La violation de données

VS.

La violation de l'éthique

Comment prévenir ces événements

Quentin Roulier

OneTrust

Privacy Management Software

Violation de l'éthique ou violation des données ?

Comment les différencier ?

OneTrust
Privacy Management Software

Les violations sont omniprésentes

THE WALL STREET JOURNAL.

Données des utilisateurs de Google exposées, répercussions de la divulgation au public

npr

Le groupe Marriott a annoncé une violation de données concernant 500 millions de ses clients

Forbes

Des experts en sécurité se sont prononcés sur la violation massive de données de 150 millions de comptes MyFitnessPal

TechCrunch

Fermeture du service Google+ après la dissimulation d'un bogue exposant des données

ZDNet

Equifax annonce qu'un plus grand nombre de données sur la confidentialité ont été volées qu'il n'en a été révélé en 2017

eWEEK

La FTC (Commission fédérale du commerce) sanctionne le fabricant de jouets IoT VTech pour violation de la vie privée

The New York Times

Facebook a révélé qu'une faille de sécurité avait compromis près de 50 millions de comptes de ses utilisateurs

CNN

Tous les comptes utilisateurs de Yahoo ont été piratés - un total de 3 milliards

Violation de l'éthique vs violation des données

Violation de l'éthique

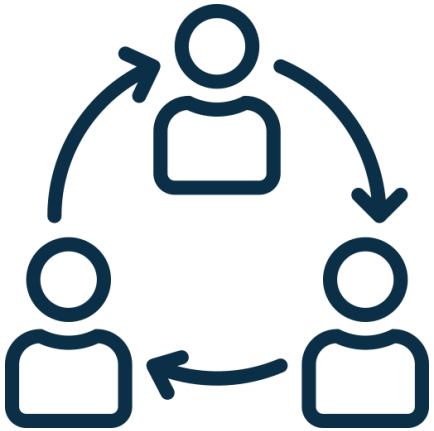
- Décision / choix éthique en contradiction avec la bonne conduite / les lois
- Intentionnel
- Résultats : donner l'exemple aux autres -> changement fondamental dans l'éthique de l'organisation, traitement erroné des données

Violation de données

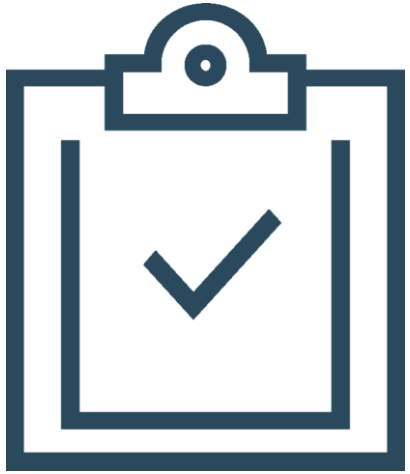
- Suppression, transfert ou divulgation non autorisés de données à une partie non autorisée
- Intentionnel ou non intentionnel
- Résultats : perte de confidentialité, d'intégrité, de disponibilité des données

LES DEUX REPRÉSENTENT : UN RISQUE DE PÉNALITÉS, DES PERTES FINANCIÈRES, UNE PERTE DE CONFIANCE

Dans le cas de Facebook / Cambridge Analytica : violation de l'éthique ou violation des données ?

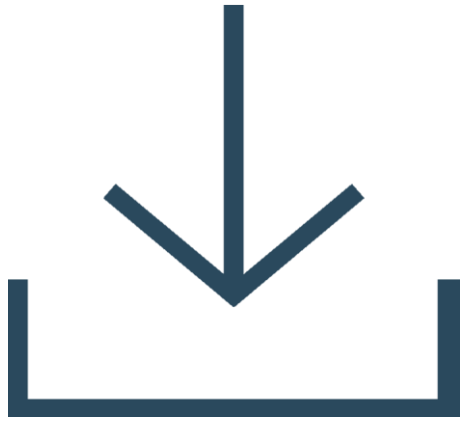


87 millions d'utilisateurs



L'enquête à des fins académiques est devenue un outil de microciblage

Pas de transparence et des dommages collatéraux pour ceux qui mènent l'enquête



Perte de confiance

Dans le cas de Marriott : Violation de l'éthique ou violation des données ?

383 millions de registres (dont 25 millions de numéros de passeport et 8,6 millions de numéros de carte de crédit)

Attaque ciblée de piratage informatique : Base de données des réservations des clients compromise depuis plusieurs années

Marriott a signalé l'infraction aux autorités de réglementation du monde entier - même dans les États où elle n'est pas obligatoire

Dans le cas d'Equifax : violation de l'éthique ou violation des données ?

Délai entre la prise de conscience de l'équipe de sécurité et l'annonce de la violation = 42 jours

OneTrust
Privacy Management Software

Objectifs d'éthique et objectifs de sécurité

- Faire ce qui est approprié
- **Subjectif**
  - Qu'est-ce que nos clients attendent de nous ?
  - Cela va-t-il avoir des répercussions sur le public ?
  - Cette décision sera-t-elle toujours considérée adéquate dans cinq ans ?
- Point d'attention : **mauvaise gestion des données**

- Limiter, atténuer, récupérer
- **Objectif**
  - Mesures à prendre pour limiter les violations
  - Processus d'atténuation des violations
  - Techniques appropriées de récupération des données
- Point d'attention : **Violations de la sécurité des données**

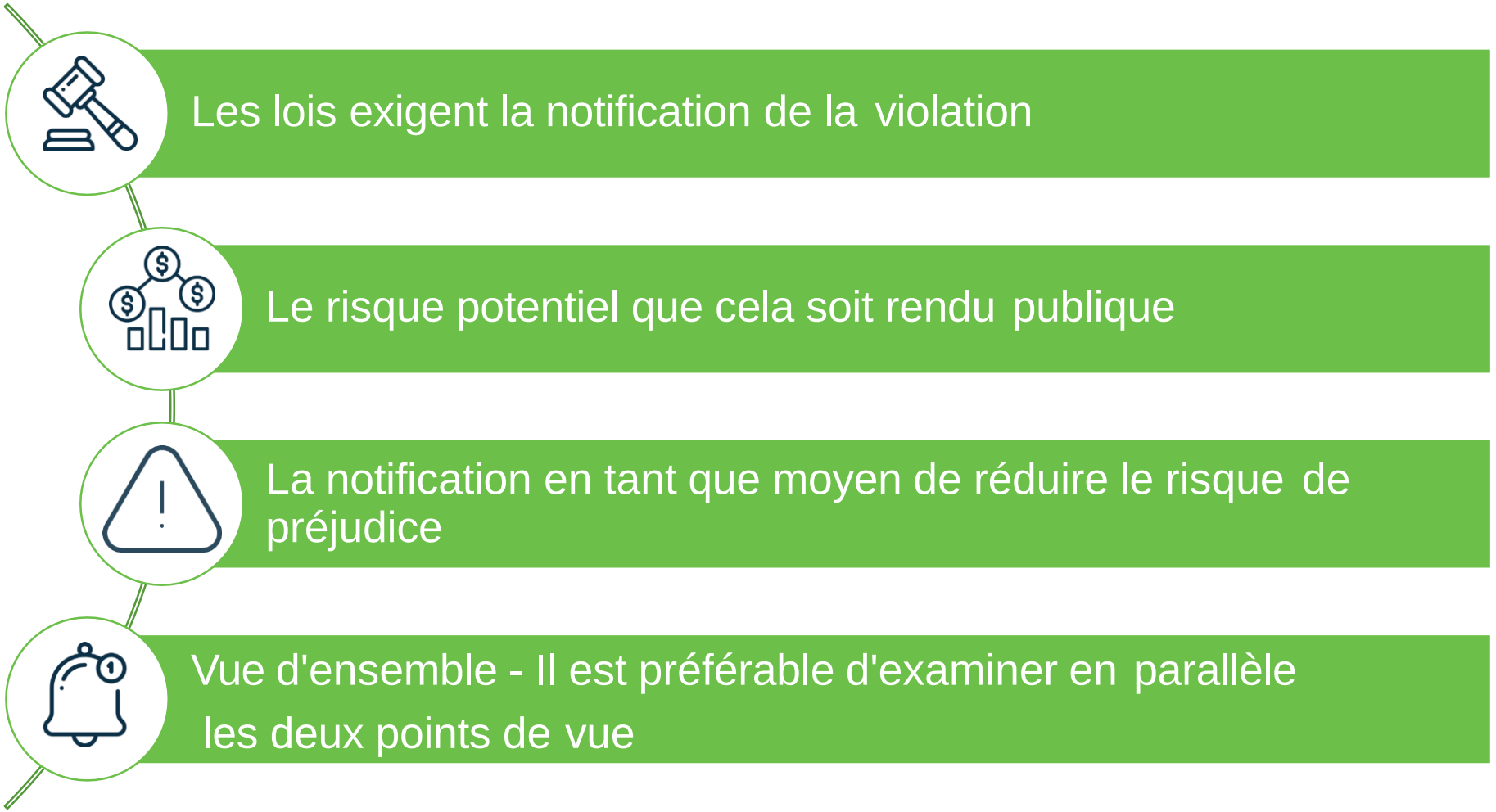
QUE FAUT-IL FAIRE EN MATIÈRE DE CONFIDENTIALITÉ ?

Notifier ou non?

Considérations éthiques clés dans les signalements de violation de données personnelles

OneTrust
Privacy Management Software

Doit-on notifier la violation au public ?



Comment y répondre correctement dans tous les cas ?

Une évaluation adéquate et complète des risques est essentielle

Déterminer tous les risques (réglementaires, juridiques, relations publiques, financiers) et les facteurs à prendre en considération lors de l'évaluation des risques

Créer un cadre d'évaluation des risques à l'avance

Entités clés : clients, partenaires commerciaux, marques, réputation

Prévention des violations

Ce que vous devriez mettre en place préalablement à toute violation

OneTrust
Privacy Management Software

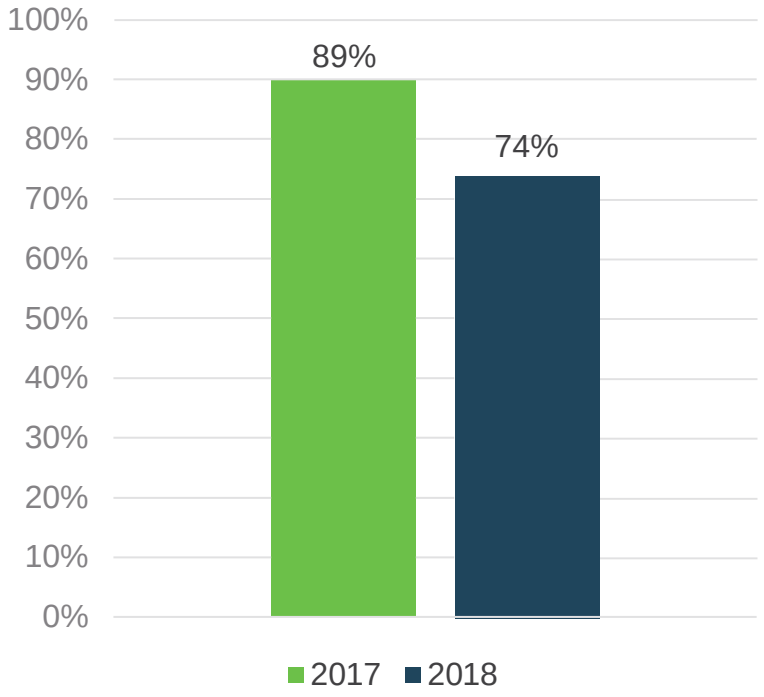
Check-list de gestion des violations de l'éthique et de la confidentialité

- Mettre en œuvre la politique de pratique éthique
- Examiner régulièrement la politique
- Politiques d'éthique pour les équipes informatiques et de sécurité
- Formation et ateliers pour les employés
- Éthique et confiance dans le cadre de la gestion des risques de l'entreprise
- Envisager une « garantie client »

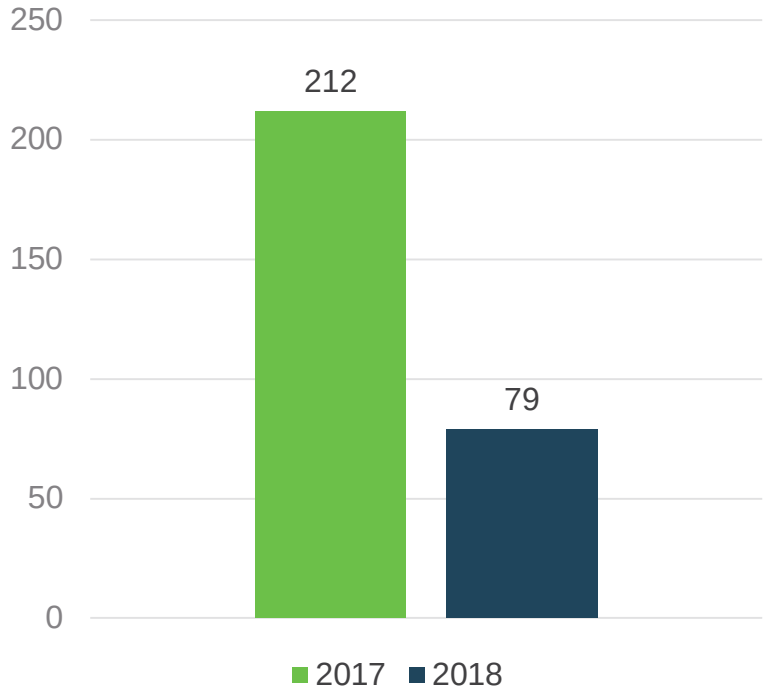
Préparez-vous et sachez comment vous prévenir des violations - Plan d'intervention OneTrust - « Playbook des incidents »

Conforme au RGPD = moins de violations

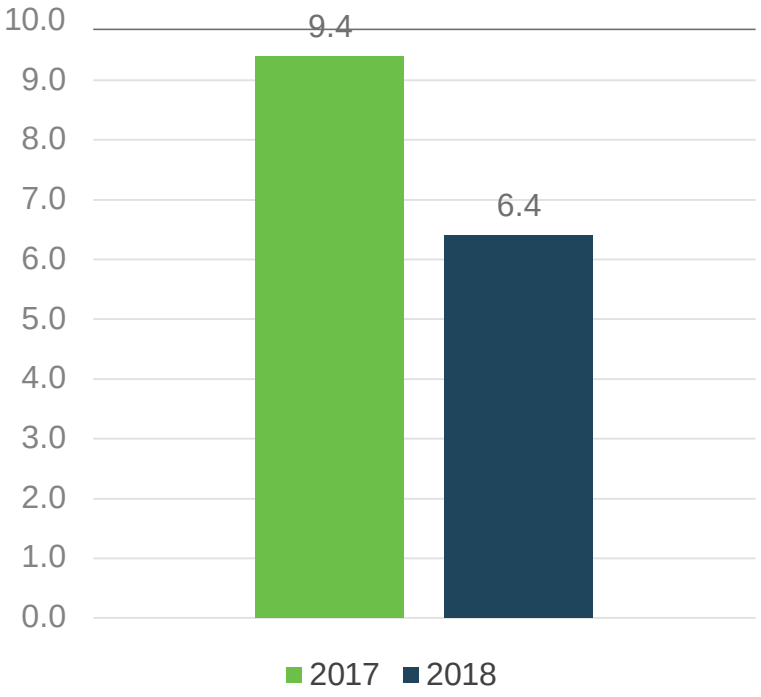
Taux de risque potentiel de violation de données au cours de la dernière année



Nombre de registres affectés lors d'une violation de données
(en milliers)



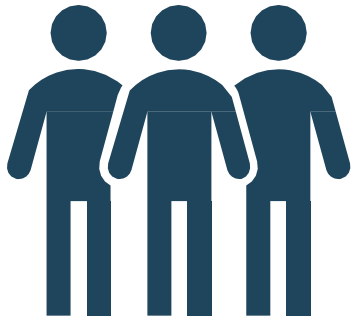
Durée d'indisponibilité du système en cas de violation de données
(en heures)



Source : Étude comparative sur la confidentialité des données - Cisco 2019

OneTrust
Privacy Management Software

Créez le Playbook



Équipes

Exigences législatives et contractuelles

Obligations supplémentaires en matière de violation

Mettre en place le playbook à l'avance

Donnez à votre organisation les moyens d'agir

- **Faites-en la responsabilité de chacun**
- **Organisez régulièrement des formations**
- **Informez-les en conséquence à l’aide de :**
  - **Badges nominatifs détaillés**
  - **Lignes directes internes / serveurs de courriel électronique**
  - **Webinaires, courriels**
- **Encouragez la transparence, la confiance et le respect pour éliminer toute crainte relative à la notification**

Exercices de simulation

Les exercices de simulation vous permettent de mieux appréhender la mise en pratique de votre réponse

Lorsque la violation se produit

Répondre aux violations conformément aux exigences des lois en matière d'éthique et de confidentialité.

OneTrust
Privacy Management Software

Catégorisation des incidents

Niveau 1	Niveau 2	Niveau 3
Généralisé **Grave** **Préjudiciable à la réputation**	**Limité au marché** **Inférieur à un seuil**	**Non confirmé** **Perte de dossiers personnels** **Courrier électronique mal acheminé**
Communications - 24h/24, 7j/7	*Réunions - 2 à 3 fois/jour*	*Réunion - Pas nécessaire*

Chaque niveau a son propre plan de réponse et de communication

Plan d’action de réponse aux violations

Si vous ne signalez pas l’incident, vous devez être en mesure de justifier votre décision

Toutes les étapes ci-dessus ne sont pas suivies pour tous les incidents. Ceci correspondà un maximum.

Stratégie de communication claire et immédiate

Stratégie de communication

Les individus affectés

Les entités pertinentes

Relations publiques

Avec les lois de notification de violation différant à travers le monde, songez à utiliser le « plus simple dénominateur commun » pour les mesures d'intervention

Documentez les violations

- Décrire la façon dont l'organisation enregistre les incidents liés aux violations de données (y compris ceux qui ne sont pas signalés)
- Requis en vertu de certaines lois relatives à la protection de la vie privée
- Contenu : les circonstances entourant la violation, les conséquences de la violation, les mesures correctives prises

Révision

Comment la violation s'est produite

Efficacité du plan d'intervention

Mise à jour du Playbook

Ressources gratuites disponibles

Le manuel de gestion des incidents et des violations

Le playbook de réponse aux incidents

onetrust.com/incident-toolkit

OneTrust
Privacy Management Software

OneTrust

Privacy Management Software

Venez visiter notre stand

Des démonstrations de produits

Des livres contenant le texte intégral du RGPD

Des outils & modèles gratuits

Des ateliers sur le RGPD

@OneTrust | onetrust.com | info@onetrust.com

Questions ?

OneTrust

Privacy Management Software