PHYSICAL MEETS DIGITAL

Guide du paysage informationnel hybride d'aujourd'hui

IRON MOUNTAIN®

INTRODUCTION : NOUS NE SOMMES PAS ENCORE À L'ÈRE DIGITALE.

Oui, nous sommes plus connectés que jamais. La croissance exponentielle du nombre d'équipements connectés, qui devraient être trois fois plus nombreux que les humains d'ici 2021, nous en a convaincus. De plus, le volume total des données électroniques que les entreprises gèrent, sécurisent et exploitent est passé de 16 zettaoctets en 2016 à 33 zettaoctets fin 2018. Cependant, prétendre que nous sommes désormais dans un monde digital et que le monde analogique est derrière nous n'est pas ce que nous vivons actuellement.

En effet, les documents et les archives papier sont encore au cœur des opérations métier quotidiennes des entreprises. Peut-être cela changera-t-il un jour et que le bureau sans papier ne sera plus qu'une simple aspiration. Mais où en sommes-nous aujourd'hui ? Nous ne sommes pas entrés dans l'ère du numérique car toutes les entreprises sont tiraillées entre la fiabilité des supports physiques et le souhait de passer au tout digital.

Aujourd'hui, les responsables de l'information n'ont pas d'autre choix que de gérer deux sources de données hétérogènes, et souvent de plus en plus volumineuses, de manière globale et stratégique, de crainte d'être victimes d'une fuite de données, de violations de la conformité et/ou d'atteinte à la réputation de l'entreprise en raison d'un manque de responsabilité envers leur capital informationnel.

Le côté positif cependant est que maîtriser ce nouveau paysage informationnel est la seule façon pour les entreprises de :

- sécuriser et protéger leurs données critiques et sensibles
- se conformer aux normes du marché et réglementaires
- garantir la continuité de leur activité et
- tirer une véritable valeur métier de leurs données

- Comment faire pour gérer à la fois vos données physiques et numériques afin de piloter efficacement un programme de gestion de l'information à la fois fiable et conforme ?
- Comment savoir si vous tirez la meilleure valeur de vos données ?
- Et comment préparer votre entreprise au succès en adoptant un mode de travail plus digital ?

Cet e-book répondra à toutes ces questions.

Divisé en quatre sections et fruit de l'expérience d'experts du marché et de clients Iron Mountain, cet e-book propose des **pratiques recommandées testées et éprouvées pour contrôler, protéger et optimiser** les informations vitales pour l'activité de votre entreprise dans le paysage informationnel hybride d'aujourd'hui et de demain.

Transformation digitale

Découvrez pourquoi convertir les données physiques dans des formats numériques est indispensable pour éviter les nombreuses complications liées au paysage informationnel hybride contemporain.

Stockage hybride

Apprenez à stocker ces deux sources de données de manière stratégique pour améliorer l'accès aux données et leur visibilité et pour optimiser les coûts.

Sécurité

Familiarisez-vous avec des pratiques recommandées testées et éprouvées pour sécuriser votre capital informationnel contre l'ensemble du paysage des menaces, qu'il s'agisse de catastrophes naturelles inattendues ou de cyberattaques sophistiquées.

Conformité

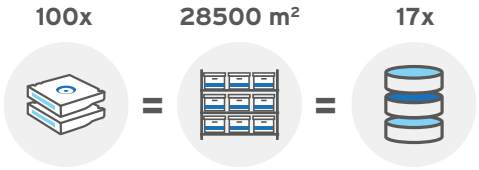
Informez-vous sur les toutes dernières contraintes du marché et de la réglementation pour que vos informations soient toujours gérées de manière éthique et conforme.

« Les deux facteurs de [la transformation digitale] : Productivité et nécessité d'exploiter les données plus rapidement et efficacement. »

Bill Meany, CEO d'Iron Mountain lors de son intervention « Avancer sur le chemin vers la transformation digitale » pendant le forum virtuel Physical Meets Digital ».

La **transformation digitale** est un atout majeur pour toutes les entreprises. Il s'agit d'une stratégie vitale pour maîtriser le nouveau paysage informationnel car passer de données physiques à des formats numériques épargne de nombreuses complications liées à l'environnement informationnel hybride et décousu d'aujourd'hui. En effet, plutôt que de gérer deux sources *volumineuses* de données hétérogènes, la transformation numérique vous rapproche d'une seule1 et améliore ainsi la visibilité et facilite l'accès.

Raisonnons de la manière suivante :



Au-delà de son impact sur la gestion de l'information elle-même, la transformation digitale offre d'autres avantages majeurs à toute l'entreprise.

Tout d'abord, la digitalisation des données vous permet de supprimer les processus et procédures manuels et fastidieux liés au papier et de rationaliser les flux de travail en back-office au sein de services aussi importants que les ressources humaines et la comptabilité fournisseurs ou clients. Cela permet aussi à vos collaborateurs de se concentrer sur des tâches à plus grande valeur ajoutée. De plus, avec une meilleure visibilité sur vos données, vous pouvez mieux les exploiter pour **prendre des décisions stratégiques**, une tendance qui va aller crescendo dans la mesure où de plus en plus de technologies de pointe et de solutions analytiques ayant besoin de données de qualité pour fonctionner correctement sont au cœur de vos processus métier.

En résumé, la transformation digitale garantit :

1. Une productivité accrue
2. Une plus grande capacité d'exploitation des données qui aide à la prise de décisions
3. De meilleures interactions avec la clientèle et
4. Un chiffre d'affaires supérieur

1. À noter qu'il est cependant impossible de supprimer tous les documents papier, du moins pour l'instant. En effet, vous devrez toujours satisfaire à des obligations légales ou du marché ou tout simplement conserver des versions papier pour la postérité de l'entreprise.

Mais quelles sont ces nouvelles technologies ?

Les paragraphes suivants décrivent ce qui, selon Iron Mountain, aura un **impact majeur** sur les entreprises dans les mois et années à venir. Vous intéresser aujourd'hui à la manière de gérer vos données vous permettra de les exploiter demain au maximum de leur valeur.

Cloud

Une stratégie multi-cloud permettant aux entreprises de choisir un support de stockage approprié (public, privé ou sur site) pour chaque cas d'utilisation spécifique (sauvegarde, reprise après un sinistre, stockage à long terme, etc.) est un atout majeur pour **organiser vos données** de manière sécurisée, accessible et rentable. Plus vous avez de contrôle sur vos données, plus vous avez de chances d'optimiser leur stockage.

EN SAVOIR PLUS ▷

Internet des Objets (IoT)

D'ici 2020, **50,1 milliards** d'objets devraient être connectés et générer des quantités de données extraordinaires. Se préparer dès aujourd'hui à ce flux massif facilitera le traitement de volumes de données encore plus gros.

Intelligence artificielle

Des volumes de données toujours plus importants ouvrent la voie à une **prise de décision automatisée** grâce à l'intelligence artificielle. Alors que l'IoT entraîne la création de centres gigantesques où sont stockées les données collectées, l'intelligence artificielle gère et extrait de la valeur de ces immenses réservoirs de données. Reconnaissance d'images statiques, classifications et balisage, maintenance prédictive, détection automatique de caractéristiques géophysiques et distribution du contenu sont quelques-uns des cas d'utilisation possibles. Plus le volume de données destiné à alimenter ces processus est important, plus ces derniers sont performants.

Solutions de protection de la vie privée et de sécurité

À mesure que nous avançons vers le nouveau paysage de la gestion de l'information, il est important de tenir compte de la manière dont vous **protégez vos données** contre tout type d'incident, qu'il soit d'origine naturelle ou humaine, qu'il s'agisse de cybermenaces basées sur du ransomware ou encore d'employés mécontents ou malveillants.

Blockchain

La transition du physique vers le digital justifie de se préoccuper de garantir l'authenticité des formats numériques. En effet, les formats numériques sont plus facilement modifiables et copiables que leurs alter egos physiques.

C'est là qu'intervient la technologie de blockchain que les professionnels du Records Management se doivent impérativement de maîtriser en raison de son **rôle précieux** pour sécuriser et authentifier la propriété intellectuelle à moindre coût et plus efficacement. En **intégrant l'authentification** au document lui-même et en utilisant un système de suivi en boucle fermée qui empêche d'altérer ou de modifier un document, la technologie de blockchain permet à des personnes qui ne se connaissent pas de s'investir dans des transactions de confiance en ayant l'assurance de l'intégrité des actifs qui sont échangés.

Transformation digitale : Étude de cas

Par quoi commencer ? Comment opérer la transition d'un maximum de données physiques vers des formats numériques pour que votre entreprise gagne en rapidité et en souplesse ? Comment rationaliser vos flux de travail ?

Assureur d'envergure mondiale, **Generali** se posait les mêmes questions. L'entreprise était prisonnière de flux de travail manuels et papier qui pénalisaient sa productivité et retardaient son objectif de transformation digitale. Les coûts devenant trop importants, il lui a fallu investir dans l'automatisation.

« Generali a commencé son voyage vers le digital en 2008. Nous avons donc lancé ce projet il y a 10 ans. Mais sous l'impulsion des nouvelles technologies, davantage d'informations électroniques natives sont arrivées directement sur des plateformes nous permettant d'exécuter des actions métiers simples. Il nous fallait intégrer cette transformation de flux entrants. L'avenir de notre programme passait donc par l'intégration et l'introduction d'encore plus d'automatisation et d'intelligence artificielle pour que nos équipes puissent générer davantage de valeur ajoutée. Notre objectif était d'automatiser, d'améliorer les performances et d'offrir un service supérieur, » déclare Patrick Zakrzewski de Generali France.

Dans les mois qui suivirent, Iron Mountain s'est installée au siège de Generali pour étudier les processus quotidiens du géant de l'assurance et proposer une solution permettant de scanner le maximum de documents physiques existants, et donc de les soustraire aux processus traditionnels, et aussi de convertir automatiquement les documents récemment créés dans des formats numériques.

Le résultat ? Grâce aux projets numériques et aux flux sans papier, Generali a renforcé sa productivité et ses performances et simplifié massivement la gestion des données tout en optimisant son fonctionnement général.

REGARDER LE RÉCIT ▷

« Nous avons tous déjà entendu parler de différentes versions du sans papier en 2010 ou du digital à l'horizon 2020 ; (...) Parfois les gens pensent que c'est l'un ou l'autre, que c'est avec ou sans papier, autrement dit du numérique. Cependant, en réalité, nous constatons que nous devons gérer à la fois des données physiques et digitales de manière plus unifiée pour renforcer nos performances, réduire les coûts de gestion de l'information, garantir la sécurité et la conformité et aussi définir des politiques à l'échelle de l'entreprise. »

Charlotte Marshall, Senior Vice President, General Manager Western Europe, Iron Mountain au cours de son intervention « Franchir le gouffre entre les données physiques et les données numériques » pendant le forum virtuel Physical Meets Digital ».

Pour la digitalisation des données physiques, il est important de prendre en compte le lieu de stockage de ces deux types de données.

- Qu'adviendra-t-il des documents physiques convertis en numérique ?
- Où les stockerez-vous ?
- Pourrez-vous les détruire ?
- Quid des données digitales ?
- À qui appartiendront-elles ?

Cela se complique un peu.

Mais comme pour tout, la réponse est... ça dépend. Tandis que certains **documents papier** peuvent être voués à la destruction, la plupart d'entre eux doivent cependant être conservés et stockés pour des raisons légales, réglementaires ou liées à la poursuite de l'activité. Il est toujours possible d'avoir des armoires remplies de dossiers papier dans votre bureau, mais si vous souhaitez réaffecter les locaux ou les sécuriser contre des risques tels qu'un incendie, une inondation, l'humidité et contre les accès non autorisés, un stockage hors site peut alors s'avérer être le choix le plus raisonnable.

D'autre part, concernant les **données digitales**, la réponse dépend à la fois de l'utilisation souhaitée pour ces données et de l'infrastructure sur site. Les données qui doivent être accessibles le plus rapidement possible sont davantage destinées au Cloud ou à des serveurs sur site, à condition que ces serveurs puissent gérer des volumes de données importants. Dans le cas contraire, mieux vaut alors opter pour du stockage hors site mutualisé. Quant aux données plus anciennes, moins sollicitées ou de sauvegarde, elles peuvent être stockées hors site pour une solution plus économique. La plupart du temps, la stratégie de stockage de données la plus efficace est une approche multi-solutions et hybride où les données sont segmentées en fonction de critères tels que la facilité d'accès, les obligations légales et du marché, les normes de **sécurité** et de chiffrement, les **sauvegardes** et les temps d'arrêt avant **reprise**, etc. Elles sont ainsi hébergées sur la solution de stockage la plus adaptée. La solution retenue dépend entièrement de la stratégie de l'entreprise.

EN SAVOIR PLUS ▷

Concernant le stockage à la fois des données physiques et digitales, d'autres facteurs entrent en jeu, à savoir la sécurité et la conformité. Pour illustrer notre propos concernant le stockage physique et de données, voici un exemple concret de transformation digitale et de décisions de stockage associées :

Selon Liam Kennedy, Directeur des Opération Adjoint du **West Birmingham Hospitals NHS Trust**, la conservation d'archives sur site était devenue un fardeau. Les salles d'archives ont commencé à envahir des espaces qui auraient pu être utilisés à meilleur escient. Le suivi des documents et des archives faisait perdre un temps précieux aux employés qui devaient fouiller dans les armoires et dans les salles de stockage. Pire encore, Liam Kennedy craignait que si rien n'était fait pour améliorer la situation, les soins aux patients pourraient en pâtir. Pour les hôpitaux West Birmingham, les documents physiques auparavant pratiques et économiques constituaient une entrave à leur mission de déployer un système de soins mondialement reconnu.

Aussi, avec l'assistance d'Iron Mountain, ces établissements ont mis au point un **plan de transformation digitale** destiné à alléger leur charge de données physiques et à faciliter la recherche et la récupération de documents. Les dossiers patients furent donc **numérisés** et **stockés** dans le Cloud pour réduire la durée de recherche d'informations et faciliter la **gouvernance des informations** qu'ils détenaient, ce dernier point revêtant une importance capitale pour un système hospitalier devant se conformer à une réglementation stricte en matière de protection de la vie privée. Les archives physiques furent donc externalisées, ce qui a permis de **réaffecter de l'espace** auparavant encombré par des armoires remplies de documents.

Au final, les établissements se sont délestés de la gestion des archives physiques et digitales et ont réalisé des **économies** annuelles entre 280 000 et 335 000 euros.

Conclusion : une stratégie de **stockage hybride** est la solution idéale pour gérer un paysage informationnel hybride.

« La complexité est grande dans le domaine de la sauvegarde des actifs [transformés numériquement]. Et comme nos clients essaient d'établir une passerelle entre les méthodes traditionnelles de stockage et le digital, il est important de savoir comment maintenir une bonne connexion [à vos données], sachant que les conditions de stockage d'un carton sont bien différentes de celles de données à conserver dans un data center. »

John Wegman, Directeur Général région DACH, au cours de son intervention « Emporter l'équipement approprié pour protéger votre entreprise et préserver votre héritage » pendant le forum virtuel Physical Meets Digital ».

D'une manière plus générale, les données, et a fortiori la continuité de l'activité, sont à la merci des **cybermenaces et des sinistres**. La première catégorie de menaces est le fait d'un ou plusieurs acteurs malveillants qui cherchent à divulguer, modifier, paralyser ou dérober des données digitales ou encore à y accéder de manière non autorisée par le biais de ransomware, de codes malveillants ou d'opérations d'hameçonnage (phishing), etc. Quant à la deuxième catégorie, il s'agit d'un terme général qui englobe tous les sinistres naturels ou leurs conséquences, qu'il s'agisse par exemple d'un tremblement de terre ou des ravages de l'humidité pouvant rendre les données physiques irrécupérables et inutilisables. Les sinistres peuvent prendre bien d'autres formes, notamment celle d'un incendie pouvant détruire un serveur ou d'un employé mécontent qui cambriole une armoire de documents pour y voler des données sensibles. Il y a d'autres problèmes de sécurité à affronter, mais le bon sens voudrait que l'on commence par **planifier la protection** des données physiques contre les sinistres et des données digitales contre les cybermenaces.

Même si cela tombe sous le sens, mieux vaut le rappeler. En effet, dans le cadre de la transformation digitale, il est facile de se perdre dans les méandres du processus et de ne plus considérer la sécurité comme une priorité. Il est préférable d'anticiper et de se protéger plutôt que de subir les conséquences d'une mauvaise sécurité.

7,600 euros/h

Le coût moyen d'un arrêt lié à la déconnexion des données nécessaires à votre activité quotidienne s'élève à 7600 euros par heure. À vous de voir s'il s'agit d'un risque acceptable.

LIRE UN ARTICLE ▷

Sécuriser les données physiques

Comme nous l'avons déjà indiqué, **sécuriser les données physiques** consiste essentiellement à prévenir les dommages liés à un sinistre imprévu, qu'il s'agisse d'un incendie, d'une inondation, d'une invasion d'insectes, d'humidité ou d'un problème de tuyauterie. Il est donc primordial de travailler avec des fournisseurs de solutions de conservation qui offrent une protection environnementale de facto ou intégrée.

Les principaux **critères de sélection** d'un fournisseur sont notamment des locaux éloignés de zones inondables, une surveillance 24h/24, 7j/7 et un système de lutte contre l'incendie et la régulation de l'environnement. Il faut également garder à l'esprit que les archives physiques devront parfois être conservées pendant plusieurs décennies. Il est donc important de s'intéresser à la capacité d'un site de stockage de garantir l'intégrité des archives physiques dans un avenir proche et lointain.

Mais quid des préoccupations non liées à un sinistre ? Trois autres facteurs de sécurité doivent être pris en compte :

1

Aussi évident que cela puisse paraître, il faut se préoccuper de la sécurité générale. Il y a des chances pour qu'un fournisseur de stockage qui offre une **protection contre les risques environnementaux** propose aussi des protocoles qui garantiront que seules les personnes autorisées auront accès à vos informations. Néanmoins, il est important de s'assurer que vos données sont à l'abri des regards indiscrets.

2

Nous avons évoqué la sécurité de vos documents physiques sur un site de conservation hors site, mais pas pendant leur transport. Les **risques de perte et de vol** d'informations confidentielles étant à leur pic pendant leur transport, il est vital de veiller à ce que le transport utilisé comporte des protocoles de sécurité, des systèmes de climatisation, un suivi et une chaîne de traçabilité auditable.

3

Beaucoup de vos données physiques ne sont peut-être pas au format papier, mais elles existent sur d'autres supports analogiques (bobines de films, CD, DVD, etc.) qui peuvent se dégrader avec le temps et finir par devenir inutilisables. Il est important de confier votre stockage à un fournisseur capable de convertir, récupérer et diffuser vos actifs dans le format de votre choix, ce qui **garantira une disponibilité** ad vitam æternam.

Sécuriser les données digitales

Même si cela peut sembler défaitiste, en réalité, il est quasiment impossible d'empêcher des cyberattaques. Ces menaces contemporaines sont trop sophistiquées et les points d'entrée dans les entreprises sont trop nombreux pour qu'une quelconque solution de prévention puisse être efficace 100% du temps.

Même un taux de succès de 99,9999% n'est pas suffisant. En effet, une seule faille suffit pour qu'un ransomware, un malware ou un programme d'hameçonnage cause des dommages importants voire irréversibles à une entreprise.

LA RÉALITÉ DES CYBERATTAQUES

Le **coût moyen d'une compromission de données** continue de grimper. L'estimation actuelle est de **3 millions d'euros**.

Une étude récente portant sur **4100** entreprises européennes et américaines a révélé que **près de la moitié** d'entre elles avaient rapporté une **faille au cours de l'année précédente**.

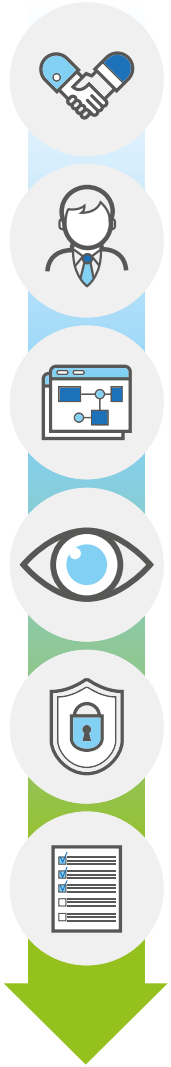
La durée moyenne pour **détecter** une faille et y réagir est de **197 jours**. Une fois détectée, **69 jours** supplémentaires sont en moyenne nécessaires pour **contenir cette faille**.

Aussi, concernant vos données digitales, il est préférable de raisonner aussi bien en termes de prévention des cyberattaques que de neutralisation d'une attaque devenue inévitable.

Prévention

Pour renforcer vos efforts de prévention, une **puissante gouvernance en matière de données** est indispensable. Elle peut vous aider à aligner vos stratégies de gestion des données sur vos efforts de cybersécurité, à appliquer des contrôles pour atténuer les risques, à réduire l'impact des failles de sécurité et à améliorer l'affectation et la gestion des ressources de sécurité. Il vous faut comprendre comment les données sont collectées, utilisées et acheminées à travers votre entreprise et également veiller à les protéger tout au long de leur cycle de vie.

Aspects importants d'un cadre de gouvernance des données :



- Adoption par l'équipe dirigeante.
- Désignation d'une personne clairement responsable de la cybersécurité dans votre entreprise.
- Politiques et procédures claires en matière de gestion de données.
- Supervision du programme pour garantir la conformité.
- Appréciation par les employés des risques et de leurs responsabilités. Une puissante culture de la cybersécurité exige des comportements cohérents et l'adhésion aux politiques.
- Plan de cyber-réponse impliquant de se préparer à un piratage et d'avoir un plan opérationnel en cas de besoin.

De plus, la sécurité physique est indispensable pour empêcher tout accès non autorisé ainsi qu'un accès physique et des dommages à vos systèmes. Une certaine forme de contrôle traditionnel du réseau et des systèmes, de même que des firewalls, une prévention des intrusions et des mesures de contrôle d'accès, sont nécessaires.

Atténuation

Lorsque le pire se produit et que vos données sont inaccessibles à cause d'une cyberattaque ou d'un datacenter à l'arrêt, des **solutions de sauvegarde et de reprise après un sinistre** peuvent vous aider à faire basculer votre environnement principal vers un environnement de secours pour assurer la continuité de votre activité en cas de problème grave.

Quelques avantages des solutions de sauvegarde et de récupération :

Détection du ransomware

Le ransomware, ou logiciel de rançonnage, modifie systématiquement les fichiers en les chiffrant. En supervisant la sauvegarde en cours et en surveillant toutes les modifications, il est possible de détecter une attaque potentielle.

En effet, une analyse permet de détecter toute modification par rapport aux sauvegardes antérieures. Si le scan détecte un chiffrement de masse, un style de chiffrement qui ne correspond pas aux normes acceptables ou qui est généralement utilisé pour du **ransomware**, une alerte signale qu'une attaque potentielle est en cours. Des sauvegardes antérieures saines peuvent ainsi être utilisées pour recouvrer un système intègre.

Fonctionnalités de restauration rapide

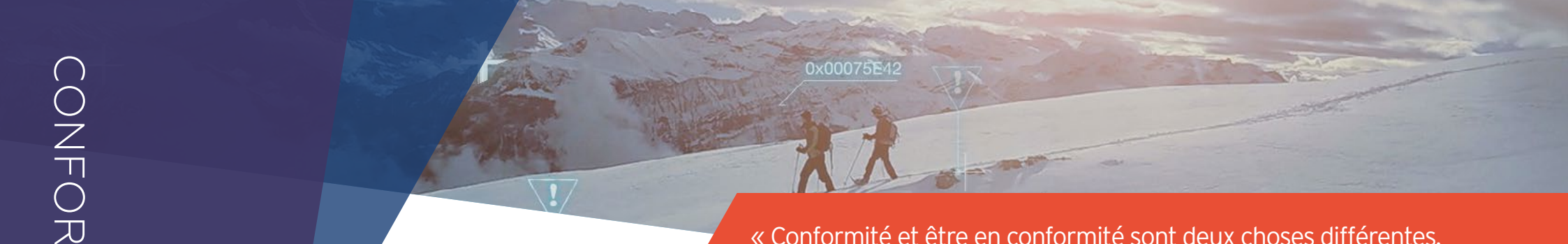
En cas de panne non planifiée, des fonctionnalités de **récupération de pointe** permettent de basculer facilement vers un environnement secondaire le temps que votre environnement principal soit à nouveau disponible, le tout avec un temps d'arrêt réduit au minimum.

Récupération après une attaque par ransomware

Une machine compromise **chiffrera les fichiers utilisateurs** et exigera une rançon pour fournir une clé permettant de déverrouiller le système. Pire encore, ce chiffrement peut s'étendre à travers le réseau et infecter d'autres machines, ce qui impactera sérieusement l'activité de l'entreprise. Plutôt que de payer une rançon, déployer une version antérieure sur les systèmes affectés au moyen d'une solution de reprise après un sinistre permet d'éviter toute attaque.

Options de reprise après un sinistre (DR) en local

Des appliances locales peuvent aider à sauvegarder des serveurs physiques et virtuels. En cas d'incident, vous pouvez exécuter vos données en local sur l'appliance ou dans le Cloud pendant la résolution du problème puis restaurer la configuration sur une machine Bare Metal, une solution sans disque ou dans le Cloud afin que vos données critiques restent disponibles.



« Conformité et être en conformité sont deux choses différentes. Aussi, avoir un programme qui démontre que vous faites tous les efforts nécessaires est vraiment important, plus particulièrement vis-à-vis de toutes les contraintes réglementaires, le RGPD n'étant qu'une des nouvelles réglementations auxquelles nous devons nous conformer au niveau global. »

Larry Jarvis, SVP, Chief Information Security Officer, Iron Mountain, lors de son intervention « Naviguer à travers les périls de la sécurité, de la conformité et de la gouvernance de l'information » pendant le forum virtuel Physical Meets Digital ».

Dans la section précédente, nous avons abordé les éventuelles répercussions négatives d'un sinistre accidentel ou d'une cyberattaque. Cependant, tout cela n'est rien ou presque par rapport aux conséquences d'une seule violation de la conformité.

EN SAVOIR PLUS ▷

Prenons l'exemple du **RGPD**. Dans le cadre de ce règlement, les autorités européennes chargées de superviser la protection des données disposent de larges pouvoirs d'investigation et de répression. Elles peuvent notamment envoyer des **avertissements pour non-conformité, réaliser des audits** d'entreprises hébergeant des données personnelles de résidents européens, exiger une **remédiation** spécifique dans un délai donné, ordonner la **suppression** de certaines données ou encore **suspendre les transferts de données** vers un pays tiers. Toutes vos obligations dans le cadre du RGPD sont consultables ici.

Tout le monde s'accorde sur le fait que le RGPD est la seule législation au monde aussi étendue et sévère et qui donne un bon aperçu des conséquences pour votre entreprise en cas de non-conformité. Et à l'heure où la **confidentialité des données** est une préoccupation croissante, d'autres réglementations du même genre verront probablement le jour dans un avenir plus ou moins proche. La seule chose qui soit certaine est que nous ne ferons pas marche arrière.

Les entreprises doivent donc se tenir prêtes et maîtriser les données personnelles qu'elles possèdent. En outre, elles doivent s'assurer que ces données sont **gérées de manière responsable et éthique** et que ces dernières sont uniquement utilisées aux fins prévues, tout en veillant à ce que seuls les collaborateurs autorisés puissent y accéder.

Les pages suivantes vous expliquent comment y parvenir.

Gérer les données pour garantir votre conformité

Pour assurer la conformité de votre entreprise, l'une des priorités est de gérer les données tout au long de leur cycle de vie, depuis leur création jusqu'à leur destruction.

Le **volume de données toujours plus important**, et plus particulièrement de données digitales, est en train de poser de nouveaux défis aux équipes informatiques, aux responsables de la conformité ainsi qu'aux départements juridiques qui doivent satisfaire aux exigences de conformité et répondre aux demandes de découverte électronique. Les instances réglementaires et juridiques ont bien peu de patience avec les entreprises incapables de réagir rapidement

Un plan de gestion du cycle de vie des données intègre des stratégies, des technologies et des processus qui permettent à la Direction informatique de répondre aux exigences en matière de conformité et de découverte électronique grâce aux moyens suivants :

Définir **où stocker** les données à mesure qu'elles évoluent dans leur cycle de vie (production, sauvegarde, reproduction, archivage ou destruction).

S'assurer que les données sont correctement **balisées, catégorisées et indexées** pour être facilement localisées le moment venu, même si elles n'ont pas été utilisées depuis plusieurs années.

Veiller à ce qu'une fois localisées, les données soient **consultables facilement et sans délai**, que ce soit sur site, dans le Cloud, dans un coffre de conservation des bandes hors site ou ailleurs.

Définir des politiques et des procédures applicables pour une **conservation et une destruction des données** conformes à la réglementation et fournir aux avocats et aux juges la preuve que les données qui leur sont communiquées sont complètes et non altérées.

Conseils pour une conformité optimale

La conformité de l'entreprise est un sujet trop spécifique et vaste pour être abordé en détails dans cet e-book. Néanmoins, voici quelques pratiques recommandées en guise d'introduction.

1

Conserver, sécuriser et éliminer

Savoir **quoi conserver**, pendant combien de temps et comment stocker est un véritable défi pour un grand nombre d'entreprises. Et en matière de conformité, un seul faux pas peut avoir des conséquences à la fois importantes et coûteuses. Mais vous devez néanmoins faire la distinction entre données critiques et données standard parmi toutes les informations que vous générez et diffusez chaque jour.

Pour ce faire, la meilleure solution consiste à missionner le **conseiller juridique** de votre entreprise pour qu'il développe un programme de conservation à la fois formel et justifié qui concerna les informations au format papier et numérique. Cette politique devra définir avec clarté ce qui doit être conservé, et pendant combien de temps, et ce qui doit s'appliquer à travers toute l'entreprise. Cependant, mettre en place dès aujourd'hui ce processus fastidieux paiera sur le long terme car il permettra à votre entreprise d'atténuer les risques financiers et réputationnels en cas de problèmes, notamment l'échec d'un audit ou la divulgation accidentelle d'informations sensibles.

2

Mieux gérer les archives électroniques

Cela fait si longtemps que le papier est la norme que vous avez probablement déjà déployé des **processus de conservation et de découverte** pour ce type d'archive. Mais quid des informations électroniques ? L'activité des entreprises étant toujours plus électronique, vos politiques doivent également tenir compte des données dans ce format.

Veillez à ce que toutes les informations électroniques, peu importe où elles se trouvent (postes de travail, serveurs, bandes de sauvegarde, équipements mobiles, clés USB, etc.), figurent bien dans votre **programme de conservation**. Définissez clairement les informations considérées comme des archives et **développez des politiques et des procédures** pour gérer de manière cohérente et sécurisée les gels des archives en cas de litige ainsi que la destruction de ces informations en fin de période de conservation.

EN SAVOIR PLUS ▷

3

Garantir une sécurité de bout en bout

Protéger l'information en permanence est essentiel pour éviter les risques. Mais lorsque vous ne savez pas lorsqu'une archive change de site, si elle est mise dans un carton ou transférée sur un support de bande, assurer sa sécurité à long terme peut constituer un véritable défi.

Pour résoudre ce casse-tête, assurez-vous que vos flux de travail intègrent une chaîne de traçabilité auditable qui renseigne sur tous les mouvements d'une archive spécifique. Ainsi, vous saurez toujours où se trouve une archive à un moment donné. En renseignant la chaîne de traçabilité de la sorte, vous serez en mesure de garantir en permanence la sécurité de vos archives les plus précieuses, ce qui vous protégera contre toute faille de **sécurité de l'information** accidentelle et contre les amendes et pénalités associées.

EN SAVOIR PLUS ▷

4

Adopter une approche programmatique

Le paysage réglementaire d'aujourd'hui évolue à un rythme effréné. Même s'il est important d'avoir un ensemble complet de **politiques de gestion des documents et de l'information (GDI)**, son efficacité dépend de l'investissement des personnes chargées de les appliquer, mettre à jour et communiquer à travers votre entreprise. Et sans la bonne dose de responsabilité, vos activités quotidiennes peuvent pâtir de lacunes critiques, ce qui peut entraîner la divulgation non autorisée ou la destruction d'informations sensibles.

Pour minimiser ces risques, vous devez envisager la gestion de l'information sous la forme d'un **programme complet** défini par des politiques et des procédures gérées par un individu spécifique, avec le renfort d'un **comité de direction** pouvant définir et imposer des responsabilités à travers l'entreprise. En désignant les bonnes personnes et les bons processus pour auditer ce programme, vous pourrez savoir si ce dernier est en phase avec toutes les réglementations appropriées. Intégrer de cette manière la responsabilité à vos processus de gestion de l'information vous aidera considérablement à renforcer l'état de conformité de votre entreprise.

CONCLUSION

S'il y a bien une chose que vous devez retenir de la lecture de cet e-book, c'est que le monde d'aujourd'hui n'est pas encore entré dans l'ère numérique.

Le monde actuel ne sait pas faire sans le papier. Il n'est même pas économe en papier. D'énormes volumes de données physiques et digitales ont créé un paysage informationnel unique et sans précédent, une **ère hybride** en quelque sorte. Et pour garantir l'intégrité des informations de leur entreprise, les responsables de l'information doivent pouvoir **gérer et sécuriser l'ensemble des données et aussi en tirer de précieux renseignements.**

Pour ce faire, ils doivent :

1. Procéder à la **transformation digitale** chaque fois que possible pour se rapprocher toujours plus d'une certaine maturité digitale et s'éloigner des sources de données hétérogènes et difficiles à gérer.
2. Étudier attentivement les différentes formules de **stockage** pour renforcer la visibilité et l'accès à leurs informations physiques et digitales.
3. Garantir la **sécurité** de leurs données pour protéger ces dernières contre toute une série de menaces, qu'il s'agisse d'une inondation, d'un incendie ou encore d'attaques via du ransomware ou du malware.
4. Garantir la **conformité** à une réglementation qui évolue sans cesse pour protéger leur entreprise contre des amendes et des dommages à sa réputation.

À PROPOS D'IRON MOUNTAIN

Fondé en 1951, Iron Mountain Incorporated (NYSE : IRM) est le spécialiste mondial des services de stockage et de gestion de l'information. Avec plus de 225 000 clients qui lui font confiance à travers le monde et des installations dont la surface cumulée atteint plus de 8 millions de m^2 avec 1450 implantations dans plus de 50 pays, Iron Mountain conserve et protège des milliards d'actifs de valeur, y compris des documents vitaux pour l'activité de l'entreprise, des données hautement sensibles ainsi que des artefacts culturels et historiques. Proposant des solutions de gestion de l'information, de transformation numérique, de stockage et de destruction sécurisés, ainsi que des services de centres de données, Cloud et de stockage d'œuvres d'art et de logistique, Iron Mountain aide ses clients à réduire les coûts et les risques, à se conformer à la réglementation, à accélérer la reprise après un sinistre et à faciliter un mode de travail plus numérique. Pour en savoir plus, rendez-vous sur www.ironmountain.fr.

IRON MOUNTAIN®

NOUS PROTÉGEONS CE QUI A LE PLUS DE VALEUR POUR VOUS