L'audit d'un programme de gestion de la protection de la vie privée

David Henrard, CISA, CISM, CRISC

ISACA-Québec - 5 décembre 2017

IN|FIDEM
SÉCURITÉ DE L'INFORMATION

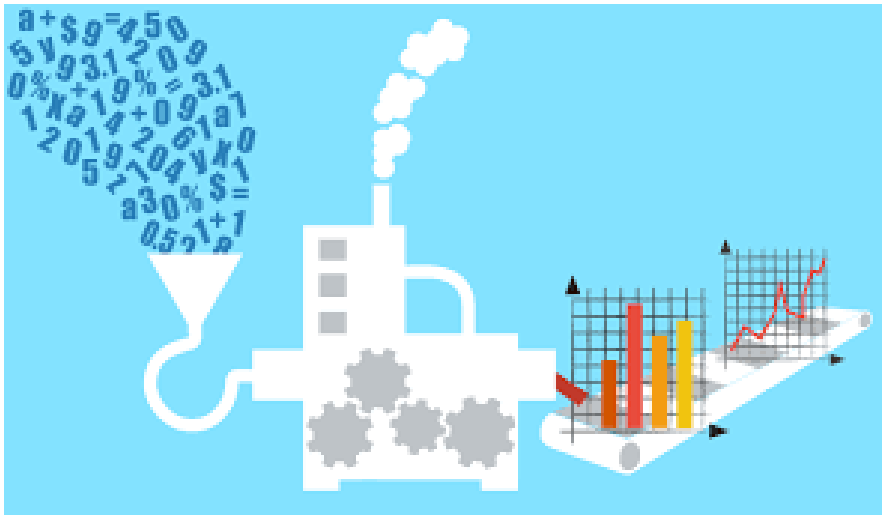
2ab & Associates

ISACA®
Section de Québec

Agenda

- Mise en contexte
- Présentation du programme d'audit de la protection de la vie privée d'ISACA

L’exploitation des données



Les sources de données

Les formulaires

Les réseaux sociaux

La mobilité

Les objets connectés

Les drones

Les accessoires portables

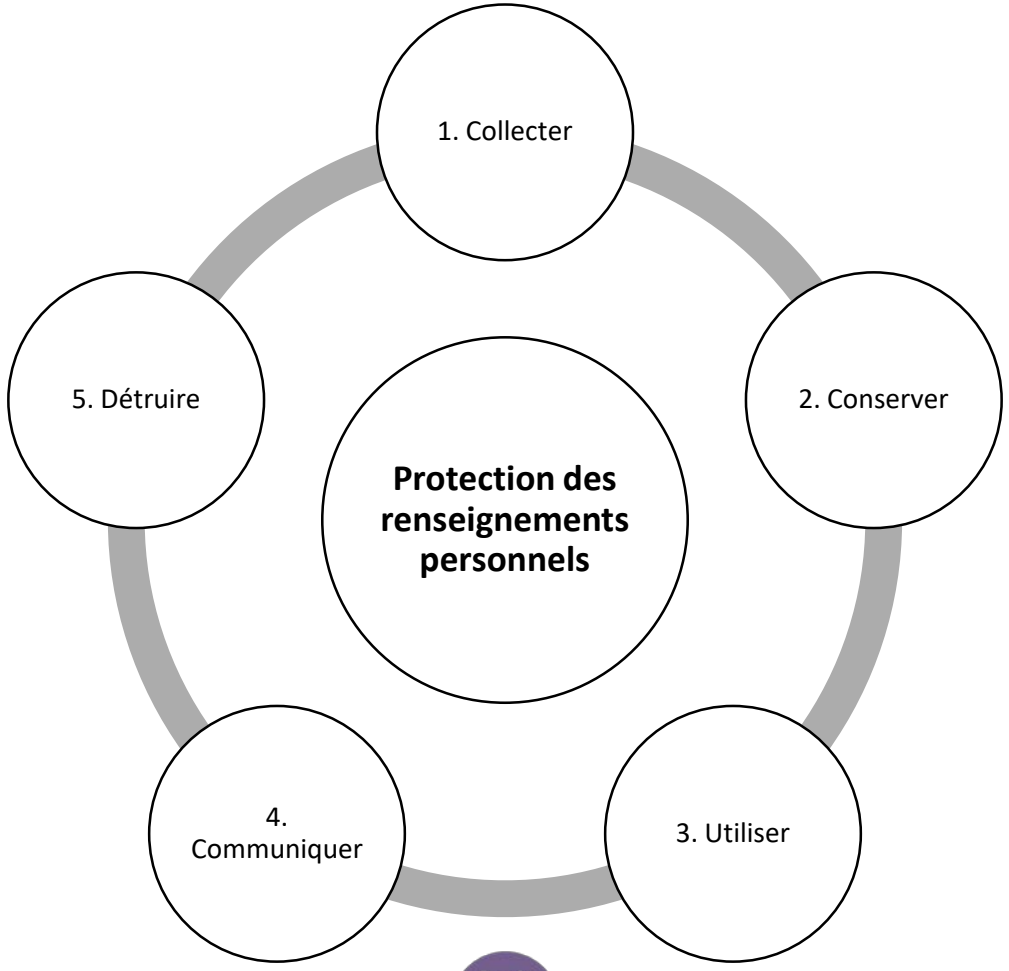
Les accessoires intégrés

INFIDEM
SÉCURITÉ DE L'INFORMATION

2ab & Associates

ISACA
Section de Québec

La responsabilité de protéger les renseignements personnels tout au long de leur cycle de vie

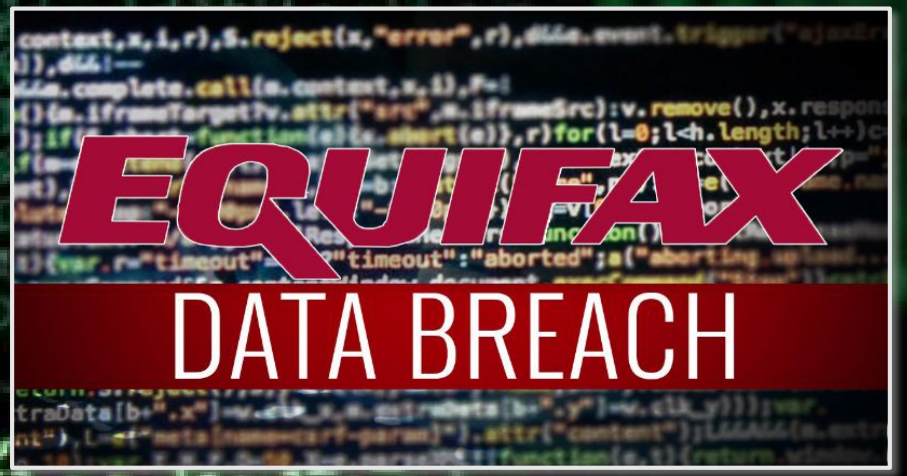


INFIDEM
SÉCURITÉ DE L'INFORMATION

2ab & Associates

ISACA
Section de Québec


EQUIFAX
Centre des membres
Connexion
Produits
Centre d'éducation
Comprendre son dossier de crédit
Recherche rapide
Centre d'éducation
English
Éducation sur le vol d'identité
Découvrez comment mieux protéger vos informations et que faire en ce qui concerne le vol d'identité.
Qu'est-ce que le vol d'identité?
Développez vos connaissances sur le vol d'identité et la façon dont les voleurs d'identité peuvent utiliser vos informations personnelles pour leur profit.
En lire plus
Comment le vol d'identité arrive-t-il?
Les voleurs d'identité développent des méthodes de plus en plus sophistiquées. Cette liste montre diverses façons dont un vol d'identité peut se produire.
En lire plus
Comment puis-je me protéger contre le vol d'identité?
Découvrez les étapes que vous pouvez prendre pour aider à protéger vos informations personnelles.
En lire plus
Développez vos connaissances sur…
Cotes de crédit
Dossiers de crédit
Vous ne trouvez pas ce que vous cherchez? Nous vous invitons à consulter nos questions fréquemment posées.
©2017 Equifax Inc. Tous droits réservés.
Plan du site | Politique de confidentialité | Modalités d'utilisation | Avis juridique
Equifax et les marques d'Equifax utilisées aux présentes sont des marques déposées d'Equifax Inc.
Propulser le monde à l'aide de connaissances


EQUIFAX
DATA BREACH


Equifax Inc., J, Nyse
O 92.50 H 93.38 B 91.88 C 92.71
différé
Volume (true) 2.351M 6.017M
MA (20) 126.2208
MA (50) 136.1465
MA (100) 136.8551
142.72
115.96
92.98
charts by TradingView

La notification obligatoire des incidents

Les sanctions

- Atteinte à la réputation - Perte de marché

- Sanction pour non-respect du RGPD
- De 10 M€ à 20 M€
- De 2% à 4% du chiffre d'affaires mondial

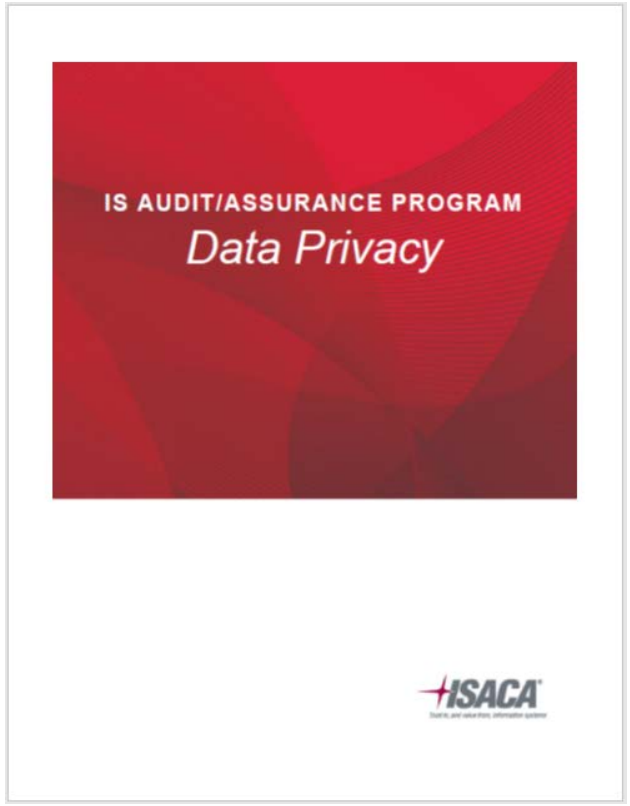
Les signes qui devraient vous alerter

- Les dirigeants ne sont pas sensibilisés ou impliqués
- La légitimité des données utilisées est inconnue
- Personne ne sait où se trouve l'information
- Les exigences de conformité sont inconnues
- Les risques associés à la protection de la vie privée et la cybersécurité ne sont pas considérés dans les prises de décision d'affaires
- Les opérations gèrent les risques
- La protection de la vie privée n'est pas prise en compte dans le cycle de développement des processus d'affaires et des systèmes
- Les politiques ne sont pas appliquées dans les opérations
- Il y a des incidents de sécurité et des pertes de renseignements personnels
- Les résultats d'audit sont négatifs
- La confiance des parties prenantes envers l'organisation est faible

Quelques exemples de questions

- Quels sont les raisons pour lesquelles des RP sont collectés?
- Quels sont les RP qui font l'objet d'un traitement?
- Quels types de RP sont collectés?
- Comment sont collectés les RP?
- Est-ce que le consentement de la personne est obtenu?
- En quoi les RP collectés sont pertinents pour le traitement?
- Quelles sont les mesures prises pour assurer l'exactitude des RP pendant la période de rétention?
- Quelle est la durée de la période de rétention?
- Où et comment sont stockés les RP?
- Quelles sont les mesures techniques et organisationnelles prises pour protéger les RP contre les accès non autorisés, dommages ou effacement?
- Est-ce que les RP sont communiqués à des tiers?
- Est-ce que les RP sont transférés en dehors du pays où ils ont été collectés
- Y-a-t-il des procédures en place pour permettre aux individus d'accéder et de contrôler l'usage de leurs RP?
- Comment sont détruits les RP qui ne sont plus nécessaires?

Le programme d'audit de la protection de la vie privée d'ISACA



https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/data-privacy-audit-program.aspx

Le contexte du programme

- Sujet de l'audit : la protection de la vie privée
- Objectifs de l'audit
  - Évaluer la gouvernance des données pour la PVP, la confidentialité et la conformité et déterminer si une gestion effective des données existe
  - Évaluer les contrôles en place
  - Réviser la gestion des données par les tierces parties
  - Évaluer les politiques et pratiques de gestion des incidents
- Portée de l'audit
  - Politiques et pratiques de PVP aux niveaux local, régional et global
  - Documentation de formation et de sensibilisation en PVP
  - Évaluation de l'impact de la PVP dans l'organisation
- Impacts et risques d'affaires

Les domaines couverts

Gestion de la PVP

- Gouvernance
- Politiques et procédures
- Formation et sensibilisation
- Analyse d'impact sur la PVP (gestion des risques)

Gestion et collecte de données

- Gestion d'affaires des données
- Utilisation et conservation
- Gestion des journaux (électroniques et physiques)

Sécurité des données

- Gestion des accès aux données
- Communication des données
- Stockage des données

Conformité des tierces parties et accords contractuels

- Gestion des tierces parties et interaction avec les données
- Obligations contractuelles avec les tierces parties

Gestion des incidents et escalade

- Réponse aux incidents et plan d'escalade
- Notification des parties externes
- Cyber assurance

IN FIDEM SÉCURITÉ DE L'INFORMATION

2ab & Associates

ISACA® Section de Québec

Gestion de la PVP

- Gouvernance
  - Rôles et responsabilités définis en matière de gouvernance des données
- Politiques et procédures
  - En fonction des besoins de l'organisation et de son usage des renseignements personnels (RP)
- Formation et sensibilisation
  - Appropriées, à jour et diffusées de manière appropriée
- Analyse d'impact sur la PVP
  - Existence de critères (pour les processus, systèmes et application)
  - Intégrés aux processus d'affaires et de développement

Gestion et collecte de données

- Gestion d’affaires des données
  - Définition claire de ce qui constitue des r
  - Mécanismes et outils de « désidentification » des RP
- Utilisation et conservation
  - En lien avec les besoins d’affaires légitimes et autorisés
- Gestion des journaux
  - Mise en place de procédure de gestion des journaux contenant des RP

Sécurité des données

- Gestion des accès aux données
  - Définition et mise en œuvre de règles d'accès aux RP au sein de l'organisation
- Communication des données
  - Mesures de protection durant le transport ou la transmission de renseignements personnels
- Stockage des données
  - Existence de processus et de procédures la sécurité des données stockées

Conformité des tierces parties et accords contractuels

- Gestion des tierces parties et interactions avec les données
  - Alignement des informations divulguées aux tierces parties et engagements contractuels
- Obligations contractuelles avec les tierces parties
  - Évaluation des tierces parties (préalable et continue)

Gestion des incidents et escalade

- Réponse aux incidents et plan d'escalade
  - Recueil des informations pertinentes
  - Implication des équipes de réponse
- Notification des parties externes
  - Présence d'un processus au sein des parties externes qui gèrent les RP pour l'organisation
- Cyber assurance

Des questions ?

IN FIDEM SÉCURITÉ DE L'INFORMATION

2ab & Associates

ISACA Section de Québec

Merci !

DAVID HENRARD, CISA, CISM, CRISC

david.henrard@infidem.biz

david.henrard@2abassociates.com

david.henrard@isaca-quebec.ca