PRÊT POUR **L'AVENIR?**

Déclaration des atteintes aux mesures de sécurité

Nouveaux mandats pour les entreprises canadiennes

À compter du 1er novembre 2018, les organisations canadiennes seront tenues d'observer le Règlement sur les atteintes aux mesures de sécurité. Ce nouveau règlement de la Loi sur la protection des renseignements personnels numériques (la « LPRPN ») exige de déclarer immédiatement aux autorités de réglementation fédérales toutes les atteintes à la protection des données qui peuvent présenter un « risque réel de préjudice grave ».

Incidence pour l'ensemble des organisations canadiennes

Bien que la LPRPN et la Loi sur la protection des renseignements personnels et les documents électroniques (« LPRPDE ») s'appliquent expressément aux organisations qui recueillent, utilisent et communiquent de l'information personnelle dans le cours de leurs activités commerciales au Canada, le nouveau Règlement sur les atteintes aux mesures de sécurité aura une portée plus grande et s'appliquera de manière générale à toutes les organisations canadiennes, ce qui comprend les petites entreprises, conformément au programme « Lentille des petites entreprises » mis de l'avant par le gouvernement du Canada.

Responsabilités en matière de déclaration

Si une organisation est victime d'une atteinte à la sécurité pouvant présenter un « risque réel de préjudice grave », elle doit s'acquitter des obligations suivantes :

1. **Réaliser une évaluation de risque officielle** pour déterminer si l'atteinte présente un « risque réel de préjudice grave » (et dans quelle mesure).
2. **Aviser tous les clients touchés** en décrivant l'atteinte à la sécurité et les circonstances dans lesquelles elle s'est produite, y compris :
   - Le moment approximatif où elle est survenue
   - L'information personnelle qui est compromise ou à risque
   - Les mesures prises pour réduire les dommages additionnels.
   - Les mesures à prendre par le personnel pour atténuer ou empêcher les dommages additionnels
   - Le nom du principal intervenant de l'organisation à qui s'adresser pour faire un suivi ou obtenir d'autres informations
3. **Aviser le ou la commissaire à la protection de la vie privée du Canada** des circonstances et de la cause (si elle est connue) de l'atteinte à la sécurité, y compris :
   - Le moment où elle s'est produite
   - Les informations personnelles qui sont à risque
   - Le nombre de personnes touchées
   - Les mesures prises pour réduire les dommages additionnels.
   - Le moyen que l'organisation utilisera pour communiquer avec les personnes touchées
   - Le principal intervenant de l'organisation à qui s'adresser pour faire un suivi
4. **Maintenir un dossier de l'atteinte à la sécurité** pendant au moins 24 mois.
5. **Observer le Règlement de la LPRPN** et conserver les documents d'attestation de conformité à portée de main.

Déterminer ce qu'est un « préjudice grave »

Les organisations doivent tenir compte de plusieurs facteurs pour déterminer ce qu'est un préjudice grave. Au-delà du vol d'identité, les organisations doivent aussi soupeser le caractère sensible de l'information et de quelle façon les malfaiteurs pourraient s'en servir. Voici quelques-unes des questions importantes à se poser :

- L'information pourrait-elle servir à humilier la personne touchée?
- Est-ce que l'atteinte a pour effet de nuire à la réputation ou aux relations de la personne?
- La personne touchée pourrait-elle perdre son emploi ou se voir refuser un poste dans l'avenir?
- Les personnes touchées pourraient-elles subir des dommages financiers?
- L'atteinte peut-elle entraîner la perte d'un bien ou des dommages à un bien?

N. B. : Lorsqu'il détermine si l'atteinte à la sécurité est susceptible d'avoir causé un « préjudice grave », le gouvernement ne fait pas de distinction entre l'information cryptée et celle qui ne l'est pas. Comme les malfaiteurs pourraient parvenir à décrypter l'information, les consignes énoncées ci-dessus doivent être suivies d'une manière ou d'une autre.

Comprendre les risques

Les cybermenaces exposent votre organisation à des risques importants de perte financière et d'atteinte à la réputation. Le resserrement des exigences de déclaration fait qu'il est encore plus important de répondre aux questions suivantes pour protéger vos activités, votre personnel et vos clients.

- Êtes-vous prêt à répondre à une atteinte à la sécurité des données? Autrement dit, avez-vous une procédure en place pour contenir l'incident, analyser son incidence et décrire les mesures à prendre pour rétablir la situation?
- Avez-vous prévu des protocoles qui indiquent clairement comment déclarer une atteinte et les informations à fournir?
- Vos contrôles et votre technologie de cybersécurité sont-ils suffisants pour limiter votre exposition à une atteinte à la sécurité ou une à cyberattaque?
- Si vous menez des affaires en Europe, vos protocoles et votre technologie de cybersécurité répondent-ils aux exigences du Règlement général sur la protection des données (RGPD)?

Comment MNP peut vous prêter main forte

MNP peut vous aider à évaluer vos besoins en sécurité de l'information, à déterminer vos priorités et à mettre en place un programme de protection concret et efficace. Nos spécialistes sont prêts à répondre à l'appel si votre sécurité devait malencontreusement être compromise. L'équipe d'intervention en cybersécurité de MNP vous accompagnera pas à pas, de la réponse au rétablissement.

Renseignements

Tom Beaupre
Leader régional, Cybersécurité
Tél. : 514.228.7844
Courriel : tom.beaupre@mnp.ca