Avant-propos

Sue Trombley

Directeur général du leadership intellectuel

Iron Mountain - Amérique du Nord

Christian Toon

Responsable des risques liés à la gestion des informations

Iron Mountain - Europe

Dans un monde dont le moteur est le savoir, les informations sont devenues un actif commercial de plus en plus précieux, et cette valeur croissante des informations entraîne un risque plus important.

Il s'agit de la troisième étude annuelle réalisée par PwC et Iron Mountain afin d'apprendre comment les entreprises européennes de taille moyenne (celles dont les effectifs vont de 250 à 2 500 employés) perçoivent et gèrent le risque lié à la gestion des informations. L'étude 2012 a révélé une large insouciance vis-à-vis des menaces et des vulnérabilités potentielles. L'étude 2013 indiquait que les entreprises de taille moyenne avaient réagi, mais que leurs initiatives préliminaires pour s'attaquer à la gestion des risques liés aux informations étaient noyées dans un océan de données massives.

Cette année, nous avons décidé de regarder si les tendances en matière de risques liés à la gestion des informations sont confinées aux entreprises européennes de taille moyenne ou s'il s'agit d'un phénomène plus général. Dans l'étude 2014, qui s'appuie elle aussi sur les moyens de recherche et d'analyse puissants de PwC combinés à la profondeur de l'expertise de Iron Mountain, porte sur les organisations de taille moyenne aux États-Unis et au Canada, ainsi que sur les grandes entreprises (celles de plus de 2 500 employés) sur les deux continents.

Où que nous regardions, nous avons observé un écart entre la situation actuelle des entreprises en termes de capacité de gestion des risques liés aux informations et l'objectif qu'elles se sont fixé ou qu'elles ont besoin d'atteindre.

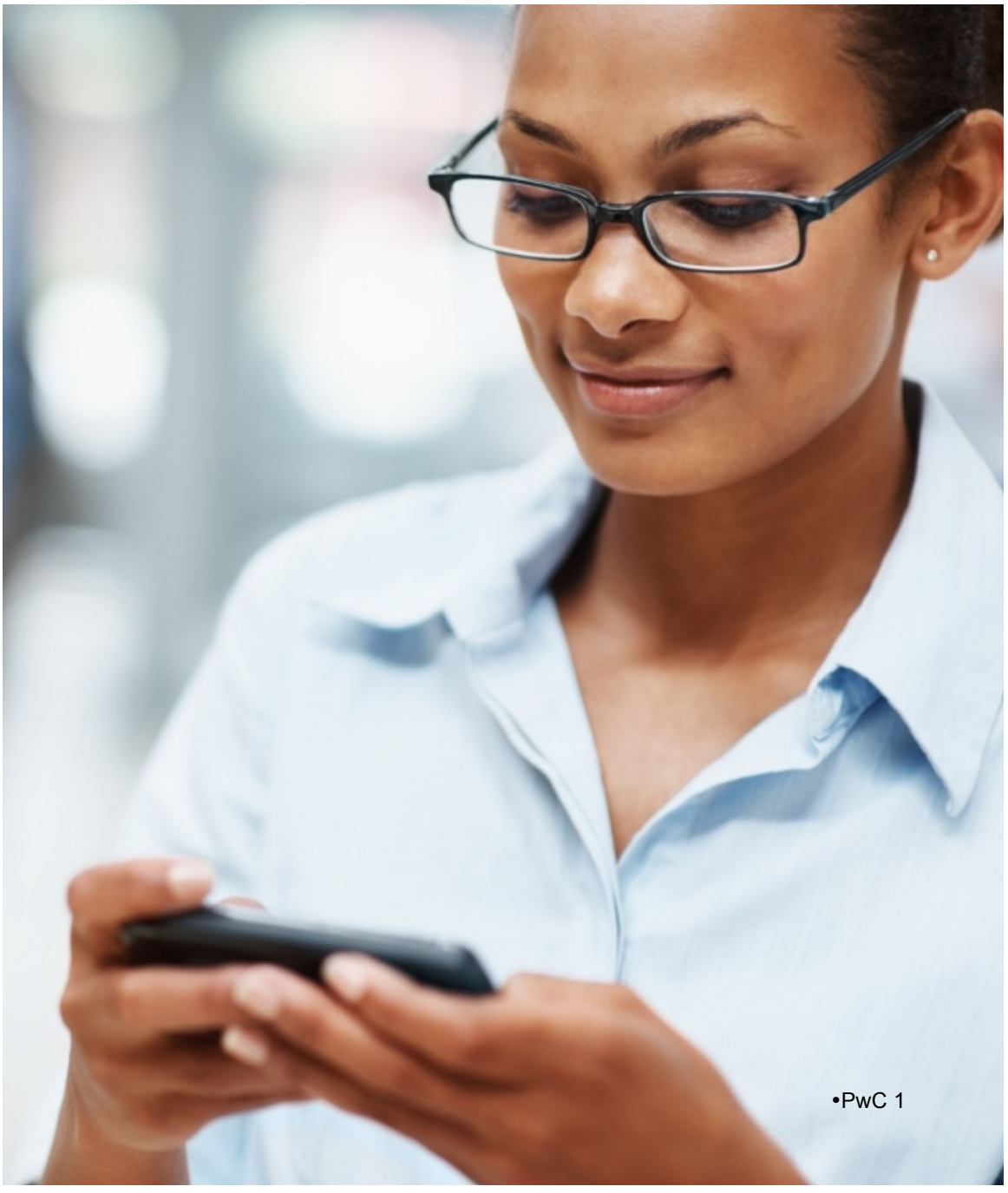
Les tendances majeures sont mondiales.

- Qu'il s'agissait des entreprises les plus grandes et les plus établies ou des entreprises de taille moyenne les plus jeunes, elles se révèlent toutes incapables de combler l'écart entre le fait d'avoir mis en place un plan ou règlement bien intentionné et le stade auquel elles pourraient affirmer qu'un tel plan ou règlement fonctionne effectivement.
- La responsabilité en matière de risques liés à la gestion des informations est invariablement et presque exclusivement confiée au service des technologies de l'information, ce à un moment où des informations sont pourtant générées et utilisées par l'ensemble des fonctions des entreprises, et où l'impact potentiel d'une violation des données – impact sur la notoriété et/ou impact juridique, financier ou commercial – exige des dirigeants d'entreprise qu'ils prêtent attention aux problème et requiert que les autres services d'une entreprise s'impliquent davantage à cet égard.

- En dépit du fait qu'il existe partout des organisations comprenant parfaitement que les informations ont de la valeur, la majorité de ces organisations préfèrent les sécuriser en les verrouillant afin d'éviter toute violation de données ou toute action en justice, plutôt que de les utiliser à des fins d'avantages concurrentiels, d'innovation et de croissance.
- Enfin et surtout, alors que les entreprises se concentrent sur des initiatives numériques, elles découvrent qu'il est difficile de gérer les risques associés à leurs documents papier. Environ deux tiers des participants à l'étude ont déclaré que ce risque est le plus important de tous, soit deux fois plus que concernant le risque de menaces externes, qui arrive au deuxième rang.

Tout ceci entraîne que ces organisations sont exposées à un risque de perte de données ou de dommages causés à leurs données. Et pourtant, ceci peut parfaitement être évité. Nous avons découvert des entreprises ayant adopté un concept général clair et effectif en matière de gouvernance d'informations et de gestion des risques liés aux informations - des organisations qui comprennent les menaces pesant sur leurs informations et la façon d'en tirer parti. Plus loin dans ce livre blanc, nous présentons les caractéristiques clés de ces précurseurs et proposons des conseils pratiques pour aider les autres à suivre sur cette voie.

Énoncer de bonnes intentions constitue le point de départ, et non la ligne d'arrivée, du chemin à parcourir pour gérer vos risques liés aux informations.



Synthèse

Les informations constituent l'oxygène d'une entreprise. Elles lui sont essentielles et sont omniprésentes. Elles comprennent les savoirs et l'acquisition de savoirs, les données générées par des systèmes, les informations sur les produits et les clients, les communications au quotidien et les documents archivés sur papier, ainsi que les propriétés intellectuelles de l'entreprise.

Cependant, la croissance de leur volume, leur plus grande diversité et les différents types d'informations professionnelles utilisés aujourd'hui entraînent des risques, lesquels sont extrêmement variés. S'ils ne sont pas correctement gérés et/ou atténués, ils peuvent avoir un impact critique et préjudiciable sur une entreprise.

Ces risques, menaces et impacts potentiels sont maintenant mieux identifiés et compris, par rapport à ces dernières années. Le monde des entreprises de taille moyenne, à la fois en Europe et en Amérique du Nord, a réagi aux violations de données, fuites et incidents d'espionnage divers hautement médiatisés en adoptant davantage de stratégies organisationnelles et en mettant en oeuvre des plans et procédures d'actions internes, mais également en investissant dans des technologies de sécurité et des programmes de communication internes.

Néanmoins, notre recherche montre que, bien que ceci constitue une évolution positive et très bienvenue, l'écart se creuse entre eux les « bonnes intentions », énoncées dans des déclarations d'engagement incluses aux règlements organisationnels et aux programmes internes des entreprises, d'une part, et la mise en oeuvre de mesures concrètes sous forme d'application effective de tels règlements et programmes, d'autre part.

Cet écart représente un problème essentiel, car il contribue à exposer les entreprises de taille moyenne à un très large éventail de risques d'informations susceptibles d'avoir des répercussions durables et potentiellement irréparables sur leur viabilité générale et leurs avantages concurrentiels.

En outre, bien que cet écart entre les engagements déclarés et les mesures concrètes contribue à une plus grande exposition aux risques d'informations, il limite également la capacité des entreprises de taille moyenne à utiliser efficacement leurs informations en tant qu'actif précieux susceptible de leur permettre de se démarquer sur leur marché.

De nombreuses entreprises de taille moyenne en Amérique du Nord et en Europe reconnaissent que leurs informations ont de la valeur, mais elles ne s'en servent pas pour en tirer un avantage concurrentiel. Notre étude montre que le secteur des entreprises de taille moyenne reste indûment passif et protectionniste, plutôt que proactif et innovant, en ce qui concerne la façon d'utiliser ses portefeuilles d'informations croissants.

Il est intéressant de noter que ce phénomène est général, quel que soit le pays, le secteur d'activité, le continent ou la forme ou taille des entreprises, et qu'il est sans rapport avec leurs effectifs ou leurs ressources. Par conséquent, il s'agit d'un défi absolument général.

Selon nous, les entreprises de taille moyenne ont significativement besoin de traduire leurs politiques et objectifs organisationnels en mesures concrètes et applicables, et la majorité de ces entreprises ne sont ni suffisamment protégées ni en mesure de pleinement optimiser les données/informations qu'elles détiennent.

Principales conclusions de l'étude :

- Le score sur l'indice de maturité en matière de risques, qui couvre un échantillon d'entreprises de taille moyenne européennes et nord-américaines, atteint 55,3 par rapport à un idéal de 100,0.
- Un tel score de 55,3 correspond, selon notre définition, au segment « Conscientes du risque » de cet indice. Ceci est symptomatique des entreprises ayant graduellement pris conscience du besoin de gérer ce risque, mais qui ne savent toujours pas comment réagir et qui restent mal équipées pour confronter cette menace.
- L'absence de mesures, de politiques et de procédures proprement mises en œuvre et contrôlées contribue partiellement à empêcher les entreprises de taille moyenne à parvenir à un niveau de « maturité » plus élevé.
- Seules 37 % de ces entreprises en Europe et 47 % en Amérique du Nord ont mis en place une stratégie en matière de risques liés à la gestion des informations pleinement contrôlée. Ceci devrait constituer le socle sur lequel des

mesures de protection appropriées sont élaborées, et pourtant plus de la moitié des entreprises de taille moyenne ne le font pas.

- Seules 26 % des entreprises européennes et 20 % des entreprises nord-américaines prennent les mesures nécessaires pour déterminer dans quelle mesure leurs programmes de formation en matière de gestion des risques liés aux informations sont efficaces.
- En termes de responsabilité et d'affectation appropriée des compétences, 46 % des entreprises européennes et 32 % des entreprises nord-américaines déclarent que leur directeur de la sécurité des technologies de l'information est le plus haut responsable en charge des risques liés à la gestion des informations. Lorsque nous leur avons demandé à qui cette responsabilité globale devrait incomber, ces pourcentages atteignent respectivement 73 % et 74 %. Selon nous, ceci limite la capacité d'une organisation à anticiper et à réagir à l'ampleur des risques vue sous un angle plus large, à savoir sous un angle dépassant la simple responsabilité du service des technologies de l'information de l'entreprise.
- Plus de la moitié des entreprises estiment qu'il n'existe aucun écart de compétences en matière de gestion des informations au sein de leur personnel. Ceci semble indûment optimiste, mais reflète également l'absence de compréhension des compétences qui sont requises pour à la fois protéger et optimiser les informations des entreprises de manière appropriée.
- 87 % des entreprises européennes et 80 % des entreprises nord-américaines pensent qu'aucun ancien employé n'a emporté avec lui et fourni à son nouvel employeur des informations détenues par leur organisation. Dans le meilleur des cas, il s'agit d'une vision optimiste, et dans le pire des cas, ceci démontre plus amplement leur naïveté, selon laquelle les informations de tous types et de tous degrés de confidentialité ne sont pas rendues vulnérables par des employés existants ou futurs d'une manière susceptible de procurer un avantage à des concurrents et/ou de constituer une menace.

Afin d'atteindre adéquatement et de surpasser le double objectif fondamental de la protection adéquate et de l'optimisation de la valeur de leurs informations, les entreprises de taille moyenne doivent s'atteler à un certain nombre d'enjeux.

Combler l'écart entre les déclarations d'intention et les mesures concrètes

(1) Afin d'avoir un impact, les stratégies organisationnelles, les initiatives du personnel, les programmes de communication et les procédures de sécurité doivent être examinés, testés, évalués, affinés et pleinement compris.

Les hauts dirigeants d'entreprises de taille moyenne doivent coordonner et affecter adéquatement la responsabilité en matière de risques liés à la gestion des informations.

(2) Les informations sont visibles ou invisibles, physiques ou électroniques, en ligne ou sur papier, et, par conséquent, la haute direction de chaque entreprise doit coordonner la façon dont ceci est à la fois géré et/ou optimisé, de façon à ce que ***chacun*** connaisse à la fois son rôle et les conséquences potentielles de toute absence de conformité.

Les informations peuvent uniquement avoir de la valeur pour une entreprise si elles sont proprement gérées et efficacement utilisées. Ceci nécessite de réaliser un audit en bonne et due forme des écarts de compétences, afin de réduire de tels écarts et de répartir les compétences de manière appropriée.

(3) La gestion et l'optimisation des informations ne devraient pas être principalement du ressort des professionnels du service des technologies de l'information. Les données doivent être plus largement partagées avec les analystes et les innovateurs à travers l'ensemble de l'organisation.

La confiance accordée aux employés doit être protégée et sous-tendue par des procédures évaluées et contrôlées.

(4) Il est important d'investir dans du matériel de sécurité et des technologies de protection adaptés. Cependant, ceci doit être appuyé par des procédures du personnel à la fois surveillées et contrôlées, de façon à conjurer toutes menaces susceptibles d'émerger au sein même de l'organisation et qui sont souvent les sources exposition les plus courantes et les plus dommageables.