Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Le 6 janvier 2025

PAR COURRIEL

PERSONNEL

Maître Elmira Chimirova
Avocate principale
Coordonnatrice de l'accès à l'information
Services juridiques
Toronto District School Board
5050, rue Yonge
Toronto ON M2N 5N8

Objet : Atteinte à la vie privée MR23-00097

Maître,

Le 12 octobre 2023, le Toronto District School Board (le « conseil scolaire » ou le « TDSB ») a signalé une atteinte à la vie privée en contravention de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (la « *Loi* » ou la « LAIMPVP ») au Bureau du commissaire à l'information et à la protection de la vie privée (CIPVP), qui a ouvert le dossier MR23-00097 pour traiter cette affaire.

Cette atteinte à la vie privée a fait intervenir l'accès non autorisé d'un auteur de menace inconnu à des renseignements concernant des élèves actuels, d'anciens élèves, des parents et des membres du personnel de cinq écoles du TDSB, et l'exfiltration éventuelle de ces renseignements. Cet individu a accédé sans autorisation aux systèmes des écoles en question en obtenant les données d'accès d'une directrice adjointe d'une école par piratage psychologique, ainsi que l'accès non autorisé à un cache de navigateur de la directrice adjointe.

I. Contexte

Que s'est-il passé?

Le 6 octobre 2023, le TDSB a découvert que l'une de ses écoles avait été la cible d'une cyberattaque lorsqu'un auteur de menace a publié sur Telegram (un service de messagerie instantanée) des messages alertant l'école de cette attaque. Celle-ci a fait intervenir l'accès non autorisé à des organisateurs appartenant à la directrice adjointe du Lakeshore Collegiate Institute (LCI). L'auteur de menace a accédé à des renseignements personnels contenus dans les ordinateurs et le compte OneDrive de la directrice adjointe qui concernent des élèves actuels, d'anciens élèves,

des parents et de membres du personnel de cinq écoles du TDSB, y compris le LCI, et les a peut-être exfiltrés.

Le conseil scolaire a établi que les ordinateurs de la directrice adjointe avaient été compromis le 28 septembre 2023, le premier accès non autorisé à des renseignements personnels ayant eu lieu le 3 octobre 2023. Le TDSB croit que l'auteur de menace a volé les données d'accès de la directrice adjointe du conseil scolaire par piratage psychologique; ensuite, il a accédé à l'ordinateur de bureau et à l'ordinateur portable de la directrice adjointe sur place dans son bureau, puis a compromis son compte OneDrive. Le conseil scolaire croit que l'auteur de menace a obtenu les données d'accès à OneDrive de la directrice adjointe à partir du cache du navigateur de son ordinateur.

Lors de son attaque, l'auteur de menace a utilisé une clé USB qui, selon le conseil scolaire, avait été programmée pour servir de « voleur d'informations ». L'auteur de menace a eu accès à des renseignements contenus dans le compte OneDrive, notamment des renseignements personnels sur des élèves actuels, d'anciens élèves, des parents et des membres du personnel du LCI et de quatre autres écoles. Cette attaque a également touché deux serveurs Web du conseil scolaire, et le site Web du LCI a été piraté par l'affichage d'un message de menaces.

L'auteur de menace a publié sur Telegram un message dans lequel il menaçait de divulguer les renseignements exfiltrés à moins que le conseil scolaire n'informe le public de cet incident dans un délai précis. Le 16 octobre 2023, l'auteur de menace a supprimé toutes ses publications en ligne sur cette affaire, et le conseil scolaire a alors conclu qu'il avait retiré ses exigences.

Le fournisseur autorisé de services de sécurité du conseil scolaire a mené une enquête. Le conseil scolaire ne dispose d'aucune indication sur l'identité de l'auteur de menace, mais il croit qu'il s'agit probablement d'une personne qui est allée dans le bureau de la directrice adjointe alors que celle-ci s'était absentée. Le conseil scolaire soutient que son enquête n'a permis de trouver aucune preuve voulant que l'auteur de menace ait exfiltré des renseignements personnels, mais il n'a fourni aucune précision à ce sujet au CIPVP.

II. Enjeux

Les institutions qui subissent une atteinte à la vie privée faisant intervenir des renseignements personnels doivent prendre des mesures appropriées : déterminer la portée de l'atteinte à la vie privée, la maîtriser, aviser les personnes concernées, mener une enquête et prendre des mesures correctives. Le CIPVP a publié des lignes directrices aux institutions à ce sujet dans son document *Les atteintes à la vie privée : lignes directrices pour les organismes du secteur public*[1].

Il est incontesté que le TDSB est une institution et que les renseignements auxquels l'auteur de menace a eu accès de façon irrégulière sont des renseignements personnels au sens du paragraphe 2 (1) de la *Loi.*

[1] Les atteintes à la vie privée : lignes directrices pour les organismes du secteur public

Les questions suivantes ont été posées au cours de l'examen de cette atteinte à la vie privée au stade du règlement anticipé :

1) **Le TDSB a-t-il pris des mesures adéquates pour maîtriser l'atteinte à la vie privée?**
2) **Le TDSB a-t-il pris des mesures adéquates pour aviser les particuliers concernés par l'atteinte à la vie privée?**
3) **Le TDSB a-t-il pris des mesures correctives raisonnables pour éviter qu'une telle atteinte à la vie privée ne se reproduise?**

Le TDSB a-t-il pris des mesures adéquates pour maîtriser l'atteinte à la vie privée?

D'après son analyse des données concernées, le TDSB a établi que l'auteur de menace avait accédé sans autorisation à des renseignements personnels concernant des élèves actuels, d'anciens élèves et des parents de cinq écoles. Il avait également accédé à des renseignements sur des membres du personnel.

Appelé à préciser combien de particuliers avaient été touchés par cet incident, le conseil scolaire a fait savoir que des élèves actuels, d'anciens élèves et des parents de cinq écoles étaient concernés. Il n'a pas fourni le nombre estimatif de personnes concernées.

Les renseignements personnels consultés de façon irrégulière comprenaient les suivants : nom des élèves, numéros d'élève, dates de naissance, années d'études, matières, horaires de cours, calendriers, adresses courriel, cours réussis ou échoués, adresse courriel des parents et coordonnées. Dans certains cas, des formules d'éducation spécialisée et des numéros de carte Santé ont été consultés et exfiltrés.

Le 6 octobre 2023, le TDSB a découvert qu'une de ses écoles avait fait l'objet d'une cyberattaque lorsque l'auteur de menace a affiché des messages sur Telegram pour l'en alerter. Sur Telegram, l'auteur de menace a menacé de divulguer les renseignements exfiltrés si le TDSB n'informait pas le public de l'incident dans un délai précis. Le conseil scolaire croit que l'auteur de menace a retiré ses exigences, car il a supprimé toutes ses publications en ligne sur cette affaire.

Pour maîtriser l'atteinte à la vie privée, le conseil scolaire a déconnecté les ordinateurs de la directrice adjointe et obtenu des images disques à des fins d'enquête. Il a également déconnecté le site Web du LCI du réseau. Le conseil scolaire a demandé à tous les membres du personnel de LCI de changer leurs mots de passe et d'activer l'authentification multifacteur pour tous les utilisateurs du LCI, et les services de TI du TDSB ont rétabli les images disques de tous les ordinateurs du LCI.

TDSB a également fait appel aux services d'un spécialiste des atteintes à la vie privée et négociateur.

D'après les renseignements dont je dispose, il semble que l'atteinte à la vie privée n'ait pas été maîtrisée. Le conseil scolaire a dit croire que l'auteur de menace avait retiré ses exigences parce qu'il avait supprimé ses publications en ligne sur cette affaire, mais il s'agit là d'une hypothèse et

non d'une conclusion fondée sur des faits. Aucune indication permettant d'étayer l'affirmation du TDSB selon laquelle les renseignements auxquels l'auteur de menace a eu accès n'ont pas également été volés ne m'a été fournie.

Je considère toutefois que le conseil scolaire a pris des mesures raisonnables pour maîtriser l'atteinte à la vie privée.

Le TDSB a-t-il pris des mesures adéquates pour aviser les particuliers concernés par l'atteinte à la vie privée?

Soulignons d'abord que rien dans la *Loi* n'oblige l'institution qui a la garde ou le contrôle de renseignements personnels à aviser les particuliers concernés par ces renseignements si ces derniers ont fait l'objet d'une atteinte à la vie privée. Comme il est indiqué dans le document *Les atteintes à la vie privée : lignes directrices pour les organismes du secteur public* du CIPVP, l'institution devrait aviser les personnes concernées si l'atteinte à la vie privée risque de leur causer un préjudice important, en tenant compte du caractère délicat des renseignements et de la probabilité d'usage abusif.

Le 12 octobre 2023, le conseil scolaire a remis une lettre aux membres actuels de la communauté du LCI (élèves, parents d'élèves et membres du personnel de l'école) les informant de l'atteinte à la vie privée. Cet avis contenait des précisions sur cet incident, les mesures prises, le fait que le conseil scolaire en avait informé le CIPVP, des renseignements sur la façon de porter plainte au CIPVP et les coordonnées d'un responsable du TDSB à qui les particuliers pouvaient s'adresser pour toute question. Cet avis ne comportait pas de description des renseignements personnels en cause, car le TDSB ignorait encore de quels renseignements il s'agissait. Après avoir envoyé cet avis aux membres actuels de la communauté du LCI, le TDSB a donné un avis aux membres actuels des autres écoles touchées.

Le conseil scolaire a affirmé qu'il ne disposait pas des coordonnées des anciens élèves, parents et membres du personnel concerné, et qu'il avait l'intention de donner un avis public général. À cette fin, il a demandé conseil au CIPVP.

Le CIPVP a recommandé au conseil scolaire d'afficher son avis général à des endroits visibles dans chaque école, et de le publier dans le site Web de chaque école et dans celui du conseil scolaire.

Le 19 avril 2024, le conseil scolaire a fourni au CIPVP une ébauche d'avis général pour examen. Cet examen a révélé que les particuliers concernés étaient informés que l'on avait eu accès à leurs renseignements personnels, mais pas que l'auteur de menace avait ou aurait pu avoir exfiltré ces renseignements. Le 23 avril 2024, le CIPVP a recommandé au conseil scolaire de modifier son avis général pour faire savoir aux particuliers concernés que l'on avait eu accès à leurs renseignements personnels et que ces derniers avaient été exfiltrés. Au moment de la rédaction du présent rapport, le CIPVP n'avait reçu aucune preuve montrant qu'il n'y avait pas eu exfiltration.

Le 25 avril 2024, l'école a fourni une ébauche modifiée de son avis général. Cet avis modifié ne comportait aucune mention informant les particuliers concernés du fait que l'auteur de menace aurait pu avoir exfiltré leurs renseignements personnels. TDSB a dit qu'il souhaitait simplifier l'avis dans toute la mesure du possible, compte tenu du fait que des parents ne connaissent pas certains termes (p. ex., « exfiltré »). Je conviens avec le TDSB qu'il est préférable de rédiger l'avis en langage simple; cependant, il a lieu de supposer que la plupart des parents ou tuteurs connaissent le terme « exfiltré » et sa définition. De plus, le 1er mai 2024, compte tenu du fait que le TDSB souhaitait donner un avis en langage simple, le CIPVP lui a recommandé de remplacer le terme « exfiltrés » par « volés ». Or, le TDSB n'a pas accepté cette recommandation. Il jugeait qu'il n'était pas nécessaire d'indiquer que les renseignements avaient été exfiltrés, car il n'existait aucune preuve d'exfiltration. Au moment de cette discussion, en avril 2024, le TDSB n'avait fourni aucune preuve montrant qu'il n'y avait pas eu exfiltration, et il ne semblait pas qu'il eût adopté cette position à ce moment-là.

Le 6 mai 2024, le conseil scolaire a publié son avis général dans le site Web de chacune des écoles. Contrairement à la recommandation du CIPVP, cet avis n'informait pas les particuliers de l'exfiltration de leurs renseignements personnels par l'auteur de menace, et il n'a pas été affiché dans les écoles concernées. Le même jour, le conseil scolaire a remis un avis par courriel aux membres du personnel concernés. Cet avis ne précisait pas non plus que l'auteur de menace avait exfiltré des renseignements les concernant.

Analyse des mesures prises par le TDSB

Il est louable que le TDSB ait mis en place un processus de notification, mais j'estime qu'omettre des renseignements essentiels dans son avis et ne pas afficher d'avis dans les écoles concernées pourrait nuire à la capacité des particuliers concernés à déterminer de façon éclairée comment protéger leurs renseignements personnels qui ont fait l'objet de cette atteinte à la vie privée.

Je tire cette conclusion sachant qu'il est généralement préférable pour les institutions de donner un avis direct aux particuliers qui auraient pu être touchés par une atteinte à la vie privée. Une correspondance directe est plus susceptible qu'un avis affiché d'attirer l'attention sur les répercussions possibles de l'incident sur la vie privée d'un particulier. Cependant, en l'occurrence, étant donné le nombre éventuellement élevé de particuliers concernés et les circonstances de cet incident, il était raisonnable pour l'institution de conclure qu'il n'était pas possible de fournir un avis direct aux anciens élèves, parents et membres du personnel.

Le TDSB a fait savoir aux parties concernées que l'on avait accédé à leurs renseignements personnels sans autorisation, sans fournir toutefois des informations importantes au sujet de la possibilité que l'auteur de menace ait exfiltré ces renseignements.

Comme le TDSB n'a fourni au CIPVP aucun renseignement étayant son affirmation voulant que l'auteur de menace n'ait pas exfiltré de renseignements personnels ni ne semblait avoir adopté cette position au moment de l'avis, je crains qu'il n'ait pas pris de mesures adéquates pour informer les particuliers concernés des conséquences réelles pour leurs renseignements personnels. Ainsi,

le TDSB n'a pas donné à ces particuliers la possibilité de prendre des mesures de protection adéquates.

Le TDSB a-t-il pris des mesures correctives raisonnables pour éviter qu'une telle atteinte à la vie privée ne se reproduise?

D'après le document *Les atteintes à la vie privée : lignes directrices pour les organismes du secteur public* du CIPVP, l'enquête et les mesures correctives à la suite d'une atteinte à la vie privée devraient comprendre : un examen des circonstances ayant entouré l'atteinte à la vie privée; un examen des politiques et procédures de protection des renseignements personnels pour s'assurer qu'elles sont suffisantes; la question de savoir si l'atteinte à la vie privée résultait d'un problème systémique; des mesures correctives pour éviter que de telles atteintes à la vie privée se reproduisent.

Enquête sur l'attaque

TDSB a fait appel à un expert sur les atteintes à la vie privée et négociateur. D'après son enquête, l'auteur de menace a d'abord compromis les ordinateurs de la directrice adjointe le 28 septembre 2023. Le conseil scolaire a précisé qu'il y était parvenu par piratage psychologique. L'auteur de menace a ensuite obtenu les données d'accès à OneDrive de la directrice adjointe à partir d'un cache de navigateur.

Le conseil scolaire a établi que le premier accès non autorisé aux données contenues dans les ordinateurs était survenu le 3 octobre 2023, et il a découvert l'attaque le 6 octobre 2023 sur Telegram.

Le conseil scolaire ne connaît pas l'identité de l'auteur de menace, mais il croit que ce dernier est allé dans le bureau de la directrice adjointe pendant que celle-ci s'était absentée.

Le conseil scolaire a signalé cet incident au Service de police de Toronto et au CIPVP.

Mesures correctives

D'après les renseignements fournis, cette atteinte à la vie privée a résulté d'un piratage psychologique et de la présence de données d'accès dans un cache de navigateur.

Après avoir découvert l'atteinte à la vie privée, le conseil scolaire a déconnecté du réseau les ordinateurs de la directrice adjointe et le site Web du LCI, afin d'éviter tout autre accès à des renseignements personnels.

Le conseil scolaire a demandé à tous les membres du personnel du LCI de changer leurs mots de passe et d'adopter l'authentification multifacteur, laquelle sera mise en place dans l'ensemble de l'organisation. Le conseil scolaire a également installé la fonctionnalité Credential Guard de Microsoft Defender, instauré une protection antisabotage et retiré tous les systèmes non opérationnels de son réseau. En outre, le conseil scolaire s'appuiera sur les recommandations de

son fournisseur autorisé de services de sécurité pour rehausser ses mesures de sécurité et de protection.

Le 25 octobre 2024, tous les membres du personnel du LCI ont suivi une formation de sensibilisation à la cybersécurité donnée par un représentant de l'équipe de cybersécurité du TDSB. Cette formation portait sur des stratégies courantes pour prévenir une autre atteinte matérielle à la protection de la vie privée. Elle est fournie régulièrement, tous les trimestres, et traite de sujets tels que les suivants : « Qu'est-ce que le piratage psychologique? », « Quel est le type de piratage psychologique le plus courant? », « Techniques de distraction d'élèves », « Tendances relatives au piratage des bibliothèques », « Les utilisateurs d'enregistreurs de frappe », « Pratiques exemplaires relatives aux mots de passe ».

Examen des politiques et procédures en place en matière de protection de la vie privée

Le conseil scolaire fournit une formation de sensibilisation à la sécurité à tous les membres du personnel tous les trimestres, ainsi qu'une formation sur la protection de la vie privée au moment de l'entrée en fonction. Les membres du personnel qui ont besoin d'une formation complémentaire sur la protection de la vie privée peuvent utiliser la plateforme de perfectionnement professionnel du conseil scolaire.

En plus de donner une formation sur la protection de la vie privée au moment de l'entrée en fonction, je recommande au conseil scolaire de fournir une formation annuelle à tous les membres de son personnel.

Le programme de gestion des incidents de cybersécurité et le protocole de protection de la vie privée de TDSB font intervenir l'équipe de gestion des risques de cybersécurité, le bureau de l'accès à l'information et de la protection de la vie privée, les services juridiques, le service de gestion des risques d'entreprise, le service des communications, le service d'administration, le service de l'analytique et des systèmes, le service d'administration des applications et les services extérieurs du conseil scolaire ainsi que l'école ou le service touché.

Concernant les atteintes à la vie privée telles que celle-ci, le conseil scolaire dispose d'un guide et d'un protocole sur les atteintes à la vie privée. Ses principales politiques et procédures sont les suivantes :

- Code de conduite en ligne
- Politique P094 – Accès à l'information et protection de la vie privée
- Procédure opérationnelle PR676 – Accès à l'information et protection de la vie privée
- Politique P088 – Utilisation acceptable des ressources de technologie de l'information
- Procédure opérationnelle PR736 – Procédure en cas d'atteinte à la vie privée

Après chaque incident, le conseil scolaire tient une réunion pour dresser un bilan et discuter des améliorations et des changements à apporter au guide.

III. Conclusion et recommandations

D'après les renseignements dont je dispose, il semble que l'atteinte à la vie privée commise contre les systèmes du conseil scolaire aurait pu être attribuable à une sensibilisation et à une formation insuffisantes du personnel concernant le piratage psychologique, à une authentification insuffisante pour accéder aux ordinateurs, à l'absence de mesures de sécurité matérielle, laquelle a permis à l'auteur de menace d'accéder aux ordinateurs, au fait que des données d'accès et d'authentification aient été sauvegardées dans un cache de navigateur et au fait que les renseignements personnels n'étaient pas chiffrés.

Le conseil scolaire a pris des mesures correctives en fournissant une formation de sensibilisation à la cybersécurité à son personnel, en instaurant l'authentification multifacteur, en installant la fonctionnalité Credential Guard de Microsoft Defender, en assurant une protection antisabotage et en retirant de son réseau tous les systèmes non opérationnels, mais je lui recommande de prendre également les mesures suivantes :

- adopter des contrôles matériels [consulter le document SP 800-12 du National Institute of Standards and Technology (NIST), qui traite de la sécurité matérielle et environnementale];
- mettre à jour sa politique de sécurité et ses procédures de configuration pour s'assurer qu'aucune donnée d'authentification n'est sauvegardée dans les caches de navigateur;
- chiffrer les données délicates et les renseignements personnels;
- mettre en œuvre un programme de cybersécurité afin d'assurer la gestion globale des risques en la matière.

Après avoir examiné les circonstances de cette atteinte à la vie privée, les mesures susmentionnées qui ont été prises et les recommandations qui ont été formulées, j'estime qu'il n'est plus nécessaire de poursuivre le traitement de ce dossier. Veuillez noter que nous pourrions rouvrir ce dossier si des renseignements supplémentaires nécessitant un examen étaient portés à notre attention.

Le CIPVP vous remercie de votre coopération dans cette affaire ainsi que de votre souci d'assurer le respect de la *Loi*. La présente confirme que ce dossier est maintenant clos.

Veuillez agréer, Maître, mes sincères salutations.

Raymond Borja
Analyste