IRON MOUNTAIN®

UN AUTRE REGARD
SUR L'INFORMATION

GESTION DE L'INFORMATION ET DES DOCUMENTS :

POUR PARTIR SUR DE BONNES BASES

LE B. A.-BA DE LA PRÉPARATION FACE AUX RISQUES

INTRODUCTION

UN GUIDE RAPIDE QUI VOUS AIDERA À PLANIFIER, EXÉCUTER ET EXPLOITER UN PLAN LIMITANT VOTRE EXPOSITION AUX RISQUES LIÉS À L'INFORMATION.

Une gestion réussie de l'information et des documents nécessite une planification, une organisation et une stratégie afin de prendre le contrôle des documents papier et numériques, de la création au stockage permanent ou à la destruction planifiée, en passant par l'utilisation active. Intelligemment effectuée, la gestion de l'information et des documents permettra à votre entreprise de limiter les risques liés à l'information, de gérer les coûts et de jeter les bases de l'analyse du Big Data.

Quelles que soient leur taille et leur renommée, les entreprises s'efforcent de combler l'écart existant entre un plan pour limiter les risques liés à l'information et la mise en œuvre effective de ce plan.

LA PROBLÉMATIQUE LIÉE AUX RISQUES

Les raisons de l'écart entre la théorie et la pratique de la gestion des risques liés à l'information sont variées. D'une part, l'information concerne toutes les équipes et tous les services. Dans de nombreuses entreprises, elle doit être accessible immédiatement à de multiples équipes, qui doivent pouvoir la consulter partout et à tout moment. Dans le contexte actuel de globalisation des affaires, l'accès à l'information doit être rapide, indépendant des périphériques et sécurisé.

En raison de la croissance rapide du volume, de la diversité et de la rapidité des données pénétrant dans les entreprises, les gestionnaires de l'information et des documents doivent non seulement traiter plus de données, mais doivent également prendre en compte des formats qui évoluent. Des documents papier aux publications des réseaux sociaux et aux e-mails, les difficultés ne semblent pas s'atténuer. En outre, il n'est pas toujours facile de déterminer qui doit avoir accès à quelle information et qui ne doit pas y avoir accès. Et l'on s'interroge également sur la manière dont les utilisateurs doivent accéder à l'information et à quel endroit. Il peut être acceptable qu'un chef de service examine et utilise des données sensibles, mais qu'arrive-t-il si ces données sont imprimées et laissées dans un lieu public ? Ou enregistrées sur un ordinateur portable oublié dans un restaurant ?

Il existe également des risques liés au stockage de l'information. Les bases de données numériques peuvent être violées, tandis que les communications en ligne sont la cible des logiciels malveillants, des fraudeurs et des attaques malveillantes. Les documents papier sont facilement perdus ou détruits. Vouloir gérer les risques liés à l'information est une chose, mais mettre en pratique un plan détaillé en est une autre.

POURQUOI S'INQUIÉTER DES RISQUES LIÉS À L'INFORMATION ?

Il n'est pas question de négliger la menace posée par les risques liés à l'information. Le nombre des incidents menaçant certains aspects de la sécurité électronique est en hausse. Selon l'étude menée en 2014 par PwC, Defending Yesterday - key findings from The Global State of Information Security, les incidents détectés ont augmenté de 25 %. En fait, 24 % des participants à l'étude ont signalé une perte de données, soit une augmentation de 16 % par rapport à l'année précédente. L'étude menée en 2014 par PwC, Information Security Breaches Survey, suggère que les coûts liés aux violations individuelles ont augmenté considérablement. Elle révèle également que 10 % des entreprises anglaises ayant fait l'objet, l'année dernière, d'une violation de sécurité de l'information ont été tellement affectées qu'elles ont dû revoir entièrement leur fonctionnement. Les menaces augmentent en fréquence, en sévérité et en coûts.

QUE SIGNIFIE CECI POUR VOTRE ENTREPRISE ?

On ne recherche pas la sécurité de l'information simplement pour le plaisir. Il s'agit d'un impératif commercial. Cet aspect ne peut pas simplement relever du personnel informatique, ni même des cadres supérieurs. Votre stratégie de sécurité de l'information doit évaluer vos points forts et vos points faibles afin d'identifier et de gérer les risques. Elle doit également s'adapter à l'évolution des menaces en identifiant vos données les plus précieuses. Savoir où se trouvent ces données et qui peut y accéder vous aidera à hiérarchiser vos ressources et vos investissements.

LES MESURES À PRENDRE

1. PARTAGEZ LA RESPONSABILITÉ DE L'INFORMATION
2. SOYEZ CONSCIENT DE VOS POINTS FORTS ET DE VOS POINTS FAIBLES
3. IMPLIQUEZ VOTRE PERSONNEL
4. N'OUBLIEZ PAS LE PAPIER
5. MESUREZ ENCORE ET ENCORE
6. PRÉPAREZ-VOUS AU PIRE

1 PARTAGEZ LA RESPONSABILITÉ DE L'INFORMATION

La gestion de l'information doit relever de la responsabilité de chacun au sein de votre entreprise. Si l'information devient la responsabilité du service informatique seul, les personnes qui la créent et l'utilisent chaque jour risquent de ne pas comprendre les risques qu'elle implique. De plus, si l'information n'est pas la responsabilité de tous, vos équipes ne comprendront ou n'adopteront pas nécessairement les nouvelles méthodes de travail. Les politiques visant à sécuriser l'information doivent être visibles au sommet même de l'entreprise et comprises à chaque niveau. Les cadres dirigeants devraient encourager ouvertement les bonnes pratiques en matière de sécurité de l'information. Les dirigeants sont autant responsables que les cadres, les utilisateurs et les créateurs de l'information. Après tout, le personnel informatique ne peut pas protéger l'information si un employé du service marketing ne suit pas les consignes.

73 % des entreprises en Europe et 74 % en Amérique du Nord pensent que le service informatique doit en définitive être responsable des risques liés à l'information.

Au-delà des bonnes intentions, la nécessité de passer de l'intention à l'action pour gérer les risques liés à l'information sur le marché des entreprises de taille moyenne, rapport PwC et Iron Mountain, 2014

2 SOYEZ CONSCIENT DE VOS POINTS FORTS ET DE VOS POINTS FAIBLES

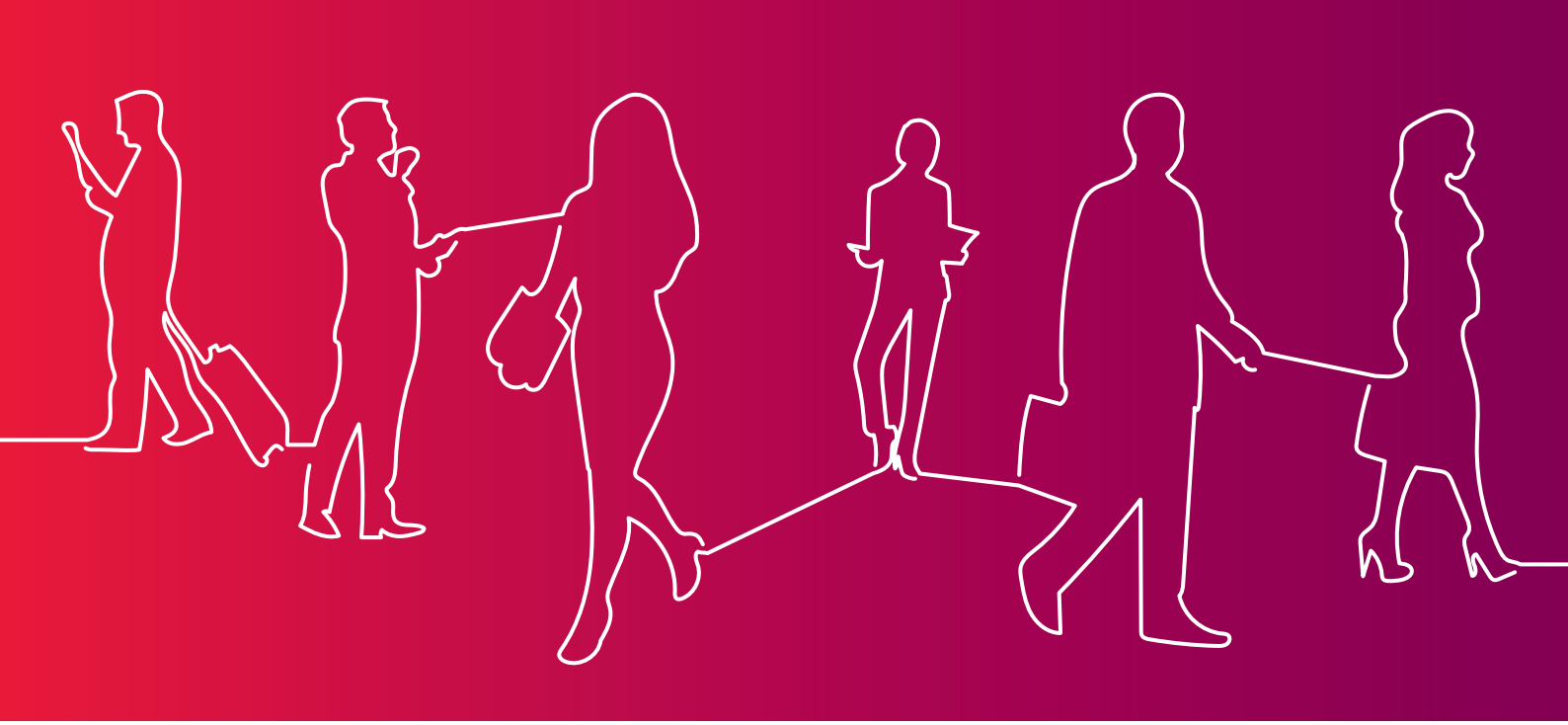
Découvrez où se situent les données les plus précieuses et les plus vulnérables de votre entreprise. Déterminez qui peut y accéder. Votre évaluation des risques doit couvrir toute l'entreprise, y compris chaque aspect et chaque site. Elle doit également inclure les questions posées par les personnes chargées de gérer les risques. Envisagez d'inclure les services de la sécurité informatique, la conformité et le juridique, la gestion documentaire ainsi que les unités commerciales. Examinez les référentiels physiques, numériques et du cloud, ainsi que les appareils mobiles. N'oubliez pas vos fournisseurs tiers. Basez-vous sur vos résultats pour planifier et prendre des décisions sur les ressources que vous investissez. Revoyez régulièrement vos conclusions car le profil de risque de différents services peut évoluer.

DERNIÈRES RÉFLEXIONS

L'information et les formes qu'elle peut prendre évoluent, tout comme les risques associés. Pour pouvoir trouver et utiliser l'information comme un actif, les entreprises doivent s'assurer que les risques sont gérés de manière cohérente et efficace. À l'avenir, les entreprises gagnantes trouveront un équilibre entre la protection de l'information et sa mise à disposition pour générer l'innovation et la croissance. L'objectif n'est pas de confiner l'information, mais de l'exploiter pleinement.

87 % des entreprises en Europe et 80 % en Amérique du Nord ne croient pas que des ex-employés partent avec des données qu'ils confient à leur nouvel employeur.

Au-delà des bonnes intentions, la nécessité de passer de l'intention à l'action pour gérer les risques liés à l'information sur le marché des entreprises de taille moyenne, rapport PwC et Iron Mountain, 2014



3 IMPLIQUEZ VOTRE PERSONNEL

La gestion des risques dépend de vos employés :

▸▸ Parallèlement à l'augmentation du volume, de la rapidité et de la diversité des données, les entreprises ont de plus en plus besoin de personnes capables de les aider à aller au-delà des politiques liées à l'information. Faire appel à des analystes de données aidera votre entreprise à établir l'équilibre entre valeur et risque. Vous pouvez également intégrer la compréhension et l'analyse des données à vos fonctions commerciales.

▸▸ Développez et mettez en place une formation sur l'information pour sensibiliser vos employés aux risques et les amener à changer de comportement. Communiquez régulièrement avec votre personnel pour vous assurer qu'il intègre la formation à ses méthodes de travail. L'information est un atout et créer une culture du respect de l'information vous permettra de protéger et de promouvoir la valeur de l'information. Cette culture doit commencer au niveau des cadres supérieurs et inclure tous les employés, ainsi que les sous-traitants et les fournisseurs tiers.

▸▸ Les employés démissionnent. Et lorsqu'ils le font, ils emportent souvent avec eux des informations précieuses ou sensibles. Mettez en place un processus permettant de protéger l'information face aux employés. Sensibilisez le personnel et encouragez une bonne conduite au sein de l'entreprise.

Seulement 26 % des entreprises en Europe et 20 % en Amérique du Nord surveillent leurs formations sur les risques pour en évaluer l'efficacité.

Au-delà des bonnes intentions, la nécessité de passer de l'intention à l'action pour gérer les risques liés à l'information sur le marché des entreprises de taille moyenne, rapport PwC et Iron Mountain, 2014

4 N'OUBLIEZ PAS LE PAPIER

Le papier est une menace majeure à la sécurité de l'information. Envisagez d'investir dans une solution combinant numérisation et stockage sécurisé des documents. Une solution hybride peut vous aider à prendre le contrôle de vos documents papier. L'expertise et les ressources d'Iron Mountain ont résisté à l'épreuve du temps et peuvent convenir à votre entreprise.

Environ deux tiers des participants à l'étude ont désigné les documents papier comme source d'inquiétude majeure face aux risques, soit deux fois plus que pour les menaces externes, qui constituent, elles, la source d'inquiétude numéro deux.

Au-delà des bonnes intentions, la nécessité de passer de l'intention à l'action pour gérer les risques liés à l'information sur le marché des entreprises de taille moyenne, rapport PwC et Iron Mountain, 2014

5 MESUREZ ENCORE ET ENCORE

Pour être efficace, le changement doit être mesuré. Définissez vos indicateurs de performances clés et établissez un plan de production de rapports ainsi que les délais à respecter. Assurez-vous que le personnel est conscient des mesures que vous mettez en place en communiquant vos objectifs à la direction et en proposant une formation aux équipes clés. Désignez un responsable pour l'évaluation et la présentation de vos résultats.

Seulement 37 % des participants à l'étude en Europe et 47 % en Amérique du Nord disposaient d'une stratégie entièrement suivie face aux risques liés à l'information.

Au-delà des bonnes intentions, la nécessité de passer de l'intention à l'action pour gérer les risques liés à l'information sur le marché des entreprises de taille moyenne, rapport PwC et Iron Mountain, 2014

6 PRÉPAREZ-VOUS AU PIRE

Que ferez-vous si, malgré vos précautions, le pire se produit ? Vos plans de continuité des activités et de gestion de crise doivent inclure une stratégie permettant de gérer les conséquences d'une violation de l'information. La manière dont vous communiquez avec vos employés, vos clients et le public aura un impact sur la situation.

DERNIÈRES RÉFLEXIONS

L'information et les formes qu'elle peut prendre évoluent, tout comme les risques associés. Pour pouvoir trouver et utiliser l'information comme un actif, les entreprises doivent s'assurer que les risques sont gérés de manière cohérente et efficace. À l'avenir, les entreprises gagnantes trouveront un équilibre entre la protection de l'information et sa mise à disposition pour générer l'innovation et la croissance. L'objectif n'est pas de confiner l'information, mais de l'exploiter pleinement.

Lisez le rapport complet de PwC.