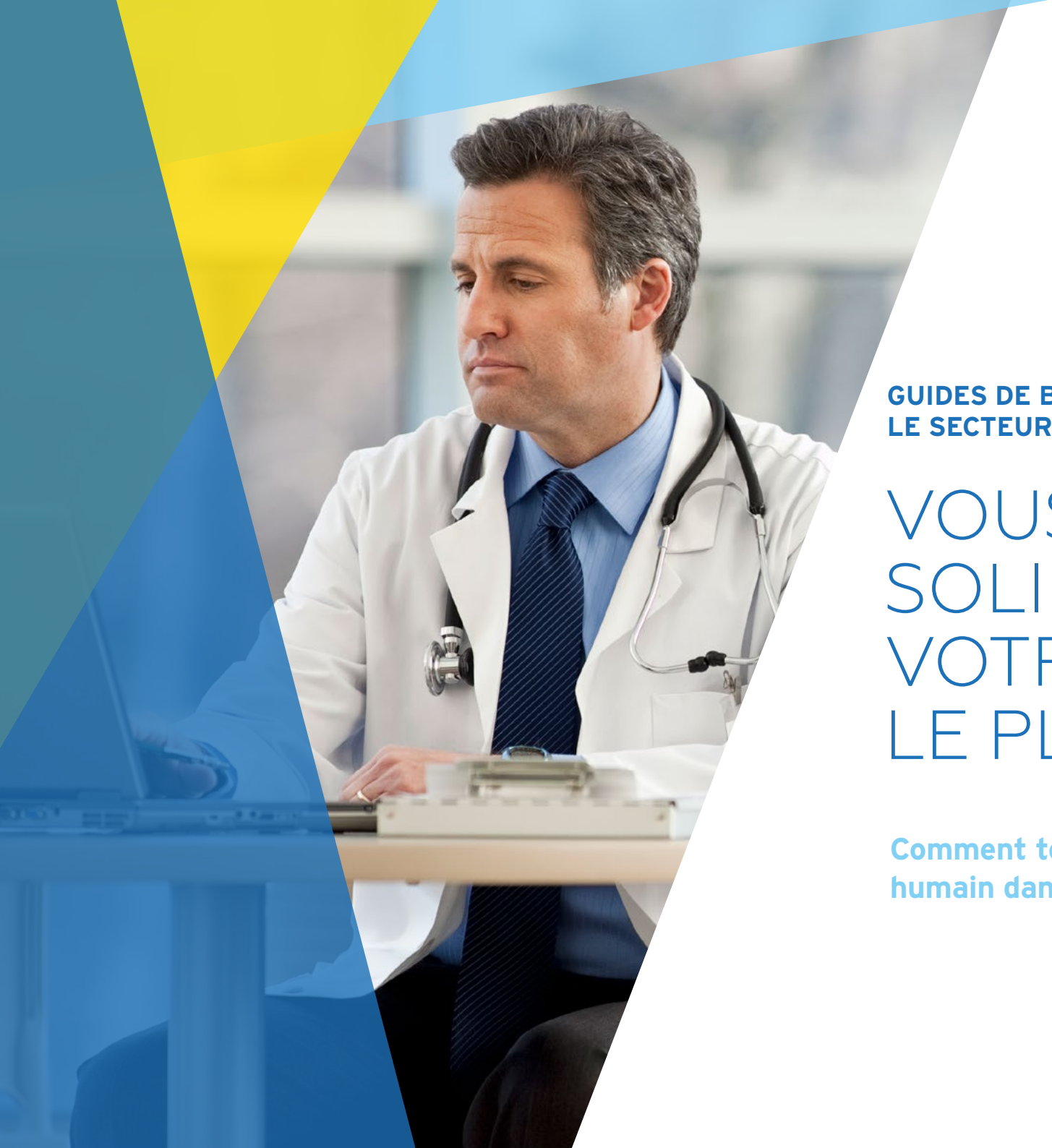


IRON MOUNTAIN®

GUIDES DE BONNES PRATIQUES POUR LE SECTEUR DE LA SANTÉ

VOUS ÊTES AUSSI SOLIDE QUE VOTRE MAILLON LE PLUS FAIBLE !

Comment tenir compte du comportement humain dans la gestion interne des risques

INTRODUCTION

Les turbulences de ces dernières années ont obligé les entreprises à repenser leurs stratégies de gestion des risques, en mettant l'accent sur la résilience à long terme.

Cela n'est nulle part plus évident que dans le secteur de la santé, où des cyberattaques de plus en plus sophistiquées mettent en danger les données confidentielles des patients. Parallèlement, les vulnérabilités se multiplient à mesure que les dossiers médicaux sont transférés sur des plateformes numériques, que la télésanté connaît un essor et que les dispositifs médicaux de l'internet des objets (IoT) deviennent de plus en plus courants. La capacité de servir les patients à distance et efficacement tout en gardant la sécurité de leurs informations et la conformité en tête n'a jamais été aussi critique.

LE SAVIEZ-VOUS ?

En mai 2021, une attaque par ransomware a **paralysé les systèmes informatiques** du service de santé irlandais, laissant la plupart des hôpitaux du pays sans ordinateurs pendant **plus d'une semaine**[1].

En 2020, une attaque par ransomware contre un hôpital en Europe a eu de **graves conséquences pour les patients**[2].

Comment protéger votre entreprise face à ces attaques croissantes ?

L'un des domaines clés souvent négligés est la menace interne. Bien que la plupart du temps involontaires, les comportements et les erreurs humaines coûtent de l'argent aux entreprises européennes, sans parler des atteintes à leur réputation. En ce qui concerne la gestion des risques, le secteur des services financiers est le plus touché.

Un récent rapport d'IBM estime le coût moyen d'une violation de données dans le secteur des soins de santé à **9,23 millions de dollars** par incident, soit plus que dans tout autre secteur[3].

C'est pourquoi Iron Mountain a commandé une étude pan-EMEA[4] mettant en évidence les domaines de gestion des risques que les organisations devraient prendre en compte en raison des faiblesses humaines - avec des résultats surprenants.

Vous trouverez ci-dessous des informations et des conseils pratiques sur la manière de gérer les risques au sein d'équipes hybrides et d'élaborer une stratégie commerciale résiliente.

1. Dix jours après une attaque par ransomware, le système de santé irlandais est en difficulté.
2. Un hôpital néo-zélandais doit faire face à une deuxième semaine de perturbations après une cyber-attaque de grande ampleur.
3. Rapport d'IBM sur le coût d'une violation de données, 2021.
4. Enquête réalisée en septembre 2021 par One Poll auprès de 11 000 employés dans 10 pays.

AU SOMMAIRE DE CE GUIDE :

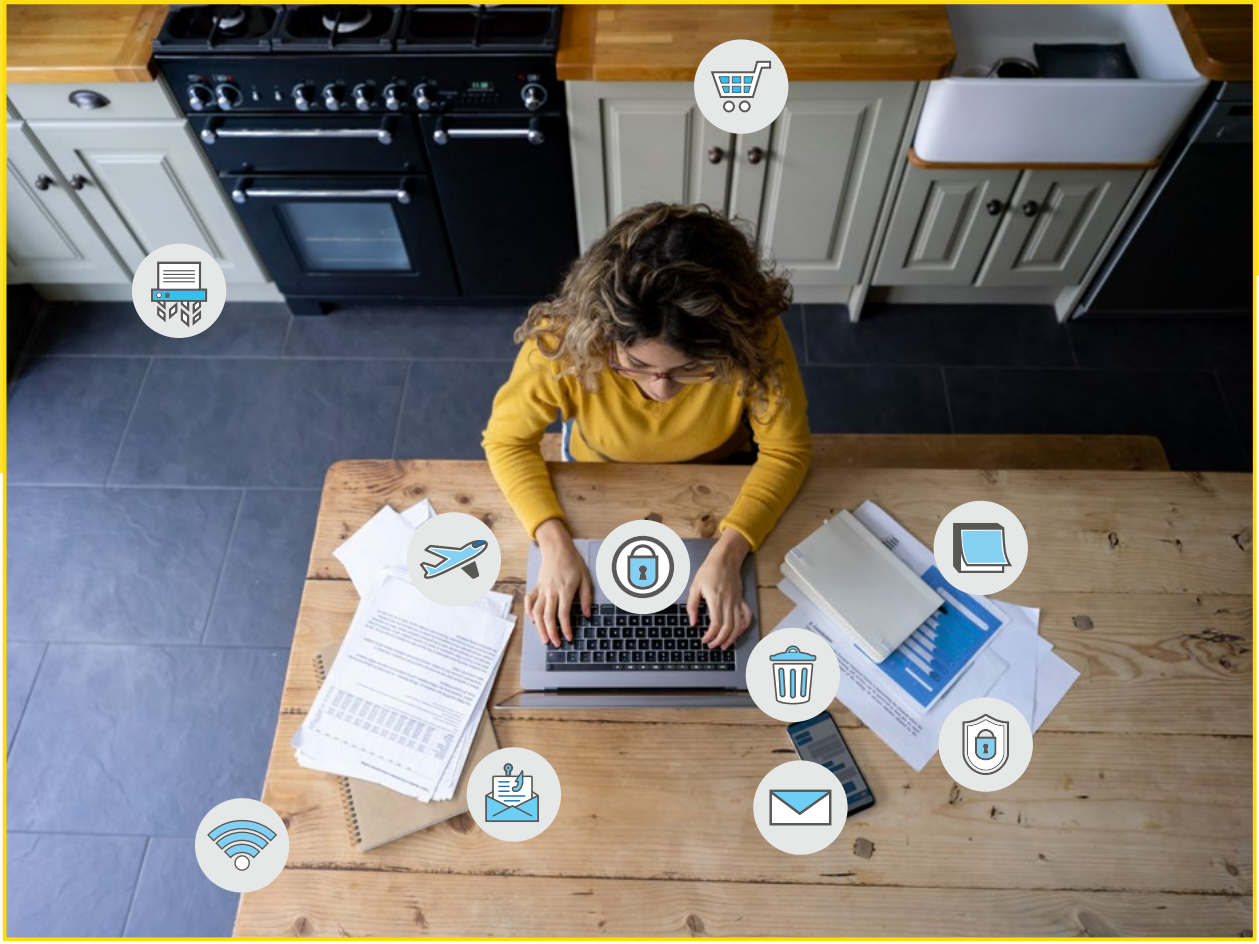
SOLUTIONS RAPIDES

1

Commençons par les fruits les plus faciles à cueillir.

Voici quelques vérités surprenantes sur notre façon de travailler - à la maison et au bureau.

Combien d'entre elles **avez-vous** commises ?



CLIQUEZ SUR LES ICÔNES POUR EN SAVOIR PLUS !

Heureusement, ces problèmes relativement simples peuvent être résolus. Pensez-y :

- Partager ces statistiques pour mettre en lumière le problème sans le montrer du doigt.
- Souligner l'importance d'un changement de comportement
- Mettre en évidence les outils, la formation et le soutien disponibles pour vous aider
- Rappeler la différence entre un risque calculé et un risque inutile
- Mettre à jour les politiques afin de garantir une compréhension maximale de la gestion des risques et une responsabilisation à cet égard.

CRÉER UNE CULTURE CONSCIENTE DU RISQUE

2

Si nous ne pouvons pas changer la nature humaine, nous pouvons changer la façon dont nous gérons les risques - tout en favorisant l'innovation - en créant une culture consciente du risque dès le départ.

Voici nos cinq étapes pour construire la résilience par la conception :

1 CHANGEZ L'ÉTAT D'ESPRIT DE VOTRE ENTREPRISE

LA RÉALITÉ :

Un employé sur trois (32 %) affirme avoir **commis une erreur "critique" au travail** et 14 % avoir pris un **risque qui aurait coûté** de l'argent à leur entreprise.

LA SOLUTION :

Commencez par donner à chaque employé les moyens de devenir un ambassadeur du risque, **en intégrant la sensibilisation au risque à votre culture**. Inculquez dans leurs mentalités qu'il s'agit d'une responsabilité fondamentale de l'employé. C'est l'affaire de tous et non de quelques-uns.

COCHEZ LES CASES AU FUR ET À MESURE QUE VOUS RÉVISEZ VOTRE PLAN STRATÉGIQUE !

2 REMODELEZ VOS POLITIQUES DE GESTION DE L'INFORMATION

LA RÉALITÉ :

La moitié (49 %) des employés considèrent qu'il **vaut la peine de prendre des risques au travail**, même si 25 % d'entre eux ont été **victimes d'escroqueries ou de phishing**.

LA SOLUTION :

Les organisations de santé ont mis en place des réponses d'urgence à la pandémie mondiale de Covid, mais elles sont désormais passées à des stratégies à long terme fondées sur le travail hybride. Pensez à **des politiques de gestion de l'information bien définies** qui s'appliquent aux employés de bureau, hybrides et/ou distants, ainsi qu'aux fournisseurs et aux sous-traitants.

Alors que les prestataires de soins de santé s'empressent de numériser les dossiers des patients, il est essentiel de garantir une **chaîne de possession complète** tout au long des processus de collecte, de transport, de numérisation et d'élimination...

3 ENCOURAGEZ UNE CULTURE DE SOUTIEN

LA RÉALITÉ :

51 % des personnes ont été **stressées par une erreur** commise au travail.

LA SOLUTION :

Il est prouvé que les environnements de travail hybrides favorisent la productivité, mais celle-ci peut être étouffée par le stress, qui est naturellement une préoccupation importante dans le secteur des soins de santé. Assurez-vous que vos **flux de travail sont conçus pour gérer les risques** et adaptés pour faire face à la complexité et au volume croissants des points de données. Envisagez de recourir à de nouvelles technologies dotées d'intelligence artificielle et d'apprentissage automatique pour **rationaliser et améliorer vos processus**, afin que votre personnel puisse se concentrer sur l'amélioration des soins aux patients et sur la gestion des listes d'attente en cas de pandémie.

Qu'est-ce que la 'résilience par la conception'

La résilience - ou la capacité de votre organisation à repousser les attaques - ne doit jamais être une réflexion après coup. Elle doit être intégrée à chaque étape de vos politiques et processus d'entreprise.

CRÉER UNE CULTURE CONSCIENTE DU RISQUE

2

Déploiement de solutions post-pandémie

Plus de la moitié (59 %) des gestionnaires de données auxquels nous avons parlé **ont acheté de nouveaux logiciels** pendant la pandémie et deux tiers (62 %) **ont mis en place des outils de partage** tels que Microsoft Teams. Ces outils doivent être intégrés aux programmes de gestion du cycle de vie des informations, notamment en **établissant des périodes de conservation pour les données non structurées**, telles que les discussions entre patients et les enregistrements de réunions, ainsi que des systèmes centralisés de gestion de la conformité et des politiques adaptés à l'environnement technologique plus complexe d'aujourd'hui.

4 FAITES ÉVOLUER VOS PROCESSUS

LA RÉALITÉ :

36 % sont plus **soucieux de la sécurité** des données professionnelles au bureau qu'à la maison.

LA SOLUTION :

Les consultations virtuelles et les dossiers hospitaliers numériques devenant rapidement la norme, des volumes de données toujours plus importants sont créés. Vous devez donc **repenser la gouvernance de l'information :** de la gestion des droits d'accès au partage des informations numériques, en passant par la conservation des données et leur destruction sécurisée, conformément aux exigences légales en vigueur. Dans un premier temps, **envisagez de créer une carte des données** pour comprendre comment les données entrent et sortent de votre entreprise.

5 RENDEZ VOS FORMATIONS PLUS MÉMORABLE

LA RÉALITÉ :

Alors que 60 % des gestionnaires de données affirment que **les sessions de formation** à la gestion des risques sont bien suivies, 36 % des travailleurs déclarent n'avoir jamais assisté à l'une d'entre elles.

LA SOLUTION :

Bien que vous ayez sans doute mis en place des modules de formation sur les risques, nos résultats indiquent qu'ils sont rapidement oubliés. Pour un meilleur impact, **rendez la formation plus attrayante, plus pertinente et plus accessible**, afin que les employés reconnaissent les opportunités quotidiennes et applique les connaissances acquises, car ils comprennent l'impact sur eux et leurs patients.

"Nous sommes tous humains et faisons des erreurs, donc le risque - par définition - est un facteur toujours présent au travail. Mais il n'est pas constant. Les nouveaux modèles d'entreprise, le travail hybride et la menace croissante des cyberattaques font qu'il est plus important que jamais de gérer efficacement les risques internes pour renforcer la résilience à long terme."

Sue Trombley, Managing Director of Thought Leadership, Iron Mountain

INTÉGRER LA "RÉSILIENCE PAR LA CONCEPTION" A VOTRE STRATÉGIE

3

"Une certaine prise de risque peut permettre à une organisation d'innover, mais le manque de sensibilisation aux dangers quotidiens peut éroder la résilience. Nous conseillons de donner à chaque employé les moyens de devenir un ambassadeur du risque en intégrant la sensibilisation au risque à votre culture. Cela crée un espace sûr dans lequel les individus peuvent innover et les organisations prospérer."

Sue Trombley, Managing Director of Thought Leadership, Iron Mountain

Selon notre enquête, **70 %** des gestionnaires de données européens estiment que tous les employés sont responsables de la gestion des risques.

Pour un impact durable, la résilience doit être intégrée à chaque étape de vos processus d'entreprise et renforcée par les actions quotidiennes de tous les employés. **C'est la résilience par la conception.**

Alors que les personnes du secteur médical s'efforcent de dématérialiser rapidement leurs opérations, il est important de comprendre que le risque de changements inattendus sur le marché est susceptible de subsister alors que nous continuons à nous remettre du ricochet du COVID-19.

C'est pourquoi **les solutions de travail hybride intégrant la "résilience par la conception"** sont essentielles à la prospérité à long terme. Des solutions qui, par exemple, permettent un accès sécurisé aux informations depuis n'importe où, rationalisent les flux de travail et aident à gérer efficacement l'ensemble du cycle de vie de vos données, quel que soit leur format ou leur type. Des solutions qui vous permettent **de libérer le potentiel caché de vos informations** et de les faire travailler plus efficacement et plus intelligemment pour l'organisation.

Pour vous aider à relever les défis de la gestion de l'information dans votre entreprise et pour discuter des solutions qui vous aideront à renforcer la résilience dans un monde de travail hybride, contactez l'équipe ou visitez ironmountain.com/fr/

À PROPOS D'IRON MOUNTAIN

Iron Mountain Incorporated (NYSE : IRM) offre des services de gestion de l'information qui permettent aux entreprises de réduire leurs coûts, de limiter leur exposition aux risques et d'éliminer les inefficacités en matière de gestion des données numérisées et sur support physique. Fondée en 1951, la société Iron Mountain prend en charge la gestion de milliards d'actifs informationnels, tels que données de sauvegarde et d'archives, documents électroniques, imagerie documentaire, documents professionnels, destruction sécurisée, pour les entreprises du monde entier. Visitez le site Web de la société à l'adresse www.ironmountain.fr pour obtenir des informations supplémentaires.

0800 215 218 | IRONMOUNTAIN.COM/FR

IRON MOUNTAIN®