Rapport Risk:Value de NTT Security : moins de la moitié des décideurs se sentent concernés par le RGPD tandis qu'un cinquième avoue être dans le flou.

Une proportion inquiétante de sondés ignorent où se trouvent leurs données, ni même si leur information critique est en sécurité

PARIS, 10 juillet 2017 (GLOBE NEWSWIRE) — Le rapport a révélé que nombre de décideurs dans le monde ne perçoivent pas les implications futures du Règlement Général sur la Protection des Données (RGPD) ou d'autres normes réglementaires comme PCI-DSS ou ISO 27001/2. En effet, un cadre sur cinq ignore ses obligations réglementaires en matière de cybersécurité selon l'étude
Risk:Value 2017
menée par Vanson Bourne

pour
NTT Security
, filiale du groupe NTT spécialisée dans les questions de cybersécurité. Cette enquête livre une information utile à double titre : elle nous éclaire sur l'attitude des entreprises face aux cyber-risques et souligne toute l'importance d'une bonne sécurité de l'information.

Pour mener cette étude, le cabinet Vanson Bourne a interrogé 1 350 décideurs hors fonction IT dans 11 pays. Premier point notable, seuls 40 % des sondés estiment que le RGPD concerne leur entreprise. Chiffre plus inquiétant encore : 19 % confient ne pas connaître leurs obligations réglementaires en matière de cybersécurité. Ainsi, au Royaume-Uni, seuls 39 % des cadres interrogés sont conscients de leurs obligations de conformité au regard du RGPD, alors que 20 % avouent être dans le flou. Sans surprise, les décideurs hors UE sont encore moins au fait des ramifications du RGPD. Bien qu'il s'applique à toute entreprise collectant des données de citoyens européens, un quart seulement des cadres américains se sentent concernés par le nouveau règlement. L'Australie (26 %) et Hong Kong (29 %) ne font guère mieux.

Le 25 mai 2018 marquera l'entrée en vigueur du RGPD. Les entreprises ont donc moins d'un an pour se mettre au diapason des nouvelles règles de sécurité et de confidentialité des données. En cas de non-respect, les régulateurs prévoient des sanctions sans précédent : 20 M€ ou 4 % du chiffre d'affaires annuel mondial, selon le montant le plus élevé.

Alors que les questions de gestion et de stockage des données sont au coeur du RGPD, le rapport
Risk:Value
révèle qu'un tiers des sondés ignorent où se trouvent leurs données. Autre chiffre inquiétant, seuls 47 % affirment que
toutes

leurs données critiques sont à l'abri. Parmi ceux qui connaissent l'emplacement de leurs données, moins de la moitié (45 %) se disent « parfaitement conscients » de l'impact du RGPD sur leurs politiques de stockage. Fait intéressant : ce sont les secteurs de la banque/finance et de l'informatique/high-tech qui obtiennent les meilleurs scores sur ces questions.

Pour Garry Sidaway, VP Security Strategy & Alliances chez NTT Security, la situation est claire. « Dans un monde rempli d'incertitudes, une chose est sûre : les entreprises à vocation internationale feraient bien de noter la date du 25 mai 2018 dans leur calendrier. Même si le RGPD est une initiative européenne, son impact se fera sentir dans le monde entier pour tous les acteurs collectant ou conservant des données personnelles de citoyens européens. Notre rapport montre clairement qu'une part considérable de décideurs ignorent ou ferment les yeux sur ce nouvel enjeu. Malheureusement, trop d'entreprises ne voient dans la conformité qu'un exercice coûteux sans réelle valeur ajoutée. Or, faire l'impasse sur ces questions, c'est justement s'exposer à des pertes de chiffre d'affaires ainsi qu'à de lourdes sanctions financières. »

Réputation, chiffre d'affaires, démissions – Bien peser les conséquences

- Un sondé sur huit estime qu'une mauvaise sécurité de l'information représente le risque n° 1 pour son entreprise. La « perte de parts de marché » reste toutefois le principal risque évoqué (28 %).
- 57 % des sondés sont convaincus que leur organisation subira tôt ou tard une violation de données.
- Interrogés sur les conséquences d'une violation, les sondés citent d'abord des pertes financières à court terme puis, à plus long terme, une entrave au développement de l'entreprise. Ils mentionnent également la perte de confiance du client (55 %), l'atteinte à la réputation (51 %), l'impact financier (43 %) et, dans une moindre mesure, le départ de collaborateurs (13 %) et de cadres dirigeants (9 %).
- Entre 2015 et 2017, le coût moyen de rétablissement des activités a grimpé de 907 000 dollars à 1,35 million de dollars.
- Entre 2015 et 2017, l'impact sur le chiffre a reculé de près de trois points (de 12,51 % à 9,95 %). Il reste néanmoins considérable.
- 56 % des cadres interrogés affirment que les questions de cybersécurité sont régulièrement débattues aux réunions de direction. Du chemin reste encore à parcourir pour que les dirigeants s'impliquent davantage dans ces questions.
- En moyenne, les entreprises ne consacrent que 15 % de leur budget informatique à la sécurité de l'information, même si ce chiffre est en hausse par rapport à 2015 (13 %) et 2014 (10 %). Une part considérable de sondés affirment privilégier la R&D (31 %), le commercial (28 %) ou le marketing (27 %).

L'importance d'une culture axée sur la sécurité

- 56 % des sondés affirment disposer d'une politique formelle de sécurité de l'information, contre 52 % en 2015. Un peu plus du quart (27 %) se disent en phase d'implémentation, tandis que 1 % ne possèdent ni ne prévoient d'instaurer une politique de sécurité.
- Parmi les participants ayant mis en place une politique formelle, 79 % déclarent en avoir

communiqué le contenu de façon active auprès de tous les collaborateurs. Sur ce terrain, l'Allemagne et l'Autriche décrochent la palme (85 %), talonnée par les États-Unis (84 %) et le Royaume-Uni (83%). Néanmoins, seuls 39 % des sondés assurent que leurs collaborateurs connaissent réellement le contenu de ces politiques.

- La mise en place d'une politique de sécuriré de l'information varie fortement d'un pays à l'autre. Alors que certains pays comme la Suède (30 %) traînent des pieds, d'autres comme le Royaume-Uni prennent les devants (72 %).
- Si l'on procède à une analyse par secteur, la santé émerge en tête de peloton, avec 69 % des entreprises possédant une politique formelle de sécurité de l'information. La finance suit de près avec 66 %.
- Moins de la moitié des entreprises (48 %) disposent d'un plan d'intervention sur incidents, même si 31 % affirment qu'un plan est en cours d'implémentation Toutefois, seuls 47 % des décideurs en connaissent précisément le contenu.

Téléchargez le rapport
Risque-Valeur 2017
de NTT Security :

www.nttsecurity.com/fr/RiskValue2017

Échantillon de l'étude

Cette étude a été réalisée par Van Bourne pour NTT Security, de mars à mai 2017. Le cabinet a interrogé 1 350 décideurs hors fonction IT (65 % de cadres dirigeants), répartis dans les pays suivants : France, Royaume-Uni, Allemagne, Autriche, Suisse, Suède, Norvège, États-Unis, Australie, Hong Kong et Singapour. Les entreprises sélectionnées appartiennent à différents secteurs et comptent toutes plus de 500 salariés. Enfin, un tiers des réponses environ proviennent du secteur financier.

Le cabinet Vanson Bourne :

Vanson Bourne est un cabinet d'études marketing indépendant et spécialisé dans les technologies. Réputées pour leurs analyses fiables et crédibles, nos études s'appuient sur des principes de recherche rigoureux et sur notre capacité à recueillir l'avis de grands décideurs des fonctions techniques et métiers, et ce dans tous les secteurs économiques et sur tous les principaux marchés. Pour plus d'informations, rendez-vous sur
www.vansonbourne.com
.

A propos de NTT Security

NTT Security est la branche sécurité du groupe NTT. Nous mettons notre expertise sécurité au service des entités du groupe (Dimension Data, NTT Communications et NTT DATA) en délivrant des solutions métiers résilientes pour accompagner leurs clients dans leur transformation digitale. Forte de ses 10 centres opérationnels de sécurité (SOC), ses 7 centres de R&D et plus de 1 500

experts en sécurité, NTT Security intervient chaque année sur des centaines de milliers d'incidents à travers six continents.

Pour optimiser l'utilisation de nos ressources locales et libérer le potentiel de nos capacités mondiales, nous offrons un ensemble adapté de services managés et de conseil aux entreprises. NTT Security fait partie intégrante du groupe NTT (Nippon Telegraph and Telephone Corporation), l'une des plus grandes entreprises de TIC au monde. Pour en savoir plus, rendez-vous sur nttsecurity.com

Pour plus d'informations, veuillez contacter Lucie Curabet ou Angélique De Barros d'Oxygen à :

luciec@oxygen-rp.com
/
angelique@oxygen-rp.com

01.41.11.37.77 / 01.41.11.37.78
