

Gouvernance documentaire sécurisée

Sécurisez vos informations confidentielles

Troisième partie de la série de livres blancs sur l'Indice de Gouvernance Documentaire Ricoh
Février 2010

Ce livre blanc est basé sur l'enquête réalisée par Coleman Parkes Research pour Ricoh en Belgique, France, Allemagne, Italie, Espagne, Irlande, aux Pays-Bas et au Royaume-Uni



Sommaire

1.0	Introduction – Gouvernance documentaire et sécurité	3
2.0	Résumé de l'enquête	5
3.0	Résultats principaux	
	Véritable conscience de l'importance de la sécurité documentaire	6
4.0	Les entreprises s'exposent à un risque important	8
5.0	Une approche de la sécurité documentaire différente selon les secteurs d'activité	10
6.0	Conclusion	12
7.0	L'approche Sécurité Ricoh	13





1.0 Introduction – Gouvernance documentaire et sécurité

La sécurité de l'information et des documents occupe un rôle primordial au sein de l'entreprise, notamment en matière de confidentialité, d'intégrité et de disponibilité des données. Le recours croissant aux technologies augmentant les risques de fuite de l'information, les entreprises sont en droit de se demander si les périphériques d'impression multifonctions n'occasionnent aucune faille dans la sécurité de leur système d'information. Ricoh a ainsi saisi l'enjeu que représente la Sécurité pour ses clients et y consacre un livre blanc. Celui-ci correspond au troisième opus de la série de livres blancs Ricoh à paraître au sujet de la gouvernance documentaire.

L'étude réalisée par le bureau d'étude indépendant Coleman Parkes nous démontre que plus de la moitié des entreprises européennes (57 %) disposent d'un système de gouvernance documentaire décentralisé. Résultat : perte d'efficacité, de sécurité et de productivité entre autres désagréments affectant à terme la pérennité des organisations.

Pour rappel, le terme « gouvernance documentaire » décrit les méthodes employées par les entreprises pour contrôler et gérer leurs processus documentaires, à savoir : coûts, technologie, impact environnemental et sécurité du document tout au long de son cycle de vie.

Ce livre blanc étudie la façon dont les grandes entreprises européennes intègrent la sécurité dans leur gouvernance documentaire. L'enquête a plus particulièrement porté sur la confidentialité des documents et l'exposition des entreprises aux risques inutiles causés par l'absence d'une politique d'impression sécurisée.

La divulgation d'informations peut en effet occasionner plusieurs types de conséquences néfastes sur l'entreprise :

Droits de propriété intellectuelle :	perte de l'investissement en Recherche et Développement
Informations personnelles :	les informations personnelles sont protégées par la loi. En cas de transgression, votre entreprise est passible d'amendes.
Informations commerciales :	la divulgation d'informations confidentielles ou stratégiques peut affaiblir la compétitivité de votre entité.
Information clients :	il s'agit de l'information traitée au cours des actions de sous-traitance. La divulgation de ces données peut entraîner la perte de confiance de clients et l'obligation de verser une compensation financière.

En Europe, les exemples de documents sensibles perdus ou oubliés dans un espace public et sans aucun dispositif de sécurité pour protéger les données sont fréquents. En effet, c'est le cas pour les données médicales personnelles, les informations bancaires ou même certains documents politiques stratégiques classés confidentiels. En plus de l'impact négatif sur la réputation de l'entreprise, les failles de sécurité peuvent coûter cher. Prenons l'exemple de l'industrie de la Formule 1¹ : un designer McLaren a été retrouvé en possession d'un document de 780 pages contenant des informations confidentielles sur la F1 Ferrari. Le préjudice causé à Ferrari a été jugé si important par le comité d'organisation que McLaren fut lourdement pénalisé pour la suite de la saison.

¹ <http://edition.cnn.com/2007/SPORT/09/11/f1.spygate/>



Cependant, une faille dans la confidentialité des informations n'est pas toujours manifeste. Il existe au quotidien des risques invisibles au sein de l'entreprise. Citons comme exemple les informations commerciales sensibles (les business plans, les informations stratégiques et financières), qui peuvent parfois arriver aux mains de la concurrence sans que l'entreprise en soit avisée.

Afin d'assurer la mise en œuvre de dispositifs de sécurité au sein l'entreprise, des exigences réglementaires et légales ont été créées : nous pouvons citer le PCI-DSS Payment Card Industry Data Security Standard, les lois sur la protection de données (CNIL) ou la loi Sarbanes-Oxley pour la protection des informations sensibles. Cependant, l'étude démontre que dans certaines organisations, l'information reste parfois mal protégée et vulnérable. En effet, seuls 47%² des dirigeants interrogés affirment avoir instauré une politique de contrôle de l'impression d'informations relatives aux clients.

Méthodologie de l'étude sur la Gouvernance Documentaire

Sur la période juillet-août 2009, 311 interviews ont été réalisées au total auprès de cadres supérieurs (DG et équivalent). Ces entretiens ont ciblé de grandes et moyennes entreprises européennes issues de différents secteurs (finance, services aux entreprises, services publics, télécommunications et médias) dans plusieurs pays (Belgique, France, Allemagne, Italie, Espagne, Irlande, Pays-Bas et Royaume-Uni). Toutes les personnes interviewées sont responsables de toute ou partie de la gestion documentaire au sein de leur entreprise. L'étude a été réalisée de façon à garantir une information représentative à travers l'Europe et au sein de chaque secteur d'activité analysé.

² Moyenne dans les secteurs des finances, des services professionnels et publics, des télécommunications et des média



2.0 Résumé de l'enquête

Les résultats de l'étude Ricoh sur la Gouvernance Documentaire démontrent qu'en dépit de la connaissance des risques liés à la mise en œuvre d'une politique documentaire sécurisée, seule une minorité de dirigeants d'entreprise opte pour une démarche de gestion sécurisée des impressions et des flux de documents.

Une réelle prise de conscience de l'importance de la sécurité documentaire

A l'évidence, les dirigeants d'entreprises européennes font preuve de lucidité et ont conscience de la nécessité de garantir la sécurité des documents circulant au sein de leur organisation. La majorité d'entre eux (76%) s'accordent sur l'idée que les failles de sécurité augmentent en raison de l'évolution technologique. En matière de sécurité documentaire, 91% adhèrent au proverbe "Mieux vaut prévenir que guérir", et 68% des interviewés pensent qu'un environnement d'impression contrôlé permettrait d'améliorer la sécurité. En ce qui concerne les documents professionnels, près de la moitié des dirigeants (49%) attache autant d'importance à la sécurité de l'information numérique qu'à celle de l'information imprimée.

Les entreprises s'exposent à un risque important

Malgré cette clairvoyance, seule une minorité de dirigeants a concrètement instauré une politique de protection des informations confidentielles. Moins de la moitié des entreprises (47%) dispose en effet d'une politique rigoureuse de contrôle en matière d'impression des informations clients et 41% concernant les autres types de documents confidentiels.

Plus grave : seules 44% des personnes interviewées affirment avoir instauré une politique destinée à éviter la conservation d'informations confidentielles par des collaborateurs quittant l'entreprise.

Cette absence de politique peut être directement mise en relation avec une approche décentralisée de la gouvernance documentaire, qui prive souvent les entreprises d'une vision globale des domaines dans lesquels la sécurité doit être améliorée. Résultat : les entreprises sont vulnérables aux failles de sécurité accidentelles ou intentionnelles.

Une approche de la sécurité documentaire différente selon les secteurs d'activité

Les résultats obtenus selon les différents secteurs d'activité ciblés mettent en évidence des résultats surprenants : le secteur financier est le moins concerné avec seulement 46% d'entreprises concernées par la mise en place d'une politique de réduction de l'impression des informations clients. Seules 33% des entreprises du secteur public disposent d'une stratégie de sécurité documentaire. On atteint 43% dans le secteur des services professionnels et 48% dans celui des télécommunications et des médias. Par ailleurs, les résultats démontrent que même les secteurs les plus réglementés et conscients de l'importance de la sécurité sont en mesure d'optimiser davantage et de manière significative la protection de leurs informations confidentielles ainsi que la gestion de leurs documents.



Résultats principaux

3.0 Véritable conscience de l'importance de la sécurité documentaire

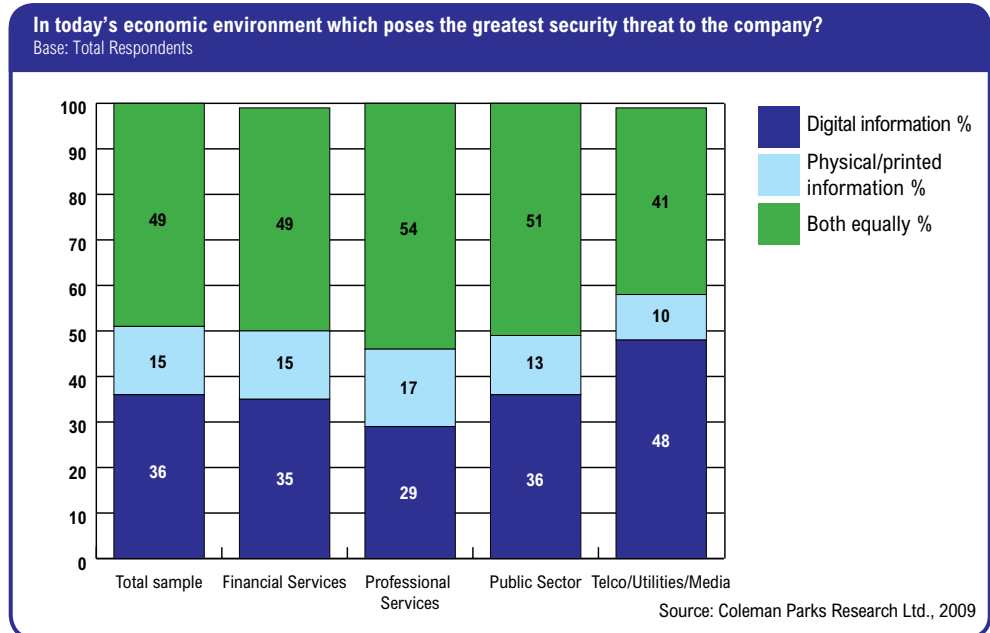
49% des entreprises attachent autant d'importance à la sécurité de l'information numérique qu'à celle de l'information imprimée

A l'évidence, les dirigeants d'entreprises européennes font preuve de lucidité et ont conscience de la nécessité d'assurer la sécurité documentaire dans leur organisation. La majorité d'entre eux (76%) s'accorde sur l'idée que les failles de sécurité sont corrélés avec l'évolution technologique.

En matière de sécurité documentaire, 91% des responsables d'entreprise interrogés sont d'accord avec le proverbe "Mieux vaut prévenir que guérir", et 68% pensent qu'un environnement d'impression optimisé permettrait d'améliorer la sécurité. En ce qui concerne les documents professionnels, près de la moitié des personnes interrogées (49%) attache autant d'importance à la sécurité de l'information numérique qu'à celle de l'information imprimée. Ces résultats démontrent clairement que les entreprises ont conscience de l'importance de la sécurité au niveau du flux documentaire.

Pour pallier l'absence de gestion documentaire sécurisée au sein des entreprises, de nombreuses solutions de sécurité sont mises à la disposition des dirigeants, telle que la Gestion de Services Documentaires par exemple. Il existe également des solutions plus spécifiques qui permettent d'identifier l'utilisateur, de créer des quotas d'impression ou encore de mettre en place une comptabilité intelligente (dite smart-accounting). Les contrôles s'effectuent dès lors par mot de passe de façon à ce que seuls les utilisateurs autorisés puissent accéder aux informations confidentielles et les imprimer. L'intégrité des documents peut aussi être assurée grâce à des codes intégrés qui indiquent les modifications et/ou empêchent toute reproduction (copie ou scan). Un autre processus d'écrasement de données permet d'effacer automatiquement et régulièrement les données temporaires stockées sur le disque dur des périphériques multifonctions.

Figure 1 : Attitudes des entreprises face au risque sécuritaire de l'information imprimée et numérique



4.0 Les entreprises s'exposent à un risque important

Seules 47% des entreprises disposent d'une politique stricte de contrôle de l'impression des informations clients

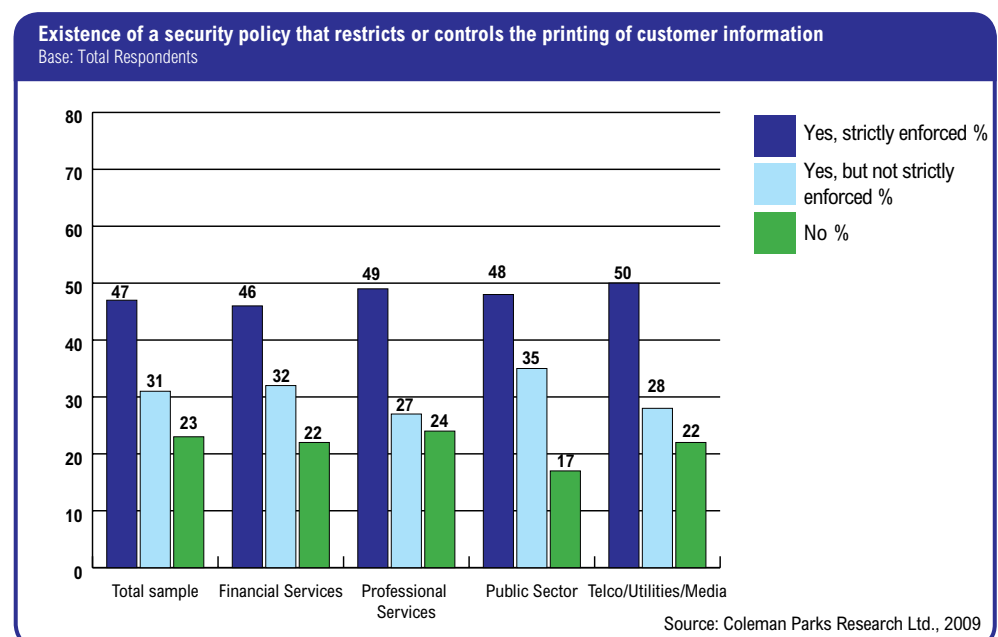
Bien que les dirigeants d'entreprises interrogés aient conscience des risques encourus par leurs documents professionnels, ils n'ont pas encore recours aux solutions disponibles pour réduire ces risques.

Seuls 47% des dirigeants d'entreprise affirment disposer d'une politique de contrôle de l'impression des informations client et ils sont encore moins nombreux (41%) à limiter l'impression d'autres documents confidentiels. Plus grave : seules 44% des personnes interviewées affirment avoir instauré une politique destinée à éviter la conservation d'informations confidentielles par des employés quittant l'entreprise.

Sans politique de sécurité opérationnelle, les entreprises s'exposent à des risques importants. La divulgation d'informations professionnelles confidentielles, qu'elle soit intentionnelle ou accidentelle, peut en effet avoir des répercussions considérables et hautement pénalisantes pour l'entreprise.

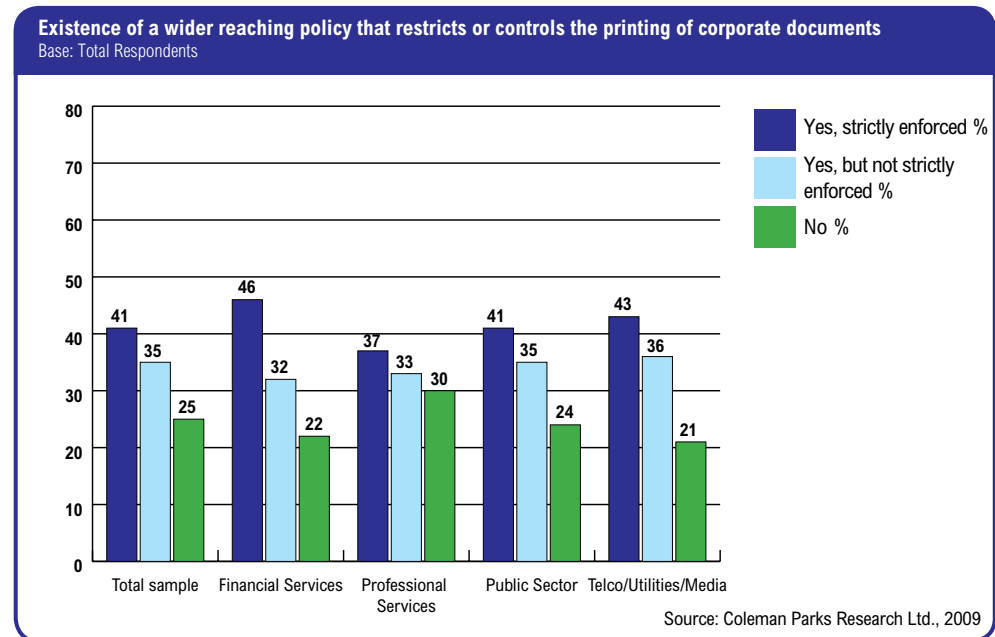
L'absence de politique peut être directement liée à une approche décentralisée de la gouvernance documentaire qui prive souvent les entreprises d'une vision globale des domaines dans lesquels la sécurité doit être améliorée. Résultat : les entreprises sont plus vulnérables aux failles de sécurité accidentelles ou intentionnelles.

Figure 2 : Présence de politiques de contrôle de l'impression des informations client



Au sein des entreprises, le contraste entre la connaissance des enjeux liés à la sécurité du document et les mesures prises peut être corrélé aux résultats de l'étude Ricoh sur la Gouvernance Documentaire³. Pour rappel, l'étude démontre que la gouvernance documentaire est souvent décentralisée entre plusieurs directions de l'entreprise, sans responsable clairement identifié. Dans certains cas, plusieurs personnes sont responsables de la gouvernance documentaire, bien que cette responsabilité incombe le plus souvent aux chefs de service ou aux employés. Dans l'ensemble, disposer d'une gouvernance documentaire décentralisée génère duplication et inefficacité impactant de fait la productivité et la durabilité de l'entreprise. Grâce au livre blanc, nous constatons que cela affecte également la sécurité documentaire.

Figure 3 : Présence de politiques de contrôle de l'impression d'autres informations sensibles



³ Coleman Parkes Research. Octobre 2009



5.0 Une approche de la sécurité documentaire différente selon les secteurs d'activité

L'étude précise les écarts d'attitudes des entreprises issues de différents secteurs d'activité suivants en matière de sécurité :

- Finances
- Secteur public
- Services professionnels
- Télécommunications / Média

Nous constatons que, tous secteurs confondus, moins de la moitié des entreprises a mis en place une stratégie complète de sécurité documentaire (48%) ou de contrôle de l'impression des informations client (47%). De même, seulement 44% des entreprises interrogées estiment pouvoir empêcher la sortie des documents stratégiques de l'entreprise.

Finances

Le secteur financier, qui est l'un des plus réglementés, obtient des résultats inattendus en matière de sécurité documentaire. Seuls 46% des dirigeants d'entreprise de ce secteur affirment avoir une politique de contrôle de l'impression des informations client au sein de leur entreprise, le plaçant de ce fait en dernière position dans ce domaine.

Inversement, le secteur financier est plus enclin (49%) à mettre en place une politique visant à empêcher les collaborateurs de quitter l'entreprise avec des informations confidentielles.

Ce résultat n'est cependant pas le reflet d'une volonté du secteur financier. Il est plus vraisemblablement le résultat d'une gouvernance documentaire décentralisée, sans aucune gestion globale de l'ensemble du flux d'information et de documents. Les actifs documentaires du flux informatique sont donc invisibles, les risques ne sont pas connus et l'information n'est par conséquent pas protégée.

Secteur public

Le secteur public affiche également une tendance inattendue avec seulement 39% d'entreprises disposant d'une politique de contrôle afin d'éviter que les employés ne quittent l'entreprise avec des informations confidentielles ou sensibles. Bien en dessous de la moyenne du marché (44%), ce résultat est problématique étant donné l'importance des informations issues de ce secteur et la quantité d'informations perdues ou divulguées.

Les entreprises publiques sont également les moins propices à mettre en place une stratégie de gouvernance documentaire globale (33%), qui leur permettrait de gérer et sécuriser leur environnement d'impression. De même, une sécurité accrue n'est considérée comme un bénéfice clé d'une approche optimisée de l'impression que par très peu d'entre eux (59%).

Services professionnels

En plus des actions déjà déployées pour protéger et sécuriser l'impression de données client, l'étude démontre que nombre de solutions sont disponibles pour restreindre ou contrôler l'impression de documents confidentiels de l'entreprise (business plans, informations relatives aux employés et aux budgets notamment). Cependant, seulement 37% (la plus faible proportion en Europe) des dirigeants d'entreprise de services professionnels ont mis en place une politique de sécurisation de l'impression contre 46% dans le secteur financier (la plus forte proportion en Europe).

Télécommunications et média

Les dirigeants d'entreprise des secteurs des télécommunications et média s'accordent sur le fait que le volume d'informations imprimées augmente. Pour autant, seuls 43% de ces dirigeants ont mis en place une politique stricte de contrôle d'impression des documents confidentiels. Ils sont légèrement plus nombreux que les dirigeants des secteurs des services professionnels et public (41%).

Figure 4 : Présence d'une politique de sécurisation évitant que les employés quittent l'entreprise avec des informations confidentielles

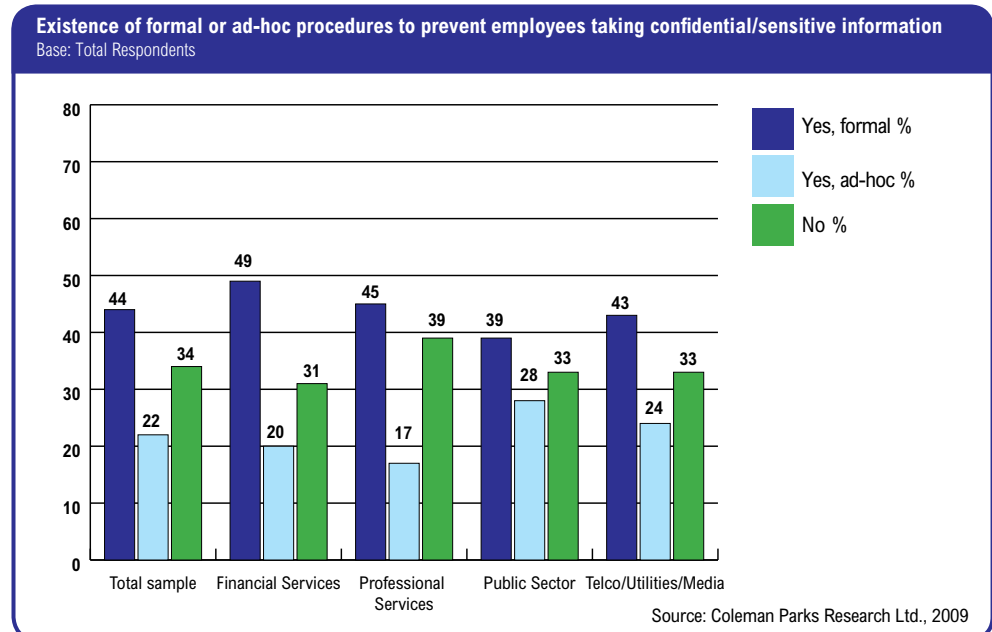
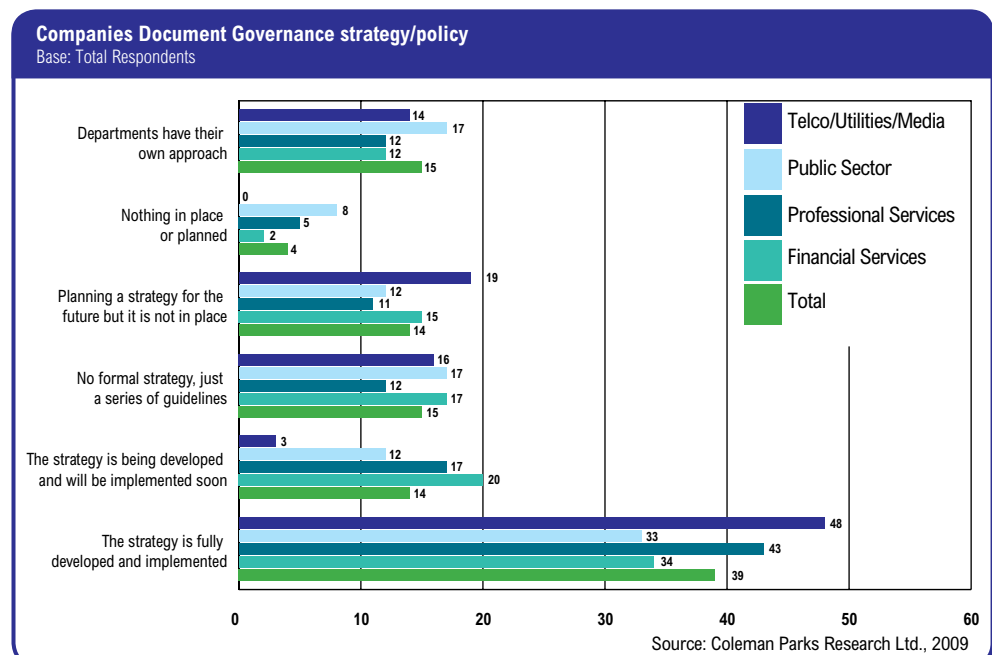


Figure 5 : Comportement des différents secteurs d'activité par rapport aux politiques de gouvernance documentaire





6.0 Conclusion

Bien que près de la moitié des dirigeants d'entreprise interrogés attache de l'importance aux risques liés à la confidentialité des documents numériques et imprimés, l'étude Ricoh démontre qu'ils ne disposent pas pour autant de politique efficace de protection de ces documents. Les chiffres démontrent clairement qu'en dépit des risques encourus, des exigences réglementaires accrues et de la demande de responsabilité émanant des clients, seules 48% des entreprises disposent d'une stratégie complète de sécurité documentaire.

Dans tous les secteurs, même les plus réglementés, des améliorations sont possibles, notamment en optant pour une gouvernance documentaire centralisée. En effet, le manque de connaissance des avantages offerts par une gestion centralisée permet de réduire les risques et d'atteindre leurs objectifs en termes d'efficacité et de durabilité. Les actifs documentaires doivent être considérés comme partie intégrante de la stratégie de sécurité de l'entreprise et gérés parallèlement aux autres propriétés du réseau professionnel.

À un niveau décisionnel, la sécurité documentaire peut également jouer un rôle clé pour permettre aux entreprises d'être en conformité avec la réglementation et pour permettre d'augmenter la productivité des employés grâce à un workflow simplifié. La sécurité documentaire peut aussi permettre aux entreprises de faire la différence en montrant qu'elles travaillent de manière éthique et responsable, en étant intègres et transparentes. Cela favorise la confiance des clients et offre un réel avantage compétitif. De la même façon qu'elles ont requis une transparence et une responsabilité complètes de la part de leurs fournisseurs, les entreprises commenceront peut-être à promouvoir leur processus interne de sécurité documentaire comme facteur de différence potentiel pour leurs futurs clients.



7.0 L'approche Sécurité Ricoh

Pour aider les entreprises à protéger leurs données, Ricoh place la sécurité au cœur de son offre, de la conception des solutions d'impression (département Recherche & Développement) jusqu'aux services de maintenance, sans oublier dans ses propres processus internes. La sécurité documentaire permet de gérer la confidentialité, l'intégrité et la disponibilité de l'information.

Ricoh est conscient de l'importance cruciale de la sécurité de l'information pour ses clients, du fait des réglementations imposées par le marché et le gouvernement. Quelques soient les besoins ou les attentes des entreprises européennes, ceux-ci peuvent trouver une réponse pertinente et adaptée dans le catalogue de solutions de sécurité de Ricoh.

Ce catalogue a été développé pour aider les entreprises à gérer et à protéger leur flux d'information. En mettant en place des mesures de sécurité, les entreprises peuvent gérer l'équipement et se prémunir de toute divulgation ou perte d'informations. Le catalogue Ricoh propose une gamme d'outils qui s'intègrent facilement au système de gestion de sécurité de l'information des entreprises.

Des composants testés

La sécurité fait partie intégrante de la conception d'équipements et de logiciels Ricoh. Nous avons en effet été la première entreprise à recevoir la certification ISO/IEC 15408 en 2002 pour une imprimante multifonction. Ricoh continue depuis à concevoir et à développer des périphériques certifiés. Ces matériels incluent notamment l'option DataOverwriteSecurity qui est également certifiée ISO/IEC 15408.

Définir et renforcer les politiques de sécurité

Les consultants et les clients Ricoh travaillent ensemble dans le but de définir une politique d'impression qui met en corrélation les besoins en termes de sécurité et de gestion documentaires avec les impératifs de flexibilité et d'efficacité des entreprises. Une fois la politique d'impression définie, les utilisateurs doivent être formés à ses impératifs et modalités de mise en œuvre. La consolidation de la politique d'impression peut être automatisée par l'utilisation de différents produits du catalogue Ricoh.

Accès restreint aux périphériques

L'un des risques les plus importants en matière de sécurité est causé par l'absence de restriction d'accès aux zones de travail et aux systèmes d'impression. En effet, tant qu'aucune mesure de sécurité n'est activée, les périphériques multifonctions peuvent être utilisés pour l'exportation ou la copie non autorisée d'informations sensibles. Il est préférable d'implanter des fonctionnalités d'identification des utilisateurs, que ce soit par badge ou mot de passe, afin de pouvoir utiliser le matériel d'impression. Les droits affectés à chaque utilisateur peuvent de plus être retroints en fonction des besoins professionnels et des fonctions.

Restitution sécurisée des documents

Les impressions non récupérées sont une marque évidente de gaspillage, mais constituent également un risque sécuritaire. Une fois commandées par l'utilisateur préalablement identifié, les impressions confidentielles peuvent être stockées et récupérées. Des fonctions simples d'identification du propriétaire du document peuvent être ajoutées au périphérique d'impression (code personnel ou carte à puce magnétique). Les fichiers non récupérés peuvent être automatiquement effacés du serveur après une durée déterminée.



D'autres fonctionnalités peuvent également être mises en place pour assurer la sécurité du document au cours de son transfert jusqu'au périphérique. Un processus d'écrasement des données peut effacer automatiquement toutes les données temporaires stockées sur le disque dur des périphériques multifonctions.

Audit

Les rapports d'audit sont une part essentielle de la gestion documentaire puisqu'ils permettent de détecter efficacement des dysfonctionnements en matière de sécurité. Le responsable sécurité peut ainsi obtenir les informations relatives à l'utilisation des matériels (qui scanne, faxe et imprime) pour détecter et, si besoin proscrire, les mauvaises utilisations et autres failles de sécurité interne

L'approche interne de Ricoh sur la gestion de la sécurité de l'information

Ricoh propose une approche pertinente et globale de la sécurité de l'information. Depuis 2004, l'ensemble des filiales du groupe sont certifiées ISO 27001, une distinction unique pour une entreprise du secteur documentaire. Les échanges entre Ricoh et ses clients se multiplient sans cesse en raison des offres de services d'impression et de maintenance en réseau ainsi qu'à travers l'outsourcing de services et de gestion de services d'impression ; Ricoh manipule donc des informations clients dont ils doivent rester propriétaires. La confiance des clients est donc essentielle. Pour cela, la certification ISO 27001 est un gage de confiance.

Liens utiles

www.ricoh-europe.com

<http://www.ricoh-europe.com/solutions/index.xhtml>

<http://www.ricoh-europe.com/products/output-management-and-security/index.jsp>

<http://securite.ricoh.fr/>

Relations presse

Sophie MC DONAGH

Tél.: 01 56 72 29 49

E-mail: Sophie.mcdonagh@ricoh.fr

A propos de Ricoh

Depuis 2000, Ricoh a su évoluer avec le marché et les technologies. Ainsi, au métier de fournisseur de matériel bureautique, Ricoh France a associé la maîtrise des « solutions d'impression » puis des « solutions documentaires » afin de pouvoir assurer la gestion globale du flux documentaire de ses clients, en s'appuyant sur la performance de ses choix technologiques, la pertinence de ses offres de services et la qualité de ses équipes.

Effectif : 2500 personnes

CA 2008 au 31 Mars 2009 : 712,9 millions€

N°1 des constructeurs de systèmes d'impression avec 27.2% de parts de marché (1er semestre 2009 - Source Infosource - constructeur Marché Office MFP N&B et B to C).

Pour davantage d'information, rendez-vous sur notre site : www.ricoh.fr