MISE À JOUR OCTOBRE 2022

FEUILLE-INFO
**SUR LA TECHNOLOGIE**

# Se protéger contre les rançongiciels

Les rançongiciels constituent une menace de taille pour les organisations ontariennes. Les attaques par rançongiciel peuvent détruire des documents essentiels, mettre des systèmes hors service, interrompre des services essentiels et faire en sorte que des renseignements sensibles se retrouvent entre les mains de criminels.

Les organisations assujetties aux lois ontariennes sur l'accès à l'information et la protection de la vie privée doivent s'assurer que leurs programmes de cybersécurité comprennent des mesures raisonnables pour protéger leurs fonds de renseignements. La présente feuille-info se veut un aperçu utile pour ces organisations et les personnes qu'elles servent.



## QU'EST-CE QU'UN RANÇONGICIEL?

Une attaque par rançongiciel a pour but d'extorquer de l'argent à une organisation par voie numérique. L'attaquant prend le contrôle de ses fonds de données et, dans bien des cas, menace d'y porter atteinte à moins de recevoir une rançon. La plupart des attaques par rançongiciel comprennent au moins une des tactiques suivantes :

- **Accès bloqué.** L'attaquant prend le contrôle de systèmes essentiels, de référentiels et de copies de sauvegarde. Il utilise aussi des outils comme le chiffrement pour empêcher l'organisation d'accéder à ses propres renseignements et systèmes, et exige une rançon pour rétablir l'accès.

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

- **Vol de données.** L'attaquant obtient l'accès à de grandes quantités de renseignements, en conserve une copie à un emplacement dont il a le contrôle, et menace de les publier à moins de recevoir une rançon.

D'après un **rapport** du Centre canadien pour la cybersécurité, cet organisme était au courant de 235 incidents liés à des rançongiciels ayant touché des organisations canadiennes en 2021. On croit cependant que ce nombre est beaucoup plus élevé, car bien des incidents ne sont pas signalés. Par exemple, une **étude menée en 2020 par TELUS** auprès de 463 entreprises canadiennes a constaté que 83 % des répondants avaient été la cible d'une tentative d'attaque par rançongiciel. Selon un **sondage mené en 2022** par CIRA (Canadian Internet Registration Authority), la proportion d'organisations victimes d'une attaque par rançongiciel avait augmenté de plus de 40 % au cours de l'année précédente, passant de 17 % (1 sur 6) à 24 % (1 sur 4).

## CONSÉQUENCES DES ATTAQUES PAR RANÇONGICIEL

Les attaques par rançongiciel peuvent causer des préjudices sérieux découlant notamment d'atteintes à la vie privée, de la divulgation de documents confidentiels, de la perte d'accès à des documents ou de la perturbation des systèmes et services. En voici quelques exemples :

### Pour les particuliers et les collectivités

- **Atteintes à la santé, à la sécurité et à l'ordre public.** Des pannes majeures de systèmes informatiques d'organisations qui fournissent des services essentiels ont entraîné l'**annulation de chirurgies** dans des hôpitaux et fait en sorte que des premiers intervenants ont **perdu contact avec leur centre de répartition**.
- **Détresse.** L'incertitude quant à la nature des renseignements qui ont été volés ou à l'individu qui y a eu accès peut susciter un sentiment d'impuissance ou de détresse. C'est particulièrement le cas lorsque ces renseignements sont sensibles et que leur publication pourrait causer un préjudice à la personne concernée, par exemple, s'ils ont trait à des **personnes ayant subi de la violence conjugale** ou ayant reçu des services de santé mentale.
- **Perte financière**. Les attaques par rançongiciel ont souvent pour but de voler des renseignements sur des cartes de crédit ainsi que d'autres renseignements personnels et financiers qui sont utilisés ensuite à des fins de fraude d'identité.
- **Incapacité d'exercer son droit d'avoir accès à l'information.** La perte de documents gouvernementaux et de renseignements personnels peut empêcher des particuliers d'avoir accès aux renseignements les concernant et de tenir des organisations responsables de leurs pratiques et de leurs décisions.

### Pour les organisations

- **Interruption des activités internes.** Des **institutions publiques**, y compris des municipalités, ont perdu l'accès aux renseignements nécessaires pour fournir des services ou accomplir des activités internes à la suite d'attaques par rançongiciel.
- **Atteinte à la réputation.** Vingt-cinq pour cent des répondants à un **sondage mené en 2021** auprès de responsables de la cybersécurité des secteurs public et privé du Canada dont l'organisation avait subi une attaque par rançongiciel ont déclaré que cette attaque avait terni la réputation de leur organisation.
- **Perte de confiance des employés.** Des documents internes contenant des **renseignements sensibles sur des employés** sont souvent visés par les attaques par rançongiciel, et cela peut porter atteinte aux relations de travail.
- **Perte financière**. Les organisations peuvent **accuser des pertes de revenus** lorsque des systèmes de paiement ou d'information sur les clients sont chiffrés, bloqués ou indisponibles en raison d'une attaque par rançongiciel.

## OBLIGATION LÉGALE DE SE PRÉMUNIR CONTRE LES RANÇONGICIELS

Les organisations qui sont assujetties aux lois ontariennes sur l'accès à l'information et la protection de la vie privée[1] doivent prendre des mesures raisonnables pour protéger les renseignements[2] dont ils ont la garde contre la divulgation et l'accès non autorisés, ainsi que contre la disposition ou la destruction non autorisée ou accidentelle. Les dépositaires de renseignements sur la santé et les fournisseurs de services à l'enfance et à la famille doivent également protéger les renseignements personnels contre l'utilisation, la duplication et la modification non autorisées, et contre le vol et la perte. Ils doivent aussi veiller à ce que les renseignements personnels soient conservés, transférés et éliminés de manière sécuritaire[3].

---

[1] **La Loi sur l'accès à l'information et la protection de la vie privée** (LAIPVP), la **Loi sur l'accès à l'information municipale et la protection de la vie privée** (LAIMPVP); la **Loi sur la protection des renseignements personnels sur la santé** (LPRPS) et la partie X de la **Loi sur les services à l'enfance, à la jeunesse et à la famille** (LSEJF).

[2] Le terme « renseignements » dans le présent document désigne les renseignements que les organisations sont tenues de protéger en vertu des lois ontariennes sur l'accès à l'information et la protection de la vie privée. Il s'entend des documents gouvernementaux en vertu de la LAIPVP/LAIMPVP, ainsi que des renseignements personnels et des renseignements personnels sur la santé au sens de la LAIPVP/LAIMPVP, de la LPRPS et de la LSEJF. Dans le présent document, le terme « renseignements personnels » s'entend à la fois des renseignements personnels et des renseignements personnels sur la santé, mais non des documents gouvernementaux qui ne sont pas des renseignements personnels au sens de la LAIPVP ou de la LAIMPVP.

[3] **Règl. de l'Ont.** 460, par. 4 (1) et (3); **Règl. de l'Ont. 823**, par. 3 (1) et (3); **LPRPS**, par. 12 (1) et 13 (1); **LSEJF**, par. 308 (1) et 309 (1).

Une attaque par rançongiciel comprend généralement plusieurs étapes. Voici des exemples de circonstances où une utilisation ou un accès non autorisé ou encore la perte ou le vol de renseignements personnels pourrait se produire au cours d'une ou de plusieurs de ces étapes[4].

## Accès

L'attaquant utilise généralement des logiciels pour prendre le contrôle à distance d'un compte utilisateur légitime appartenant à l'organisation cible. Il parcourt ensuite l'environnement informatique de sa cible. Souvent, il **traite des listes de fichiers et de documents** pour se renseigner sur le fonds de données de l'organisation. Il n'examine ou ne regarde pas nécessairement chaque document, mais il tente d'obtenir ou d'utiliser les renseignements afin de les voler ou de les chiffrer, ou les deux.

## Utilisation

L'attaquant profite généralement de cet accès pour s'en prendre au fonds de données de l'organisation cible. Il peut se servir de ces renseignements pour exiger d'elle une rançon. Par exemple, les attaquants copient souvent des documents contenus dans divers systèmes d'une organisation dans une **zone de préparation des données**, où ils compriment les fichiers pour en faciliter la transmission. Ils peuvent également passer les renseignements dans un logiciel de chiffrement qui **les rend illisibles** à moins de détenir une clé secrète qu'eux seuls possèdent.

## Perte

Dans la plupart des cas, si un attaquant chiffre les renseignements que détient une organisation, celle-ci ne peut plus y accéder et les utiliser, que ce soit pour fournir un service ou pour exécuter des fonctions importantes. L'organisation pourrait également être incapable de répondre aux demandes d'accès aux renseignements chiffrés. Même si elle est en mesure de récupérer des renseignements à partir de ses copies de sauvegarde, un tel incident peut quand même être considéré comme une **perte de renseignements**.

## Vol

Les attaques par rançongiciel comportent souvent la **transmission non autorisée** de renseignements hors d'une organisation (que l'on appelle également « exfiltration »). Ainsi, l'attaquant copie des renseignements et les utilise à des fins illicites. Les renseignements obtenus lors d'une attaque par rançongiciel seraient généralement considérés comme ayant été volés.

[4] Ces exemples sont fournis uniquement à titre d'information. Ils ne constituent pas un exposé exhaustif ou définitif de l'incidence des attaques par rançongiciel sur l'obligation d'une organisation de protéger les renseignements personnels.

## RESPONSABILISATION EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

Les exemples précédents montrent pourquoi les organisations assujetties aux lois ontariennes sur l'accès à l'information et la protection de la vie privée doivent prendre des mesures raisonnables pour se prémunir contre les attaques par rançongiciel. Pour que votre organisation puisse respecter ses obligations en matière de sécurité, le CIPVP recommande ce qui suit :

- **Jetez les bases de la responsabilisation.** La mise en place de mesures raisonnables pour identifier et déceler des menaces comme les rançongiciels, se protéger contre elles, y réagir et reprendre ses activités normales nécessite l'engagement de l'organisation et une surveillance interne. Par exemple, un comité de gouvernance de la protection de la vie privée et de la sécurité composé de cadres supérieurs chargés de la technologie de l'information, des services juridiques, de l'accès à l'information et de la protection de la vie privée pourrait être mis sur pied.
- **Intégrez la responsabilisation** dans une politique générale de sécurité de l'information. Cette politique devrait prévoir les rôles, les responsabilités, des mécanismes de communication et des exigences pour la mise en place de mesures de précaution d'ordre technique, administratif et matériel. Une telle politique peut aider votre organisation à se tenir au fait des risques émergents, comme les rançongiciels.
- **Assurez la responsabilisation** en veillant à ce que les mesures établies dans votre politique de sécurité de l'information soient appliquées et suivies. Vous pouvez, par exemple, surveiller l'application de ces mesures, les mettre à l'essai ou les vérifier.
- **Maintenez la responsabilisation** lorsque vous faites appel à des fournisseurs de services en obligeant ceux-ci par contrat à se conformer à des pratiques exemplaires en matière de cybersécurité, y compris celles qui sont décrites dans le présent document, et à signaler immédiatement les atteintes à la vie privée réelles ou présumées à votre organisation dès qu'ils en sont informés.
- **Rehaussez la responsabilisation** en renforçant continuellement votre programme de sécurité. Ainsi, évaluez l'efficacité des mesures que vous avez instaurées et adaptez votre programme de sécurité à l'évolution de la situation.

# SÉCURISEZ VOTRE ORGANISATION

Vous pouvez réduire le risque d'attaque par rançongiciel et ses conséquences pour votre organisation en mettant en place un programme de cybersécurité solide. Suivez les étapes suivantes pour protéger votre organisation contre une attaque par rançongiciel.

## Recensement des actifs et des fonds de renseignements dans l'ensemble de leur cycle de vie

Avant de prendre des mesures raisonnables pour protéger les renseignements contre des attaques par rançongiciel, vous devez bien connaître le fonds de renseignements de votre organisation[5]. Ainsi, vous devez prendre note de la sensibilité, du volume et de la nature de vos divers documents, et des endroits où ils sont conservés. Cela s'applique aux services d'infonuagique et aux fournisseurs de services qui traitent des renseignements pour le compte de votre organisation.

Vous devriez prendre les mesures suivantes dans votre organisation :

- **Tenez un inventaire des actifs** qui permet de savoir où et comment l'information circule dans votre organisation, comme les systèmes informatiques (serveurs, postes de travail, appareils mobiles) connectés à votre réseau, les renseignements stockés dans ces systèmes, les secteurs de programme responsables de ces renseignements, les versions du matériel et des logiciels utilisés ainsi que les coordonnées des administrateurs en informatique qui en sont responsables.
- **Classez et identifiez les renseignements et les éléments de votre parc informatique** en fonction de leur sensibilité (c.-à-d. le degré de préjudice qui résulterait de la perte de confidentialité, d'intégrité et d'accessibilité de ces renseignements). Mettez en place des mesures de précaution proportionnelles au niveau de sensibilité.
- **Mettez en place un programme de gestion des risques** qui prévoit des évaluations régulières de la sécurité des systèmes informatiques internes et de ceux des fournisseurs de services externes. Ces évaluations peuvent comprendre des audits de vulnérabilité, des tests d'intrusion, des évaluations de la menace et des risques et des évaluations de l'incidence sur la vie privée.
- **Veillez à ce que les renseignements personnels et les documents sensibles soient éliminés de façon sécuritaire** conformément aux calendriers de conservation et aux exigences sur l'élimination des supports.

5 Par exemple, le **rapport sur une plainte concernant la protection de la vie privée PR16-40** souligne que [traduction] « 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 ».

## Appréhension et atténuation des menaces

Votre organisation devrait se tenir au courant de la situation en ce qui a trait aux menaces que représentent les rançongiciels. Les attaques par rançongiciel peuvent faire intervenir des organisations criminelles sophistiquées qui renouvellent sans cesse leurs méthodes.

Vous pouvez prendre plusieurs mesures dans votre organisation pour améliorer la sécurité aux étapes clés d'une attaque par rançongiciel typique[6].

### Accès initial

Votre organisation devrait mettre en place des mesures de précaution pour détecter les méthodes que les attaquants par rançongiciel utilisent pour accéder initialement à un réseau et prendre d'autres mesures, et prévenir une telle intrusion[7]. Les méthodes d'accès initial les plus courantes utilisées dans les attaques par rançongiciel sont les suivantes :

- **Piratage psychologique**. Un attaquant communique avec une personne qui a accès au réseau cible et l'incite à poser un geste qui lui permet de prendre le contrôle de son ordinateur ou de son compte utilisateur. Ces attaques sont généralement effectuées au moyen de courriels d'hameçonnage, de sites Web trompeurs et d'annonces en ligne. Elles ont pour but d'inciter les employés à installer des logiciels malveillants ou à fournir des mots de passe ou d'autres données de connexion.
- **Exploitation des vulnérabilités des systèmes reliés à Internet**. Les attaquants recherchent sur Internet des systèmes qui n'ont pas fait l'objet de correctifs ou qui n'ont pas été configurés en vue d'éliminer des vulnérabilités reconnues, et leur envoient un programme malveillant. Ils peuvent notamment commettre une attaque par force brute, qui consiste à trouver un mot de passe en essayant des millions de combinaisons possibles, pour obtenir l'accès au système. Les attaques visent généralement les éléments de l'infrastructure de l'organisation qui gèrent des applications d'accès à distance et de courriel et des applications Web, ou des plateformes d'infonuagique incorrectement configurées.

6 La présente feuille-info ne contient pas une liste exhaustive des outils, tactiques et procédures que peuvent employer les auteurs d'attaques par rançongiciel.

7 Les organisations ne devraient pas supposer que les menaces par rançongiciel sont d'origine externe car il est possible qu'elles proviennent d'individus malveillants à l'interne. Prenons, par exemple, cette **atteinte** aux mesures de sécurité des renseignements personnels (qui ne représentait pas une attaque par rançongiciel) qui a touché près de 10 millions de personnes au Canada et à l'étranger.

- **Atteinte à la chaîne d'approvisionnement**. Des attaquants sophistiqués peuvent porter atteinte aux produits ou services de tiers qu'utilise votre organisation afin d'obtenir un accès direct à votre réseau. Par exemple, ils peuvent insérer un code malveillant dans une bibliothèque logicielle libre[8] ou porter atteinte aux outils d'administration à distance utilisés par les fournisseurs de services informatiques[9].

Votre organisation devrait prendre des mesures proactives pour réduire le risque que des attaquants aient accès à ses systèmes informatiques :

- **Assujettissez 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. Pour en savoir plus, consultez la feuille-info **Se protéger contre l'hameçonnage**.
- **Élaborez un programme de gestion des vulnérabilités** prévoyant les mesures suivantes :
    - abonnements à des avis techniques sur les vulnérabilités récemment découvertes qui touchent l'environnement informatique de votre organisation (et celui de vos fournisseurs de services);
    - examen des systèmes de votre organisation pour déterminer s'ils présentent des vulnérabilités;
    - installation de correctifs ou d'autres solutions dans les plus brefs délais;
    - élimination prioritaire des vulnérabilités que les auteurs d'attaques par rançongiciel tendent à exploiter.
- **Vous pouvez également réduire les risques auxquels s'expose votre organisation en adoptant des pratiques exemplaires de renforcement de la sécurité de vos systèmes.** Il s'agit généralement de réduire le nombre de voies d'accès à votre réseau

8 Les logiciels libres sont souvent élaborés publiquement; le public peut souvent proposer des changements au code qui peuvent se retrouver dans le logiciel final. Des technologies populaires et de grands services d'infonuagique utilisent couramment du code source libre. Dans un **rapport publié en 2020**, GitHub, une plateforme logicielle ouverte de premier plan, a signalé que dans un échantillon aléatoire de code source libre présent sur sa plateforme, 17 % des vulnérabilités semblaient avoir été introduites délibérément à des fins malveillantes (pour permettre des attaques ultérieures).

9 De nombreuses organisations font appel à des entreprises qui jouent le rôle de « fournisseurs de services de gestion informatique » et remplissent à distance des fonctions qui relèvent normalement du personnel informatique interne. Ils utilisent des outils de gestion à distance qui souvent autorisés à installer des logiciels, à gérer la configuration et à effectuer d'autres tâches sensibles, et qui sont des cibles prisées des auteurs de cybermenaces. Plusieurs attaques très médiatisées, comme les **attaques par rançongiciel commises en 2021 par l'entremise de logiciels de Kaseya**, ont été associées à des outils de gestion à distance compromis que des attaquants ont utilisés pour infiltrer des centaines d'organisations.

qu'un attaquant est susceptible d'emprunter. Par exemple, voici des mesures que votre organisation pourrait prendre afin de renforcer ses systèmes (y compris les systèmes d'infonuagique) :

  - Désactiver les services informatiques inutilisés.
  - Limiter les privilèges d'installation de logiciels et d'exécution de scripts personnalisés.
  - Limiter la capacité des utilisateurs de lancer des macros dans Microsoft Office.
  - Veiller à ce que les ordinateurs soient configurés de façon uniforme à partir d'images système normalisées. Les images système peuvent permettre d'automatiser la configuration des nouveaux systèmes pour assurer le bon réglage des paramètres de sécurité et l'installation d'applications de sécurité.

- **Élaborez des stratégies pour atténuer le risque lié aux systèmes qui ne sont pas à niveau**, par exemple en remplaçant régulièrement les systèmes qui ne peuvent fonctionner que sous des versions vulnérables de systèmes d'exploitation ou des cadres d'applications Web vulnérables.
- **Limitez l'accès du personnel** aux sites Web suspects.
- **Veillez à ce que tous les employés reçoivent une formation à jour sur la cybersécurité** décrivant notamment les attaques par rançongiciel.
- **Installez dans tous les ordinateurs des outils de sécurité** qui les protègent contre les logiciels malveillants, mettent en quarantaine les fichiers suspects et lancent des alertes, notamment des outils antivirus d'entreprise ou des outils de détection et d'intervention pour la sécurité des terminaux.
- **Utilisez de bonnes pratiques d'authentification**, notamment des **mots de passe efficaces**, la gestion des mots de passe et une authentification multifacteur forte, et limitez la réutilisation des mots de passe. Les organisations devraient également se tenir au fait des progrès réalisés sur le plan de l'authentification, notamment le virage vers l'authentification sans mot de passe.

### Escalade de privilèges et mouvement latéral

Les attaquants profitent généralement de leur accès initial à un système pour s'introduire dans d'autres systèmes reliés au même réseau. Ils exploitent souvent des vulnérabilités du système pour obtenir des privilèges d'administrateur et utiliser des outils de gestion informatique courants pour obtenir l'accès à de grandes quantités de renseignements sensibles et en prendre le contrôle, ou pour bloquer la prestation de services essentiels.

Pour limiter l'accès d'un attaquant à votre réseau, votre organisation devrait prendre les mesures suivantes :

- **Suivez le « principe de privilège minimal »**, selon lequel les utilisateurs devraient jouir de privilèges d'accès limités aux systèmes informatiques et ne pouvoir les utiliser que pour certaines tâches. Vous devriez accorder des privilèges d'accès et des autorisations supplémentaires uniquement si cela est nécessaire à l'utilisateur pour l'exercice de ses fonctions. Envisagez d'adopter **un modèle de cybersécurité à vérification systématique**.
- **Minimisez le recours aux comptes d'administrateur** et surveillez leur utilisation. Par exemple, les comptes d'administrateur ne devraient pas être utilisés pour des tâches de bureau courantes. Les organisations devraient également envisager le recours à des outils de gestion de l'accès qui peuvent accorder des privilèges temporaires sur demande.
- **Divisez votre parc informatique en différentes zones de sécurité.** Par exemple, une organisation pourrait prévoir des zones distinctes pour les serveurs d'application accessibles au public, les bases de données internes et les postes de travail des employés. Il serait alors possible de surveiller ou de limiter l'activité du réseau entre ces zones.
- **Établissez une base de référence de l'activité typique** de votre réseau et de vos terminaux et mettez en place des mesures permettant de détecter un trafic irrégulier qui pourrait révéler la présence d'un attaquant.

### Chiffrement et vol de données

Après avoir obtenu l'accès au réseau d'une organisation et pris le contrôle des renseignements et des systèmes, l'auteur d'une attaque par rançongiciel peut menacer de détruire des documents ou de rendre publics des renseignements sensibles. Il arrive aussi souvent que les attaquants s'en prennent aux copies de sauvegarde et aux systèmes opérationnels pour empêcher l'organisation de reprendre ses activités normales après une attaque.

Pour permettre à votre organisation de déceler et de prévenir les attaques par rançongiciel et faciliter la reprise de ses activités à la suite d'une telle attaque, prenez les mesures suivantes :

- **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.

## Intervention en cas d'incident de cybersécurité

S'assurer que des mesures opportunes sont prises pour évaluer les incidents de cybersécurité et que des procédures sont en place pour réagir aux atteintes réelles et présumées est un élément essentiel de tout programme de cybersécurité. Dans plusieurs décisions, le CIPVP a établi que l'adoption d'un plan d'intervention en cas d'atteinte à la vie privée représente un volet important des mesures raisonnables qu'une organisation doit prendre pour protéger les renseignements dont elle a la garde[10]. Ce plan comprend l'élaboration d'un plan officiel de gestion des incidents de cybersécurité qui comporte au moins les éléments suivants :

- **Description** des rôles, des responsabilités et de la formation et identification des cadres supérieurs qui sont chargés de déceler les incidents de cybersécurité et d'y réagir.
- **Formation d'une équipe spécialisée d'intervention en cas de cyberincident** comprenant des cadres supérieurs, du personnel en informatique (y compris des fournisseurs de services externes, le cas échéant) ainsi que des membres du personnel juridique, des communications et des ressources humaines, au besoin.

10 Par exemple, selon la **Décision 110 en vertu de la LPRPS**, [traduction] « l'obligation de prendre des mesures raisonnables pour protéger les renseignements personnels sur la santé comprend celle de répondre adéquatement à une plainte pour atteinte à la vie privée. Une réponse adéquate permet notamment de s'assurer que cette atteinte à la vie privée sera maîtrisée et ne se reproduira pas ». Le **rapport sur une plainte concernant la protection de la vie privée PR16-40** aborde également certains aspects de l'intervention en cas d'incident de cyberattaque, y compris la tenue d'une enquête en temps opportun en cas d'alerte et de rapport de sécurité.

- **Critères** uniformes d'identification et de classification des incidents de cybersécurité et des atteintes à la vie privée en fonction de leur nature et de leur gravité.
- **Procédures et échéanciers** pour les communications internes et l'escalade compte tenu de la nature et de la gravité de l'incident.
- **Processus, procédures et outils technologies** pour la détection, l'analyse, la maîtrise et l'élimination des incidents, la reprise des activités et les mesures correctives.
- **Autorisation explicite** de débrancher du réseau des systèmes essentiels, de désactiver des comptes utilisateur et de prendre d'autres mesures décisives pour maîtriser l'incident.
- **Procédures claires** permettant de déterminer les circonstances où il y a lieu de signaler des incidents aux organismes de réglementation et aux forces de l'ordre.
- **Plan de communication** décrivant comment votre organisation communiquera avec les employés, les particuliers concernés, le public et d'autres parties prenantes au sujet de l'incident.

Ce programme de gestion des incidents de cybersécurité devrait également comprendre des procédures et plans documentés pour composer avec les attaques par rançongiciel. Ces plans devraient comprendre les aspects suivants :

- **Tenue d'une liste d'entreprises de cybersécurité reconnues** qui pourraient contribuer sans délai à la tenue d'une enquête (comprenant notamment des recherches sur le Web caché pour déterminer si les données ont été publiées en ligne), à la prise de mesures correctives et, au besoin, à des interactions prudentes avec les attaquants (ou conclure un contrat avec une telle entreprise).
    - Les procédures devraient prévoir les circonstances dans lesquelles l'entreprise sera appelée à intervenir, notamment à la suite de quels types d'incidents, et à quel moment du processus d'intervention.
    - L'entreprise devrait suivre les pratiques exemplaires énoncées dans la présente feuille-info, et s'engager à fournir les éléments de preuve recueillis lors de son enquête aux organismes de réglementation et aux forces de l'ordre si une enquête pour atteinte à la vie privée était menée.
    - Des procédures d'analyse des journaux du réseau devraient être établies afin de déterminer si des données ont été exfiltrées.
- **Élaboration de plans généraux de continuité des activités** et de reprise comprenant :
    - des procédures visant la récupération sécurisée et en temps opportun des fichiers et systèmes à partir des copies de

sauvegardes et des images système, et la mise à l'essai régulière de ces procédures.

- **Obtention possible d'une police de cyberassurance** pour compenser les coûts associés aux mesures prises à la suite d'un incident, notamment les enquêtes, les honoraires d'avocats, les services de récupération de données et la fraude financière.

### Notification des atteintes à la vie privée

Les incidents de cybersécurité, y compris les attaques par rançongiciel, qui font intervenir des renseignements personnels peuvent aussi constituer des atteintes à la vie privée au sens des lois ontariennes. Dans ce cas, les dépositaires de renseignements sur la santé et les fournisseurs de services à l'enfance à la famille sont généralement tenus de prendre les mesures suivantes[11], et il est fortement recommandé aux institutions provinciales et municipales de faire de même :

- **Notifiez les particuliers concernés**. Déterminez l'identité des particuliers dont les renseignements personnels ont été touchés par l'attaque par rançongiciel et avisez-les de l'atteinte à la vie privée.
- **Signalez l'attaque au CIPVP**. Signalez les attaques par rançongiciel au Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario. Vous pouvez le faire **en ligne** ou nous joindre au 1 800 387-0073 ou à **info@ipc.on.ca**. Pour en savoir davantage sur les mesures à prendre en cas d'atteinte à la vie privée et la notification, veuillez consulter ces documents du CIPVP :
    - **Le signalement d'une atteinte à la vie privée au CIPVP : lignes directrices pour le secteur de la santé**
    - **Lignes directrices sur les interventions en cas d'atteinte à la vie privée dans le secteur de la santé**
    - **Les atteintes à la vie privée : lignes directrices pour les organismes du secteur public**
    - **Le signalement d'une atteinte à la vie privée au Commissaire à l'information et à la protection de la vie privée : lignes directrices pour les fournisseurs de services**

11 Par. 12 (2) et (3) de la LPRPS et par. 308 (2) et (3) de la LSEJF. Un rapport au CIPVP est exigé en cas de vol, de perte ou d'utilisation ou de divulgation non autorisée de renseignements personnels répondant à certains critères prescrits.

## Adaptation à l'évolution de la conjoncture

Les mesures qui peuvent sembler raisonnables dans une situation ne le seront pas nécessairement dans une autre. Lorsqu'il s'agit des mesures de précaution, les organisations doivent s'adapter à l'évolution de la conjoncture et tenir à jour continuellement leur programme de gestion de la cybersécurité[12].

Pour mieux vous adapter à l'évolution des menaces, y compris les rançongiciels, vous devriez prendre les mesures suivantes dans votre organisation :

- **Mettez sur pied un programme de renseignement** sur les menaces de cybersécurité pour surveiller de façon proactive l'évolution de la conjoncture quant aux menaces et échanger des renseignements avec d'autres organisations. Ce programme devrait aussi permettre de trouver des occasions stratégiques et tactiques de se protéger contre les menaces et de réduire l'exposition aux risques.
- **Effectuez des évaluations des risques** pour la vie privée et la sécurité chaque fois que des changements technologiques importants sont apportés, et veillez à réévaluer régulièrement toutes les composantes essentielles de votre parc informatique.
- **Examinez et mettez à l'essai et à jour régulièrement les plans d'intervention** en cas d'incident et les politiques et procédures de cybersécurité en fonction des menaces émergentes.
- **Tirez la leçon des attaques par rançongiciel** et prenez des mesures correctives sans délai afin d'éviter que des incidents semblables se produisent à l'avenir.

## Conformité aux normes et pratiques exemplaires de l'industrie

Il est important de vous tenir au courant des normes et pratiques exemplaires de l'industrie pour déterminer si votre organisation a mis en place des mesures de précaution raisonnables[13]. Parmi les cadres et normes à envisager, mentionnons le **cadre de cybersécurité** du NIST, la norme **Management de la sécurité de l'information** (ISO/IEC 270001) de l'Organisation internationale de normalisation et les **contrôles de sécurité critiques** du Center for Internet Security.

12 Dans l'**ordonnance HO-013**, l'ancien commissaire Brian Beamish a déclaré, en ce qui concerne les mesures de sécurité requises aux termes de la LPRPS : [traduction] « À mesure que sont élaborées, adoptées ou instaurées de nouvelles technologies et que surgissent de nouvelles menaces et vulnérabilités, les "mesures qui sont raisonnables dans les circonstances" au sens du paragraphe 12 (1) de la Loi évolueront également. »

13 Par exemple, l'**ordonnance HO-010** souligne que la norme du caractère raisonnable consiste à tenir compte de [traduction] « l'évolution des normes et pratiques de l'industrie, et des mesures de précaution d'ordre technique employées par d'autres hôpitaux de la province ».

Ces cadres de cybersécurité ne proposent pas une approche universelle. Chacun établit plutôt différentes catégories d'objectifs en matière de sécurité. Une organisation peut investir plus largement dans certains aspects de la sécurité que dans d'autres, en fonction de son profil de risque établi, de son orientation stratégique et de ses obligations légales.

Le CIPVP recommande vivement aux organisations d'adopter un cadre de cybersécurité standard de l'industrie et d'investir davantage dans des mesures qui permettent de mieux faire face aux menaces graves comme les rançongiciels. Par exemple, le National Institute for Standards and Technology (NIST) des États-Unis propose un **guide de démarrage rapide** qui permet de déterminer les catégories de son cadre de cybersécurité dans lesquelles il y a lieu d'investir en priorité afin de se protéger contre les rançongiciels.

## PRENEZ DES MESURES IMMÉDIATES ET PROACTIVES DÈS AUJOURD'HUI

Votre organisation peut agir immédiatement pour améliorer sa posture de sécurité par les moyens suivants :

- **Relevez immédiatement et réduisez les vulnérabilités des systèmes reliés à Internet dont on sait qu'ils sont pris pour cibles.** Pour commencer, envisagez de classer les vulnérabilités en ordre de priorité en consultant la liste annuelle des **vulnérabilités les plus exploitées** que dresse la Cybersecurity and Infrastructure Security Agency des États-Unis en collaboration avec le Centre canadien pour la cybersécurité. Vous devriez suivre vos procédures d'intervention en cas d'incident si vous constatez que votre réseau présente des vulnérabilités souvent exploitées qui n'ont pas été réduites en temps opportun.
- **Réalisez un exercice de table.** Invitez les cadres supérieurs à prendre part à un jeu de rôle ou à un exercice de simulation portant sur les mesures que le personnel devrait prendre en réponse à une attaque par rançongiciel. Un tel exercice peut constituer un moyen peu coûteux et efficace de relever de graves lacunes dans les mesures de sécurité. Il peut également contribuer à justifier des investissements dans la cybersécurité.
- **Adoptez ou mettez en œuvre un programme de formation du personnel** afin de sensibiliser vos employés aux risques de l'hameçonnage et de leur montrer comment identifier les courriels suspects, éviter d'être la proie d'attaquants et signaler immédiatement les risques éventuels au service de technologie de l'information. Envisagez d'envoyer de temps à autre à vos employés de faux messages d'hameçonnage pour aiguiser leurs réflexes.
- **Joignez-vous à des réseaux d'échange de renseignements sur la cybersécurité.** La communauté de pratique coordonnée par le **Centre d'excellence en cybersécurité** du gouvernement de

l'Ontario propose des ressources et du soutien en matière de cybersécurité au secteur public élargi.

## POUR EN SAVOIR PLUS

**Portail de l'Ontario pour l'apprentissage pour la cybersécurité**

**Centre canadien pour la cybersécurité : Guide sur les rançongiciels (ITSM.00.099)**

**National Cyber Security Centre (Royaume-Uni) : A guide to ransomware**

**Cybersecurity and Infrastructure Security Agency : Stop Ransomware**

**Cybersecurity and Infrastructure Security Agency : Tabletop Exercises Packages**

**NIST Cybersecurity Framework**

**Center for Internet Security**

**Conseil stratégique du DPI : Contrôles de cybersécurité de base des petites et moyennes organisations**

**Bonnes pratiques de sécurité Microsoft : Qu'est-ce qu'un ransomware ?**

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