

Données sur les consommateurs : enseignements tirés des incidents liés à la sécurité

Toutes les entreprises qui collectent et conservent les données sur les consommateurs sont confrontées à une vaste gamme de menaces raffinées en constante évolution visant la sécurité des données qu'ils détiennent, et à des risques accrus de responsabilité légale et d'atteinte à la réputation. L'intervention initiale de votre organisation à la suite d'un incident lié à la sécurité est critique à la détermination de l'impact à long terme de l'incident sur votre entreprise. Les mesures immédiates que vous prenez après une atteinte à la sécurité peuvent donner le ton à l'intervention, influencer sur la facilité avec laquelle votre organisation peut se remettre de l'événement et avoir une incidence sur le risque de litiges et de recours collectifs liés à la protection des renseignements personnels ou menés par des consommateurs, et d'autres recours collectifs et litiges.

Cinq priorités en cas d'incident lié à la sécurité des données



Circonscrire

- Prendre immédiatement des mesures pour identifier et circonscrire l'incident
- Former une équipe d'intervention
- Ne pas compromettre la capacité d'enquête



Enquête

- L'enquête préliminaire
- Évaluer l'exposition Enquête judiciaire à long terme



Communiquer

- Intervention immédiate
- Sensibilisation à long terme



Aviser

- Aviser les organismes de réglementation
- Aviser les particuliers
- Aviser les parties intéressées



Corriger

- Prendre les mesures correctives pour remédier aux préjudices subis par les parties

Éléments clés

d'un protocole d'intervention en cas d'incident

- L'établissement d'un protocole et d'une structure de reddition de compte efficaces
- L'identification des fournisseurs de services et des autres parties intéressées clés
- La mise en œuvre de mesures pour protéger la confidentialité
- La disponibilité de l'assurance
- La valeur de la vérification de l'état de préparation en cas d'incident

Les Dix

Meilleures pratiques pour préserver la confidentialité lors d'incidents liés à la sécurité des données

1. Demander à votre conseiller juridique de participer à l'enquête
2. Procéder à un gel de documents
3. Faire parvenir au conseiller juridique une copie des communications internes et des communications avec des tiers
4. Inscrivez sur les documents la mention « Privilégié et confidentiel »
5. Transmettre les demandes de tiers au conseiller juridique, s'il y a lieu
6. Créer des dossiers confidentiels distincts
7. Limiter la circulation des avis juridiques et des rapports confidentiels
8. Faire appel à des témoins experts par l'intermédiaire du conseiller juridique
9. Aviser les membres de l'équipe que l'enquête vise à obtenir des conseils juridiques
10. Envoyer le rapport définitif du chef d'équipe au conseiller juridique

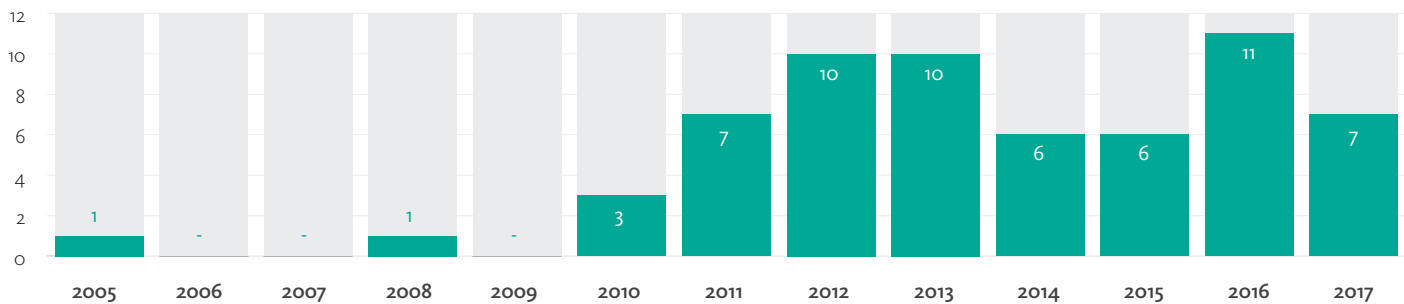
Risques de recours collectifs pour atteinte à la vie privée intentés par des consommateurs

Points clés :

- Le nombre de recours collectifs pour atteinte à la vie privée intentés par des consommateurs a augmenté rapidement au cours des dernières années
- Le piratage informatique est la principale cause d'incident à l'origine de ce type de recours
- L'utilisation abusive des renseignements ainsi que la perte ou le vol de supports matériels sont les principaux risques
- Les entreprises dans le secteur de la technologie ou des médias ainsi que les fournisseurs de soins de santé ont été les plus souvent visés

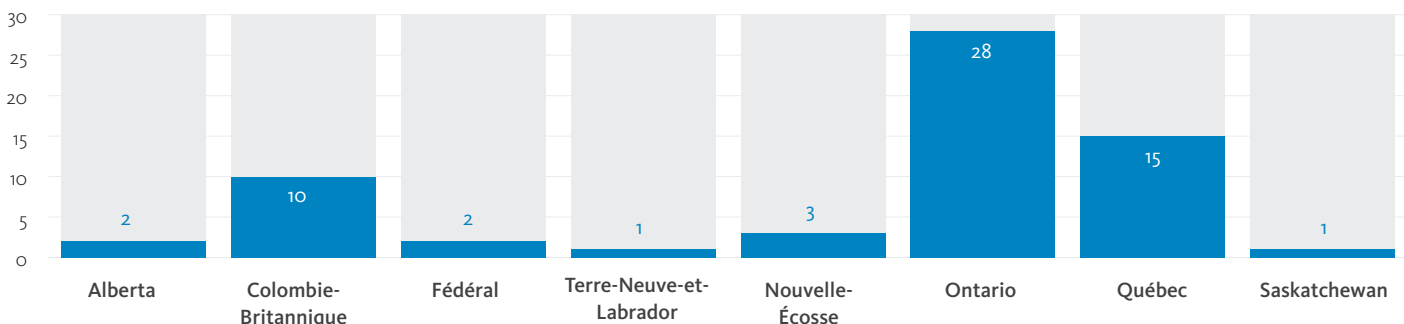
Nombre de recours collectifs pour atteinte à la vie privée par année

Total : 62



Nombre de recours collectifs pour atteinte à la vie privée par territoire

Total : 62



Nombre de recours collectifs pour atteinte à la vie privée par type d'incident

Total : 62

