CHAPITRE 3

# LES RISQUES LIÉS À L'INFORMATION ?

## COMBIEN COÛTE LE FAIT D'IGNORER

COMMENT MINIMISER VOTRE EXPOSITION



IRON MOUNTAIN®

# POURQUOI VOUS DEVEZ VOUS PROCURER LE GUIDE ÉLECTRONIQUE L'ÉCONOMIE DE L'INFORMATION

Ce guide électronique comportant cinq sections vous aidera à bien comprendre le rôle que l'information joue au sein de votre entreprise. Il examine chaque aspect lié à l'économie de l'information.

1. Qu'est-ce que le retour sur l'information ?
2. Comment accéder à mes données pour en extraire la valeur maximale ?
3. Combien coûte le fait d'ignorer les risques liés à l'information ?


Menaces


Erreurs courantes


Opportunités d'amélioration

4. Comment concevoir un programme fonctionnant à la fois pour le personnel et pour l'entreprise ?
5. Comment les futures tendances dans la gestion de l'information affecteront-elles mon entreprise ?

**VOUS DÉCOUVRIREZ**

Comment reconnaître les pièges liés à la gestion de l'information et s'y préparer, en évitant les risques tels que les violations de données et la non conformité

# ÉCONOMIE DE L'INFORMATION

## LE POINT DE CONVERGENCE ENTRE VALEUR, RISQUE ET COÛT

L'économie de l'information consiste à gérer et exploiter les données créées et reçues par l'entreprise en vue d'améliorer les résultats. Chaque entreprise a besoin d'une stratégie de gestion de l'information visant à limiter les risques, à assurer la conformité, à réduire les coûts et, aujourd'hui, avec l'émergence du Big Data, à préparer les données en vue de l'analytique. L'économie de l'information apporte une stratégie collaborative et d'ensemble qui aide les entreprises à optimiser la valeur de leurs données et à limiter les risques à chaque étape, de la création initiale des documents et des données à leur exploitation et à leur destruction sécurisée.

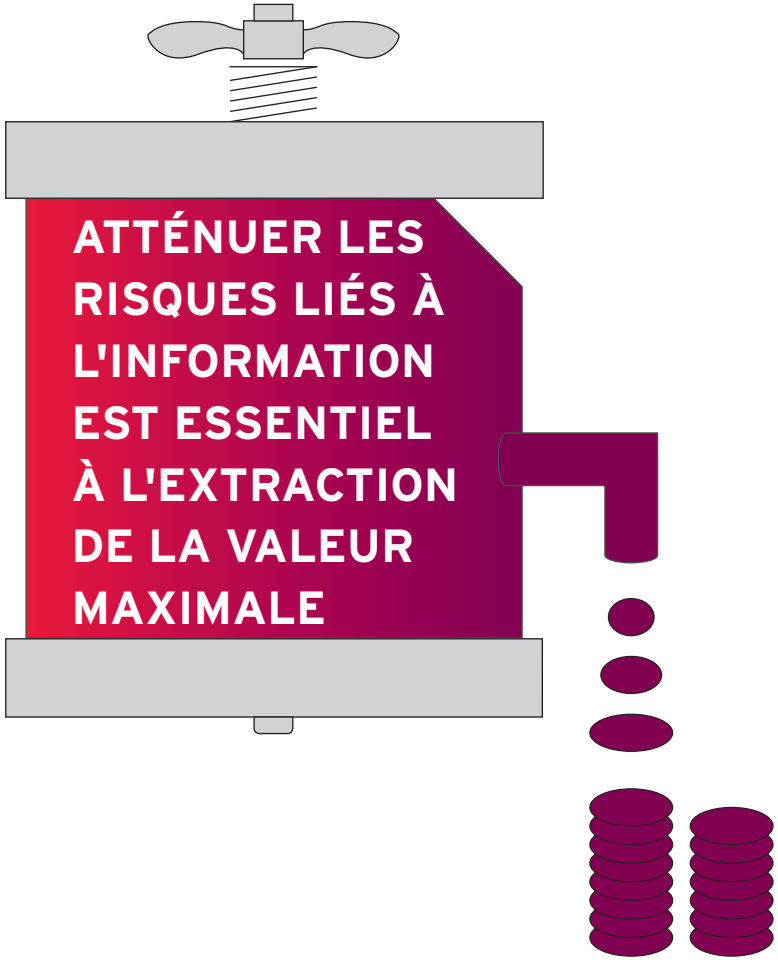
# CHAPITRE 3

# ÊTRE CONSCIENT ET PRÉPARÉ FACE AUX RISQUES

Dans les chapitres précédents de ce guide électronique, nous avons vu comment garantir un retour sur l'information en extrayant la valeur maximale des documents et de l'information. Nous avons également vu comment minimiser les coûts en conservant les documents que la législation vous oblige à conserver et en stockant les autres documents de manière permanente ou en les détruisant de manière sécurisée. Mais, en termes de coûts ou d'économies, les aspects de l'économie de l'information ne peuvent pas être tous évalués de manière transparente.

Il peut être difficile de quantifier économiquement les risques liés à l'information, mais éviter les catastrophes touchant l'information doit constituer une priorité majeure car les conséquences peuvent être extrêmement graves. Toutefois, l'atténuation des risques doit être équilibrée avec le besoin impérieux de laisser le personnel travailler efficacement, en extrayant la valeur maximale de ses données.

Ce chapitre examine les menaces spécifiques et explique comment planifier une stratégie permettant d'éviter les catastrophes et d'obtenir un retour positif sur l'information.



## LES RISQUES LIÉS À L'INFORMATION : LES FAITS

Une recherche très instructive sur les risques liés à l'information nous provient du cabinet d'expertise-conseil d'envergure mondiale PwC et d'Iron Mountain. Leur rapport de 2014, *Au-delà des bonnes intentions – la nécessité de passer de l'intention à l'action pour gérer les risques liés à l'information*, analyse les recherches portant sur 600 entreprises européennes et 600 autres entreprises d'Amérique du Nord, chacune ayant entre 250 et 2 500 employés.

Ce rapport définit les bonnes pratiques dans l'atténuation des risques liés à l'information et quantifie les performances par rapport à ce repère en utilisant l'indice de maturité face aux risques liés à l'information. Un indice de 100 indique que l'entreprise est prête à affronter les risques. L'index moyen des entreprises européennes a été établi aux alentours de 56,1, ce qui montre que la vaste majorité des entreprises sont exposées à des risques bien plus grands qu'ils ne devraient l'être.

L'ENTREPRISE EUROPÉENNE MOYENNE OBTIENT LA NOTE DE

**56,1 %**

**DANS LA PRÉPARATION FACE AUX MENACES**

## POSÉES PAR LES RISQUES

### VIOLATION DE DONNÉES

Pour les entreprises, la violation des données est catastrophique et le pire des cauchemars. Bien que le piratage informatique soit une menace sérieuse, dans le rapport 2014 de PwC, Global State of Information Security Survey, le pourcentage de cadres (31 %) qui désignent les employés comme source probable d'incident de sécurité de l'information est presque égal à celui des cadres (32 %) qui désignent, eux, les pirates informatiques.

Au Royaume-Uni, une recherche récente menée par l'administration montre que 31 % des pires violations de sécurité survenues en 2014 ont été causées par une erreur humaine, tandis que 20 % ont pour origine un abus délibéré des systèmes par le personnel[1]. Selon la même recherche, les coûts liés aux incidents individuels ont considérablement augmenté.

**31 % DES PIRES VIOLATIONS DE SÉCURITÉ SURVENUES EN 2014 ONT ÉTÉ CAUSÉES PAR UNE ERREUR HUMAINE**

[1] Information Security Breaches Survey 2014 - UK Department for Business Innovation and Skills

## NON-CONFORMITÉ

Le chapitre 1 de ce guide électronique examine le retour sur l'information et l'importance de réduire les volumes de documents afin de libérer de l'espace de bureau et d'améliorer l'accès à l'information. Un calendrier de conservation des documents réaliste vous aidera à faire les deux – et à être conforme. En termes d'amendes, la législation sur la protection des données est peut-être la plus significative, avec des sanctions pouvant atteindre 690 000 euros en cas de violation sérieuse[2].

Lorsqu'il s'agit de perte de données, en particulier si des informations client sensibles sont impliquées, une amende peut être le moindre de vos soucis. À long terme, les dommages à la réputation de votre entreprise peuvent vous coûter bien plus. 90 % des entreprises qui subissent des pertes de données significatives mettent la clé sous la porte dans les deux ans qui suivent.[3].


# EN CAS DE VIOLATION SÉRIEUSE

[2] UK Information Commissioner's Office
[3] Chambre de commerce de Londres

## ERREURS COURANTES

### UNE RÉFLEXION CENTRÉE SUR L'INFORMATIQUE

Selon le rapport de PwC, 73 % des entreprises européennes pensent que la responsabilité globale de la sécurité de l'information doit revenir au responsable de la sécurité informatique. Toutefois, la même étude révèle que 62 % des entreprises considèrent les documents papier comme principale menace à la sécurité de l'information[4]. On perçoit donc aisément une lacune dans la perception des risques liés à l'information.

Réfléchissez à ceci : quel élément est mieux protégé par des mesures de sécurité spécifiques ? Vos documents papier ou les données figurant sur vos disques durs ?

73%

**DES ENTREPRISES EUROPÉENNES PENSENT QUE LE SERVICE INFORMATIQUE DOIT SUPERVISER LA GESTION DE L'INFORMATION**

### POLITIQUES ET FORMATION

Ici, les résultats de l'étude PwC désignent sans détour le manque général de préparation des entreprises européennes face aux risques liés à l'information. Seulement 27 % des entreprises observent des politiques concernant la sécurité, le stockage et la destruction des données confidentielles. Et pas plus de 26 % surveillent leurs formations sur les risques liés à l'information pour en évaluer l'efficacité[5].

La sécurité de l'information, c'est chaque personne au sein de l'entreprise prenant tous les jours les bonnes mesures. Ceci implique une formation universelle et continue sur les politiques et les procédures, à l'instar de n'importe quel autre aspect opérationnel vital de l'entreprise.

[4,5] Au-delà des bonnes intentions – Rapport PwC, 2014

# OPPORTUNITÉS D'AMÉLIORATION

## GOUVERNANCE

Seulement 37 % des entreprises européennes ont mis en place une stratégie entièrement suivie face aux risques liés à l'information[6]. Examiner les politiques de l'entreprise constitue une bonne base de départ. Les mettre en œuvre est bien entendu tout autre chose.

Obtenir l'implication des personnes clés à tous les niveaux et dans tous les services, en commençant par la direction, est la voie à suivre. Mettez en place un comité de gestion de l'information capable de piloter votre initiative et de sensibiliser sur le problème afin que celui-ci ne puisse pas être ignoré. Élaborez un calendrier de réunions et de révisions et respectez-le.

## STOCKAGE SÉCURISÉ

Bien entendu, la sécurité de l'information doit être équilibrée avec l'accès à l'information. Verrouiller simplement vos documents peut les protéger contre le vol et les abus, mais risque d'en diminuer la valeur pour votre entreprise si leur accès est compromis. D'autres considérations incluent le risque de dommage dû à un incendie, à une inondation et même à des rongeurs. Il faut également prendre en compte les implications de coûts liées au stockage sur site et l'espace de bureau peut presque toujours être utilisé de manière plus rentable.

Le stockage sur site distant spécialisé et sécurisé intégrant des systèmes de protection d'avant-garde et un accès aux documents selon l'approche « payez au fur et à mesure » offre généralement le meilleur retour sur l'information lorsqu'il s'agit des documents papier.

[6] Au-delà des bonnes intentions – Rapport PwC, 2014


PASSEZ AU CHAPITRE SUIVANT

# CHAPITRE 4 COMMENT CONCEVOIR UN PROGRAMME FONCTIONNANT À LA FOIS POUR LE PERSONNEL ET POUR L'ENTREPRISE ?

Pour limiter vos risques liés à l'information, téléchargez notre guide POUR PARTIR SUR DE BONNES BASES – Le b. a.-ba de la préparation face aux risques

IRON MOUNTAIN®

FR-RM-EXT-240215-001

0800 215 218 | ironmountain.fr