info·SIRCO
ENQUÊTE ET PROTECTION
Mai 2011

L'ANALYSE DE RISQUE DORENAVANT INDISPENSABLE DEVANT LA LOI

--Gestion de l'information/ Vol d'identité--

Dans le cadre d'une volonté du gouvernement américain d'établir une coopération internationale dans la prévention et protection à travers le cyberespace, la maison blanche a fait l'annonce de projets de loi visant à contrer les cyber-attaques.

Parmi de nombreux projets soumis à l'intérieur de ce programme législatif de cybersécurité, une proposition de loi déterminant des lignes de conduites à adopter quant à la gestion des données personnelles est en phase d'être appliquée. Cette **politique fédérale de notification des violations de données (federal data breach notification policy)** prévaudra sur l'ensemble des différentes législations en vigueur dans les différents États.

Cette proposition définit la violation des données comme « *la compromission de la sécurité, la confidentialité et l'intégrité des données ou la perte de données informatisées qui résultent d'une acquisition non autorisée de données personnelles ou l'accès à des informations à des fins non autorisées* ».

À qui s'applique cette loi ?

La loi s'applique à toutes organisations dont leur activité commerciale interétatique utilise, a accès, transmet, conserve, dispose ou collecte des informations personnelles pour plus de 10 000 individus pendant une période de 12 mois, à l'exception des organisations de la santé et leurs partenaires qui doivent se conformer à la loi « HITECH » déjà en vigueur.

Comment s'applique cette loi ?

Les entreprises concernées devront prévenir immédiatement, par courrier ou par téléphone, les individus touchés par la violation des données, dès lors qu'elle aura été détectée, dans les 60 jours à moins qu'il n'existe aucun risque de préjudice ou de fraude. Elles devront par ailleurs faire état de la brèche de sécurité auprès du « Federal Trade Commission » (FTC), l'autorité compétente.

© U.S Government

Les compagnies concernées devront par ailleurs informer les médias si plus de 5000 personnes sont touchées, et ce, dans n'importe quel État. Il convient donc que l'erreur ou la négligence quant à la sécurisation des données, portera nettement atteinte à l'image de l'organisation.

La FTC, ainsi que les procureurs généraux pourront intenter une action civile contre les contrevenants. La sanction s'élèverait jusqu'à 1000 $ par jour et par personne touchée par les données compromises, jusqu'à un maximum de 1 million de dollars par violation de données, sauf si elle est jugée intentionnelle.

Exceptions de la loi

Une entreprise serait exemptée de l'obligation de notification si :

- elle participe à un programme de sécurité dans lequel les transactions sont bloquées avant d'être transféré sur un compte personnel et qui mentionne en préavis les consommateurs ;
- elle a mené une évaluation des risques concluant à l'absence de risque raisonnable que la violation porte atteinte à la sécurité des personnes dont les renseignements et informations sensibles ont été soumis à la violation.

- Une violation n'aurait pas à être déclarée si les données ont été rendues inutilisables, illisibles ou indéchiffrables grâce à la mise en place de technologie de sécurité ou de méthodes acceptées par les experts en sécurité informatique.

La FTC peut accorder un délai supplémentaire de 30 jours à l'organisation pour effectuer une enquête plus approfondie après une violation des données personnelles.

Comment se préparer à cette loi ? Quelles sont les bonnes pratiques à adopter ?

Évaluer les risques que représentent les données dont vous disposez : peuvent-elles faire l'objet de fraude ? Peuvent-elles être utilisées ? À quelles fins ? Peuvent-elles causer des préjudices à des clients, des partenaires, des entreprises si elles sont mal protégées ? Combien de données sont stockées, collectées, utilisées ?

Diagnostiquer régulièrement les angles d'attaque possible : D'où peut provenir la menace ? À l'interne ? À l'externe ? Quelles sont les failles possibles ? Quelles sont les actions possibles pour prévenir des failles de sécurité ?

Mettre en application une sécurité renforcée des informations personnelles : Réduire l'accès à ces informations ; protéger les accès à ces informations ; rendre ces informations illisibles ou inutilisables en cas d'accès non autorisé.

Anticiper : À quels problèmes peut-on être confronté ? À qui doit-on rendre des comptes ? Quels sont les impacts au niveau des clients, des partenaires, des médias, des autorités ?