www.pwc.co.uk

Au-delà de la sensibilisation : L'urgence croissante de la gestion des données sur le marché européen des PME

Une étude sur les attitudes, le comportement et les meilleures pratiques au sein du marché européen, incluant un répertoire mis à jour de l'indice de la maturité des pratiques de gestion des risques.

Un rapport PwC en partenariat avec Iron Mountain
Juin 2013

pwc

Sommaire

Préambule	
i	*Synthèse*
1	*L'état actuel du risque lié aux informations*
5	*Le besoin de gérer un nombre croissant de données*
7	*La nécessité de former vos collaborateurs : pouvez-vous leur faire confiance ?*
9	*La valeur des informations*
11	*Adopter les meilleures pratiques*
14	*Annexe : Méthodologie de recherche*
17	*Auteurs du rapport*

Préambule

Christian Toon Responsable des risques liés aux informations, Iron Mountain Europe

Naviguer dans le domaine de l'information

Le domaine de l'information en Europe a évolué bien plus qu'on ne l'imaginait. Quel que soit le pays, tous les secteurs rencontrent des difficultés à s'adapter à cette transformation. Nombre d'entre eux ont des doutes quant à la manière de s'adapter au volume d'informations de tous formats qui ne cesse d'augmenter et ce, rapidement ; l'explosion des médias sociaux, la prolifération des appareils mobiles, les changements dans la législation et l'augmentation des menaces. Nous observons en parallèle une volonté croissante de maîtriser la valeur pouvant être contenue à la fois dans les informations structurées et celles non structurées. En conséquence, la gestion des informations est plus complexe aujourd'hui qu'elle ne l'a jamais été. Et une complexité croissante va de pair avec une augmentation du risque.

Il est donc opportun que Iron Mountain et PwC aient entrepris des recherches pour examiner l'état des lieux du risque lié aux informations auquel font face les entreprises moyennes en Europe. Ceci est le deuxième indice de maturité face aux risques liés aux informations. Si l'on considère les données, il est encourageant de constater que des progrès ont été faits au cours des 15 derniers mois. La sensibilisation aux risques liés aux informations se développe, les entreprises partout dans le monde augmentant leur score. La moyenne européenne est passée de 40,6 l'an dernier à 56,8, pour un objectif de 100. Notre enquête suggère qu'une meilleure prise de conscience crée de l'incertitude ; les entreprises reconnaissent effectivement la nécessité d'agir mais ne savent pas vers qui se tourner ou quelles nouvelles actions entreprendre.

Cette prise de conscience améliorée doit désormais se transformer en une stratégie et un ensemble de mesures visant à réduire l'exposition aux risques liés aux informations. Cela nécessite l'adhésion et l'implication de la haute direction de l'entreprise. Les responsables de la gestion des informations doivent apprendre à parler le langage du conseil d'administration et à ouvrir un dialogue avec les autres parties prenantes clés. La perte de fidélisation de la clientèle, les atteintes à la réputation de la marque et l'érosion du chiffre d'affaires sont des préoccupations importantes pour les personnes chargées de la gestion des informations. Ces inquiétudes devraient être communiquées sans hésiter au conseil d'administration. Il est clair, cependant, que si de réels progrès doivent être accomplis, les entreprises ne doivent pas seulement se préoccuper des risques encourus par leur réputation et la fidélisation de leur clientèle, mais devraient également s'efforcer de prendre conscience des opportunités et de la valeur qui peuvent être débloquées si les informations sont bien gérées en tant qu'actif de l'entreprise.

En rédigeant ce livre blanc, nous avons cherché à découvrir non seulement le niveau et la complexité du problème, mais également à produire un support utile pour les entreprises européennes. L'indice de risque et l'outil d'évaluation des risques en ligne www.ironmountain.fr/evaluation-risques sont conçus pour fournir un aperçu qui aidera les entreprises à s'investir dans la prochaine étape vers la gestion responsable de leurs informations. Ce livre blanc présente un ensemble d'actions qui peuvent donner les outils aux entreprises pour améliorer leur approche et ainsi réduire leur exposition aux risques liés aux informations et les aider à maîtriser la valeur des informations qu'elles possèdent.

Synthèse

« En résumé, les PME européennes n'accordent pas assez de valeur à leurs données ou ne mesurent pas leur importance en tant qu'actif de l'entreprise. »

Claire Reid, Associée, Sécurité de l'information chez PwC

Les entreprises ont du mal à gérer les informations qu'elles détiennent et par conséquent, elles sont exposées à des niveaux de risque sans précédent. Les fraudes, violations de données et catastrophes liées aux médias sociaux se multiplient tellement vite que les entreprises ne peuvent pas réagir à temps. Les entreprises moyennes en Europe sont particulièrement exposées et demeurent pourtant dans une forme de nonchalance quant à leurs pratiques de gestion de données. Notre étude révèle que la confusion quant aux étapes à suivre empêche ces entreprises d'agir pour se protéger et prendre conscience de la valeur des données dont elles disposent.

Éléments clés de l'étude :

La prise de conscience n'est plus le problème. Notre étude montre que parmi les entreprises de taille moyenne, la prise de conscience de la menace posée par l'exposition aux risques liés aux informations est croissante et que la compréhension de la nécessité de prendre des mesures s'améliore.

- L'indice moyen cette année s'élève à 56,8 sur un score idéal de 100. C'est un peu plus que l'année dernière (où la moyenne était de 40,6) où peu d'entreprises géraient leurs informations à un niveau satisfaisant. Alors même que certaines améliorations ont été constatées, l'indice est toujours bas et il reste un long chemin à parcourir avant que les méthodes de gestion des données atteignent un niveau satisfaisant.

- 68 % des personnes estiment qu'une attitude responsable en matière de gestion des informations est essentielle pour la réussite de l'entreprise. Les informations, à la fois physiques et numériques, client ou internes, sont considérées comme un bien de valeur. Leur bon traitement peut avoir des avantages commerciaux et permettre d'éviter une catastrophe.

- Les résultats de l'étude indiquent que les professionnels sont soit incertains de la marche à suivre ou restent mal équipés pour affronter les menaces. Seuls 45 % des interrogés disposent d'une stratégie de gestion du risque et en mesurent l'efficacité, alors que 44 % s'attendent à une augmentation du risque de violation de leurs données.

Le défi de la gestion des informations :

Notre étude montre que nombreux sont ceux submergés de paperasserie en tout genres et de données numériques dont ils ne savent que faire. En conséquence, les données confidentielles et sensibles ont toutes les chances d'être exposées à un risque accru de violation.

- 36 % conservent toutes leurs informations au cas où elles s'avéreraient utiles.

- 42 % sont inquiets pour la sécurité de leur données conservées.

L'image que l'on peut se faire de la gestion du risque dans le milieu des PME est celle de la confusion, de la contradiction et d'une attitude suffisante. Mais de plus en plus, l'écart se creuse entre l'état d'esprit et les actes réels.

« 93 % des entreprises ayant plus de 250 employés ont été victimes d'une infraction l'année passée. Le coût moyen du cas le plus grave de toutes les infractions est compris entre 450 000 et 850 000 £ »

Source : Étude sur les atteintes à la sécurité des informations 2013 de PwC

- 78 % estiment qu'elles doivent faire tout ce qu'elles peuvent afin d'éviter une violation de leurs données. Cependant, 47 % avouent que leurs conseils d'administration ne considèrent pas la protection des données comme un élément d'importance.
- Les entreprises moyennes attendent de leurs fournisseurs qu'ils suivent les plus hautes normes de sécurité. Seuls 14 % d'entre elles accepteraient de travailler avec un partenaire ayant été victime d'une atteinte à la sécurité de ses données, alors que ces entreprises elles-mêmes échouent à respecter ces normes.
- Dans les cas où aucune politique suivie ou de contrôle permettant de préserver les données n'est en place, un haut niveau de confiance est placé dans les cadres moyens ou subalternes, voire dans le personnel administratif. Par exemple, 58 % ne font aucun suivi de leurs systèmes de contrôle des accès à l'information.

Dans ce livre blanc, nous nous concentrerons sur les attitudes et les comportements révélés par notre étude. Nous mettons en lumière certains facteurs clés qui freinent l'avancée des entreprises moyennes vers leur plein potentiel.

Meilleurs pratiques pour réduire les risques liés aux informations :

Sur la base du livre blanc de l'année dernière, nous avons identifié une série d'étapes et d'actions qui aideront les PME à prendre toute leur dimension et à tirer les bénéfices commerciaux qui vont de pair avec une protection et une pleine compréhension de la valeur de leur bien le plus précieux, les informations aussi bien papier que numériques. Ces actions comprennent :

- **L'implication de la direction**: obtenir le soutien de la direction en adoptant une approche stratégique de la gestion de l'information.
- **La prise de contrôle de votre bien**: identifier les informations que vous possédez, savoir où elles se trouvent et décider si oui ou non elles vous sont toujours utiles.
- **L'implication du personnel** -Mettre en place une politique de confiance contrôlée soutenue par une série d'outils de suivis, de politiques et de procédures.

L'état actuel du risque lié aux informations

Le message est clair : toute entreprise ayant des informations à protéger, quelle que soit sa taille ou son secteur, court un risque. Dans une période où les atteintes à la sécurité, les cyber-attaques et les catastrophes issues des médias sociaux sont plus répandues que jamais, les entreprises sont également exposées à des risques sans précédent. Pourtant, les entreprises moyennes continuent de s'exposer aux dégâts irréparables que peut causer une brèche dans leur sécurité.

Une attitude suffisante, des comportements contradictoires, des méthodes de gestion des données médiocres et un manque de discernement quant à la valeur de leurs données font non seulement courir un risque aux entreprises, mais les empêchent également d'avancer dans leur développement commercial. Les entreprises qui ont subi une violation de leurs données sont clairement victimes d'un manque de confiance et celles qui peuvent démontrer qu'elles les gèrent correctement sont fortes d'un avantage concurrentiel évident.

Notre étude récente, commandée par Iron Mountain, révèle que le marché des entreprises moyennes ne traite toujours pas ses données comme il le faudrait. Même si une certaine amélioration dans ce domaine peut être prouvée, des pratiques médiocres de gestion des données au sein des PME européennes restent répandues. PwC a mené la deuxième enquête de sa série annuelle auprès de 600 entreprises de taille moyenne (celles comprenant entre 250 et 2 500 employés) dans six pays européens : le Royaume-Uni, la France, l'Allemagne, les Pays-Bas, l'Espagne et la Hongrie. Le présent document s'appuie sur les conclusions de notre rapport de 2012 « Au-delà de cyber menaces », qui a introduit pour la première fois l'indice de maturité face aux risques liés aux informations en Europe, et a souligné le besoin pour les moyennes entreprises de beaucoup mieux s'équiper pour gérer les risques de l'information.

L'indice 2013 indique qu'une certaine amélioration dans les pratiques de sécurisation de l'information au sein des PME, mais qu'avec un score de 56,8, il y a encore un long chemin à parcourir.

Indice de maturité face aux risques liés aux informations.

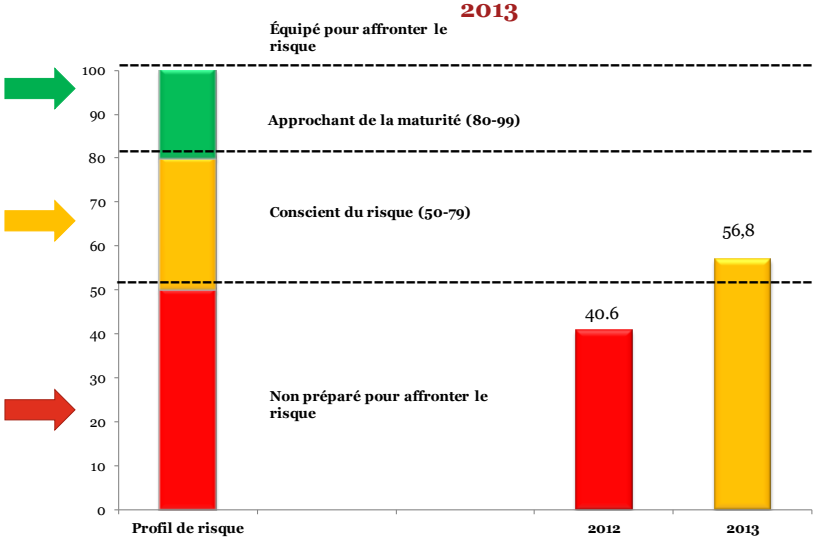
Équipées contre les risques Les entreprises ont mis en œuvre une approche responsable qui englobe une stratégie, le personnel, de la communication et des mesures de sécurité de façon transversale. Elles surveillent, évaluent et améliorent leur approche pour gérer efficacement leur exposition au risque.

S'approchant de la maturité Les entreprises ont mis en place certaines mesures et une meilleure prise de conscience des hauts dirigeants est constatée. Elles ont limité leur exposition, mais n'arrivent pas à mettre en œuvre une stratégie solide.

Conscientes du risque Les entreprises ont découvert la nécessité de se prémunir des risques. Cependant, elles sont incertaines de la marche à suivre ou restent mal équipées pour affronter les menaces.

Non préparées aux risques Les entreprises sont gravement exposées aux risques liés aux informations. Il est peu probable qu'elles aient une stratégie de gestion du risque de l'information en place et la direction n'est pas consciente de l'impact potentiel pour son entreprise

Indice de maturité face aux risques liés aux informations 2012-2013



Base :600

L'attitude suffisante des PME perdure...

Seules 45 % des entreprises ont une stratégie des risques liés aux informations en place et en contrôlent l'efficacité.

Seules 38 % ont un plan officiel de redressement de l'activité.

Seules 32 % surveillent l'efficacité de leur registre des risques d'entreprise.

Seules 28 % possèdent et évaluent des programmes de communication à destination des employés et visant à renforcer les procédures relatives aux risques liés aux informations.

Seules 45 % surveillent l'efficacité de l'équipe responsable des risques de l'information.

Seules 39 % surveillent l'efficacité de leurs classifications de données.

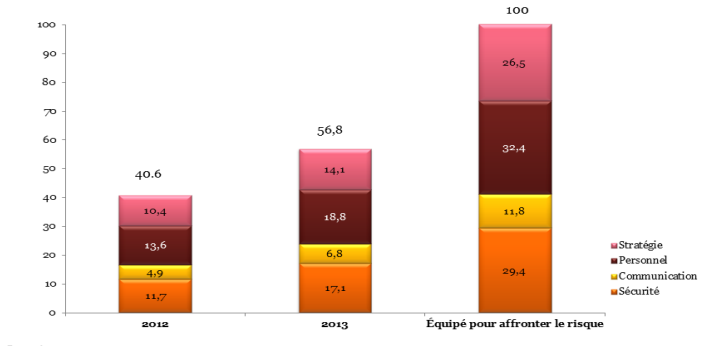
Seules 26 % évaluent le retour sur investissement de leurs dépenses en sécurité de l'information.

Les entreprises doivent adopter une nouvelle façon de penser selon laquelle la sécurité des informations représente à la fois un moyen de protéger les données et la possibilité de créer de la valeur pour l'entreprise.

Enquête mondiale sur la sécurité de l'information 2013 de PwC

Le mid-market est sorti de la zone de danger mais les entreprises doivent rester vigilantes quant au niveau de risque auquel elles sont exposées. Dans un monde où la probabilité quotidienne d'une violation des données augmente de façon exponentielle, les entreprises se doivent de disposer de meilleurs plans pour se protéger. Il n'y a aucune raison pour que les entreprises moyennes ne visent pas le score maximum de 100, un chiffre qui signifie qu'elles sont équipées pour affronter le risque.

Indice de maturité face aux risques liés aux informations 2012-2013 : Analyse par type de risque



Base :600

PwC

Pour atteindre un score de 100, les entreprises doivent mettre en place et surveiller l'efficacité des 34 mesures énoncées dans notre indice (décrites dans l'annexe du présent document). Aucune de ces mesures n'est, selon nous, difficile à mettre en œuvre ou à surveiller, mais notre étude indique que le mid-market a encore un long chemin à parcourir et semble ne pas être certain de la manière dont il doit agir.

Il est positif que les entreprises du mid-market surveillent désormais plus assidûment l'efficacité de leurs pratiques de gestion des informations, en particulier dans le domaine de la sécurité des données. De plus, les intentions des collaborateurs font désormais l'objet d'un intérêt accru. Dans l'ensemble, cependant, environ la moitié des entreprises de notre étude doivent encore améliorer sensiblement leurs pratiques de gestion de l'information.

Éléments clés de l'étude

55 % des entreprises françaises disposent d'une stratégie des risques liés aux informations suivie comparativement à 34 % au Royaume-Uni et 45 % dans l'ensemble de la zone étudiée.

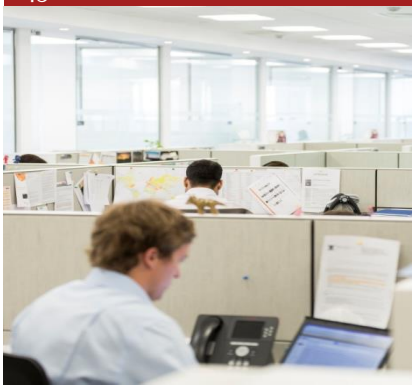
40 % des entreprises néerlandaises et 38 % des hongroises ont un registre des risques d'entreprise suivi contre 21 % en Allemagne et 32 % dans l'ensemble de la zone étudiée.

52 % des entreprises néerlandaises ont une stratégie portant sur l'élimination sécurisée du matériel et des documents confidentiels. Seules 26 % des entreprises en ont une en Espagne, et 41 % dans l'ensemble des pays étudiés.

61 % des entreprises en Hongrie et 59 % aux Pays-Bas offrent des conseils clairs à destination des employés quant à l'élimination sécurisée des documents confidentiels, comparativement à 50 % dans toute la zone et 36 % en Espagne.

35 % des cabinets juridiques ont une stratégie suivie de risques liés aux informations en place, contre 55 % dans le secteur de l'assurance et 45 % dans l'ensemble des secteurs.

54 % des entreprises de fabrication et d'ingénierie disposent d'une équipe dédiée à la gestion des risques de l'information. 34 % des cabinets juridiques en ont une et 45 % dans l'ensemble des secteurs.



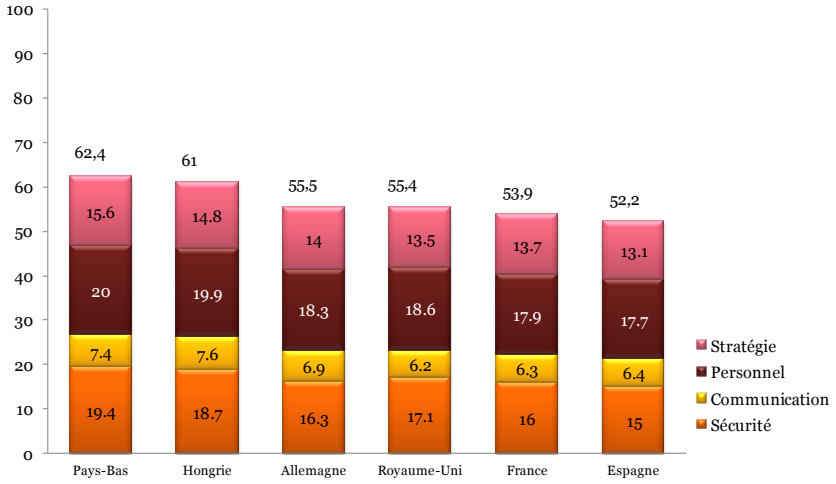
La zone clé d'amélioration concerne le manque d'orientation stratégique quant à la gestion de l'information. Plus de la moitié des entreprises ne contrôlent pas l'efficacité de leur stratégie des risques liés aux informations, si toutefois elles en ont une.

Le mid-market doit accepter le fait que la détention d'informations est un atout stratégique essentiel pour les entreprises et doit être traitée et considérée en conséquence. Dans une période de récession, c'est encore plus important. Faire plus avec moins de moyens nécessite de travailler certes plus dur mais surtout plus intelligemment et les entreprises les plus prospères sont celles qui relèvent le défi non seulement en considérant et en exploitant leurs données comme un atout, mais aussi en leur attribuant une certaine valeur. Elles ont compris que l'on ne prend vraiment soin que des choses dont on connaît la valeur.

Variations par pays

Les Pays-Bas et la Hongrie ont atteint les scores les plus élevés, avec 62,4 et 61,0 respectivement. Les Pays-Bas ont notamment fait preuve d'une amélioration significative lors de la dernière année.

Indice de maturité face aux risques liés aux informations 2012-2013 : Analyse par pays



Parmi les six pays concernés par notre étude, les Pays-Bas se distinguent comme étant le pays le plus stratégique dans son approche des risques de l'information. Par exemple, les entreprises néerlandaises ont plus tendance que celles des autres pays à avoir un plan d'urgence en place pour répondre aux problèmes de petite envergure liés aux données, un registre des risques d'entreprise, une stratégie de sécurité couvrant les téléphones mobiles, les appareils personnels et les ordinateurs portables ainsi qu'une stratégie pour une élimination sécurisée du matériel et des documents confidentiels. En outre, les Pays-Bas, avec la France, étaient les plus susceptibles d'aborder le sujet des risques liés aux informations dans le cadre du conseil d'administration.

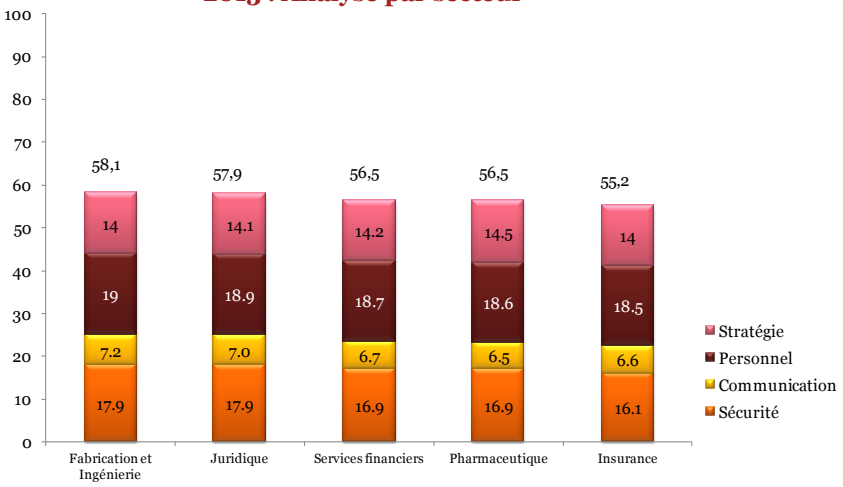
En Hongrie, les principales améliorations ont porté sur les mesures de formation des employés et la communication, avec un accent particulier porté à l'orientation des employés quant à l'archivage et à l'élimination des documents électroniques et physiques.

En revanche, l'Espagne détient le score le plus bas avec 52,2. Fait intéressant, les entreprises espagnoles sont celles qui estiment le moins que leurs employés peuvent être une menace à la sécurité de l'information. Dans le même temps, elles se placent derrière leurs homologues européens en ce qui concerne la transmission de conseils aux employés quant aux politiques et procédures internes. Elles sont moins susceptibles de disposer de certaines des mesures clés de sécurité, tels que les programmes de diligence raisonnable pour la gestion des informations liées au personnel ou aux clients, ou des systèmes de détection d'intrusion et des systèmes de classification des données reconnues.

Variations par secteur

D'un point de vue sectoriel, les cinq secteurs de notre étude ont tous fait preuve d'amélioration et ont atteint un niveau similaire de maturité, même s'ils se situent encore au niveau le plus bas de la zone dite « jaune » à savoir à un niveau de risque élevé.

Indice de maturité face aux risques liés aux informations 2012-2013 : Analyse par secteur



Base :600

Les secteurs du juridique, de la fabrication et de l'ingénierie ont connu les plus fortes hausses depuis 2012. Des preuves soulignent que les entreprises œuvrant dans la fabrication et l'ingénierie adoptent de plus en plus une approche plus stratégique. Elles sont plus nombreuses à avoir une stratégie des risques liés aux informations en place et un plan officiel de redressement de l'activité. Ce secteur a également beaucoup plus tendance que les autres à considérer les employés comme une menace à la sécurité des informations et par rapport à l'année dernière, il s'est davantage concentré sur le personnel et les mesures de communication.

Le secteur juridique s'est amélioré dans la plupart des 34 mesures, mais il reste le moins susceptible de disposer d'une stratégie des risques liés aux informations ou d'une équipe ou d'une personne responsable de ce point.

Indice de maturité face aux risques liés aux informations
Classement par pays 2012-2013

Pays	2012	2013
Pays-Bas	**5e**	**1er**
Hongrie	**1er**	**2e**
Allemagne	**4e**	**3e**
Royaume-Uni	**6e**	**4e**
France	**3e**	**5e**
Espagne	**2e**	**6e**

La nécessité de gérer un nombre croissant de données

Dans le monde hybride actuel où les données sont tout à la fois papier et numériques, les entreprises risquent de se noyer dans un océan de complexité et de confusion à moins qu'elles ne prennent en charge leurs données.*Une approche responsable des informations est essentielle si les entreprises veulent profiter des avantages de cet atout commercial important.Une telle approche est primordiale si les entreprises souhaitent mériter et conserver la réputation de leur marque et la fidélité de leur clientèle durement gagnées ».*

Christian Toon
Responsable des risques liés aux informations
Iron Mountain

« Chaque heure, les informations constituant le trafic Internet pourraient remplir 7 millions de DVD. Mis bout à bout, ils mesureraient 95 fois le Mont Everest.

Enquête IMS pour IBM, 2013

Beaucoup d'entreprises du mid-market sont lentement submergées de données non structurées dont elles ne savent que faire. Cette inondation de données est le résultat direct de l'absence de politiques, de processus ou de technologies au sein des entreprises pour les aider à classer l'information et à identifier ce qui doit être conservé, comment cela doit être conservé et ce qui peut être détruit. En conséquence, de nombreuses entreprises conservent toutes leurs informations numériques et papier, ce qui signifie souvent que de grandes quantités de données confidentielles et sensibles peuvent être consultées par les employés ou des prestataires, ce qui augmente les risques d'une violation de données.

Plus d'un tiers des entreprises de notre étude conservent toutes leurs informations au cas où elles s'avéreraient utiles. Un autre tiers sont tributaires d'un accord juridique avant de décider du sort des données qu'elles détiennent. Il est bien connu que la quantité de données, papier et numériques, générée sur une année croît de manière exponentielle. Aussi, si les entreprises continuent de tout conserver, alimentant ainsi le flot incessant de données, cela leur sera de plus en plus coûteux et pourrait les exposer à des risques. Par exemple, certains types de documents doivent être détruits de façon sécurisée suivant des périodes de conservation prévues par la loi et le défaut d'élimination peut entraîner des amendes et des dommages à la réputation de l'entreprise. En outre, de nombreuses entreprises sont préoccupées par la sécurité de leurs données archivées. De toute évidence, l'accès aux données archivées doit être géré et des contrôles appropriés mis en place pour empêcher qu'une quelconque violation des données ne se produise.

L'essor des données numériques, en de multiples formats distants et notamment la prolifération des canaux d'informations partagées, crée également un environnement dans lequel le mid-market a du mal à contrôler sa « chaîne de traçabilité ». Les informations critiques de l'entreprise sont désormais disponibles en plusieurs formats, en versions papier et numérique, diffusées à de plus grands groupes de personnes, augmentant encore le risque d'une violation des données.

Plus une entreprise conserve d'informations, plus grandes sont les probabilités qu'elles soient à la portée d'un personnel peu scrupuleux, curieux, non averti, mécontent ou malveillant. Comme nous l'avons souligné dans *Au-delà des cyber-menaces*, l'une des plus importantes menaces à l'intégrité des informations sur le lieu travail est le comportement et les attitudes des employés. Les entreprises qui se débattent au milieu d'un nombre croissant de données non classées exacerbent infiniment cette menace.

90 % des données dans le monde d'aujourd'hui ont été créées au cours des deux dernières années

IBM - Comprendre le Big Data - Plateforme Big Data d'IBM

« Les trois quarts des employeurs britanniques ont révélé qu'ils n'avaient aucun système exécutoire pour empêcher les employés d'accéder de façon non autorisée aux données de l'entreprise ».

Enquête sur les menaces internes au Royaume-Uni, LogRythm. Avril 2013

Même le peloton de tête - les entreprises qui mènent la marche dans le domaine de la sécurité des informations - sont aux prises avec la conservation des données. Notre étude montre qu'elles sont tout aussi susceptibles de tout conserver juste au cas où.

Si on la compare aux autres pays, la France présente le plus grand océan de données, en effet, la moitié des entreprises de notre étude conservent toutes leurs données. Les entreprises espagnoles ont les plus bas niveaux de données conservées et sont les plus susceptibles de recourir à un tiers pour gérer la conservation de leurs données en leur nom.

Nous avons plutôt là une situation où les entreprises ne savent pas quoi faire, plutôt que celle d'une ignorance insouciante. Lorsqu'il leur a été demandé ce qu'elles considéraient comme étant leur principal défi pour l'avenir, 41 % ont mentionné qu'elles étaient inquiètes quant à la gestion de leur patrimoine papier. Cela était particulièrement vrai en Allemagne et en Hongrie, et dans le secteur juridique en Europe, où presque la moitié des entreprises à qui nous avons parlé considéraient la gestion de leurs documents papier comme un défi. Une autre préoccupation des PME est la sécurité des données archivées. Globalement, 42 % expriment cette préoccupation, ce chiffre augmentant jusqu'à 48 % en France et 52 % dans le secteur de l'assurance.

Tout en se concentrant sur le développement des bons comportements du personnel, les entreprises du mid-market doivent s'attaquer aux océans de données avant qu'il ne soit trop tard. Agir pour accélérer la législation et les directives sur la conservation des données est essentiel. Classer et archiver en toute sécurité les données qui doivent être conservées et procéder à la destruction sécurisée de données inutiles est primordial. Les entreprises doivent agir maintenant avant que l'océan de données ne devienne incontrôlable et qu'il ne commence à fuir.

Éléments clés de l'étude

36 % conservent toutes leurs informations au cas où elles s'avéreraient utiles

31 % demandent un avis juridique concernant la conservation des données avant d'agir

41 % considèrent la « gestion de leur patrimoine papier » comme un défi majeur pour l'avenir

42 % sont préoccupées par la sécurité de leurs données archivées

61 % ne contrôlent pas l'efficacité de leurs systèmes de classification des données, si toutefois elles en ont un

Éléments clés de l'étude

Seuls 14 % des répondants accepteraient de traiter avec une entreprise ayant été victime d'une atteinte à la sécurité de ses données.

Seuls 25 % croient que les employés constituent une menace sérieuse pour la sécurité des informations.

82 % font confiance à leurs employés pour suivre leur politique relative au risque de l'information

45 % ne surveillent pas l'utilisation des médias sociaux de leurs employés

Étude de cas

Une démarche innovante de la police du Kent ayant consisté à nommer une « jeune » commissaire de police s'est retournée contre elle de façon spectaculaire du fait des comptes personnels de l'adolescent sur les médias sociaux. Paris Brown, 17 ans, a été choisie parmi plus de 160 candidats pour être « la voix de la jeunesse » pour la police du Kent. Cependant, il est apparu plus tard que son compte Twitter personnel comportait des tweets racistes, homophobes et crus remontant à plusieurs mois. Le commissaire de police du Kent a admis que les comptes des médias sociaux de l'adolescente n'avaient pas été vérifiés avant sa nomination.

L'obligation de former vos collaborateurs : pouvez-vous leur faire confiance ?

Le marché des moyennes entreprises montre des signes de confusion et d'incohérence dans ses attitudes face aux risques liés aux informations. Notre étude révèle que la plupart d'entre elles (58 %) n'envisageraient pas de traiter avec une entreprise ayant été victime d'une violation de ses données, mais beaucoup continuent à mettre leurs propres données en péril. Avec seulement 45 % d'entre elles disposant d'une stratégie suivie de risques liés aux informations, cela témoigne d'une vision à deux vitesses où la vigilance externe est tempérée par une complaisance interne.

Les entreprises du mid-market doivent commencer à appliquer elles-mêmes les normes qu'elles définissent lorsqu'elles sélectionnent leurs fournisseurs et prestataires. Elles n'ont pas conscience du fait qu'il y ait de grandes chances que leurs propres clients partagent le même point de vue et qu'ils pourraient leur retirer le marché en cas de violation de données.

L'an dernier, *Au-delà des cyber-menaces* a souligné qu'un changement radical dans la culture d'entreprise et le comportement des employés était essentiel pour préserver les actifs informationnels du mid-market européen. L'étude de cette année montre que les entreprises sont tout à fait conscientes de l'impact d'une violation de données sur leurs activités, mais restent impassibles face aux menaces pouvant exister en interne. 25 % des entreprises que nous avons consultées estiment que les employés constituent une menace sérieuse pour la sécurité des informations, mais 82 % font confiance à leurs employés pour suivre leur politique de risques liés aux informations (si toutefois elles en ont une).

Les entreprises du mid-market nous informent que le responsable de la sécurité informatique reste le gardien principal de leurs données, et, en fin de compte, la personne responsable des risques liés aux informations au sein de l'entreprise. Ironie du sort, quand on leur demande qui ils considèrent comme la plus grande menace de violation des données, plus de la moitié a cité l'équipe informatique. Il est compréhensible que les personnes ayant la plus grande responsabilité et l'accès le plus important aux données les plus sensibles et confidentielles soient considérées comme les plus à risque.

Qui vous inquiète le plus quand il en vient aux questions de violation des données ?

Base : 600
Réponses multiples

« 80 % des employeurs britanniques affirment qu'ils ne croient pas que l'un de leurs employés puisse dérober des informations confidentielles, mais un sondage auprès d'employés a montré que 23 % avaient accédé ou pris des données confidentielles sur leur lieu de travail ».

Enquête sur les menaces internes au Royaume-Uni, LogRythm, Avril 2013

Selon notre étude, les cadres intermédiaires, le personnel subalterne, les assistants personnels et le personnel de nettoyage sont considérés comme posant un faible risque en matière de violation de données, probablement en raison de leur accès relativement limité. Cependant, alors même que le salarié le plus digne de confiance peut potentiellement faire une erreur, de nombreuses entreprises ne disposent pas des contrôles nécessaires pour se protéger contre une simple erreur humaine. Par exemple, 61 % des entreprises à qui nous avons parlé ne surveillent pas l'efficacité de leurs systèmes de classification des données et 58 % ne disposent pas de systèmes de contrôle d'accès aux archives d'entreprise et aux autres informations sensibles ou ne les évaluent pas.

Il a également été constaté que les procédures de sélection du personnel font défaut dans de nombreuses entreprises du mid-market, avec moins de la moitié vérifiant les références employeurs, et seulement 40 % effectuant des vérifications d'antécédents criminels ou de casier judiciaire. En outre, peu d'entre elles vérifient les informations facilement accessibles, publiquement disponibles sur les sites de médias sociaux tels que Twitter. Il semble que de nombreuses entreprises du mid-market accordent une grande confiance à des personnes qu'elles ne connaissent que très peu. De nombreuses entreprises s'impliquent également assez peu dans la communication et la formation de leur personnel quant à leurs politiques et procédures d'information (quand elles existent). À la place, elles se reposent grandement sur la confiance qu'elles accordent à leurs employés.

Avoir confiance en ses employés peut être une bonne chose, mais le problème est que la plupart des infractions qui ont eu lieu à ce jour sont le résultat d'erreurs humaines. Il est donc important de disposer d'une politique de confiance et de la contrôler ainsi que d'avoir des politiques adéquates, des formations, une bonne communication et des contrôles de sécurité pour protéger les informations à la fois de toute intention malveillante et des maladresses fortuites.

Dans un monde où les médias sociaux sont omniprésents et avec 88 % des consommateurs utilisant un même appareil mobile à des fins personnelles et professionnelles (données PwC), le risque de dommage est énorme et de nombreux exemples très médiatisés le prouvent.

Le voleur de données moyen est :

- *Un employé actuel*
- *Un homme*
- *Âgé de 37 ans*

Dans environ la moitié des cas étudiés, l'employé a dérobé des secrets commerciaux, puis des informations sur l'entreprise (informations de facturation ou listes de prix) et dans 75 % des cas, il disposait d'un accès autorisé aux données volées.

Voleur interne de données : quand de bons employés tournent mal
Symantec, Décembre 2011

La valeur des informations

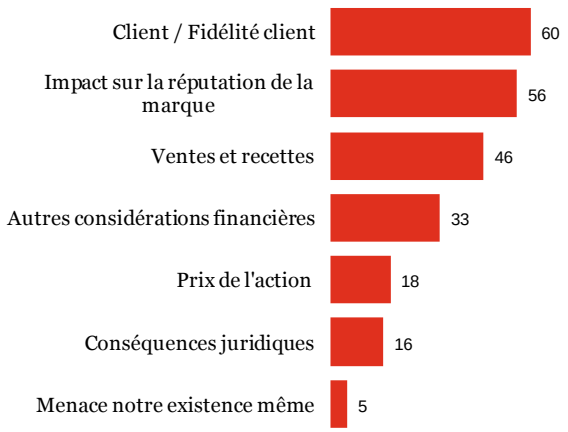
Le monde des affaires a changé et les entreprises de tous les pays et de tous les secteurs partagent désormais régulièrement des informations au delà les frontières commerciales, que ce soit avec des partenaires commerciaux ou par le biais des appareils personnels de leurs employés.Cela ne se limite plus seulement à un défi informatique, les chefs d'entreprise doivent s'assurer qu'ils protègent ce qui est le plus essentiel à la croissance et à la réputation de leur entreprise.

Andrew Miller, PwC directeur de la sécurité de l'information

L'information est un bien stratégique pour une entreprise, et la traiter en tant que telle peut offrir l'opportunité de nombreux avantages commerciaux, tout du moins un fort avantage concurrentiel. Malheureusement, malgré le fait que la plupart des entreprises de taille moyenne estiment que considérer leurs données en tant que véritable actif de l'entreprise est « le prochain grand enjeu », très peu agissent véritablement en ce sens.

Le mid-market est également bien conscient de l'impact d'une violation de données. Deux tiers pensent qu'une violation de données aura un impact négatif sur la confiance et la fidélité d'un client. En effet, le fait que la plupart des entreprises de notre étude ne feraient pas confiance à une autre entreprise ayant connu une violation de données démontre également ce point. Près de la moitié considèrent que la violation de données serait préjudiciable à la réputation de leur marque et pensent qu'un préjudice serait subi au niveau des ventes.

À votre avis, quel serait l'impact d'une violation de données sur votre entreprise ?



De toute évidence, c'est le souci de fidélisation de la clientèle et non pas le désir de conformité qui est la principale motivation pour les entreprises de mieux gérer leurs informations.

« Nous avons passé plus de quinze ans et dépensé 100 millions de livres pour le développement de moteurs sans balais à grande vitesse, pour alimenter nos aspirateurs et sèche-mains Airblade.Nous exigeons la rétrocession immédiate de notre propriété intellectuelle ».Documents judiciaires de Dyson étayant une plainte pour espionnage industriel.Octobre 2012

.

Éléments clés de l'étude

59 % estiment que les coûts engendrés par une protection adéquate de leurs données l'emportent sur les risques encourus.

54 % estiment qu'elles n'arriveront jamais à suivre le rythme ahurissant auquel se font les changements.

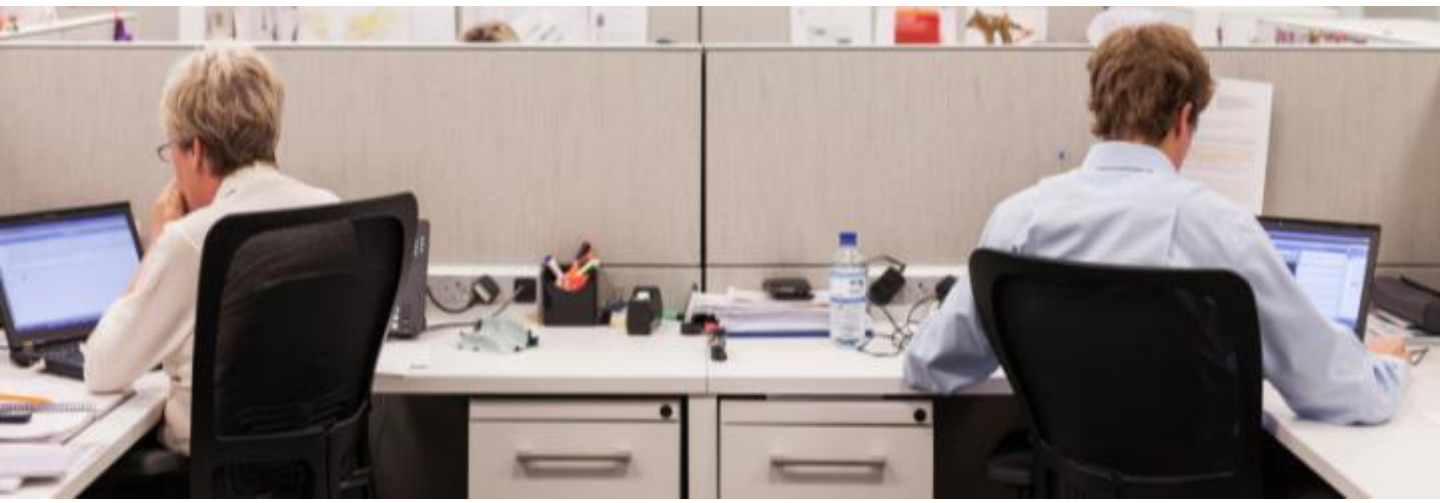
Les membres du UK Civil Service Sports Club, au nombre de 130 000 dans le pays, ont été informés que leurs noms, adresses, dates de naissance et numéros de sécurité sociale avaient été volés dans la base de données de l'ordinateur central.Les données ont été ensuite utilisées dans le cadre de fraudes.

Daily Telegraph 27.11.2012

Nous savons que l'attitude suffisante est un gros problème, mais quels autres éléments freinent les entreprises ? Notre recherche suggère que c'est avec les aspects stratégiques de la gestion de l'information que le mid-market européen éprouve le plus de difficultés. Les entreprises sont également préoccupées par les coûts et se sentent dépassées par le rythme du changement.

Seule une minorité d'entreprises arrivent plus ou moins à gérer leurs données comme un actif et moins encore y attachent de l'importance. La plupart (74 %) ne mesure pas, ou ne sait pas comment mesurer le retour sur investissement de leurs dépenses dans le domaine de la sécurité des informations. Beaucoup n'ont pas la capacité ni les compétences au sein de leur entreprise leur permettant de gérer de façon adéquate leur actif informationnel et 35 % considèrent cela comme un défi. Quand on ne sait pas ce qu'il faut faire, il est rare que l'on fasse bien les choses.

Les recherches académiques montrant que les entreprises sous-estiment systématiquement la valeur à la fois absolue et relative des informations par rapport aux biens matériels soutiennent nos conclusions. Par conséquent, les entreprises doivent (a) investir, à la fois en argent et en temps, pour développer des programmes de gestion des informations efficacement intégrés et contrôlés et (b) rééquilibrer les priorités en considérant la valeur des informations plutôt que leur coût et et les risques qui y sont liés.



Adopter les meilleurs pratiques

« La seule façon de sécuriser les données en mouvement et des données en sommeil est de concevoir une stratégie globale de sécurité de l'information basée sur une bonne compréhension des menaces qui pèsent sur l'entreprise et sur la mise en œuvre d'une approche de surveillance de la sécurité en couches qui traite les données tout au long de leur cycle de vie. »

Claire Reid
Associée, Sécurité des informations chez PwC

Les résultats présentés dans ce rapport sont des défis qui sont constatés dans tous les secteurs. Fort heureusement, les experts en sécurité trouvent des solutions et des actions qui peuvent réduire le risque de perte d'information. A notre avis, les éléments suivants sont quelques-unes des actions les plus efficaces qui peuvent donner de bons résultats.

Étape 1 :L'implication de la direction

Obtenez le soutien du conseil d'administration en adoptant une approche stratégique de la gestion de l'information

- Développez une stratégie efficace des risques liés aux informations et surveillez son efficacité. Adoptez une approche structurée pour l'élaboration d'une stratégie, comme suit :
    - Déterminez comment les données sont archivées, transférées et éliminées sur les réseaux à la fois internes et externes ;
    - Déterminez les contrôles des technologies, les processus et les personnes nécessaires à la gestion des informations à différents stades de leur cycle de vie ;
    - Concevez et mettez en œuvre des contrôles en utilisant les principes fondamentaux de la sécurité, la résilience et la fiabilité des informations ;
    - Favorisez une culture d'entreprise autour de la responsabilité de l'information. Travaillez avec l'équipe des ressources humaines qui a un rôle prépondérant à jouer dans l'atténuation des risques de l'information.
    - N'oubliez pas les données papier : des mesures simples telles que la classification des documents, le stockage sécurisé et l'accès à une broyeuse peut contribuer à éveiller la culture d'entreprise nécessaire pour atteindre ce changement.
- Placez la sécurité des informations à l'ordre du jour du conseil d'administration. Influencez les priorités du conseil d'administration en parlant leur langage et en découvrant ce qui est important pour eux. Le lien entre la fidélité client et l'image d'une entreprise concernant la gestion et la protection de ses données client est évident. Les comportements et actions de la direction générale peuvent générer un avantage commercial s'ils sont appliqués et surveillés efficacement.
- Considérez vos données comme un actif et montrez aux employés que vous y croyez vraiment - inscrivez-les au bilan, ou demandez des conseils afin de mesurer le retour sur investissement des dépenses de sécurité des informations. Identifiez ce qu'il en coûterait pour remplacer vos données.
- Favorisez une culture de la responsabilité partagée de la gestion des informations entre les employés. Assurez vous que les employés se rendent compte qu'il en va de leur responsabilité personnelle également.

Étape 2 : Prenez le contrôle de ce qui vous appartient

Connaissez les informations que vous possédez, sachez où elles se trouvent, et décidez si vous en avez encore besoin

- Il est facile de penser que vos données archivées ne sont que des données électroniques, mais n'oubliez pas vos dossiers sur papier, la façon dont ils sont gérés ainsi que tous les autres formats que vous pouvez utiliser.
- Identifiez des parrains expérimentés pour défendre et promouvoir la responsabilité des informations pour chacun de ces formats au sein de l'entreprise.
- Identifiez ce que vous possédez, le volume de stockage électronique par types de fichiers ou par bases de données, les volumes de documents physiques et / ou multimédia. Idéalement, triez-les en fonction de leur fonction ou de leur type.
- Localisez ces données. Sont-elles stockées en interne, auprès d'un tiers, dans votre pays d'origine, en dehors de l'UE ?
- Vous devez identifier et localiser ce que vous possédez. Cela facilite la définition des priorités dans la gestion du risque et des coûts.
- Développez et communiquez un processus de gouvernance des informations qui doit comprendre la classification des données, le protocole d'archivage, les conditions de traitement des données, la conservation des données ou les règles d'évaluation et de sauvegarde.
- Les périodes de rétention de l'information sont essentielles pour gérer les coûts et rester en conformité. Ne les gardez pas plus longtemps que vous en avez besoin.
- Une fois que vous avez décidé d'une politique de classification, assurez-vous de définir un processus de contrôle d'accès à certaines informations sensibles et à des restrictions de transferts sur de grandes quantités de données.
- Définissez une période d'« amnistie » pour les employés en interne pour qu'ils agissent de façon juste et conforme au modèle de gouvernance de l'information. Cela signifie que les employés soit archivent des données sur les serveurs d'archive désignés ou se débarrassent de toutes les données locales qui ne sont plus nécessaires.
- Récompensez les comportements positifs et remédiez à une mauvaise performance quand il est question de gestion de l'information.
- Demandez à vos parrains de surveiller et de vérifier le modèle de gouvernance de l'information.

Étape 3 : L'implication du personnel

Mettez en place une politique de confiance contrôlée

- Il est important et profitable que les chefs d'entreprises fassent confiance à leurs employés. Cependant, avec des menaces toujours croissantes (à la fois malveillantes ou involontaires), cette confiance doit se maintenir dans un contexte contrôlé.
- Elle est définie par un ensemble d'outils de suivi déterminé, des politiques et des procédures qui sous-tendent et complètent la confiance globale.
- Développez une politique d'utilisation des médias sociaux claire pour le personnel et mettez en place un programme de formation pour les sensibiliser.
- Promouvez l'utilisation des médias sociaux par les voies appropriées, notamment par des directives claires en termes de ce qui peut et ne peut pas être dit.
- Soyez précis sur ce que vos employés peuvent ou ne peuvent pas publier en terme de contenu. Par exemple interdire les « commentaires inappropriés » est une notion trop vague. Demandez-leur de ne pas mentionner les noms de société, les projets spécifiques et les personnes.
- Encouragez et responsabilisez les employés « champions » en tant qu'ambassadeurs de la marque pour qu'ils parlent positivement de votre entreprise en tant que lieu de travail sur leurs comptes personnels des médias sociaux.
- Effectuez des exercices de contrôle interne pour donner un aperçu de la façon dont les employés se comportent lorsqu'ils sont confrontés à une menace potentielle pour la sécurité.
- Communiquez l'objet et la nature des exercices de surveillance et utilisez les comme une occasion de sensibiliser les employés à la façon de réagir en cas de violation de données.
- Gagnez en discipline dans la façon dont les données confidentielles sont rédigées, fabriquées et stockées. Par exemple, identifiez les documents confidentiels et concevez une méthode pour les documents originaux permettant de savoir s'ils sont sortis de l'entreprise (par le biais d'outils de prévention des pertes de données).
- Contrôlez les mouvements de messagerie vers des adresses de messagerie personnelles en plaçant des contrôles sur la passerelle de messagerie.

Annexe : Méthodologie de recherche

Présentation

Afin d'appuyer ce livre blanc, PwC et Iron Mountain ont développé une méthodologie de recherche solide pour étayer les conclusions présentées. Cette méthodologie s'est appuyée sur les enseignements et les leçons appris dans le cadre de l'étude de 2012. Dans un premier temps, nous avons travaillé en étroite collaboration avec Iron Mountain pour évaluer les thèmes qui ont émergé de l'étude 2012. Nous avons par ces enseignements élaboré un questionnaire exhaustif qui a été en grande partie basé sur les thèmes clés du document, en termes de portée et d'efficacité des approches de la gestion des risques liés aux informations de l'entreprise d'un point de vue des employés, de la communication et de la sécurité.

Cela a été complété par une série de « déclarations attitudinales » pour former une meilleure compréhension des raisons pour lesquelles ces pratiques se rapportaient à la fois à un niveau global et au niveau sectoriel et national. Par souci de comparabilité, les déclarations générales qui sous-tendent l'indice de maturité face aux risques ont été conservées dans le même format qu'en 2012. Le questionnaire a été conçu par l'équipe de spécialistes en recherche interne de PwC avec une perspective d'expert et des contributions de l'équipe d'assurance risque de PwC, dirigée par Claire Reid.

Nous avons travaillé en étroite collaboration avec notre partenaire de recherche sur le terrain, Coleman Parkes, pour assurer que le questionnaire soit conçu dans un format compatible au téléchargement sur leur solution d'entretiens assistés par ordinateur (CATI) et qu'il serait disponible dans les langues maternelles des répondants de notre échantillon.

À qui nous sommes-nous adressés ?

Les répondants au sondage téléphonique étaient généralement PDG, directeurs financiers, DSI ou directeurs de manière à ce que nous obtenions une perspective expérimentée et comprenions la nature et l'ampleur des risques informatiques les plus urgents et la manière dont ils sont gérés. Les entretiens téléphoniques ont été réalisés proportionnellement auprès de répondants des marchés et des secteurs clés afin de permettre un niveau d'analyse comparative détaillé.

Pour comprendre le mieux possible les résultats de cette étude, nous avons entrepris une « analyse » complète des données en complétant les résultats les plus marquants avec des coupes spécifiques, notamment en termes de marché et de tendances sectorielles. Cette analyse a également inclus une évaluation des principales modifications entre les résultats 2012 et 2013 soutenus et informés par les déclarations attitudinales. Nous avons également cherché la participation particulière de nos experts en la matière dans le réseau PwC de chacun des pays européens représentés dans l'enquête.

De la même manière qu'en 2012, nous avons élaboré un indice de maturité face aux risques liés aux informations. Cet indice a été élaboré par l'application d'une moyenne pondérée de toutes les réponses de chaque entreprise aux 34 déclarations présentes dans notre étude. Les 34 déclarations ont été regroupées en 4 rubriques d'activités : Stratégie, Employés, Communication et Sécurité et ont été catégorisées comme telles.

Parmi les propositions suivantes, laquelle a été mise en place pour votre entreprise ?

Stratégie

1. Stratégie ou approche du risque liés aux informations.
2. Plan ou stratégie officiels de redressement d'activité.
3. Plan d'urgence pour répondre aux problèmes de petite envergure liés aux informations ou à la perte de données.
4. Révisions régulières de la politique de confidentialité.
5. Registre des risques de l'entreprise.
6. Stratégie de sécurité de l'information couvrant les appareils mobiles personnels et les ordinateurs portables.
7. Stratégie de gestion des informations structurées et non structurées sous forme numérique et physique dans divers emplacements.
8. Stratégie pour l'élimination sécurisée du matériel informatique et des documents confidentiels.
9. Stratégie hiérarchisant l'accès aux documents critiques de l'entreprise et à ceux présentant un risque plus élevé qui sont utilisés le plus souvent dans les demandes de mise en conformité.

Employés

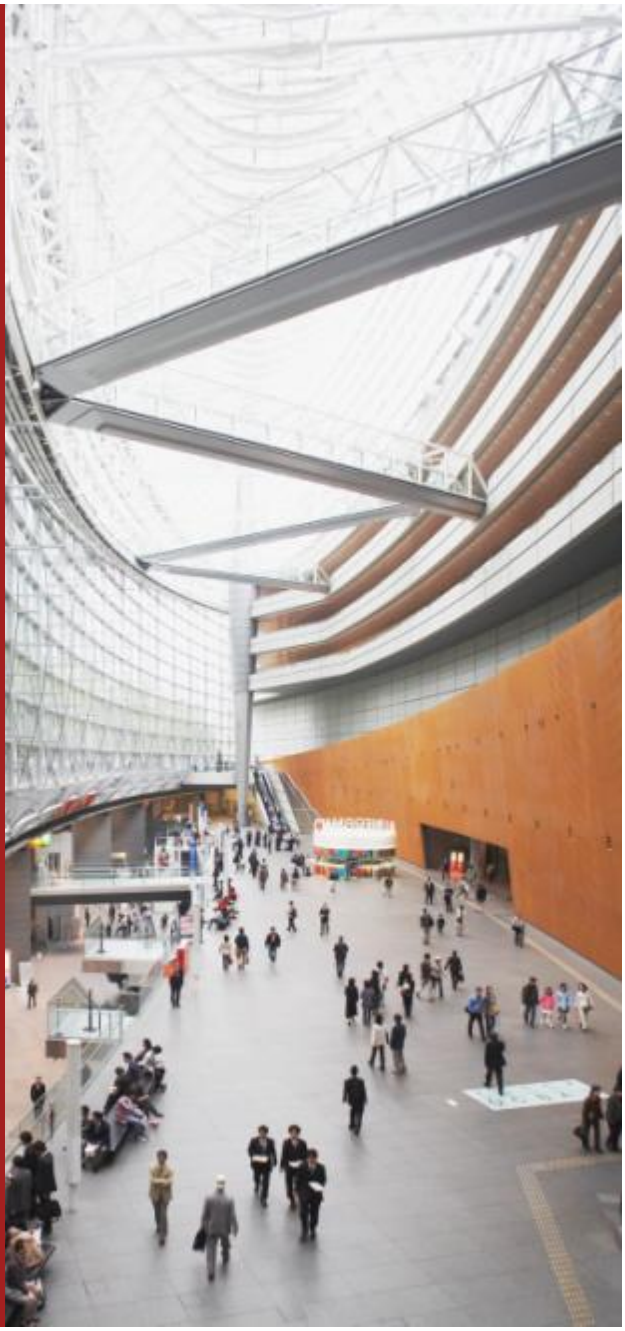
10. Personne ou équipe spécifique responsable des risques liés aux informations au sein de votre entreprise.
11. Processus de sortie pour les employés qui quittent votre entreprise afin de prévenir le vol ou la copie d'informations.
12. Programmes de formation pour sensibiliser les employés aux questions de risques liés aux informations.
13. Sensibilisation aux risques liés aux informations comprise dans le cadre de la formation initiale.
14. Programmes de formation « de rappel » de manière continue.
15. Programmes efficaces de formation en ligne sur les risques liés aux informations.
16. Vérification du passé des employés.
17. Code de bonne conduite sur les comportements adéquats pour tous les employés.
18. Outil pour mesurer la confiance des employés dans l'efficacité des activités liées aux risques liés aux informations.
19. Politique d'utilisation d'Internet pour l'ensemble du personnel.
20. Politique d'utilisation des médias sociaux pour l'ensemble du personnel (par exemple, Facebook, Twitter et LinkedIn).

Communications

21. Informations au sujet des risques facilement accessibles par tous les employés.
22. Programmes de communication auprès des employés afin de renforcer les procédures du risque liés aux informations.
23. Orientation claire des employés quant aux procédures internes concernant l'élimination et l'archivage des documents physiques.
24. Orientation claire des employés quant aux procédures internes concernant l'élimination et l'archivage des documents électroniques.

Sécurité

25. Politiques de l'entreprise en matière de sécurité, d'archivage et d'élimination des informations confidentielles.
26. Programmes de diligence raisonnable concernant le traitement des renseignements personnels, des clients ou des employés.
27. Inventaire des lieux où vos informations sont archivées.
28. Base de données sécurisée et centralisée de gestion des informations.
29. Technologie contrôlant les systèmes de détection d'intrusion et les systèmes de prévention des intrusions.
30. Validation par une tierce partie, par exemple avec des tests d'intrusion.
31. Classification claire, actualisée et reconnue des données.
32. Procédures de contrôle en matière d'accès aux bâtiments, aux zones réglementées, aux archives de la société et à d'autres informations sensibles.
33. Utilisation de règles et de procédures différentes pour archiver des données en tenant compte des différentes périodes de conservation des documents et des exigences en matière de protection des données.
34. Processus de signalement d'incident, par exemple, comment repérer une information qui ne devrait pas se trouver à tel endroit.



Auteurs du rapport

Claire Reid

Associée, Assurance risque chez PwC

T: +44 (0)207 212 5513

M:+44 (0)7734 607594

claire.reid@uk.pwc.com

David Armstrong

Associé, Service Études Internationales chez PwC

T: +44 (0)28 90 245454

M: +44 (0)7713 680266

david.m.armstrong@uk.pwc.com

Julie McClean

Responsable Senior, Service Études Internationales chez PwC

T: +44 (0)28 90 245454

M: +44 (0)7738 313241

julie.mcclean@uk.pwc.com

Biju Mukund

Responsable Senior, Assurance Risque chez PwC

T: +44 (0)207 213 1701

M: +44 (0)7850 907913

biju.mukund@uk.pwc.com

Kieran Jones

Associé Senior, Service Études Internationales chez PwC

T: +44 (0)28 90 245454

M: +44 (0)7845 635383

kieran.p.jones@uk.pwc.com

www.pwc.com

Cette publication a été préparée pour prodiguer des conseils d'ordre général sur les questions d'intérêt uniquement et ne constitue pas un avis professionnel. N'agissez pas sur la base des informations contenues dans cette publication sans obtenir un avis professionnel spécifique. Aucune représentation ou garantie (expresse ou implicite) n'est donnée quant à l'exactitude ou l'exhaustivité des informations contenues dans cette publication, et, dans la mesure permise par la loi, PricewaterhouseCoopers LLP, ses membres, ses employés et ses agents n'acceptent pas et n'assument aucune responsabilité ou obligation de diligence des conséquences dans le cas où vous-même ou quiconque agissait ou s'abstenait d'agir, en se fondant sur les informations contenues dans cette publication ou de toute décision prise en s'y rapportant.

© 2013 PricewaterhouseCoopers LLP. Tous droits réservés. Dans le présent document, « PwC » désigne PricewaterhouseCoopers LLP (une société à responsabilité limitée au Royaume-Uni), société membre de PricewaterhouseCoopers International Limited, chaque société membre étant une entité juridique distincte.