QUOI FAIRE APRÈS

VOTRE OBLIGATION DE DIVULGATION

Qu'est-ce que la loi impose

La loi fédérale

1. Divulguer l'incident
La loi fédérale impose à toutes les organisation une obligation de notifier une atteinte aux mesures de sécurité lorsque celle-ci compromet la confidentialité des renseignements personnels détenus par l'organisation si l'incident représente un « risque réel de préjudice grave » pour les personnes affectées.

Le risque de préjudice grave s'applique notamment pour :
- Données bancaires ou financières
- Numéro d'assurance sociale

Les lois provinciales

1. Avant le 22 septembre 2022
Pour l'instant les lois provinciales en vigueur ne prévoient pas d'obligation de divulgation.

2. À partir du 22 septembre 2022
Le Projet de loi 64 adopté ajoute l'obligation de tenir un registre des incidents de sécurité et d'aviser, dans certaines situations précises, la Commission d'accès à l'information du cybercrimident lorsque l'incident présente un risque de préjudice sérieux pour les personnes concernées.

3. Responsabilité civile
La non-divulgation de l'incident pourrait engager votre responsabilité civile si l'omission empêcherait les personnes concernées de prendre des mesures pour protéger leur identité ou autre.

À QUI DÉCLARER

1 — Au niveau fédéral: le Commissaire à la protection de la vie privée (CPVP)

2 — Au niveau provincial (à compter du 22 septembre 2022): la Commission d'accès à l'information

3 — Toute personne concernée par le cybercrimident (clients, partenaires d'affaires, employés)

4 — Organismes fédéraux et provinciaux de réglementation

5 — Ordre professionnel

6 — Autorités policières en cas de cybercriminalité

Révise vos contrats

Il est aussi important de réviser vos contrats afin de vérifier s'ils contiennent des obligations en matière de cybercrimident.

N'hésitez pas à contacter notre équipe qui pourra vous aider à effectuer la révision de vos clauses contractuelles.

NOUS CONTACTER

Les normes internationales

Si votre entreprise fait affaire à l'international, il faudra que vous respectiez les règles qui s'appliquent.

Par exemple, en Europe, les entreprises doivent respecter le Règlement général sur la protection des données.

Utilisez votre plan de communication

Assurez-vous d'utiliser le plan de communication que vous avez créé pour déclarer le cybercrimident.

Servez-vous des gabarits de notification pour vous assurer de divulguer l'incident aux bonnes personnes rapidement.

Dans quel laps de temps divulguer?

Le plus tôt possible selon les lois fédérales et le Projet de loi 64.

En avril 2021, la cour supérieure a jugé qu'un délai de 46 jours était raisonnable dans certaines conditions considérant la nécessité de mener au préalable une enquête.

NOTRE CABINET

Contactez-nous à la suite d'un cybercrimident et nous vous aiderons à identifier les personnes à qui vous devez divulguer le cybercrimident et sur la meilleure manière de le faire.

LES SANCTIONS

Des sanctions administratives et pénales élevées peuvent être imposées en cas d'infraction aux lois.

PRÉSERVATION DES TRACES DE L'INCIDENT

Tenir un registre

- La loi fédérale impose et les lois québécoises imposeront à compter du 22 septembre 2023 à toute organisation de tenir un registre des incidents de confidentialité.
- Au fédéral, ceci s'applique pour les 24 mois suivant la date à laquelle l'organisation conclut qu'il a été victime d'un cybercrimident.

Contenu du registre

- Le règlement fédéral concernant les atteintes aux mesures de sécurité prévoit que le registre doit contenir toute information qui permet au Commissaire de vérifier que vous avez respecté votre obligation de notification:
  - Au Commissaire
  - À tout individu dont les renseignements personnels ont été touchés par un cybercrimident.

AMÉLIORATIONS

Cette étape consiste en la prise de nouvelles mesures ou de la mise à jour de celles-ci afin de prévenir un nouvel incident de cybersécurité.

Effectuer un audit de l'incident afin d'évaluer votre réaction à l'incident et implémenter des mesures de sécurité aux vulnérabilités découvertes

Effectuer une mise à jour du plan d'intervention en fonction de l'audit afin d'en améliorer l'efficacité

Penser à effectuer une nouvelle formation de vos employés

Effectuer un nouvel audit de la sécurité de votre entreprise

Utilisez notre questionnaire technojuridique qui vous permettra d'évaluer votre maturité en cybersécurité

LA CYBERSÉCURITÉ...

QUOI FAIRE AVANT
- Prévenir un cybercrimident
- Planifier une réponse

QUOI FAIRE PENDANT
- Détection et signalement
- Confinement de l'incident et enquête

QUOI FAIRE APRÈS
- Votre obligation de divulgation
- Préservation des traces de l'incident
- Améliorations à vos processus

MONTRÉAL
Bureau 4000
1 Place Ville Marie
Montréal QC H3B 4M4
Itinéraire
Téléphone : 514.871.4163
Télécopieur : 514.871.8977

QUÉBEC
Bureau 500
925, Grande Allée Ouest
Québec QC G1S 1C1
Itinéraire
Téléphone : 418.688.5000
Télécopieur : 418.688.3458

SHERBROOKE
Bureau 200, Cité du Parc
95, Boul. Jacques-Cartier Sud
Sherbrooke QC J1J 2Z3
Itinéraire
Téléphone : 819.346.5000
Télécopieur : 819.346.5007

TROIS-RIVIÈRES
Bureau 310
1600, rue Royale
Trois-Rivières QC G9A 6J5
Itinéraire
Téléphone : 819.375.5000
Télécopieur : 819.375.6963

© 2021 Lavery de Billy, S.E.N.C.R.L. Tous droits réservés.