NTT Communications | NTT Com Security

# Brèches de sécurité – quel est le coût réel pour votre business ?

## Le rapport Risk:Value 2016

# Avant-propos

Les entreprises saisissent bien la menace que représentent les cybercriminels cherchant à subtiliser ou endommager leurs données. Pourtant, il leur reste encore beaucoup de chemin à effectuer pour mieux s'en prémunir. Les infrastructures des entreprises regorgent de données sensibles. En théorie, il revient donc à leurs dirigeants de mettre en place une protection efficace contre les accès non autorisés.

Mais dans la pratique, les entreprises n'en font rien, ce qui les expose à de graves conséquences, allant de pertes financières directes, à une érosion de la réputation difficile à enrayer à long terme.

Pour affronter ce problème, elles doivent commencer par mettre en place des politiques de sécurité informatique fiables qu'elles devront ensuite communiquer efficacement à leurs collaborateurs. L'enjeu est ici d'établir une culture de la sécurité dans laquelle la prévention des violations de données prévaut sur une approche réactive dans laquelle les dirigeants doivent littéralement limiter les dégâts.

# Synthèse

## Droit dans le mur

Tous les spécialistes de domaines dits « à risque » vous le diront : la plupart des gens connaissent les risques encourus, mais n'affrontent bien souvent le problème que lorsqu'il est déjà trop tard. Par exemple, ils fument, font peu d'exercice et mangent mal, même s'ils connaissent parfaitement les statistiques de mortalité. À une échelle plus large, nous sommes conscients des risques liés au changement climatique, ce qui ne nous empêche pas d'émettre du carbone à un rythme inquiétant. Comme si nous étions programmés pour tout remettre au lendemain.

Et la cybersécurité n'échappe pas à la règle. Les entreprises connaissent les risques d'un vol de leurs données. Elles ont même conscience des conséquences désastreuses d'un tel événement. Malgré tout, elles réagissent souvent de façon impulsive après le vol, plutôt que d'entamer en amont une réflexion sur la prévention d'un tel acte.

C'est ce que révèle une enquête menée par Vanson Bourne pour NTT Com Security. Le cabinet a interrogé 1 000 décideurs dans des entreprises de six pays d'Europe et aux États-Unis afin d'évaluer leur attitude face aux enjeux du risque et de la cybersécurité. L'objectif de l'étude était de connaître le coût de la cybersécurité pour ces entreprises et les mesures de protection mises en place. Certains résultats sont alarmants, comme le montrent les chiffres ci-contre.

**25 %**

**Parmi les personnes interrogées, 25 % sont certaines que leur entreprise subira tôt ou tard une violation de sécurité.**

**$1m**

**Cette violation coûtera près d'1 million de dollars en moyenne, et même bien plus pour les plus grandes entreprises.**

**75 %**

**75% des décideurs ne pensent pas que toutes les données de leur entreprise soient totalement protégées.**

**4 sur 10**

**4 personnes sur 10 affirment que les données sont davantage en sécurité sur leur ordinateur personnel qu'au travail.**

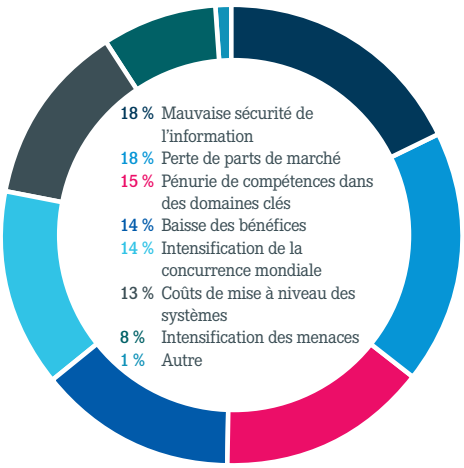
## Cyberintrusion : une conséquence inéluctable

Pour de nombreux dirigeants, la question n'est pas de savoir si, mais bien quand un incident de cybersécurité se produira. De fait, un quart des sondés sont sûrs et certains que cela leur arrivera, tandis que 40 % en sont quasiment sûrs.

Pour 18 % des personnes interrogées, une mauvaise sécurité de l'information reste le risque n° 1 pour leur entreprise, à égalité avec la perte de parts de marché au profit d'un concurrent. En d'autres termes, une protection inadaptée des informations de l'entreprise est désormais perçue comme un danger plus grand que la concurrence mondiale et la baisse des bénéfices.

Difficile à imaginer il y a cinq ans ! On assiste donc à un changement de perception des risques métiers. Et les mentalités évoluent vite. Pour preuve, en 2014, lorsque NTT Com Security avait interrogé les entreprises sur le plus grand risque à leurs yeux, seuls 9 % des sondés avaient cité une mauvaise sécurité de l'information. Que s'est-il passé entre-temps ?

**Figure 1** « Quel est à vos yeux le risque n°1 pour votre entreprise ? » – *Question posée à la totalité de l'échantillon (1 000 sondés)*



## Évolution du champ sécuritaire

Cette nouvelle perception des risques métiers reflète bien la réalité. Les gros titres nous en fournissent chaque jour la preuve : les violations de données de grande ampleur se multiplient. En 2015, les répercussions sont allées du simple mauvais coup de pub à des pertes financières lourdes.

En février et mars 2015, les compagnies d'assurance santé Anthem et Premera Blue Cross ont chacune annoncé le vol de dizaines de millions de dossiers de patients : 78,8 millions pour Anthem[1] contre 11 millions pour Premera[2]. Les analystes en sécurité ont alors émis l'hypothèse selon laquelle les attaques provenaient d'un seul et même groupe. Plus tard, en juillet 2015, le collectif de pirates Impact Team a exfiltré 37 millions de dossiers clients du site de rencontres extraconjugales Ashley Madison. Il a ensuite fait chanter les opérateurs du site avant de révéler l'identité de nombreux utilisateurs, y compris quelques gros bonnets.[3]

En clair, les entreprises saisissent le danger d'une mauvaise sécurité car leurs cadres en voient chaque jour les effets dans les médias. Et que font-ils pour se prémunir contre de telles intrusions ? En deux mots, pas assez.

## L'attentisme des entreprises

Les entreprises savent ce qu'elles ont à faire pour protéger leurs données, du moins en théorie et dans les grandes lignes. Pourtant, l'enquête révèle qu'il reste encore des progrès à faire.

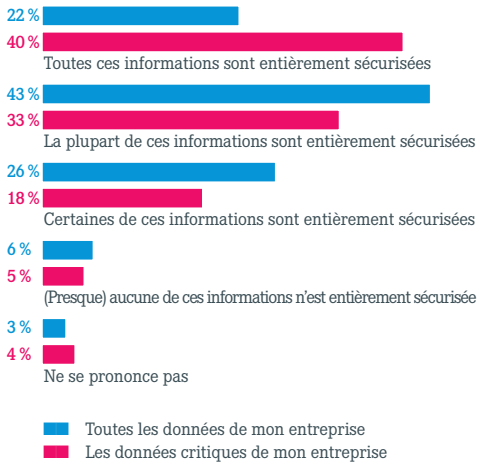
De fait, la majorité des personnes interrogées associent la protection des données à la sécurité de l'information. Beaucoup y voient même une priorité majeure. Ainsi, plus de la moitié (54 %) jugeaient la sécurité de l'information comme « vitale » pour leur entreprise.

Les trois quarts des sondés citaient même cet adjectif parmi les trois mots et expressions qui leur viennent le plus rapidement à l'esprit en matière de sécurité de l'information. Puisque le « respect de la vie privée » – un concept intimement lié à la protection des données personnelles – figurait également dans le top 3, on peut affirmer sans crainte qu'une politique de sécurité informatique axée sur les données devrait désormais constituer l'ossature de tout dispositif de cybersécurité.

La plupart des entreprises savent également quelles sont leurs données les plus sensibles. Ainsi, les cadres interrogés désignent les données clients (B2B et B2C) comme les plus importantes à protéger, suivies de près par les données opérationnelles. Toutefois, et on peut légitimement s'en inquiéter, les données des salariés n'arrivent qu'en cinquième position dans leurs priorités. Or, dans la plupart des pays, les dossiers RH des salariés sont soumis aux mêmes lois de protection de la vie privée que les données clients.

Malgré cela, les trois quarts des participants à l'enquête NTT Com Security admettent que toutes leurs informations ne sont pas complètement sécurisées. Les données critiques se trouvent légèrement en meilleure posture, même si plus de la moitié des entreprises (56 %) sont incapables de garantir la protection de toutes leurs données critiques. Ces résultats révèlent donc une bonne compréhension du problème qui ne se matérialise pourtant que peu dans les faits.

**Figure 2** « Quel est le niveau de sécurité des informations stockées dans votre entreprise ? » – *Question posée à la totalité de l'échantillon (1 000 sondés)*




1. *http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364*
2. *http://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach/#2715e4857a0b3406879b2143*
3. *http://www.techworld.com/news/security/impact-group-leaks-data-on-up-37m-ashley-madison-adulterers-3620132/*

## L'importance des politiques de sécurité

Pour bien identifier les lacunes, cernons d'abord certaines des composantes de base d'une stratégie de sécurité solide. En l'occurrence, des processus bien définis constituent l'un des piliers d'une bonne sécurité. Du transport de données hors des bureaux à la gestion des changements dans le département informatique, des règles et procédures reproductibles et documentées devraient sous-tendre chaque action. À défaut, des failles s'entrouvrent et le dispositif de sécurité se lézarde.

Les processus de sécurité sont habituellement codifiés sous la forme de standards allant de la norme ISO 27001[4] aux bonnes pratiques de l'Information Security Forum (ISF)[5], en passant par la publication 800-12 du NIST[6] et le référentiel COBIT de l'ISACA[7]. De nombreuses entreprises piochent dans ce type de directives les éléments de leur politique, le but étant de se concentrer sur les spécificités propres à leurs métiers.

Les premiers résultats de l'enquête s'avèrent prometteurs, puisqu'ils montrent un réel volontarisme des entreprises pour le resserrement et l'amélioration de leurs pratiques de sécurité. En effet, huit sondés sur dix affirment qu'ils améliorent et mettent à jour en permanence leurs processus et outils de sécurité informatique.

Toutefois, une analyse approfondie des données révèle une toute autre histoire. Seule la moitié des personnes interrogées (52 %) ont mis en place une politique intégrale de sécurité de l'information, tandis que plus d'un quart (27 %) déclarent que son implémentation est en cours. Pour le reste des participants, un tel projet en est soit au stade conceptuel, soit simplement à l'étude.

Ce qui laisse un nombre alarmant d'entreprises sans un ensemble de règles fiables pour guider leurs salariés et dirigeants à travers les méandres du champ des menaces.

Fait révélateur, l'absence de politique semble particulièrement endémique dans les PME. En effet, seules 43 % des entreprises de 1 000 salariés ou moins ont mis en place une politique complète, contre 70 % pour les entreprises de plus de 5 000 salariés.

Le même schéma s'observe pour les plans de reprise d'activité (PRA). Le nombre d'entreprises préparées en cas de perte massive de données est légèrement moindre, puisque seulement 49 % possèdent un plan de restauration complet. Là encore, la taille semble être proportionnelle au niveau de préparation.

*4. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm*
*5. https://www.securityforum.org/tool/the-standard-of-good-practice-for-information-security/*
*6. http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf*
*7. http://www.isaca.org/cobit/pages/default.aspx*

## La communication au cœur des enjeux

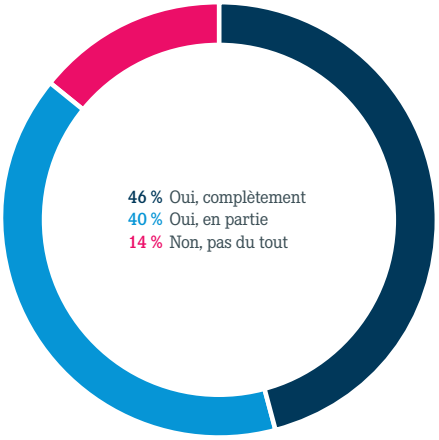
Même lorsque les entreprises disposent d'un plan de reprise en cas de violation de sécurité, elles ne sont pas toujours capables de le mettre en œuvre. Or, tout plan ne vaut que par les gens qui l'appliquent. Le problème ? Dans l'ensemble, plus de la moitié des participants à l'enquête ne connaissent pas complètement le contenu du PRA de leur entreprise. Pire encore, 14 % d'entre eux n'ont aucune idée de la marche à suivre en cas de perte massive de données.

Pour ce qui concerne la communication des politiques, la tendance s'inverse considérablement entre les PME et les grandes entreprises. En effet, bien que les grosses structures possèdent plus souvent un PRA que les PME, il est moins fréquent pour leurs dirigeants d'en connaître la teneur.

Dans les entreprises de plus de 5 000 salariés avec un PRA, seuls 32 % des cadres ont été entièrement briefés sur le contenu du plan. À l'inverse, 47 % des sondés dans les entreprises de 1 000 salariés ou moins connaissent le contenu de leur PRA.

Ces chiffres sont sans doute emblématiques de la difficulté à bien communiquer les politiques dans de grandes entreprises, dotées par essence de structures de management plus complexes. Quoi qu'il en soit, les chiffres globaux n'augurent rien de bon. Les entreprises doivent impérativement communiquer leurs politiques plus efficacement.

**Figure 3** « Connaissez-vous la teneur du plan de reprise d'activité (PRA) de votre entreprise ? » – *Question posée à ceux dont l'entreprise possède ou est en train d'établir un plan de reprise d'activité (772 sondés)*




## La réparation peut coûter cher

Si elles n'intensifient pas leurs efforts dans la création et la diffusion efficace de politiques destinées à combler les lacunes de leur système de sécurité, gare au retour de bâton ! L'enquête NTT Com Security révèle ainsi une variété d'impacts potentiels, allant d'un effet direct sur le bilan de l'entreprise à des problèmes moins tangibles comme la perte de réputation.

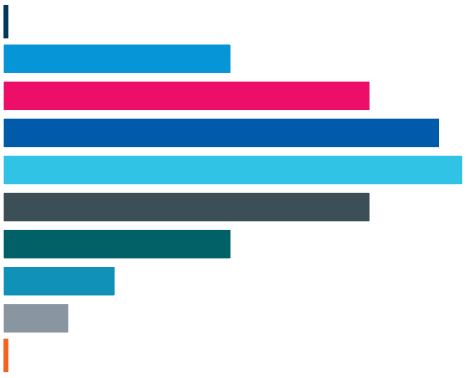
Tout d'abord, examinons l'impact financier. Bien que la majorité des sondés soient capables d'estimer le coût d'une violation de sécurité, 20 % n'en ont aucune idée. En moyenne, une violation de sécurité coûtera un peu moins d'un million de dollars (907 053 dollars, soit presque 832 000 euros) à une entreprise. Bien entendu, le coût varie en fonction de sa taille. Plus elles sont grandes, plus les pertes financières attendues seront importantes. Toutefois, les PME de 1 000 salariés ou moins risquent gros elles aussi : 362 550 dollars en moyenne, soit un peu plus de 332 000 euros. Quant aux entreprises de plus de 5 000 salariés, elles prévoient des pertes à hauteur de 1 465 976 dollars (presque 1 345 000 euros).

Également à noter : la disparité entre les différents secteurs d'activités. Ainsi, les entreprises de la branche technologies et services informatiques anticipent des pertes bien plus importantes en cas d'intrusion, soit 2 708 438 dollars en moyenne (environ 2 485 000 euros). Les acteurs de la grande distribution, de la logistique et des transports occupent la deuxième place du classement, avec 1 037 103 dollars de pertes (plus de 950 000 euros). À elles deux, ces industries élèvent considérablement la moyenne.

Ces chiffres sont par ailleurs révélateurs du rapport entre le coût d'une violation de données et le chiffre d'affaires de l'entreprise touchée. D'autres réponses des participants à l'enquête viennent étayer cette théorie, puisqu'elles associent directement le vol de données à la baisse des ventes.

En moyenne, les sondés pensent que leur chiffre d'affaires chutera de 13 % à la suite d'une compromission de leur sécurité informatique – avec un écart de moins de 2 % entre les PME et grandes entreprises. Ce chiffre est en nette hausse par rapport aux 8 % de 2014, ce qui s'explique probablement par les scandales à répétition qui, entre-temps, ont coûté des dizaines de millions à leurs victimes.

**Figure 4** « Si votre entreprise était victime d'une violation de sécurité entraînant la perte d'informations, à combien estimez-vous le coût moyen de rétablissement de la situation ? » – *Question posée à la totalité de l'échantillon (1 000 sondés)*



**0 %** **Moins de** 10 000 $
**10 %** **Entre** 10 000 $ et 50 000 $
**16 %** **Entre** 50 000 $ et 100 000 $
**19 %** **Entre** 100 000 $ et 250 000 $
**20 %** **Ne se prononce pas**
**16 %** **Entre** 250 000 $ et 500 000 $
**10 %** **Entre** 500 000 $ et 1 million de $
**5 %** **Entre** 1 et 5 millions de $
**3 %** **Entre** 5 et 10 millions de $
**0 %** **Plus de** 10 millions de $

## La confiance n'a pas de prix

Reste à comprendre la raison de ce rapport étroit entre pertes financières et chiffre d'affaires. D'après les réponses des sondés, bien que les pertes financières directes représentent un facteur significatif, la perte de confiance entraîne des conséquences plus graves encore.

Dans les chiffres, 54 % des participants s'attendent à des pertes financières directes en cas d'intrusion, tandis que 48 % citent également les sanctions financières des organes de réglementation (ce qui constitue une perte financière en soi). Ces résultats ne sont pas négligeables, mais les sondés s'inquiètent encore plus des conséquences sur leur image – et par la même occasion sur leurs ventes. Ainsi, six personnes interrogées sur 10 citent la perte de réputation comme l'une des répercussions importantes d'une violation de données, tandis que 69 % craignent une érosion de la confiance des clients (réponse qui revient le plus souvent chez les sondés). Et pour cause, si les clients ne vous font pas confiance, ils sont bien plus susceptibles d'aller voir la concurrence.

## Mieux vaut prévenir que guérir

Après une violation de données, les sondés affirment qu'ils dépenseraient en moyenne 13 % de leur budget de remédiation dans des campagnes de communication et de RP destinées à redorer leur image. Rappelons qu'il s'agit de la part d'un budget consacré au traitement des conséquences d'une attaque, plutôt que de sa cause.

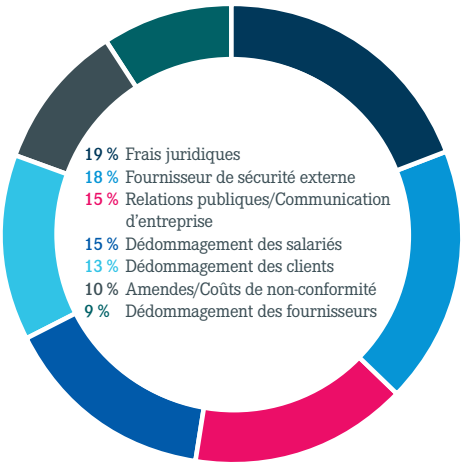
Les deux principaux postes de dépenses attendus par les entreprises après une intrusion : les frais juridiques et les dommages et intérêts versés aux clients pour la perte de leurs données. Ces deux postes représentent respectivement 19 % et 18 % du budget. Les amendes et autres coûts de non-conformité absorbent 15 % des coûts post-intrusion, tandis que le dédommagement des fournisseurs et salariés représente globalement 19 %.

En comparaison de toutes ces dépenses cumulées, le coût d'intervention et de sécurisation des systèmes et données de l'entreprise post-incident s'avère relativement minime. En effet, les services d'un spécialiste externe de la sécurité ne représentent que 15 % des coûts attendus d'une violation de données.

La leçon à en tirer : mieux vaut prévenir une intrusion que la guérir. Concrètement, le coût de la mise en place de politiques et procédures de sécurité en amont sera finalement bien moins élevé que les pertes financières et de réputation durables consécutives à une violation de données.

Il ne faut pas non plus sous-estimer le temps que prendra la réparation des dégâts. En effet, la résolution technique du problème, les démarches juridiques et les processus de dédommagement sont particulièrement chronophages. En moyenne, une entreprise a besoin de neuf semaines, pendant lesquelles elle déploie une énergie considérable qu'elle aurait pu mieux employer à la croissance de son activité. Quant à la confiance des clients, il est difficile de s'avancer sur un délai de retour à la normale, mais cela pourrait prendre bien plus de temps.

**Figure 5** *Répartition moyenne des coûts de remédiation en cas de violation de sécurité. Question posée à la totalité de l'échantillon (1 000 sondés)*

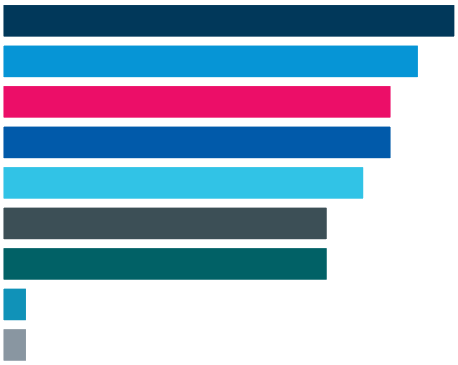


## Une assurance ne suffit pas

Face à un risque, il est tout naturel de vouloir trouver une solution passe-partout. Dans cette quête, l'assurance contre les cyber-risques constitue l'une des pistes évidentes. Cette branche du secteur des assurances est relativement nouvelle puisque ses premières offres remontent seulement au début de notre siècle. À ce titre, elle forme un espace immature, où tant les souscripteurs que les clients se trouvent aux prises avec des concepts qui évoluent rapidement.

Pour preuve : son faible taux d'adoption. La plupart des entreprises ne sont pas assurées en cas de violation de données. Plus précisément, un peu plus du tiers (35 %) disposent déjà d'une police de cyber-assurance dédiée, tandis que 27 % font au moins le nécessaire pour en souscrire une.

**Figure 6** « Quels sont à vos yeux les points susceptibles d'invalider la police d'assurance de votre entreprise ? » *– Question posée à ceux dont l'entreprise a souscrit une assurance contre la perte de données et/ou les violations de sécurité (772 sondés)*



**50 %** Non-respect des obligations de conformité
**46 %** Non-respect des politiques de l'entreprise
**43 %** Absence de plan d'intervention sur incidents
**43 %** Inattention/Négligence des salariés
**40 %** Mauvaise sécurité physique
**36 %** Systèmes informatiques obsolètes
**36 %** Protection des données insuffisante ou inexistante
**3 %** Aucun
3 % Ne se prononce pas

## Difficile de s'assurer contre toutes les pertes

Toutefois, même les entreprises assurées doivent tenir compte d'un certain nombre d'inconnues dans l'équation. À commencer par l'étendue de leur couverture. Les polices ne couvrent souvent que des aspects bien particuliers d'une perte, ou ne vous protègent pas à hauteur des montants colossaux potentiellement en jeu.

C'est du moins ce que révèlent les réponses à notre enquête. Moins de la moitié des sondés dont l'entreprise est assurée contre les cyber-risques (46 %) pensent que les frais juridiques sont pris en charge. Il s'agit là de la plus forte proportion. Un plus petit nombre encore (mais tout de même un quart des sondés) pense que l'assurance couvrira les sanctions financières et la remédiation post-incident. Enfin, 25 % seulement comptent sur l'assurance pour couvrir la perte d'activité et de capital intellectuel.

Autre question : la validité même de la couverture. La moitié des sondés travaillant dans une entreprise assurée pensent que le non-respect de certains critères de sécurité nécessaires pourrait invalider leur police,  notamment l'absence d'un plan d'intervention sur incident (43 %) et une mauvaise protection des données (36 %).

### Conclusion : dotez-vous d'une politique bien ficelée

Tout ceci prouve bien qu'essayer de traiter les symptômes d'un incident n'en éliminera jamais la cause. Les entreprises peuvent souscrire autant d'assurances qu'elles le souhaitent, celles-ci ne leur serviront à rien si elles ne s'inscrivent pas dans une démarche exhaustive et multi-facettes de la cybersécurité. Une telle approche doit s'appuyer sur des mesures fiables de prévention des attaques et d'intervention rapide et efficace en cas d'incident.

Le problème : les entreprises n'en font pas assez pour la protection de leurs données. De fait, un tiers des participants à l'enquête (34 %) dépensent plus en marketing qu'en sécurité informatique. Même constat pour les dépenses opérationnelles et commerciales. Enfin, trois entreprises sur dix investissent plus dans les RH que dans la protection de leurs données, y compris celles des dossiers de leurs salariés.

Tout comme les autres menaces qui peuvent planer sur la croissance d'une entreprise, les risques de cybersécurité peuvent être quantifiés et traités en conséquence. L'évaluation chiffrée du risque et de son impact potentiel permet aux entreprises d'allouer les ressources nécessaires pour prévenir, ou du moins atténuer, les éventuels effets d'une intrusion. Jamais auparavant autant d'entreprises n'avaient saisi les risques de leur inaction.

# Démographie

En octobre/novembre 2015, Vanson Bourne a sondé 1 000 cadres supérieurs à travers sept pays. Le cabinet a interrogé 200 personnes au Royaume-Uni, de même qu'aux États-Unis et en Allemagne. Il a également interrogé 100 personnes dans chacun des pays suivants : France, Norvège, Suède et Suisse. La majorité (32 %) travaille dans le secteur des services financiers, des banques et des assurances. Le deuxième plus grand groupe de sondés (14 %) provient du secteur de la grande distribution, de la logistique et des transports. Le reste travaille dans divers autres secteurs, y compris les services informatiques, le commerce de gros, les services publics et la santé.

Parmi les sondés, 37 % occupent des postes dans des entreprises de 1 000 salariés ou moins, tandis que 42 % travaillent dans des entreprises employant entre 1 000 et 5 000 salariés. Les autres viennent d'entreprises de plus de 5 000 salariés.

Les participants à l'enquête occupaient diverses fonctions, à l'exclusion de la fonction IT, allant de la finance (la plus représentée avec 19 % des sondés) au management et à la stratégie d'entreprise (deuxième groupe avec 14 %). Autres fonctions représentées : RH, ingénierie, communications marketing et service juridique.

** Remarque : les pourcentages étant arrondis, leur total peut ne pas correspondre à 100 %.*

## Vers un monde plus sûr

NTT Com Security est spécialiste de la sécurité de l'information et de la gestion des risques.  En choisissant l'offre WideAngle de consulting, services de sécurité managés, et d'intégration de technologies, nos clients peuvent se focaliser sur leurs opportunités « business », pendant que nous nous focalisons sur le risque.

L'étendue de nos engagements GRC (Gouvernance, Risques et Conformité), l'aspect novateur de nos Services de sécurité managés et le pragmatisme des solutions technologiques que nous déployons prouvent que nous partageons une perspective unique avec nos clients – les aider à hiérarchiser leurs projets et à fixer les standards. Nous nous focalisons sur l'essentiel de chaque client prenant des décisions affectant le risque et la conformité pour son entreprise. Nous entendons donner le conseil juste et objectif en toutes circonstances.

Notre approche globale vise à réduire les coûts et la complexité en prenant en compte la valeur croissante de la sécurité de l'information et de la gestion des risques, comme un facteur de différenciation pour les entreprises hautement performantes. Innovant et indépendant, NTT Com Security possède des bureaux sur le continent Américain, en Europe et en région APAC (Asie-Pacifique) et fait partie du groupe NTT, détenu par NTT (Nippon Telegraph and Telephone Corporation), l'une des plus grandes sociétés de  télécommunications du monde.

Pour de plus amples informations sur NTT Com Security et notre offre de services unique WideAngle en sécurité de l'information et gestion des risques, veuillez contacter votre interlocuteur commercial ou consulter le site **http://www.nttcomsecurity.com/fr/contact/** pour les contacts régionaux.

NTT Communications | NTT Com Security