Communiqués de presse

# L’étude 2015 de l’Institut Ponemon sur le coût des violations de données révèle un coût moyen record

**Les coûts pour répondre à une atteinte à la sécurité des données et la corriger représentent une moyenne de 3,8 millions de dollars dans le monde.**

**Le coût pour l’enregistrement de chaque perte ou vol de données a augmenté de 6%**

**Paris - 27 mai 2015:** Aujourd'hui, l’Institut Ponemon dévoile son étude annuelle, sponsorisée par IBM, concernant l’analyse globale du coût de la violation des données. Selon l'étude réalisée auprès de 350 entreprises dans 11 pays, le coût total consolidé moyen d'une violation de données est de 3,8 millions1 de dollars, ce qui représente une augmentation de 23% depuis 2013.

L'étude révèle également que le coût moyen induit pour chaque donnée perdue ou volée contenant des informations sensibles et confidentielles a augmenté de 6%, passant d'une moyenne consolidée de 145 à 154 dollars. La santé apparait comme l'industrie ayant le coût le plus élevé par donnée volée avec un coût moyen atteignant près de 363 dollars pour les organisations. De plus, les détaillants ont vu leur coût moyen par donnée volée augmenter considérablement de 105 dollars l'an dernier à 165 dollars cette année.

« Basé sur notre recherche sur le terrain, nous avons identifié trois principales raisons pour lesquelles le coût ne cesse de croître », a déclaré le Dr Larry Ponemon, président et fondateur de l’Institut Ponemon. Tout d'abord, les cyberattaques augmentent en fréquence, ce qui accroît les coûts de résolution. Deuxièmement, les conséquences financières de la perte de clients à la suite d'une faille de sécurité ont un impact plus important sur le coût. Troisièmement, les entreprises dépensent de plus en plus dans leurs activités de recherche et d’investigation, d’analyse et de gestion de crise ».

**A propos de la méthodologie de recherche du coût de violation de données**

La première étude sur la violation des données a été menée il y a 10 ans aux Etats-Unis. Depuis lors, la recherche s’est étendue à 11 pays. La recherche de l’institut Ponemon sur le coût de la violation des données est basée sur des données actuelles de centaines de catégories de coûts directs et indirects recueillies au niveau de l'entreprise en utilisant des méthodes de recherche sur le terrain et un cadre d'établissement des coûts par activité. Cette approche a été validée à partir de l'analyse de plus de 1600 entreprises qui ont connu une violation de données importante au cours des 10 dernières années dans 11 pays.

1 Les devises locales ont été converties en dollars US à des fins de comparaison

La recherche 2015 implique la collecte d'informations détaillées sur les conséquences financières d'une violation de données. Aux fins de cette recherche, une violation de données se produit lorsque la donnée sensible, protégée ou confidentielle est perdue ou volée et court un risque. Sur une période de 10 mois, les chercheurs de l'Institut Ponemon ont mené 1500 entretiens avec des experts IT, de la conformité, de la sécurité représentant 350 entreprises dans les 11 pays suivants : États-Unis, Royaume-Uni, Allemagne, Australie, France, Brésil, Japon, Italie, Inde, la région arabe (une consolidation des entreprises des Émirats arabes unis et de l'Arabie saoudite) et pour la première fois le Canada.

**Eléments clés :**

• **Le niveau d'implication du conseil d'administration et l'achat d'une police d'assurance peuvent réduire le coût d'une violation de données.** Pour la première fois, nous avons examiné les conséquences positives qui peuvent découler du rôle plus actif joué par le conseil d'administration en matière de violation de données dans une entreprise. L'implication de ce dernier réduit le coût de 5,50 dollars par enregistrement. La police d'assurance réduit le coût de 4,40 dollars par enregistrement.

• **La gestion de la continuité des affaires joue un rôle important dans la réduction du coût de la violation de données.** La recherche révèle qu'une implication de la gestion de la continuité des affaires dans l'assainissement de la violation peut réduire en moyenne le coût de 7,10 dollars par donnée compromise.

• **Les violations les plus coûteuses continuent à se produire aux États-Unis et en Allemagne** à respectivement 217 et 211 dollars par donnée compromise. L'Inde et le Brésil ont encore les violations les moins chères avec respectivement 56 et 78 dollars.

• **Le coût de la violation de données varie selon l'industrie.** Le coût global moyen de la violation de données par enregistrement perdu ou volé est de 154 dollars. Toutefois, si une organisation de santé subit une perte de donnée, le coût moyen pourrait atteindre 363 dollars, et dans l'éducation 300 dollars. Le coût le plus bas par donnée perdue ou volée est dans le secteur des transports (121 dollars) et le secteur public (68 dollars).

• **Les pirates et les criminels internes causent le plus de violations de données.** 45% de toutes les infractions relevées dans l'étude de cette année ont été causées par des attaques malveillantes ou criminelles.

Le coût moyen par enregistrement pour résoudre une telle attaque est de 170 dollars. En revanche, des problèmes liés au système coûtent 142 dollars par enregistrement et l'erreur humaine ou la négligence coûte 137 dollars par enregistrement. Les États-Unis et l'Allemagne sont les pays qui dépensent le plus pour résoudre une attaque malveillante ou criminelle (respectivement 230 et 224 dollars par enregistrement).

• **Les coûts de notification restent faibles, mais les coûts associés à l'activité perdue augmentent régulièrement.** Les coûts de l'activité perdue est issue d'une perte de clients anormale, ce qui augmente les activités d'acquisition de clientèle dans un contexte de perte de réputation et de diminution de la bienveillance. Le coût moyen a augmenté de 1,23 dollars en 2013 à 1,57 dollars en 2015. Les coûts de notification ont baissé passant de 190 000 dollars à 170 000 dollars depuis l'année dernière.

• **Le délai pour identifier et contenir une violation de données affecte le coût.** Pour la première fois, notre étude montre la relation entre la façon dont une entreprise identifie et contient rapidement des incidents liés à la violation de données et ses conséquences financières. Il faut environ 256 jours pour identifier les attaques malveillantes alors que les violations de données causées par une erreur humaine prennent en moyenne 158 jours pour être identifiées. Comme indiqué précédemment, les attaques malveillantes ou criminelles sont les violations de données les plus coûteuses.

« La sophistication croissante et la collaboration des cybercriminels sont directement liées à l'évolution de l'historique des coûts que nous observons en matière de violations des données », a déclaré Marc van Zadelhoff, Vice-President of strategie, IBM Security. « L'industrie a besoin de s'organiser au même niveau que les pirates pour se défendre contre ces attaques continues. L'utilisation des outils d'analyse avancés, le partage des renseignements de sécurité et la collaboration dans l'industrie contribueront à se mettre à niveau contre les attaquants tout en aidant à atténuer le coût pour le commerce et la société ».

**Prédire la probabilité d'une violation de données**

Pour la deuxième année, la recherche porte sur la probabilité qu'une société subisse une ou plusieurs violations de données dans les 24 prochains mois. Prenant appui sur l'expérience des sociétés participant à cette recherche, la probabilité est basée sur deux facteurs : le nombre d'enregistrements qui ont été perdus ou volés et le secteur d'activité de l'entreprise. Selon les résultats, les entreprises brésiliennes et françaises sont les plus susceptibles d'être victimes d'une violation de données comportant un minimum de 10 000 enregistrements. En revanche, les entreprises en Allemagne et au Canada sont les moins susceptibles de faire face à une violation de données. Dans tous les cas, il est plus probable qu'une entreprise subira une violation impliquant 10 000 enregistrements ou moins plutôt qu'une méga violation impliquant plus de 100 000 enregistrements.

Pour télécharger le rapport complet, merci d’utiliser le lien suivant : http://www.ibm.com/security/data-breach

**À propos de l'Institut Ponemon**

L’Institut Ponemon mène des recherches indépendantes qui visent à améliorer la sécurité de l'information, la protection des données, la vie privée et les pratiques de gestion de l'information au sein des entreprises responsables et des gouvernements à travers le monde. Notre mission est de mener des études empiriques de haute qualité sur les questions essentielles qui touchent à la protection de l'information et de l'infrastructure informatique. En tant que membre du Council of America Survey Research Organizations (CASRO), nous assurons la stricte confidentialité des données, de la vie privée et des normes éthiques de recherche. www.ponemon.org.

**A propos d’IBM Security**

La plateforme de sécurité IBM apporte la sécurité intelligente pour aider les organisations à protéger les personnes, les données, les applications et les infrastructures. Les solutions IBM couvrent la gestion des identités et des accès, le SIEM (Security Information and Event Management), la sécurité des données, la sécurité des applications, la gestion du risque, la gestion des terminaux, la nouvelle génération de protection contre les intrusions et d’autres sujets. IBM dispose d’une des plus importantes organisations au monde de recherche et développement et d’opérations dans le domaine de la sécurité.

Pour plus d'informations : www.ibm.com/security

Suivez notre actualité sur Twitter @IBMSecurityFR