

La première heure

Que faire dans les soixante minutes qui suivent la découverte d'un incident — et quels délais canadiens commencent à courir dès cet instant.

GRATUIT · À DIFFUSER LIBREMENT DANS VOTRE ORGANISATION

Trois règles avant de toucher à quoi que ce soit

- **Une seule personne coordonne.** Nommez-la à voix haute. Tout le reste déraile lorsque quatre personnes appellent le même fournisseur chacune de leur côté.
- **Ne détruisez pas les preuves.** Isolez les postes, ne les effacez pas. Ne supprimez pas le courriel d'hameçonnage. Les journaux que vous écrasez aujourd'hui sont ceux que votre assureur et l'autorité réclameront demain.
- **Ne promettez rien pour l'instant.** Ni à la clientèle, ni au personnel, ni sur les réseaux sociaux. Vous ne connaissez pas encore l'ampleur, et une correction ultérieure coûte plus cher en confiance qu'une heure de silence.

Les soixante premières minutes

0 – 15 MIN

Arrêter l'hémorragie

- 1 Nommez la personne responsable et ouvrez un journal écrit. Horodatez chaque entrée à partir de maintenant.
- 2 Isolez les systèmes touchés du réseau. Débranchez, n'éteignez pas — la mémoire vive contient des preuves.
- 3 Désactivez ou réinitialisez les identifiants que vous croyez compromis, y compris les jetons de session.
- 4 Vérifiez si les sauvegardes sont accessibles et, surtout, si elles sont elles aussi touchées.
- 5 Appelez la ligne d'urgence de votre assureur si vous avez une police. Plusieurs exigent un avis avant toute intervention.

15 – 30 MIN

Comprendre ce à quoi vous faites face

- 1 Ce qui s'est passé, en une phrase que vous seriez à l'aise de relire dans six mois.
- 2 Quels systèmes, quels comptes, quelles données. Notez ce que vous savez et ce que vous supposez.
- 3 Des renseignements personnels sont-ils en cause, ou pourraient-ils l'être ? C'est la question qui déclenche les délais légaux.
- 4 L'incident est-il toujours en cours ? Un incident contenu et un incident actif n'appellent pas les mêmes gestes.
- 5 Un fournisseur ou un client doit-il être prévenu parce que ses systèmes sont exposés par les vôtres ?

30 – 60 MIN

Décider et notifier

- 1 Suivez l'arbre de décision à la page suivante. Décidez, et consignez pourquoi vous avez décidé ainsi.
- 2 Ouvrez le registre exigé par la loi, que vous notifiiez ou non par la suite.
- 3 Désignez une seule personne pour répondre aux questions externes. Tout le monde y renvoie.
- 4 Informez le conseil ou le propriétaire. Une note factuelle aujourd'hui vaut mieux qu'une note soignée demain.
- 5 Fixez la revue post-incident avant de raccrocher. Sinon, elle n'aura pas lieu.

Ce qu'il faut consigner

Ce registre n'est pas de la paperasse. C'est la preuve que vous avez géré l'incident avec compétence, et c'est la première chose qu'on vous demandera.

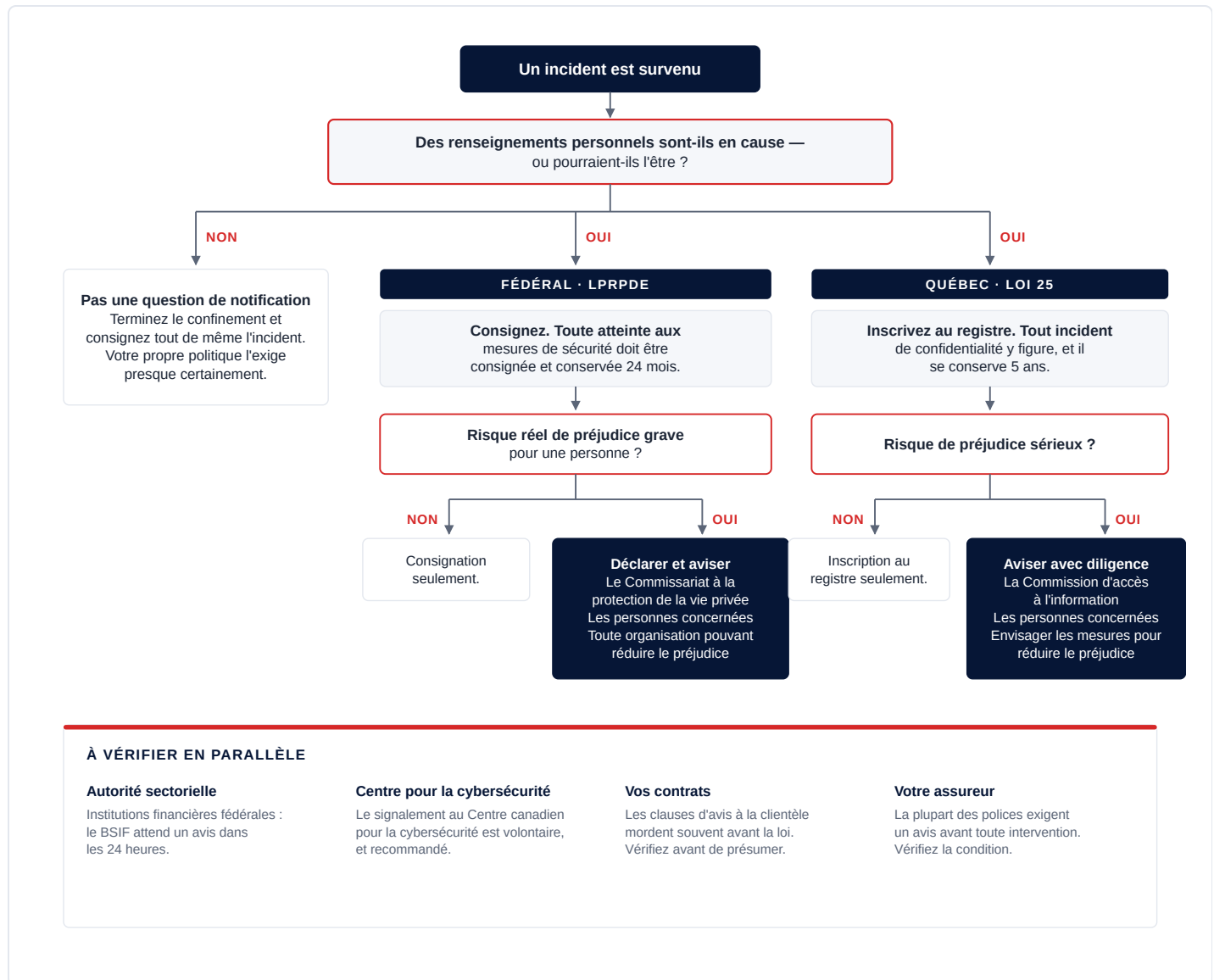
ÉLÉMENT	POURQUOI C'EST IMPORTANT
Date de la prise de connaissance	Les deux délais de conservation courent à partir d'une date que vous devez pouvoir énoncer.
Ce qui s'est passé	En mots simples. Les autorités les lisent ; la clientèle aussi, tôt ou tard.
Renseignements personnels en cause	Catégories et nombre approximatif de personnes. Écrivez « inconnu » si c'est inconnu.
Évaluation du préjudice	Votre raisonnement, pas seulement votre conclusion. C'est le raisonnement qui sera examiné.
Qui a été avisé, et quand	Autorité, personnes concernées, autres organisations, assureur, clientèle.
Ce que vous avez corrigé	La mesure que vous avez renforcée. C'est ce qui transforme un incident en amélioration.

Ce qu'il ne faut pas faire

- ✗ Ne payez pas de rançon avant d'avoir pris conseil. Cela peut constituer une infraction aux sanctions, et cela ne restaure que rarement tout.
- ✗ N'écrivez pas au sujet de l'incident à partir du système que vous croyez compromis.
- ✗ N'annoncez pas que l'incident est clos avant de savoir par où l'attaquant est entré.
- ✗ Ne laissez pas « l'enquête se poursuit » devenir la raison d'un délai manqué. Le compte à rebours ne s'arrête pas.
- ✗ Ne sautez pas le registre parce que vous avez décidé de ne pas notifier. Le registre est exigé dans les deux cas.

L'arbre de décision — notification

Deux régimes peuvent s'appliquer en même temps. La loi fédérale et la loi québécoise posent des questions différentes, retiennent des seuils différents et imposent des durées de conservation différentes. Suivez les deux — pas l'un ou l'autre.



Cet arbre vise les organisations du secteur privé. Les secteurs sous réglementation fédérale, les organismes publics et les détenteurs de renseignements de santé ont des obligations additionnelles. Il s'agit d'un point de départ pour votre avis juridique, non d'un substitut.