

Entreposage en voûte de bandes hors site**GUIDE D'AMÉLIORATION DE VOS PRATIQUES D'ENTREPOSAGE DES BANDES****PROTECTION DES DONNÉES : UNE STRATÉGIE S'IMPOSE**

Plus que jamais, il est essentiel que les entreprises adoptent des pratiques de gestion des médias qui sont fiables et uniformes tout en s'appliquant à toutes les unités fonctionnelles. Ce sont des procédures qui devraient s'intégrer à un plan-cadre de gestion de documents complet et conforme.

Les entreprises qui adoptent un modèle de planification bien structuré ont l'occasion de consolider leur marque en réduisant leurs risques : perte de leur information, divulgation fortuite et interruption survenant en raison de pannes soudaines. Dans l'ensemble, l'efficacité et l'avantage concurrentiel s'en trouvent améliorés.

Depuis des dizaines d'années, Iron Mountain collabore avec un grand nombre des plus grandes entreprises de par le monde en vue de concevoir, de planifier et de mettre en place des stratégies de protection des données *de bout en bout*. Le document qui suit fait ressortir de nombreuses pratiques exemplaires et techniques éprouvées de consolidation de toutes les phases et étapes que comportent les activités progressives de sauvegarde des données.

PROCÉDEZ À UNE ANALYSE DES RISQUES

Sur le plan *stratégique*, il serait utile au départ de vérifier chacune des étapes de votre processus de sauvegarde en vue d'y déceler les failles qui pourraient mettre la sécurité en péril. Par exemple, les boîtes et les bandes sont-elles laissées sans surveillance? Existe-t-il une procédure stricte assurant la chaîne de possession de bout en bout de vos bandes de sauvegarde? Les données

sont-elles sauvegardées et transportées sous une forme non chiffrée et clairement lisible? Conservez-vous vos bandes dans des lieux physiques distincts du centre de données afin de les protéger en cas de sinistre?

Ce genre de vulnérabilité est facile à déceler et à éliminer. Idéalement, cette analyse stratégique doit être menée par une équipe de vérification interne ou par un tiers externe. Vous pouvez même comparer cette analyse à vos pratiques réglementaires en vue d'évaluer comment le centre de données est configuré pour exécuter les processus de sauvegarde en toute exactitude.

DÉTERMINEZ QUELLES SONT LES DONNÉES SENSIBLES

Les lois portant sur le respect de la vie privée relèvent constamment le niveau de vigilance qui doit avoir cours dans les entreprises conservant des données personnelles. Ces lois contiennent en outre de plus en plus d'obligations en matière de divulgation relativement à l'information non publique et confidentielle. Il est important de bien repérer et de classer séparément ces fichiers, ces bases de données, et ces différents formats dont la sensibilité est suffisante pour justifier le chiffrement. Déterminez également l'emplacement de ces données. Il arrive souvent que les données existent en double dans l'entreprise. Mettez en place des politiques et des procédures permettant de savoir à tout moment où résident les données. Par exemple, certaines entreprises ont des données stockées à la fois sur des ordinateurs portatifs et sur un lecteur du réseau ou dans un dépôt de données de sauvegarde accessible par ordinateur personnel.

CHIFFREZ VOS DONNÉES

En fait, il est fort probable que presque toutes les copies de sûreté sur bande contiennent des données essentielles, sensibles ou confidentielles. Même si l'enregistrement chiffré des sauvegardes fait augmenter légèrement les coûts et prend plus de temps, les pratiques exemplaires actuelles exigent des entreprises qu'elles chiffrent toutes les données faisant partie des copies de sûreté. En fin de compte, si l'on compare les coûts du chiffrement aux risques potentiels d'une atteinte à la sécurité et à la probabilité qu'une telle atteinte survienne, il est économiquement pertinent de mettre en oeuvre une solution de chiffrement globale.

ADOPTÉZ UNE APPROCHE DE SÉCURITÉ À MULTIPLES NIVEAUX

Au moment même où les entreprises se soucient d'appliquer aux opérations financières sensibles des mécanismes régulateurs comportant des autorisations multiples, la prudence recommande l'application de mesures semblables au processus de sauvegarde des données. Faites en sorte que la personne qui crée la bande de sauvegarde *ne soit pas* la même qui confirme que la copie de sûreté a été placée dans le bon conteneur destiné à l'entreposage hors site. Si la sauvegarde est faite par une seule personne, une deuxième doit la vérifier. Cette manière de faire permet d'éliminer tout risque de défaillance.

- **Authentification.** Appliquez une authentification à multiples niveaux et des techniques d'antifalsification.
- **Autorisation.** Accordez des privilèges d'accès en fonction des rôles et des responsabilités de l'utilisateur plutôt que des accès complets d'administrateur. Lorsqu'elles sont disponibles, tirez parti des fonctions d'administration modulées en fonction des rôles déjà présentes dans les applications de gestion du stockage, particulièrement dans le cas des sauvegardes.
- **Vérification.** Des registres des opérations administratives effectuées par les utilisateurs doivent être tenus afin d'assurer la traçabilité et la reddition de comptes.

FAITES DES COPIES DE VOS BANDES DE SAUVEGARDE

Il n'est plus acceptable pour les entreprises de compter seulement sur un seul jeu de copies de sûreté de ses données. Bien que les bandes magnétiques aient une durée de vie appréciable, elles sont vulnérables aux dommages

physiques, environnementaux et à certains autres risques. La pratique exemplaire recommandée consiste à copier les bandes de sauvegarde et à en expédier la copie hors site. Cette pratique vous donne au moins deux possibilités au moment de la récupération puisque les données se trouvent dans des lieux physiques séparés. Votre protection s'en trouve haussée de manière exponentielle.

DÉPLACEZ LES COPIES DE SÛRETÉ HORS SITE

L'entreposage sur place est une pratique peu fiable lorsqu'il s'agit de sauvegarder les données. Même si vous avez fait des copies, celles-ci sont exposées à toute sorte d'atteintes et de menaces, allant de la catastrophe naturelle au vol, en passant par la destruction malveillante. Il ne faut pas en conclure non plus que le directeur du traitement de l'information peut simplement mettre une bande dans sa mallette pour l'apporter chez lui et la ranger dans son sous-sol ou son garage. La protection des données hors site doit prévoir des procédures élaborées sérieusement, des installations et des partenaires habilités à créer un processus rationalisé de bout en bout, éliminant ainsi les risques et les points de vulnérabilité du processus de sauvegarde des données. Les principaux points à prendre en compte sont entre autres :

- **Établissement de codes à barres.** L'imposition de codes à barres aux médias permet d'assurer un suivi approprié chaque fois qu'une bande est déplacée vers un emplacement hors site. Le suivi de tout média individuel, et le suivi du conteneur dans lequel le média est transporté ou entreposé, représentent le mécanisme de contrôle privilégié par les vérificateurs.
- **Vérification des antécédents.** Assurez-vous que votre fournisseur de services d'entreposage hors site a effectué une vérification des antécédents de chacun de ses employés.
- **Sécurité de l'emplacement.** Les installations hors site doivent être sécurisées selon les normes en vigueur. Aucune personne non autorisée ne doit avoir accès aux voûtes.
- **Régulation des conditions ambiantes.** Le transport et les emplacements d'entreposage des bandes sensibles exigent des dispositifs de régulation et de suivi constant de la température et de l'humidité. Le transport des bandes doit se faire dans des conteneurs appropriés et l'entreposage, dans des voûtes protégées et à ambiance contrôlée.

ÉTABLISSEZ ET SUIVEZ UNE CHAÎNE DE POSSESSION RIGOUREUSE

Il est essentiel d'assurer une chaîne de possession de bout en bout afin de protéger et de conserver l'intégrité des sauvegardes de données. Les points suivants sont essentiels :

- **Utiliser des conteneurs protégés.** Les boîtes et les bacs ouverts sont une incitation au vol opportuniste. Assurez-vous que vos bandes sont placées dans des conteneurs verrouillés avant même qu'elles ne quittent le centre de données. Assurez-vous que le ramassage respecte une procédure opérationnelle standard au cours de laquelle un responsable des TI remet en mains propres les données à un représentant du fournisseur. Ce représentant doit être connu, doit détenir une preuve d'identité et doit apposer sa signature en vue de témoigner de la remise.
- **Effectuer les rapprochements au quotidien.** Plus vous découvrez rapidement un problème, plus vous disposez de renseignements pour le régler. Le rapprochement quotidien de vos médias entreposés hors site avec les bandes conservées dans vos installations est une étape supplémentaire qui vous assure que vos bandes se trouvent là où elles doivent être. Si une bande demeure introuvable, vous pouvez prendre les mesures qui s'imposent pour corriger immédiatement cette anomalie.
- **Détruire le support et les données devenus obsolètes.** Une fois que le support est devenu obsolète, détruisez-le complètement de manière confidentielle, soit en brouillant les données de la bande, soit en détruisant complètement celle-ci. La destruction des données peut se dérouler sur place ou être effectuée par un fournisseur tiers pouvant fournir un certificat de destruction.

ENVISAGEZ LA POSSIBILITÉ D'UTILISER LE STOCKAGE ÉLECTRONIQUE À DISTANCE

Le chiffrement et le transfert électronique de vos données de sauvegarde par Internet vers une installation sécuritaire et distante évitent de transporter les données physiquement dans un véhicule. Cette solution peut ne pas convenir à toutes les données de l'entreprise, mais elle peut être utile pour les données essentielles de l'entreprise. Assurez-vous que le fournisseur vous offrant ce type de services procède au chiffrement des données transférées et des données entreposées. Assurez-vous aussi que les pratiques du fournisseur pour la reprise après sinistre et pour la reproduction des données répondent à des normes rigoureuses.

FAITES APPEL À LA FORMATION POUR DÉCELER ET ÉLIMINER LES RISQUES ET LES FAILLES LIÉS AU PROCESSUS

Il est important de vous assurer que les personnes responsables de la sauvegarde de vos données connaissent les risques et soient bien formées. Les politiques en matière de sécurité sont primordiales pour l'attribution des responsabilités, du pouvoir de décision et de l'obligation de rendre compte. Puisque la perte de données est du ressort des affaires de l'entreprise et non pas seulement du ressort des TI, les cadres doivent être informés des risques, des menaces et des pertes potentielles pouvant résulter de brèches de sécurité. Ils doivent aussi être informés des coûts des différentes options en matière de mesures de prévention. Ainsi, les dirigeants pourront faire des choix éclairés en tenant compte des rapports coûts-avantages des investissements en matière de sécurité des données. Les entreprises qui procèdent à l'analyse des risques et qui forment leur personnel sont celles qui sont le plus à même de mettre en place des politiques, des procédures et des technologies en matière de sécurité qui protégeront les biens essentiels de l'entreprise. Par contre, une infrastructure vulnérable et un personnel mal formé s'apparentent à une bombe à retardement.

METTEZ VOTRE PLAN À EXÉCUTION ET FAITES-EN L'ESSAI

La protection sécuritaire des données ne relève pas uniquement de la technologie. Elle suppose aussi un processus qu'il est important de vérifier. Au fil de la croissance et de la progression d'une entreprise, les pratiques en matière de sécurité de l'information doivent évoluer. Une fois qu'un plan global a été élaboré, défini et expliqué aux personnes concernées, il est temps de le mettre à l'essai en procédant à différentes simulations. N'oubliez pas, l'essai doit comprendre à la fois des activités de sauvegarde et des activités de restauration. Essayez de simuler toutes les menaces possibles au cours du processus, notamment la perte de serveurs et de bandes, les problèmes de réseau, de dispositifs, de classification de l'information et tout autre scénario pouvant se répercuter sur l'entreprise. Faites participer des membres du personnel moins au fait de la procédure. Ainsi, vous pourrez vérifier que la procédure est assez simple pour être exécutée lorsque la personne qui en est habituellement responsable n'est pas disponible en raison d'une maladie, d'un congé ou d'une cessation d'emploi.

CONCLUSION

Le déroulement sécuritaire de la sauvegarde des données n'est pas le fruit du hasard. Il exige une planification sérieuse et une maîtrise minutieuse. En raison des incidences qu'une panne peut entraîner – atteinte à la renommée de l'entreprise, coûts directs, problèmes de conformité et déroulement sous-optimal des activités – les entreprises doivent affecter les ressources nécessaires à la mise en place et au maintien d'un processus rigoureux assurant la sauvegarde sécuritaire des données.

Pour en savoir davantage, visitez notre site Web à l'adresse www.ironmountain.ca.



À PROPOS D'IRON MOUNTAIN. Iron Mountain Incorporated (symbole NYSE : IRM) offre des services de gestion de l'information qui contribuent à réduire les coûts, les risques et les inefficacités au plan de la gestion des données physiques et numériques d'une entreprise. Fondée en 1951, la société Iron Mountain gère des milliards d'actifs informationnels, notamment, des données de sauvegarde et d'archives, des fichiers électroniques, des images numérisées, des pièces commerciales, des documents à déchiqueter et plus encore, pour le compte d'entreprises du monde entier. Visitez le site Web de notre entreprise www.ironmountain.ca pour en savoir plus à notre sujet.