

## Les salariés : principal risque pour les données des entreprises

**La nouvelle étude annuelle commandée par Absolute Software montre que les salariés ne tiennent pas compte des bonnes pratiques destinées à sécuriser leurs ordinateurs portables et les données qui s'y trouvent**

**Absolute® Software Corporation (TSX :ABT), spécialiste des solutions de récupération d'ordinateurs volés, de protection des données et de gestion sécurisée des ordinateurs, et Ponemon Institute, un cabinet de recherche spécialisé dans la gestion de l'information, publie aujourd'hui les résultats de la deuxième étude annuelle « Human Factor in Laptop Encryption ». Cette étude porte sur l'impact du facteur humain sur la sécurisation des données en entreprise.**

Selon les conclusions de l'étude, les managers d'entreprise feraient courir des risques importants aux données confidentielles comme les dossiers clients, les informations liées à la santé et toute autre sorte de données privées. Malgré les efforts des départements informatiques, beaucoup de managers désactivent trop souvent les solutions de cryptage qui se trouvent sur leurs ordinateurs. En cas de vol de l'ordinateur, les données les plus sensibles de l'entreprise se retrouvent ainsi entre les mains du voleur ou de toute autre personne qui chercherait à nuire à l'entreprise.

Plus précisément, cette étude est dédiée à la façon dont sont perçues l'efficacité des solutions de cryptage et les actions menées par les responsables IT et managers d'entreprise pour sécuriser leurs ordinateurs portables. Cette année, en plus des Etats-Unis, l'étude couvre le Royaume-Uni, la Suède, le Canada, la France et l'Allemagne. Les résultats montrent que 15% des managers allemands et 13% des managers suédois ont désactivé leur solution de cryptage. En comparaison, 52% des canadiens, 53% des anglais et 50% des français ont fait de même alors que les américains arrivent en tête avec 60% des managers ayant trouvé un moyen de contourner la politique de sécurisation des données de leur entreprise.

Si les allemands et les suédois sont moins enclins à se passer de leur solution de cryptage, ils ne cherchent pas non plus à crypter toutes leurs données : 49% des responsables informatiques suédois ayant déclaré avoir perdu ou s'être fait voler un ordinateur portable ont admis que cela a conduit à une violation de données. C'est également le cas pour un peu moins de 46% des responsables informatiques allemands et 50% de responsables IT canadiens. Les Etats-Unis suivis de près par le Royaume-Uni, arrivent en tête avec respectivement 72% et 61%. Les Français n'ont déclaré qu'à 28% que le vol ou la perte d'un ordinateur a donné lieu à une violation de données.

### D'autres résultats marquants pour la France :

- 52% des responsables IT pensent que le cryptage rend superflue l'application de toute autre mesure de sécurité et 49% des managers sont du même avis.
- 45% des managers interrogés pensent que le cryptage empêche les cybercriminels d'accéder aux données d'un ordinateur et de les voler et 46% des responsables IT partagent la même opinion.
- 31% des managers déclarent noter leur mot de passe sur un document comme un post-it par exemple afin de pouvoir s'en souvenir et 25% admettent le partager avec d'autres personnes. A l'inverse, aucun responsable IT français ne note son mot de passe et seulement 10% le partagent avec d'autres personnes au cas où ils l'oublieraient.

*« Cette étude montre bien que les managers dépendent trop de leur solution de cryptage pour protéger et sécuriser les données confidentielles qui se trouvent sur leur ordinateur. Or, si le cryptage est un outil de sécurité nécessaire, certains comportements inappropriés comme la désactivation de la solution, le partage du mot de passe ou l'utilisation d'un réseau sans fil non sécurisé peuvent considérablement réduire son efficacité. »* explique le Dr. Larry Ponemon.

*« L'étude montre que les outils utilisés par les départements informatiques et les départements de conformité sont encore insuffisants pour renforcer les politiques de l'entreprise particulièrement en ce qui concerne la protection des données sensibles. Malgré de réels efforts comme le déploiement de la technologie de cryptage, ceux-ci sont souvent contrariés par des comportements inappropriés de la part des utilisateurs. Quel que soit le pays où se situe l'entreprise, il est important de savoir jusqu'à quel niveau les employés peuvent être à l'origine*

*d'une potentielle violation de données. Le facteur humain doit réellement être pris en compte dans les plans de sécurité des ordinateurs »* déclare John Livingston, chaiman et CEO d'Absolute Software.

L'étude « Human Factor in Laptop Encryption » a été menée auprès d'informaticiens incluant les responsables sécurité informatique, et auprès de managers n'ayant pas de responsabilité informatique. Les personnes interrogées étaient réparties dans 20 entreprises situées aux Etats-Unis, au Canada, en France, en Allemagne et en Suède.

Les résultats de l'étude sont accessibles en ligne via le lien suivant : [www.absolute.com/human-factor](http://www.absolute.com/human-factor)

#### **A propos du Pomenon Institute**

Le Ponemon Institute se consacre à la promotion de l'éthique en matière d'information et des meilleures pratiques en matière de gestion de la confidentialité au sein des entreprises et des administrations. Pour atteindre ce but, l'institut mène des études indépendantes, sensibilise les responsables des secteurs public et privé ou encore évalue les pratiques en matière de confidentialité et de protection des données d'organisations issues de nombreux secteurs d'activité.

#### **À propos d'Absolute Software**

Absolute Software Corporation (TSX : ABT) est le leader des solutions de récupération d'ordinateurs volés, de protection des données et de localisation sécurisée des actifs (Secure Asset Tracking®). Absolute Software offre aux organisations, aux entreprises et aux particuliers des solutions en matière de respect des réglementations, de protection des données et de récupération d'ordinateurs volés. Le logiciel Computrace est intégré au BIOS des ordinateurs des principaux constructeurs informatiques tels que Asus, Dell, Fujitsu, General Dynamics Itronix, HP, Lenovo, Motion, Panasonic et Toshiba, et la société a conclu des partenariats de revente avec ces équipementiers et d'autres entreprises, dont Apple. Pour plus d'informations sur Absolute Software et Computrace, consultez le site [www.absolute.com](http://www.absolute.com) <<http://www.absolute.com>> et le blog <http://blog.absolute.com> <<http://blog.absolute.com>> .

#### **Énoncés prospectifs**

Le présent communiqué de presse contient des énoncés prospectifs comportant des risques et des incertitudes. Ces énoncés ont également trait, entre autres, aux performances escomptées de nos produits et services, à la disponibilité et au coût de certains services et produits, à la précision et aux exigences juridiques concernant l'utilisation de certains services et produits, et à d'autres attentes, intentions et projets décrits dans ce communiqué, n'étant pas des faits historiques. Ces énoncés prospectifs sont généralement reconnaissables à l'utilisation d'expressions comme « prévoir », « s'attendre à », « croire », ou de tournures similaires. Ces énoncés reflètent nos attentes actuelles et sont assujettis à une série de risques et d'incertitudes comprenant, sans s'y limiter, l'évolution de la technologie et du marché en général. Compte tenu de ces nombreux facteurs de risque et d'incertitude, nous tenons à préciser aux lecteurs qu'il nous est impossible de garantir la concrétisation des énoncés prospectifs émis dans le présent communiqué.

©2009 Absolute Software Corporation. Tous droits réservés. Computrace, Absolute et Secure Asset Tracking sont des marques déposées d'Absolute Software Corporation. La marque BlackBerry est la propriété de Research In Motion Limited et est enregistrée aux États-Unis, et peut être en attente d'enregistrement ou enregistrée dans d'autres pays. Absolute Software Corporation n'est pas avalisé, parrainé, affilié ou autorisé de quelque façon que ce soit par Research In Motion Limited. Google et Google Maps sont des marques de Google Inc. Windows Mobile est une marque déposée de Microsoft Corporation aux États-Unis et dans d'autres pays. Motorola et MOTO Q sont des marques ou des marques déposées de Motorola Inc. Palm et Treo font partie des marques ou des marques déposées propriété ou sous licence de Palm, Inc. Samsung est une marque déposée et BlackJack est une marque de Samsung Electronics Co., Ltd. et de ses entités associées. Brevets Computrace États-Unis n° 5715174, n° 5764892, n° 5802280, n° 5896497, n° 6244758, n° 6269392, n° 6300863 et n° 6507914. Canada n° 2284806 et n° 2205370. Royaume-Uni n° EP793823 et n° GB2338101. Brevet allemand n° 695 125 34.6-08. Brevet australien n° 699045. Brevet japonais n° JP4067035. La Bourse de Toronto n'a ni approuvé ni désapprouvé les informations contenues dans ce communiqué de presse