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

Le 3 décembre 2024

PAR COURRIEL

PERSONNEL

Maître Daniel Michaluk
Associé et coresponsable national, cybersécurité
Borden Ladner Gervais S.E.N.C.R.L., S.R.L.
22, rue Adelaide Ouest, bureau 3400
Toronto ON M5H 4E3
DMichaluk@blg.com

Objet : Dossier nº MR23-00112

Maître,

INTRODUCTION

Le 10 novembre 2023, Toronto Public Library (TPL) a signalé une brèche de cybersécurité aux termes de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (la *Loi*) au Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP). Le CIPVP a ouvert le dossier MR23-00112 pour traiter cette affaire.

Cette brèche a résulté d'une attaque par rançongiciel. Les auteurs de menace ont accédé sans autorisation au réseau de TPL, chiffré certains actifs de ce réseau et exfiltré des données comprenant des renseignements personnels.

CONTEXTE

TPL a précisé qu'elle constitue le réseau urbain de bibliothèques publiques le plus fréquenté du monde, avec plus de quatre millions de visites dans ses succursales chaque année, 1,2 million de titulaires de carte de bibliothèque et 10 millions de réservations de ressources par année. En plus de prêter des documents, TPL offre l'accès à des dizaines de ressources électroniques, bases de données en ligne et autres services numériques par l'entremise de son site Web torontopubliclibrary.ca, ainsi que des programmes de quartier dans ses 100 succursales. TPL recueille des fonds par l'entremise de la Toronto Public Library Foundation (TPLF), qui a reçu des dons totalisant plus de 100 millions de dollars depuis sa création en 1997.

Le 28 octobre 2023, TPL a décelé une activité douteuse dans son réseau. Elle a appris que des auteurs de menace avaient chiffré certains réseaux et volé ou exfiltré un grand nombre de fichiers stockés dans son serveur de fichiers. Au cours des journées et des mois qui ont suivi, TPL a publié des déclarations et des questions et réponses sur cet incident de cybersécurité afin de tenir le public au courant. TPL a fait savoir que cet incident avait causé des perturbations importantes, dont « une mise hors service complète de l'environnement technique de TPL, […] la suspension de nombreux services bibliothécaires de base, y compris le site Web, l'accès au catalogue de la bibliothèque, les réservations et les services de gestion de compte, les ordinateurs et imprimantes accessibles au public et l'accès à des documents et bases de données numériques ».

Pour faire enquête sur cet incident, TPL a aussitôt mis en œuvre sa procédure d'intervention en cas d'incident majeur de cybersécurité et son protocole en cas d'atteinte à la vie privée, et fait appel à son équipe d'intervention en cas d'incident. TPL a également obtenu les services d'avocats externes et d'un expert-conseil en sécurité afin de maîtriser la situation, de mener une enquête criminalistique et de prendre des mesures correctives. Le Bureau de la mairesse a été informé, de même que le Service de police de Toronto et la ville de Toronto (« Toronto »), car TPL est un « organisme » de Toronto[1].

TPL a signalé avoir maîtrisé l'incident dans les 24 heures après l'avoir découvert, le 29 octobre 2023. Le 14 novembre 2023, TPL a publié une déclaration informant le public de l'atteinte à la vie privée en précisant que des employés actuels et d'anciens employés de TPL et de la TPLF étaient concernés. TPL a également fait savoir que l'incident avait fait intervenir des données concernant des personnes à charge et des membres de la famille d'employés. Elle a indiqué que les bases de données sur les titulaires de carte, les bénévoles et les donateurs n'avaient pas été touchées, mais que certaines données sur ces personnes se trouvaient dans le serveur de fichiers compromis. TPL a expliqué qu'elle entreprendrait un processus d'investigation numérique pour bien déterminer les données qui étaient en cause. Le 28 mars 2024, les services de TPL ont été entièrement rétablis.

TPL a terminé son investigation numérique en février 2024 dans le cas des bénéficiaires et des personnes à charge et en juillet 2024 dans le cas des autres particuliers. D'après cette investigation, en plus des quelques 8 018 employés actuels et anciens employés, environ 1 874 de leurs bénéficiaires et personnes à charge et au plus 4 100 clients, donateurs, entrepreneurs, bénévoles et demandeurs d'emploi non retenus ont été touchés par l'atteinte à la vie privée.

Renseignements personnels en cause

TPL a établi que les renseignements personnels en cause portaient sur trois catégories de personnes :

- les particuliers (clients, donateurs, entrepreneurs, bénévoles et demandeurs d'emploi non retenus);
- les employés actuels et les anciens employés de TPL et de la TPLF depuis 1998;
- les bénéficiaires et personnes à charge d'employés.

[1] Agencies – City of Toronto (en anglais).

Les renseignements personnels sur environ 4 100 particuliers liés à TPL comprennent leur nom et un ou plusieurs des renseignements suivants :

- Nom
- Coordonnées (adresse postale, adresse courriel, numéro de téléphone)
- Antécédents criminels
- Date de naissance
- Sexe
- Numéro de carte de bibliothèque
- Renseignements médicaux (références en matière de santé, traitements/diagnostics, ordonnances, fournisseurs de soins, numéros de carte Santé, renseignements sur l'assurance-maladie)
- Descriptions physiques ou photographies (dans des rapports d'incident)
- Renseignements scolaires
- Signatures
- Statut de plaignant
- Statut d'auteur de demande d'accès à l'information
- Statut de donateur
- Statut de personne impliquée dans un incident ou une plainte en lien avec TPL
- Statut d'entrepreneur de TPL

Les renseignements personnels sur environ 2 500 employés actuels de TPL, 18 employés actuels de la TPLF et un nombre inconnu d'anciens employés de TPL et de la TPLF depuis 1998 (estimé à environ 5 500) comprennent leur nom et un ou plusieurs des renseignements suivants :

- Nom
- Numéro d'assurance sociale (NAS)
- Date de naissance
- Adresse domiciliaire
- Renseignements sur l'emploi
- Renseignements sur la paie
- Pièce d'identité délivrée par le gouvernement et présentée à TPL

Les renseignements personnels concernant environ 1 874 bénéficiaires et personnes à charge d'employés comprennent le nom et au moins un des renseignements suivants :

- Nom
- Coordonnées (adresse postale, adresse courriel, numéro de téléphone)
- Date de naissance
- Pièce d'identité délivrée par le gouvernement et présentée à TPL (p. ex., NAS, autres documents et chiffres)
- Renseignements médicaux (références en matière de santé, traitements/diagnostics, ordonnances, fournisseurs de soins, numéros de carte Santé, renseignements sur l'assurance-maladie)

- Renseignements sur les cartes de paiement/comptes bancaires
- Renseignements scolaires
- Signatures

QUESTIONS

À titre préliminaire, TPL a déclaré que les renseignements auxquels les auteurs de menace avaient eu accès et qu'ils avaient exfiltrés contiennent des renseignements personnels au sens du paragraphe 2 (1) de la *Loi*. Je suis d'accord avec cette déclaration. Il est incontesté que TPL est une institution au sens du paragraphe 2 (1) de la *Loi*.

Les questions suivantes ont été posées au cours de l'examen de cette affaire au stade du règlement anticipé :

1. TPL avait-elle pris des mesures raisonnables pour empêcher l'accès non autorisé aux renseignements personnels contenus dans ses systèmes, conformément au paragraphe 3 (1) du Règlement 823 pris en application de la *Loi*?
2. TPL a-t-elle pris des mesures raisonnables pour maîtriser l'atteinte à la vie privée?
3. TPL a-t-elle pris des mesures raisonnables pour aviser les particuliers concernés par l'atteinte à la vie privée?
4. TPL a-t-elle pris des mesures correctives raisonnables en réponse à l'atteinte à la vie privée?

ANALYSE

Question 1 : TPL avait-elle pris des mesures raisonnables pour empêcher l'accès non autorisé aux renseignements personnels contenus dans ses systèmes, conformément au paragraphe 3 (1) du Règlement 823 pris en application de la *Loi*?

Le paragraphe 3 (1) du Règlement 823 pris en application de la *Loi* est libellé ainsi :

> Les personnes responsables veillent à ce que des mesures raisonnables pour empêcher l'accès non autorisé aux documents qui se trouvent dans leur institution soient déterminées, documentées et appliquées en tenant compte du caractère des documents à protéger.

Dans le rapport sur une plainte concernant la protection de la vie privée PR16-40, l'enquêteuse Lucy Costa (évoquant le règlement équivalent pris en application de la LAIPVP) a déclaré qu'il n'existe pas d'approche universelle, soulignant :

> ...Il n'énumère pas de mesures que toutes les institutions doivent prendre sans égard aux circonstances. Il exige plutôt des institutions qu'elles prennent des mesures « raisonnables » en tenant compte du « caractère » des documents à protéger. Il s'ensuit que toutes les institutions n'auront pas nécessairement à prendre les mêmes mesures de sécurité. Selon la nature des documents à protéger,

y compris leur sensibilité, leur niveau de risque et les types de menaces qui les visent, les mesures requises pourraient varier d'une institution à une autre[2].

L'attaque par rançongiciel

TPL a indiqué que les auteurs de menace avaient accédé au réseau le 2 août 2023. Il n'y a eu ensuite aucune autre activité malveillante jusqu'au 5 octobre 2023. Cet incident de cybersécurité a touché une grande partie du réseau de TPL, y compris son infrastructure de technologie de l'information (TI), ses serveurs de fichiers et ses systèmes internes. TPL a affirmé que les auteurs de menace avaient exfiltré environ 900 Go de données d'un serveur de fichiers contenant 780 000 fichiers dans 44 dossiers.

D'après les renseignements fournis par TPL, la cause de l'incident de cybersécurité demeure inconnue. Au début, les auteurs de menace ont installé un outil d'accès à distance dans un serveur connecté à Internet qui hébergeait un service d'impression de TPL. Celle-ci a indiqué que malgré ses systèmes anti-logiciels malveillants et de journalisation réseau, les auteurs de menace avaient pénétré dans le réseau sans être détectés.

TPL a fait savoir que son enquête sur cette affaire était terminée, et qu'elle n'avait permis d'obtenir aucune indication directe montrant comment les auteurs de menace avaient installé un outil d'accès à distance et étaient parvenus à assurer la persistance de leur cyberattaque. TPL a reconnu que le système en cause était vulnérable, et a précisé qu'à son avis, les auteurs de menace avaient probablement exploité cette vulnérabilité.

Mesures en place au moment de l'incident

En réponse aux questions du CIPVP concernant les mesures de sécurité qui étaient en place au moment de l'attaque, TPL a fourni les renseignements suivants :

- Certaines applications d'entreprise et certains systèmes d'exploitation étaient en fin de vie ou n'étaient plus pris en charge par le fournisseur de TPL. Cette situation avait été relevée et devait être rectifiée en priorité, par la mise à niveau des applications d'entreprise, l'adoption de solutions tout à fait nouvelles et la mise hors service du système hérité.
- Des correctifs critiques ont été installés dans les terminaux client exclusivement au moyen du Systems Centre Configuration Manager (SCCM) de Microsoft.
- Les contrôleurs de domaine sont sécurisés conformément à des procédures et politiques standard.

Analyse

Il n'existe pas de mesures de sécurité universelles qui conviennent à toutes les institutions. Cependant, celles-ci doivent prendre des mesures « raisonnables » compte tenu du « caractère » des documents à protéger.

[2] Voir le par. 72 du rapport sur une plainte concernant la protection de la vie privée PR16-40.

TPL a reconnu que certaines applications et certains systèmes d'exploitation étaient en fin de vie ou n'étaient plus pris en charge par un fournisseur externe, et que cette situation devait être rectifiée.

Je crois que TPL, une grande organisation qui est au service du public, devrait disposer de mesures de sécurité efficaces et à jour pour protéger les renseignements personnels.

À mon avis, TPL aurait pu prévenir une atteinte importante à la vie privée ou en réduire le risque si elle avait adopté une approche plus proactive afin d'identifier, d'analyser et d'atténuer les risques pour la vie privée que posent ses applications et systèmes (particulièrement ceux qui sont en fin de vie), et également d'améliorer son système d'installation de correctifs. De plus, il est préoccupant que deux mois se soient écoulés avant que la présence des auteurs de menace ne soit détectée dans le réseau de TPL, et que la cause de cet incident demeure inconnue. TPL considère cependant que les auteurs de menace ont probablement exploité une vulnérabilité, ce qui a motivé des mesures correctives rigoureuses.

En vertu du paragraphe 3 (1) du Règlement 823 pris en application de la *Loi*, les institutions doivent veiller à ce que des mesures de sécurité pour empêcher l'accès non autorisé aux documents soient « déterminées, documentées et appliquées[3] ». D'après les renseignements dont je dispose, j'estime que TPL n'avait pas pris les mesures de sécurité raisonnables qu'exige le Règlement 823 pris en application de la *Loi*.

En octobre 2022, le CIPVP a publié une feuille-info sur la technologie portant sur les attaques par rançongiciel telle que celle décrite plus haut, intitulée Se protéger contre les rançongiciels[4]. Cette feuille-info précise que ce type de logiciel malveillant est de plus en plus répandu et qu'il représente une grave menace à la sécurité des documents électroniques. Les organisations telles que TPL peuvent prendre des mesures proactives pour réduire le risque que des auteurs de menace aient accès à leurs systèmes informatiques; par exemple :

- **Assujettir les systèmes de courrier électronique à des contrôles de sécurité** afin de déceler et de prévenir l'acheminement de courriels contenant des liens suspects, des pièces jointes malveillantes et des adresses d'expéditeur usurpées.
- **Élaborer un programme de gestion des vulnérabilités.**
- **Adopter des pratiques exemplaires de renforcement de la sécurité des systèmes.** Il s'agit généralement de réduire le nombre de voies d'accès au réseau qu'un attaquant est susceptible d'emprunter.
- **Élaborer des stratégies pour atténuer le risque lié aux systèmes qui ne sont pas à niveau.**
- **Limiter l'accès du personnel** aux sites Web suspects.
- **Veiller à ce que tous les employés reçoivent une formation à jour sur la cybersécurité** décrivant notamment les attaques par rançongiciel**.**
- **Installer dans tous les ordinateurs des outils de sécurité** qui les protègent contre les logiciels malveillants, mettent en quarantaine les fichiers suspects et

[3] RRO 1990, Règl. 823 | Dispositions générales | CanLII
[4] Voir la feuille-info du CIPVP : Se protéger contre les rançongiciels.

lancent des alertes, notamment des outils antivirus d'entreprise ou des outils de détection et d'intervention pour la sécurité des terminaux.
- **Utiliser de bonnes pratiques d'authentification**, notamment des mots de passe efficaces, la gestion des mots de passe et une authentification multifacteur forte, et limiter la réutilisation des mots de passe[5].

Les institutions doivent atténuer selon un calendrier régulier les risques décelés dans leurs systèmes et applications, au lieu d'attendre qu'un problème surgisse. Je recommande à TPL de consulter le document d'orientation susmentionné du CIPVP pour s'assurer de mettre en place des mesures préventives suffisantes, d'apporter des améliorations afin de mieux s'adapter aux menaces en évolution, y compris aux rançongiciels, et de renforcer sa posture de cybersécurité.

Question 2 : TPL a-t-elle pris des mesures raisonnables pour maîtriser l'atteinte à la vie privée?

TPL a découvert l'attaque au début de la journée du 28 octobre 2023. Pour maîtriser la situation et tenir une enquête criminalistique, TPL a affirmé avoir mis hors service le jour même l'ensemble de son réseau, y compris tous les accès externes au Web et à son réseau privé virtuel, à titre de précaution, même si tous ses systèmes n'avaient pas été touchés.

TPL a maîtrisé la situation le 29 octobre 2023, dans les 24 heures suivant la découverte de l'incident. TPL a affirmé que certains de ses systèmes étaient accessibles à Internet et par réseau local, mais elle a déployé des contrôles d'accès dans l'ensemble de son réseau.

TPL a expliqué que les données volées avaient été identifiées en s'appuyant sur des indications laissées par les auteurs de menace et des éléments de preuve numériques. Elle a ensuite fait appel à un expert externe en exploration des données pour examiner les renseignements en question.

Au cours des mois suivants, TPL a pris les mesures suivantes pour maîtriser l'atteinte à la vie privée :

- Mise en quarantaine de tous les terminaux, y compris les serveurs et les postes de travail, et analyse au moyen d'outils d'investigation avant la migration ou le rétablissement dans un nouveau réseau afin de bien maîtriser l'atteinte à la vie privée. Le réseau de TPL a pu être rétabli grâce à des copies de sauvegarde sécurisées qui n'avaient pas été touchées par l'incident, ou par la reconstruction de certains éléments.
- En raison de la grande complexité matérielle de l'organisation, chaque emplacement de TPL (plus d'une centaine) a été visité afin d'effectuer l'inspection, l'analyse approfondie, la validation et la remise en état du matériel au cours du processus de rétablissement, qui a compris une période de quarantaine.
- Plus de 200 serveurs ont été examinés, nettoyés et rétablis ou reconstruits. Plus de 5 000 postes de travail ont été mis en quarantaine, évalués et migrés vers un réseau intact afin de rétablir les terminaux client utilisés par le personnel et le public.

[5] Voir la feuille-info du CIPVP : Se protéger contre les rançongiciels.

- Des outils avancés de suppression des logiciels malveillants et de journalisation ont été installés manuellement en vue de recueillir des éléments de preuve. Tous les terminaux et systèmes d'entreprise ont été mis à jour au moyen du logiciel de gestion des correctifs le plus récent avant le rétablissement des services. Un régime de gestion des correctifs plus rigoureux a été élaboré et déployé pour assurer l'installation régulière de correctifs de sécurité.
- Le service public d'impression a été reconstitué en utilisant une technologie moderne sécurisée.
- Dans des déclarations publiques, TPL a reconnu que les données volées pourraient être publiées sur le Web caché. Dans ses communications avec le CIPVP, TPL a affirmé qu'elle surveille continuellement le Web caché depuis que l'attaque a été découverte, et qu'elle n'a trouvé aucune indication selon laquelle les données en cause auraient été publiées ni de mention de cet incident.

Analyse

L'environnement informatique de TPL présentait manifestement des vulnérabilités au moment de l'incident, d'autant plus que les auteurs de menace n'ont pas été détectés entre le 2 août et le 28 octobre 2023. TPL n'a pas indiqué au CIPVP avant le 21 novembre 2024 les agissements précis des auteurs de menace dans son environnement au cours de cette période.

Compte tenu du fait que les cyberattaques se multiplient dans le monde, il est essentiel que TPL rehausse sa posture de cybersécurité et prenne des mesures de sécurité efficaces dans ses réseaux en vue de déceler et de prévenir les attaques de ce genre.

La possibilité que les renseignements en cause soient publiés ou mis à disposition dans le Web caché est décrite dans le rapport sur une plainte concernant la protection de la vie privée MR24-00114 de l'enquêteuse Jennifer Olijnyk :

> […] une fois volées, les données échappent au contrôle [de l'institution]. Dans une telle situation, il faut supposer qu'elles sont utilisées par des auteurs de menace et agir en conséquence. Si la surveillance du Web caché peut se révéler utile pour découvrir une brèche ou en déterminer l'ampleur, il n'en reste pas moins que les institutions ne peuvent pas supprimer les renseignements personnels que publient des auteurs de menace[6].

Étant donné que l'incident de cybersécurité a été maîtrisé dans les 24 heures suivant sa découverte et que TPL a surveillé continuellement le Web caché pour déterminer si les données en cause avaient été publiées, j'estime que TPL a établi de façon adéquate la portée de l'atteinte à la vie privée et pris des mesures raisonnables pour la maîtriser.

[6] Décision MR21-00114 – Commissaire à l'information et à la protection de la vie privée de l'Ontario (ipc.on.ca), par. 37.

Question 3 : TPL a-t-elle pris des mesures raisonnables pour aviser les particuliers concernés par l'atteinte à la vie privée?

Étant donné qu'il lui a fallu beaucoup de temps pour déterminer les données touchées par l'atteinte à la vie privée et les particuliers concernés, TPL a publié des déclarations, fait le point et donné des avis à maintes reprises :

14 novembre 2024 : TPL publie une déclaration informant le public de l'atteinte à la vie privée et avisant indirectement des employés actuels et d'anciens employés de TPL et de la TPLF. TPL indique alors que les bases de données sur les titulaires de carte, les bénévoles et les donateurs n'ont pas été touchées, mais que certaines données sur ces personnes se trouvaient dans le serveur de fichiers compromis. TPL explique qu'elle entreprendrait une investigation numérique pour bien déterminer les données en cause.

29 novembre 2024 : TPL tient une assemblée pour répondre aux questions du personnel. En plus de son avis général du 14 novembre 2023, elle remet des avis à environ 3 100 employés actuels et anciens employés.

1er décembre 2023 : TPL entreprend son investigation numérique et poursuit son enquête criminalistique. Elle lance également une investigation numérique distincte et plus ciblée pour les personnes à charge et les bénéficiaires, à qui elle accorde la priorité étant donné la possibilité que des renseignements délicats soient divulgués.

5 janvier 2024 : TPL annonce la fin de son enquête criminalistique, mais la poursuite de son investigation numérique. Elle fait savoir au CIPVP qu'une quantité minime de renseignements personnels sur des clients auraient pu être touchés. TPL se donne pour objectif d'identifier tous les autres particuliers concernés (y compris les clients) d'ici la fin de mars 2024.

2 février 2024 : TPL doit aviser sous peu 2 100 personnes à charge de ses employés. Elle fait savoir qu'elle poursuit l'analyse des données et espère aviser des parties concernées récemment découvertes d'ici avril ou mai 2024.

14 mars 2024 : Tous les bénéficiaires et toutes les personnes à charge des employés de TPL ont été avisés.

26 avril 2024 : Après que le CIPVP lui a accordé plusieurs prorogations, TPL lui remet son rapport sur l'atteinte à la vie privée en précisant qu'elle n'a pas encore terminé son analyse des données en vue de déterminer tous les particuliers touchés.

Juillet 2024 : TPL fait savoir au CIPVP que son fournisseur chargé de l'investigation numérique a terminé l'analyse des données.

Mesures prises par TPL pour aviser les particuliers concernés (clients, donateurs, entrepreneurs, bénévoles et demandeurs d'emploi non retenus)

En juillet 2024, j'ai demandé des éclaircissements concernant les particuliers concernés par l'atteinte à la vie privée et les mesures prises pour les aviser. J'estime que les renseignements que TPL m'a fournis concernant les clients, donateurs, entrepreneurs, bénévoles et demandeurs d'emploi non retenus depuis le signalement de l'atteinte à la vie privée en octobre 2023 présentent des incohérences.

En réponse à mes questions, TPL m'a fait savoir qu'environ 7 552 clients avaient été touchés par l'atteinte à la vie privée et qu'elle comptait aviser 226 de ces clients les 8 et 9 juillet 2024. Les données en cause concernant ces clients comprenaient le nom, l'adresse postale, l'adresse courriel, le numéro de téléphone, la date de naissance, le numéro de carte de crédit, le numéro de passeport ou le numéro de permis de travail. TPL leur a offert un service de surveillance du crédit pour une période de deux ans. Elle a indiqué que les particuliers dont elle connaissait l'adresse postale recevraient une lettre; les autres seraient avisés par courriel. Cette communication contenait des détails sur l'atteinte à la vie privée et sa portée, les renseignements en cause et les coordonnées de TPL pour obtenir de plus amples renseignements. TPL a affirmé ne pas avoir précisé dans cette communication les mesures prises pour maîtriser l'atteinte à la vie privée, car elle les avait déjà rendues publiques.

TPL a été appelée à préciser pourquoi elle avait avisé certains particuliers concernés, mais pas les autres. Elle a indiqué avoir « avisé tous les clients dont les renseignements posaient un risque réel de préjudice grave ».

Les données sur les clients concernés comprenaient le nom, l'adresse postale, des renseignements démographiques, le numéro de carte de bibliothèque et l'intérêt manifesté à participer des programmes de TPL ou la participation confirmée à de tels programmes. TPL a affirmé qu'à son avis, ces données ne présentaient pas un risque réel de préjudice grave pour ces clients, et elle a donc décidé de ne pas les aviser.

TPL n'a pas précisé les critères sur lesquels elle s'était fondée pour déterminer si ses clients concernés couraient un risque réel de préjudice grave.

Les lois ontariennes sur la protection de la vie privée régissent la façon dont les organisations du secteur public doivent gérer les renseignements personnels. Plus précisément, le paragraphe 2 (1) de la *Loi* définit « renseignements personnels » comme étant des renseignements consignés ayant trait à un particulier qui peut être identifié, et précise que cette expression s'entend notamment :

> a) des renseignements concernant la race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, le sexe, l'orientation sexuelle, l'état matrimonial ou familial de celui-ci;
> b) des renseignements concernant l'éducation, les antécédents médicaux, psychiatriques, psychologiques, criminels ou professionnels de ce particulier ou des renseignements reliés à sa participation à une opération financière;

> c) d'un numéro d'identification, d'un symbole ou d'un autre signe individuel qui lui est attribué;
> d) de l'adresse, du numéro de téléphone, des empreintes digitales ou du groupe sanguin de ce particulier;
> …
> f) de la correspondance ayant explicitement ou implicitement un caractère personnel et confidentiel, adressée par le particulier à une institution, de même que des réponses à cette correspondance originale susceptibles d'en révéler le contenu;
> …
> h) du nom du particulier, s'il figure parmi d'autres renseignements personnels qui le concernent, ou si sa divulgation risque de révéler d'autres renseignements personnels au sujet du particulier.

Le CIPVP a statué qu'il est important d'examiner le contexte dans lequel les renseignements se présentent pour déterminer s'il s'agit de renseignements « ayant trait » à un particulier ou si le particulier « peut être identifié ». Étant donné la définition de « renseignements personnels » du paragraphe 2 (1) de la *Loi* et les détails sur les données touchées, j'ai fait savoir à TPL qu'à mon avis, les différents renseignements personnels des clients pourraient, ensemble, révéler d'autres renseignements personnels à leur sujet et permettre de les identifier. J'ai également fait valoir que ces renseignements personnels pouvaient être utilisés pour porter préjudice aux clients concernés, compte tenu du fait que les auteurs de menace y avaient eu accès sans autorisation.

De plus, le document Les atteintes à la vie privée : Lignes directrices pour les organismes du secteur public du CIPVP établit un cadre dont les institutions peuvent se servir afin de déterminer les mesures à prendre pour respecter leurs obligations en vertu de la *Loi*. Ainsi, le CIPVP a établi depuis longtemps que l'institution doit aviser un particulier concerné par une atteinte à la vie privée dans les plus brefs délais s'il est démontré que cette atteinte à la vie privée pose un risque réel de préjudice grave pour ce particulier, **en tenant compte du caractère délicat des renseignements et de la probabilité d'usage abusif [les caractères gras sont de moi]**. Ce document contient d'autres précisions sur le mode de notification et sur les renseignements à fournir aux particuliers concernés.

Compte tenu des renseignements dont je disposais, j'ai recommandé à TPL d'aviser les 7 552 autres « clients » concernés dont les renseignements personnels avaient été consultés sans autorisation en vertu de la *Loi* par les auteurs de menace. Étant donné les circonstances et le nombre de particuliers concernés, j'ai suggéré au TPL d'envisager de publier un avis général.

Comme les doublons n'avaient pas été pris en compte dans l'ensemble de données en question, TPL a constaté qu'elle avait surestimé le nombre de clients concernés. Leur nombre réel s'élevait tout au plus à 4 336, et TPL a affirmé qu'il pouvait y avoir des données en double. TPL a également précisé que la catégorie des « clients » comprenait les « clients, donateurs, entrepreneurs, bénévoles et demandeurs d'emploi non retenus ». J'ai discuté avec TPL de l'application du critère du préjudice, et elle a convenu de publier un avis général à cette catégorie de particuliers concernés. TPL s'est engagée à publier cet avis dans son site Web et d'autres médias avant la fin d'octobre 2024.

Le 26 novembre 2024, TPL a mentionné avoir effectué une analyse des données et une mise en correspondance des adresses pour le reste des particuliers concernés. Elle a dit être en mesure d'aviser directement certains des particuliers concernés qui restaient, et qu'elle croyait qu'environ 4 100 particuliers de cette catégorie avaient été touchés par l'atteinte à la vie privée, et non 4 336, contrairement à ce qu'elle avait signalé plus tôt au CIPVP. TPL a expliqué que ce changement était attribuable à des doublons et au fait que certains de ces particuliers étaient des employés qui avaient déjà été avisés.

Le même jour, TPL s'est engagée à aviser les autres particuliers concernés indirectement dans son site Web et par d'autres moyens, et à envoyer par la poste des lettres aux entrepreneurs et bénévoles concernés. TPL a convenu d'entreprendre la notification indirecte et directe du reste des particuliers à la fin de novembre 2024.

Employés actuels et anciens employés de TPL et de la TPLF depuis 1998

Le 26 avril 2024, TPL a confirmé au CIPVP qu'environ 8 000 employés actuels et anciens employés de TPL et de la TPLF depuis 1998 étaient concernés et avaient été avisés. À ce moment-là, TPL a précisé que les données en cause concernant ce groupe de particuliers comprenaient des renseignements sur l'emploi et la paie, ainsi que des NAS. Elle a indiqué qu'un avis public sur l'incident avait été publié dans son site Web et les médias sociaux le 14 novembre 2023, et que cet avis avait été communiqué aux médias, remis directement aux employés actuels et aux anciens employés et publié dans son site Web jusqu'au 2 avril 2024.

TPL a affirmé avoir avisé directement de l'atteinte à la vie privée environ 3 100 de ses employés actuels et de ses anciens employés et de ceux de la TPLF (dont elle disposait alors des coordonnées) par lettre au cours de la semaine du 27 novembre 2023. TPL a précisé qu'elle avait offert par la poste à tous les employés actuels et anciens employés de TPL et de la TPLF un service de surveillance de crédit sur demande pendant une période de deux ans. Cette communication contenait des renseignements sur la portée de l'atteinte à la vie privée, les renseignements en cause et les mesures prises pour la maîtriser, indiquait que le CIPVP en avait été informé et fournissait les coordonnées de TPL pour obtenir de plus amples renseignements. TPL a affirmé avoir tenu, le 29 novembre 2023, une assemblée du personnel pour répondre aux questions sur cet avis.

Bénéficiaires et personnes à charge d'employés

Le 26 avril 2024, TPL a confirmé au CIPVP qu'environ 2 000 bénéficiaires et personnes à charge d'employés étaient concernés par l'atteinte à la vie privée et en avaient été avisés par la poste au cours de la semaine du 11 mars 2024. Cette communication contenait des renseignements sur l'atteinte à la vie privée et sa portée, les renseignements en cause et les mesures prises pour la maîtriser, indiquait que le CIPVP en avait été informé et fournissait les coordonnées de TPL pour obtenir de plus amples renseignements. TPL a précisé que les données en cause concernant ce groupe comprenaient des renseignements médicaux et des renseignements sur les demandes de règlement d'assurance.

Le 5 juillet 2024, TPL a affirmé qu'elle avait découvert 50 autres bénéficiaires et personnes à charge d'employés qui étaient concernés, et qu'elle les aviserait au cours des prochaines semaines. TPL a confirmé avoir terminé la notification le 16 août 2024.

Le 9 octobre 2024, TPL a précisé qu'elle avait avisé 1 874 bénéficiaires et personnes à charge d'employés par la poste au cours de la semaine du 11 mars 2024.

Analyse

Le CIPVP considère depuis longtemps que la notification doit être directe, c'est-à-dire par téléphone, lettre ou courriel, ou en personne[7]. La notification indirecte est acceptable dans les situations où on ne peut raisonnablement recourir à la notification directe, lorsque les coordonnées des personnes concernées sont inconnues ou lorsque l'atteinte à la vie privée touche un grand nombre de personnes[8]. Le CIPVP considère également que cette notification des personnes concernées doit être effectuée dans un délai raisonnable.

Bien que la *Loi* n'oblige pas l'institution à aviser les particuliers concernés par une atteinte à la vie privée, cette notification est préférable. L'institution devrait tenir compte du nombre de particuliers en question, du caractère délicat des renseignements en cause et du risque que ceux-ci fassent l'objet d'abus pour déterminer s'il y a lieu d'aviser les particuliers ou non. J'encourage TPL à aviser en temps opportun les particuliers dont les renseignements personnels ont fait l'objet d'une atteinte à la vie privée.

Compte tenu du fait que toutes les parties concernées ont reçu ou recevront un avis direct ou indirect, j'estime qu'il n'y a pas d'autre question à envisager dans la présente section.

Question 4 : TPL a-t-elle pris des mesures correctives raisonnables en réponse à l'atteinte à la vie privée?

Le CIPVP a publié le document Les atteintes à la vie privée : Lignes directrices pour les organismes du secteur public expliquant les pratiques exemplaires que les institutions doivent suivre en cas d'atteinte à la vie privée et décrivant les étapes à franchir pour en déterminer la portée, la maîtriser et aviser les personnes concernées. Ce document propose également des mesures préventives et correctives, par exemple, fournir une formation, pour réduire le risque d'atteinte à la vie privée[9].

[7] Les atteintes à la vie privée : Lignes directrices pour les organismes du secteur public | Commissaire à l'information et à la protection de la vie privée de l'Ontario (ipc.on.ca/fr).
[8] Les atteintes à la vie privée : Lignes directrices pour les organismes du secteur public | Commissaire à l'information et à la protection de la vie privée de l'Ontario (ipc.on.ca/fr).
[9] Les atteintes à la vie privée : Lignes directrices pour les organismes du secteur public | Commissaire à l'information et à la protection de la vie privée de l'Ontario (ipc.on.ca/fr).

Prévention

Il est préoccupant que les auteurs de menace aient eu accès au réseau de TPL pendant une longue période, dès le 3 août 2023, et qu'ils n'aient été détectés que le 28 octobre 2023, même compte tenu du fait qu'ils ont été le plus actifs immédiatement avant leur attaque, à la fin d'octobre 2023.

Le CIPVP adopte une approche prospective et invite les organisations à prendre des mesures correctives pour prévenir les atteintes à la vie privée. En l'occurrence, il est important que TPL prenne des mesures adéquates pour prévenir l'accès non autorisé à ses documents. Pour déceler les attaques par rançongiciel, les prévenir et s'en rétablir, je suggère de prendre les mesures suivantes, si ce n'est déjà fait :

- **Effectuez régulièrement des copies de sauvegarde** de vos renseignements et systèmes et conservez-les dans un environnement hors ligne.
- **Surveillez l'intégrité des documents** afin de déceler des changements irréguliers apportés à un grand nombre de fichiers ou à des renseignements très sensibles.
- **Décelez l'utilisation non autorisée d'outils et d'interfaces de programmation** qui chiffrent des données.
- Utilisez des outils de prévention de la perte de données pour consigner, surveiller et bloquer des transferts irréguliers de fichiers vers des destinations non reconnues ou des sites Web de téléversement de fichiers connus.
- **Modifiez les paramètres de base des ordinateurs** (postes de travail des utilisateurs, serveurs et infrastructure d'infonuagique) afin de consigner un large éventail d'événements et des renseignements. Pour disposer de renseignements plus détaillés aux fins d'enquêtes sur des atteintes à la vie privée, prenez les mesures suivantes :
    - Veillez à empêcher que les journaux d'événements soient modifiés, écrasés ou supprimés sans autorisation après leur création.
    - Dressez un calendrier de conservation des journaux d'événements.
- **Réunissez les journaux d'événements** du parc informatique de votre organisation (y compris son infrastructure d'infonuagique) à un endroit centralisé. Envisagez d'utiliser des outils de renseignements sur la sécurité et de gestion des événements pour avoir une meilleure idée des activités des auteurs d'attaques par rançongiciel[10].

TPL a affirmé qu'en mars 2023, des membres de l'équipe de TI et de l'équipe du marketing et des communications de TPL avaient effectué un exercice de table d'attaque par rançongiciel afin de mettre au point la procédure d'intervention en cas d'incident majeur de cybersécurité de TPL.

TPL a précisé que les membres du personnel doivent suivre une formation annuelle sur la cybersécurité. Les sujets traités sont la sécurité des mots de passe, le piratage psychologique, ChatGPT, l'authentification multifacteur, la protection intégrée de la vie privée, la fraude dans les médias sociaux et les attaques d'hameçonnage. À l'issue de la formation, les membres du personnel doivent répondre à un questionnaire d'évaluation afin d'évaluer leur compréhension des

[10] Voir la feuille-info du CIPVP : Se protéger contre les rançongiciels.

notions présentées. TPL a précisé qu'elle effectue des attaques d'hameçonnage simulées chaque année pour déterminer comment le personnel y réagit.

J'ai recommandé à TPL de passer en revue son programme de formation actuel sur la protection de la vie privée et de le modifier au besoin afin qu'il permette d'assurer une protection suffisante contre les accès non autorisés aux renseignements personnels contenus dans ses bases de données. Le CIPVP recommande vivement à TPL de se tenir au courant des pratiques exemplaires et d'adopter un cadre de cybersécurité standard de l'industrie, ainsi que d'investir dans des mesures qui permettent de faire face aux menaces graves.

TPL a indiqué que le conseil municipal de Toronto lui avait demandé, les 22 et 23 mai 2024, d'élaborer des cadres de cybersécurité correspondant aux objectifs généraux de Toronto en la matière, afin de mettre en place des cadres internationaux tels que celui du National Institute of Standards and Technology (NIST), de la norme ISO 207001 et d'autres cadres semblables, ainsi que le cadre stratégique de l'infrastructure numérique (Digital Infrastructure Strategic Framework) de Toronto.

Pour prévenir l'accès non autorisé à ses systèmes et renseignements, TPL a précisé avoir mis en place les mesures de sécurité suivantes :

- Application du principe de privilège minimal.
- Mesures de contrôle pour les comptes, serveurs et actifs, y compris l'authentification multifacteur.
- Adoption de mots de passe forts avec verrouillage en cas de tentatives infructueuses répétées.
- Pare-feu.
- Chiffrement à jour dans les applications d'entreprise, et déploiement de certificats de validation prolongée pour tous les sites Web externes hébergés.
- Mesures de sécurité améliorées pour l'accès à distance aux applications d'entreprise.

Gestion des incidents

TPL a indiqué qu'elle avait mis en place un protocole en cas d'atteinte à la vie privée en 2008 et qu'elle l'avait révisé en 2024. Son enquête en réponse à l'incident a comporté un examen des journaux d'événements de Windows, des journaux d'application, des journaux de pare-feu, des journaux de mémoire, des journaux de fournisseur Internet et de la télémétrie de détection et d'intervention aux terminaux client. L'enquête de TPL a également comporté la détection des virus et des vérifications de la persistance (lancements automatiques, planificateurs de tâches, services). TPL a utilisé un logiciel pour regrouper et analyser les journaux des terminaux client afin de déterminer la présence de logiciels malveillants résiduels. Au cours du rétablissement des services, TPL a surveillé le trafic du réseau pour s'assurer qu'il n'y avait aucune activité résiduelle dans le centre de données pendant que les processus de maîtrise de la situation et de rétablissement étaient en cours. TPL a signalé s'être fondée au cours de son enquête sur une liste de fichiers et une preuve de vol émanant directement des auteurs de menace.

Attaque par rançongiciel

TPL a affirmé avoir amélioré ses politiques et procédures de journalisation, de surveillance des événements système et de détection des problèmes éventuels de sécurité en adoptant un système de gestion des informations et des événements de sécurité pour regrouper les journaux d'événements émanant de systèmes de sécurité essentiels afin d'effectuer une surveillance intégrée. TPL a également indiqué avoir déployé une solution de détection et d'intervention aux terminaux client dans l'ensemble de son réseau, et assuré la ségrégation/segmentation réseau.

Pour déceler les changements non autorisés ou anormaux dans les systèmes de fichiers (surveillance de l'intégrité des fichiers), TPL a mis en place un système de détection des intrusions pour surveiller les tentatives d'accès non autorisé et les activités anormales aux terminaux client de son réseau. Pour protéger son réseau contre les exfiltrations de données de gravité mineure à majeure, TPL a rehaussé ses politiques de sécurité réseau afin de contrer les mouvements latéraux non autorisés des données entre systèmes. TPL a précisé que les protocoles de partage de fichiers avaient été assujettis à des restrictions au besoin, et que les protocoles déconseillés de partage de fichiers avaient été désactivés. Pour ce qui est de la sauvegarde et de la récupération, les services connexes de TPL n'ont pas été compromis lors de l'incident de cybersécurité. TPL a affirmé avoir pu récupérer toutes les données stockées jusqu'à la date de l'incident. Après cet incident, TPL a dit avoir amélioré ses services de sauvegarde et de récupération en adoptant une nouvelle solution.

Après avoir constaté la possibilité d'une attaque par rançongiciel, TPL a affirmé avoir isolé aussitôt ses dispositifs de sauvegarde et les avoir déconnectés du réseau. Elle a précisé que son architecture de sauvegarde n'avait pas été compromise, et qu'aucun référentiel ou catalogue de données n'avait été compromis. Une fois l'isolement assuré, TPL a indiqué que le rétablissement des services avait été effectué en misant sur l'environnement de sauvegarde pour rétablir les systèmes dans l'état où ils étaient avant l'incident de cybersécurité. TPL a précisé qu'une copie de sauvegarde de ses documents électroniques est effectuée régulièrement.

Exploitation à distance

TPL a affirmé que les auteurs de menace avaient installé le rançongiciel au moyen d'un outil d'accès à distance non autorisé dans un système externe non corrigé. Pour réduire la surface d'exposition de l'organisation aux exploitations à distance, des politiques et configurations standard de sécurisation des serveurs ont été mises en place, et les pare-feu ont été paramétrés afin d'exposer uniquement les ports nécessaires entre les systèmes. Pour ce qui est des politiques et procédures de gestion de la vulnérabilité et des correctifs, TPL a fait savoir que toutes ses applications d'entreprise avaient été mises à niveau dans son réseau intact. Elle a indiqué que des correctifs de sécurité à jour avaient été installés dans les systèmes d'exploitation des serveurs et les terminaux client au cours du processus de rétablissement.

Les capacités de TPL en matière de renseignement sur les menaces comprennent des technologies modernes afin de protéger son réseau contre les menaces. TPL a affirmé recevoir des mises à jour de sécurité régulières du bureau du responsable principal de la sécurité de l'information de Toronto. Elle a précisé que ses cadres de TI assistent régulièrement, toutes les deux semaines, à des séances d'information sur les menaces du Centre canadien pour la cybersécurité. De plus, le

chef de la sécurité informatique de TPL se tient au courant des enjeux et tendances en matière de cybersécurité et fait part de rapports pertinents à l'ensemble de l'équipe de direction de la TI. Un rapport annuel faisant le point sur la cybersécurité est également remis au conseil d'administration.

CONCLUSION

Après avoir examiné les circonstances de cette atteinte à la vie privée et les mesures que TPL a prises, j'estime que TPL a réagi de manière adéquate à l'atteinte à la vie privée qu'il n'est plus nécessaire de poursuivre le traitement de cette affaire.

D'après les renseignements dont j'ai tenu compte au stade du règlement anticipé, je tire les conclusions suivantes :

1. Au moment de l'incident, TPL n'avait pas mis en place des mesures de sécurité raisonnables pour protéger les renseignements personnels, comme l'exige le paragraphe 3 (1) du Règlement 823 pris en application de la *Loi*.
2. Après avoir découvert les auteurs de menace, TPL a établi adéquatement la portée de l'atteinte à la vie privée et a pris des mesures pour la maîtriser.
3. TPL a pris des mesures adéquates pour aviser les particuliers concernés de l'atteinte à la vie privée conformément à la *Loi*.
4. TPL a maintenant en place des mesures raisonnables pour protéger les renseignements personnels, comme l'exige le paragraphe 3 (1) du Règlement 823 pris en application de la *Loi*.

RECOMMANDATIONS

Compte tenu des conclusions précédentes, je recommande ce qui suit à TPL :

1. Aviser tous les particuliers dont les renseignements personnels ont été consultés sans autorisation par les auteurs de menace en contravention de la *Loi.*
2. Examiner sa formation actuelle sur la protection de la vie privée et y apporter les changements nécessaires afin d'assurer une protection suffisante des renseignements personnels contenus dans ses réseaux contre les accès non autorisés et de rester au courant des normes de l'industrie en matière de cybersécurité.

Afin qu'elle puisse prendre des mesures de sécurité raisonnables pour prévenir l'accès non autorisé aux renseignements personnels se trouvant dans son système, j'invite TPL à consulter les ressources suivantes du CIPVP :

- Rapport sur une plainte concernant la protection de la vie privée MR21-00114 (en anglais).
- Feuille-info sur la technologie Se protéger contre les rançongiciels du CIPVP, qui traite de cadres et normes de cybersécurité.
- Les atteintes à la vie privée : Lignes directrices pour les organismes du secteur public.

Je 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.

Harpreet Bains
Analyste

c. c. : Shane Morganstein, associé, BLG