent souvent que cet argent leur est dû et les autorise à choisir leurs outils technologiques sans tenir compte des questions de cybersécurité lorsqu'ils en font l'achat. Pourquoi les universités n'imposent-elles pas les mêmes exigences aux chercheurs qu'aux autres professeurs et membres du personnel en matière de cybersécurité?

Dans le système scolaire public, on voit clairement que la sûreté, la sécurité et le mieux-être des élèves et du personnel sont les priorités absolues. Il s'agit manifestement d'une obligation morale que personne ne conteste. Cependant, on transige souvent sur les exigences en matière de cybersécurité afin de pouvoir fournir des services de haut niveau à ces mandants. Pourquoi ne peut-on pas offrir des services de grande qualité en veillant aussi à la sécurité numérique?

Dans le secteur des soins de santé, les budgets des hôpitaux sont généralement affectés soit aux activités de soins aux patients, soit aux activités autres que les soins aux patients. Encore là, nul ne peut dire que les soins aux patients ne sont pas la priorité absolue des hôpitaux. Toutefois, étant donné l'omniprésence de la technologie et la place envahissante qu'elle occupe dans toutes les facettes du monde moderne, que ce soit pour les affaires ou pour notre utilisation personnelle, nous devrions mieux comprendre les risques et les conséquences néfastes associés aux atteintes à la cybersécurité en ce qui concerne les systèmes technologiques des hôpitaux (systèmes d'information, équipement médical numérique, implants et dispositifs de surveillance [Internet des objets ou IdO]) et leurs effets possibles sur la santé et le bien-être des patients.

Recommandations

Compte tenu qu'il existe un large éventail de capacités de base et de niveaux de maturité en matière de cybersécurité parmi les organismes du secteur parapublic, il serait déraisonnable de s'attendre à ce que les moins avancés rattrapent les chefs de file du jour au lendemain. Dans la plupart des cas, la réalisation de cet objectif nécessite des initiatives transformationnelles, des ressources et plusieurs cycles économiques. Les acteurs les plus avancés sont déjà bien engagés sur cette voie, mais les organisations de plus petite envergure et de moindre maturité ont désespérément besoin de conseils, de soutien et d'aide externes.

Afin de fournir une aide immédiate ou à court terme, les recommandations suivantes sont proposées :

1. Que le cadre de cybersécurité du National Institute of Standards and Technology (NIST) soit approuvé par le gouvernement de l'Ontario pour les pratiques de cybersécurité du secteur parapublic. Pour une entité ayant déjà adopté un cadre de cybersécurité autre que celui du NIST, on s'attendra à ce qu'elle aligne son cadre sur celui du NIST afin d'assurer leur compatibilité et leur harmonisation. Sachant que les entités du secteur parapublic sont de taille variable et ont différents profils de risque, il est raisonnable de penser que l'ampleur de la mise en œuvre du cadre de cybersécurité du NIST variera également selon une approche fondée sur les risques. Pour aider les organismes de petite et de moyenne taille à adopter et à mettre en œuvre le cadre du NIST, la publication intitulée « Contrôles de cybersécurité de base pour les petites et moyennes organisations » du Centre canadien pour la cybersécurité est un guide utile qui établit les exigences fondamentales relatives à des pratiques de cybersécurité efficaces et compatibles avec le cadre du NIST.

2. Que toutes les entités du secteur parapublic mettent en œuvre un programme de formation à des fins d'éducation et de sensibilisation en matière de cybersécurité. Le contenu du matériel de formation devra être mis à jour régulièrement pour garantir l'actualité de l'information. Les nouveaux employés recevront la formation dès leur arrivée dans l'entreprise dans le cadre de leur programme d'orientation, et tous les employés existants recevront une formation de recyclage au moins une fois par année. Les spécialistes des technologies de l'information et de la cybersécurité recevront régulièrement une formation technique en cybersécurité pour assurer l'actualisation de leurs compétences. Du matériel pédagogique spécialisé pourra être élaboré à

l'intention des membres des conseils d'administration, des cadres supérieurs et des autres décideurs clés. La gestion efficace des risques de cybersécurité nécessite les efforts et l'engagement de toutes les parties et ne peut pas être simplement déléguée aux professionnels de la cybersécurité. Le « ton donné par les dirigeants » sera un facteur de réussite essentiel pour renforcer la résilience des partenaires de la prestation de services en matière de cybersécurité dans le secteur parapublic.

L'approche décrite dans le présent rapport provisoire et les recommandations proposées sont des mesures progressives. Il n'existe pas de solution miracle pour résoudre les problèmes de cybersécurité auxquels sont confrontés de nombreux partenaires de la prestation de services dans le secteur parapublic. Même avec des ressources illimitées, une telle initiative requiert toujours un solide leadership, de l'engagement, de la discipline, de la persévérance et un plan bien conçu avec une structure, un enchaînement logique des interventions et des échéanciers définis. Il importe d'adopter une approche ascendante et de créer une base solide sur laquelle s'appuyer.

Les recommandations proposées dans le présent rapport provisoire sont des éléments fondamentaux qui peuvent être facilement mis en œuvre (s'ils sont adoptés) et qui permettent une excellente optimisation des ressources. Ces éléments pourraient être considérés comme des projets à « gain éclair ».

Dans ses futures recommandations, le Comité d'experts s'appuiera sur des éléments fondamentaux qui pourront être de nature plus structurelle, opérationnelle, technique ou prospective. En définitive, l'objectif consiste à élaborer une stratégie globale pour faire progresser les pratiques de cybersécurité dans l'ensemble du secteur parapublic, en incluant une feuille de route permettant d'orienter l'exécution de la stratégie.