

GUIDE DES BONNES PRATIQUES POUR LA PROTECTION DES DONNEES DES TPE

SAUVEGARDEZ LE CŒUR DE VOTRE ENTREPRISE



VOTRE ENTREPRISE repose sur des bases de données clientes, des informations confidentielles et des documents commerciaux. Protéger ces informations —les garder entre de bonnes mains, non corrompues et disponibles à l’utilisation—est le fondement de la gestion de votre entreprise.

La plupart des chefs d'entreprise sont convaincus que leurs informations sont en sécurité, et que leurs clients tolèreront des interruptions de service de “routine” — mais les faits racontent une autre version:¹

- Les entreprises de petite ou moyenne taille ne sauvegardent en moyenne que 60 % des données clientes de leur société.
- Les clients estiment qu’une panne d’ordinateur d’un fournisseur leur coûte 15,000 € par jour.
- 42 % des clients des petites entreprises ont abandonné leur fournisseur à cause d’ordinateurs ou de systèmes qui n’étaient pas fiables.

Le risque de perte d’informations, suite à une défaillance système, une attaque externe (virus) ou l’erreur d’un employé est déjà important, et continu à croître avec le volume et la valeur des informations de l’entreprise.

Le moment est venu d’évaluer clairement vos risques, accompagné d’un dispositif réaliste pour y remédier—pour vos clients, votre réputation, et l’avenir de votre entreprise.

Découvrez les meilleures pratiques pour protéger vos données d'entreprise et les solutions disponibles aujourd’hui en commençant par la lecture de ce document. Pour en savoir plus sur les solutions destinées à protéger les informations de votre entreprise, visitez notre site <http://iconet.fr>

SOMMAIRE

Planifier le meilleur. Se préparer au pire	3
Avez-vous une politique de gestion de vos informations ?	5
Comment résoudre les problèmes de sauvegarde auxquels votre entreprise fait face ?	7
Comment trouver le bon partenaire informatique pour votre entreprise ?	9

PLANIFIER LE MEILLEUR. SE PREPARER AU PIRE.

De quoi alimenter votre réflexion :

Les petites ou moyennes entreprises ont en moyenne connu trois problèmes techniques au cours des 12 derniers mois, dont les principales causes étaient des virus ou des attaques de hackers, des pannes de courant, et des catastrophes naturelles. Le coût de ces pannes : environ 15 000 € par jour.

Encore plus inquiétant, l'étude a révélé une incompatibilité importante entre la façon dont les petites et moyennes entreprises perçoivent leur état de préparation en cas de catastrophe et de leur niveau réel de préparation. Par exemple, alors que 84 % des sondés ont répondu qu'ils se sentaient protégés en cas de catastrophe, près de la moitié ont affirmé ne pas avoir de dispositif pour faire face à ces perturbations.

Evidemment, personne ne veut qu'une catastrophe se produise, mais la réalité est différente. Voilà pourquoi le moment est venu de poser des questions difficiles sur la façon dont vous protégez vos données et systèmes. Par exemple, même si vous vous considérez proactif sur la sauvegarde de vos données, comment êtes-vous protégé dans la réalité ? Si les systèmes de votre entreprise sont perdus dans une inondation ou un incendie. En combien de temps pouvez-vous retrouver l'accès à vos données et continuer vos opérations commerciales? Quelles sont les attentes de vos clients? Peuvent-ils attendre des jours ou semaines le temps que votre activité redémarre ? Plus important, le feront-ils ?

Cet article traite de l'importance de l'automatisation de la sauvegarde et de la récupération, à la fois pour vos PC et serveurs et pour les données importantes s'y trouvant.

Protégez vos systèmes.

Chaque entreprise a ses propres challenges de protection et de récupération de données après sinistre. Cependant, toutes les entreprises font face à des problèmes similaires en matière de conservation de données, de protection de systèmes et de disponibilité. Par exemple, quel que soit le nombre de serveurs que vous avez, vous comptez sur eux pour garder vos employés connectés aux applications, imprimantes et données qu'ils partagent. Si votre serveur Microsoft® Exchange tombe en panne, l'accès à ces ressources est perdu jusqu'à ce que le serveur soit remis en ligne. Cela signifie que vous perdez la collaboration, vous perdez la productivité, et (dans la plupart des cas), vous perdez de l'argent.

Lorsque le système d'exploitation d'un serveur tombe en panne, ça peut prendre des heures (voire des jours, dans certains cas) pour reconstruire et restaurer le serveur. Ce processus comprend la réinstallation du système d'exploitation, des applications et des correctifs; des paramètres de configuration et des données d'application; et ainsi de suite. En outre, il n'y a aucune garantie que le serveur sera dans le même état qu'avant l'apparition de la panne.

Pour se couvrir contre une défaillance matérielle et continuer de permettre une récupération automatique du système, certaines organisations achètent du matériel en double pour leurs systèmes informatiques les plus critiques. Mais le coût de maintenance du matériel en double est tellement prohibitif que seules quelques organisations peuvent le justifier. Il y a des chances que, une petite ou moyenne entreprise ne soit pas en mesure de se permettre le luxe d'une maintenance de serveur supplémentaire au cas où il aurait besoin de remplacer un système existant.

Cela introduit la perspective de restaurer un système sur un nouveau—et différent—matériel. Vous voulez être sûr que vous pouvez vous remettre d'une perte système ou d'une catastrophe en quelques minutes, et non en heures ou en jours — même sur des plateformes matériels différentes.

Protéger vos informations.

Selon un sondage réalisé par [Rubicon Consulting](#), la moitié des petites entreprises interrogées ont dit qu'elles avaient déjà perdues des données critiques. Des processus manuels non gérés ou aléatoires sont souvent à blâmer. Ceci parce que les processus manuels ne sont pas fiables et peuvent mettre en danger les informations. Automatiser le processus de sauvegarde assure que rien ne soit oublié ou ignoré lorsque le personnel manque de temps.

Il est également prudent de sauvegarder les données hors site; Sinon, vous risquez à la fois de perdre l'accès à vos données primaires et à vos sauvegardes en cas de perturbation ou de catastrophe naturelle.

(à suivre)

PLANIFIER LE MEILLEUR. SE PREPARER AU PIRE.

Bien qu'aucun ensemble unique de règles ne permette de protéger toutes les entreprises, les plus avisées suivent les meilleures pratiques, comme celles-ci :

- **Planifier des sauvegardes.** Mettre en œuvre et faire respecter les calendriers de sauvegarde - et **automatiser le processus** autant que possible. Les processus manuels sont longs et assujettis à l'erreur.
- **Sauvegarder aussi les systèmes.** Les sauvegardes sont seulement aussi bonnes que votre capacité à utiliser les informations récupérées, donc sauvegardez les systèmes et les applications aussi bien que les fichiers.
- **Conserver les sauvegardes hors site.** Incendies, inondations, vandalisme, et sabotage sont réels. Soyez sûr que les fichiers et les systèmes peuvent survivre à la perte de votre installation principale, ou même à une catastrophe locale.
- **Tester les sauvegardes.** Ne pas attendre une catastrophe pour découvrir une lacune sur vos ressources, processus ou moyens techniques. Testez régulièrement la totalité de la sauvegarde et le cycle de récupération. Pouvez-vous récupérer sur un matériel différent?
- **Obtenir de l'aide.** Trouver un partenaire informatique local qui vous comprend et qui peut vous aider en prenant en compte vos exigences commerciales et techniques, et en qui vous avez confiance.

Conclusion

Aujourd'hui, vous utilisez plus que jamais l'outil informatique pour rester efficace et concurrentiel. Soyez certains de continuer dans cette voie en vous assurant que vos ordinateurs et vos informations critiques sont protégées et disponibles. **Avec notre système, vous pouvez être sûr que vos données critiques et vos systèmes sont protégés en permanence, vous permettant de vous concentrer sur votre activité professionnelle.**



AVEZ-VOUS UNE POLITIQUE DE GESTION DE VOS INFORMATIONS?

Etes-vous efficace dans la gestion de l'information de votre entreprise?

C'est une question qui mérite d'être posée à n'importe quel moment, mais c'est particulièrement urgent aujourd'hui, étant donné que de plus en plus d'informations deviennent digitales, les nouveaux dispositifs informatiques se multiplient, les virus prolifèrent, et les questions concernant la vie privée et la protection des informations confidentielles ne cessent d'évoluer. Il n'est pas étonnant que de nombreuses petites entreprises aient du mal à suivre.

Une politique de gestion de données solide est essentielle pour faire face à ces défis. Si vous ne disposez pas d'une politique actuellement en place, il est maintenant temps de commencer.

Un défi plus grand que jamais

Que ce soit un message électronique, un fichier Microsoft® Word, ou un message instantané, vous devez trouver un moyen de gérer vos informations de façon responsable. La même chose vaut pour l'information qui passent sur vos ordinateurs portables, téléphones mobiles, PDA, cartes mémoire, lecteurs flash, et même les appareils grand public tels que les lecteurs multimédias. Tout doit être géré.

Cela signifie que vous devez être familier avec toutes les façons dont votre information électronique est capturée et stockée. Les étapes suivantes peuvent vous aider à dimensionner un tel projet.

Etape 1. Rassembler le personnel.

Commencez par rassembler les personnes qui ont la meilleure connaissance des besoins de votre entreprise, de la réglementation et des obligations juridiques (pouvant impliquer la consultation d'un expert juridique externe), ainsi que les emails et l'utilisation de l'information. Impliquez un représentant de chaque département pour vous assurer que tous les besoins sont pris en compte.

Etape 2. Collecter les informations.

Une fois que vous avez rassemblé le personnel, identifiez les types et les catégories d'informations que votre entreprise génère, où et comment cette information est conservée, et les gens qui sont responsables de sa conservation. Qui a la permission de voir, modifier et supprimer des informations? Vous devez être capable de classer vos informations afin de déterminer ce qui est essentiel pour garantir et protéger votre entreprise.

Etape 3. Établir une politique de gestion des données.

Ensuite, décidez combien de temps préserver vos informations, en commençant par les périodes réglementaires et autres périodes légales minimales. Par exemple, vous souhaitez conserver indéfiniment les correspondances évidentes, mais également supprimer le spam. Indiquez comment les données qui ne sont plus nécessaires doivent être purgées de façon sûre.

Etape 4. Ne pas oublier les procédures de sauvegarde.

Les petites entreprises sont vulnérables à diverses formes de perte de données. Une enquête de 2008 de plusieurs centaines de petites et moyennes entreprises par Rubicon Consulting a constaté que près d'un quart des entreprises n'ont pas sauvegardé leurs serveurs ou leurs PC. En outre, la plupart des personnes interrogées ont stocké les fichiers de sauvegarde dans le même emplacement que les ordinateurs sauvegardés. Les questions à se poser dans cette étape sont :

- Stocker les fichiers de sauvegarde à distance. L'enquête Rubicon a constaté que plus de la moitié de tous les fichiers de sauvegarde étaient stockés dans le même emplacement que les originaux. Cela peut rendre une société vulnérable à la perte permanente de données en cas de vol de matériel, de destruction malveillante des données, ou de catastrophe naturelle.
- Employer la déduplication des données. Si votre entreprise utilise une solution de sauvegarde et de restauration sur disque, la déduplication des données élimine la nécessité de stocker plusieurs copies des mêmes données dans le temps. Éliminer les copies supplémentaires réduit la capacité et le coût d'une solution basée sur disque.

(à suivre)

AVEZ-VOUS UNE POLITIQUE DE GESTION DE VOS INFORMATIONS?

Etape 5. Répondre aux besoins commerciaux spécifiques de votre entreprise.

Vous voudrez peut-être désigner des périodes de rétention sur la base des besoins commerciaux spécifiques ou sur le potentiel de litige. Par exemple, vous devriez considérer combien de fois l'accès à l'information est nécessaire sur une base régulière. Dans quelle mesure l'information est distribuée hors de l'entreprise? Quel est le potentiel de litiges futurs à l'égard du contenu? Vous devez établir des lignes directrices claires sur la façon dont le personnel externe ou temporaire accède à vos données, et comment et quand mettre fin à cet accès.

Etape 6. Tout mettre par écrit.

La politique de gestion des données nouvellement créée doit être écrite et distribuée à tous les employés. Ca ne doit pas être compliqué; en fait, le plus simple est le mieux. Mais ça devrait inclure des détails sur les différentes catégories d'informations que vous avez identifiées.

Conclusion

Comme de plus en plus de vos informations critiques passent du format papier au format numérique, la pression augmente pour gérer efficacement ces informations. Le panel des menaces en évolution rapide et la découverte grandissante des exigences légales de conformité créent des risques supplémentaires, ce qui complique encore le challenge de la gestion de l'information. Votre tâche est de veiller à ce que tous les employés connaissent les procédures appropriées pour protéger les informations critiques de l'entreprise.

Nous pouvons vous aider à élaborer une politique de gestion de données qui se concentre sur la protection de vos informations contre les fuites et les pertes tout en réduisant les coûts. Une telle politique vous montrera comment automatiser les sauvegardes pour garantir que votre information est sûre et récupérable en cas de panne de matériel ou de catastrophe naturelle, comment arrêter la fuite d'informations sensibles en prévenant sa transmission depuis vos ordinateurs, et comment minimiser les temps d'arrêt causés par la perte d'information ou la défaillance de systèmes informatiques.

COMMENT RESOUDRE LES PROBLEMES DE SAUVEGARDE AUXQUELS VOTRE ENTREPRISE FAIT FACE

En tant que gestionnaire de petite entreprise, vous investissez beaucoup de temps, d'argent et d'énergie à faire de votre entreprise une réussite.

Et tandis que vous comprenez l'importance de protéger vos actifs et de prévoir un sinistre, vous n'avez pas le temps de faire tout ce que vous devez faire pour protéger votre information contre les menaces malveillantes, une erreur humaine ou une catastrophe naturelle.



La façon dont vous êtes préparé est la clé pour réduire au minimum les effets d'une catastrophe et se remettre au travail rapidement. Considérez que: **La moitié des petites entreprises qui perdent des informations clients se retirent du marché.** En mettant en œuvre les outils technologiques et les meilleures pratiques pour se prémunir contre la perte de données et les temps d'arrêt système, vous pouvez vous assurer que vous serez en mesure de vous remettre de toute catastrophe qui surviendrait.

Voyons quelques-uns des principaux problèmes de sauvegarde auxquels les petites entreprises font face aujourd'hui, ainsi qu'à une solution qui peut aider à suivre le rythme des pratiques de sauvegarde

Les principaux challenges

Votre entreprise est confrontée à des défis importants en matière de sauvegarde efficace des données qui se trouvent sur vos PC, ordinateurs portables et serveurs. Ces challenges ont été classés par les analystes technologiques au sein du Groupe Taneja, comme suit:

- Mettre en œuvre une protection complète avec un impact minimal sur les opérations commerciales. Il y a des chances que votre personnel se concentre sur la gestion de l'entreprise plutôt que sur la sauvegarde des données.
- Répondre aux exigences de sauvegarde et de récupération de plus en plus strictes. Les exigences pour récupérer les données spécifiques et pour réduire le temps global de restauration des données deviennent de plus en plus importantes. Chaque minute d'arrêt a un impact sur votre entreprise.
- Traiter avec des ressources d'administration informatique limitées. Ceci est une question clé pour les petites entreprises, qui manquent souvent de personnel informatique dédié ou d'un administrateur de sauvegarde. En conséquence, les sauvegardes ont tendance à être manuelles et non continues.

- Déployer des stratégies de reprise après sinistre efficaces. La pratique historique consistant à sauvegarder sur bande, puis expédier les bandes à un entrepreneur extérieur peut être risquée. Au cours des dernières années, on ne manque pas de nouvelles histoires de bandes qui disparaissent pendant le transport.
- Tirer parti des nouvelles technologies. En raison de ressources limitées, les petites entreprises peuvent être réticentes à évaluer et à déployer de nouvelles technologies critiques lorsqu'elles deviennent disponibles.

Gérer facilement les sauvegardes.

Garder vos données critiques et vos systèmes sécurisés devrait être automatique.

- Assurer la continuité de l'entreprise. Vous pouvez être sûr que vos actifs - données ainsi que les ordinateurs portables, PC et serveurs - sont protégés contre les pannes informatiques, pannes de courant, erreurs humaines, et autres catastrophes.
- Profitez d'une sauvegarde fiable, automatique et d'une récupération. Vous pouvez planifier des sauvegardes pour que la protection soit automatique. Vous pouvez également restaurer des systèmes informatiques entiers à un point précis dans le temps, sans utiliser de processus de récupération manuels fastidieux.
- Réduire au minimum les temps d'arrêt. Vous pouvez retrouver vos systèmes informatiques opérationnels en quelques minutes, et non en heures ou en jours.

(à suivre)

COMMENT RESOUDRE LES PROBLEMES DE SAUVEGARDE AUXQUELS VOTRE ENTREPRISE FAIT FACE

Nous vous permettons de définir facilement, de planifier et d'exécuter les sauvegardes de vos ordinateurs. Quand une sauvegarde est exécutée, les points de récupération sont créés, qui peuvent ensuite être utilisés pour récupérer un ordinateur entier ou des lecteurs individuels, fichiers et dossiers. Les points de récupération peuvent être créés tout au long de la journée - sans interrompre la productivité de l'utilisateur ou l'utilisation des applications.

Conclusion

Les petites entreprises ont besoin de solutions de sauvegarde et de récupération qui sont faciles à utiliser et automatiques. Comme les données sur vos ordinateurs deviennent plus critiques pour votre entreprise, le risque de préjudice irrévocable pour votre entreprise augmente si ces données ne sont pas protégées. Vous pouvez être sûr que vos données critiques et vos systèmes sont protégés en permanence, vous permettant de vous concentrer sur votre activité.

COMMENT TROUVER LE BON PARTENAIRE INFORMATIQUE POUR VOTRE ENTREPRISE

Avez-vous parfois le sentiment qu'il y a des dizaines de choses plus importantes à gérer dans votre entreprise que, disons, la sauvegarde de vos informations électroniques??

Vous n'êtes pas seul. Une étude récente sur les petites entreprises faite par Applied Research West a révélé que 47% d'entre elles ne sauvegardent pas les fichiers professionnels sur les disques durs de bureau, même si elles savent que c'est important.



Mais la protection de cette information ne devrait pas être une réflexion après coup. Après tout, il est assez probable que l'information électronique et les communications sont à la base même de toutes les relations commerciales que vous avez aujourd'hui.

La bonne nouvelle—spécialement si vos employés sont déjà exploités à la limite—c'est que de l'aide est disponible. Selon un récent rapport du Yankee Group, 61% des entreprises comptant moins de 100 salariés utilisent un entrepreneur ou un partenaire commercial pour les services informatiques.

Maintenant, nous allons examiner quelques-unes des étapes clés concernant l'engagement d'un partenaire informatique et vous proposons quelques conseils pour tirer le meilleur parti de cette relation.

- Tout d'abord, identifier vos priorités technologiques. Selon le [2009 Microsoft SMB Insight Report](#), une étude de Mars 2009 portant sur les défis auxquels font face les petites entreprises, les principales priorités de cette année concernent la virtualisation, la consolidation informatique, l'intelligence d'entreprise, le logiciel comme un service, et le soutien aux travailleurs à distances. Affinez la liste des partenaires potentiels en cherchant seulement ceux dont le cœur de compétences et les domaines spécialisés correspondent à vos besoins.
- Choisir un partenaire spécialisé dans les petites entreprises. Un partenaire potentiel devrait être familier avec les défis auxquels font face les petites entreprises d'aujourd'hui et comprendre que vous n'avez pas de finances illimitées. Vérifiez quel est le pourcentage de leur clientèle qui sont des petites entreprises ou des grosses organisations.
- Vérifier la certification. Prenez en compte le niveau d'accréditation du partenaire potentiel — vérifiez qu'ils sont certifiés dans les domaines d'expertise qui répondent à vos besoins. Les principaux fournisseurs de solutions technologiques proposent des certifications,

démontrant qu'un partenaire a les qualifications et les connaissances nécessaires pour travailler efficacement avec leurs solutions. Bien que l'embauche d'un partenaire certifié puisse coûter un peu plus, cela peut vous faire économiser de l'argent au final. Vous pourriez finir par dépenser beaucoup plus en temps et coûts de mise en œuvre si vous engagez le mauvais partenaire.

- Rendre ça personnel. Un bon partenaire est quelqu'un qui veut vraiment vous découvrir, vos processus et vos employés. Alors assurez-vous que le temps passé dans le processus de découverte est important. Sachez aussi si le partenaire potentiel utilisera son propre personnel, ou si les personnes qui travailleront sur votre compte seront sous-traitées. Demandez au partenaire potentiel des références - de préférence des sociétés dont le profil est semblable au vôtre.
- Mettre en place les bonnes pratiques. Un bon partenaire de petite entreprise est celui qui pourra vous aider à établir les bonnes pratiques afin que vous tiriez le meilleur parti de votre investissement en technologies d'informations. Mais gardez à l'esprit que c'est à vous, et non au partenaire, de vous assurer que ces pratiques sont mises en œuvre par tous les employés.

Conclusion

Selon le [2009 Microsoft SMB Insight Report](#), deux tiers des petites entreprises n'ont pas de personnel informatique, ce qui rend le rôle de partenaire dans la planification et la mise en œuvre de la technologie pour votre entreprise absolument essentiel. En travaillant en étroite collaboration avec un partenaire informatique fort, vous trouverez une approche plus efficace et globale des solutions informatiques pour les petites d'entreprise qui pourra vous faire économiser de l'argent, générer des revenus, et, finalement, aider au succès de votre entreprise.

(à suivre)

COMMENT TROUVER LE BON PARTENAIRE INFORMATIQUE POUR VOTRE ENTREPRISE



Un partenaire sur qui compter

Iconet propose des solutions de sauvegardes sécurisées pour les petites entreprises.

Notre but est d'assurer la protection des données, aujourd'hui vitales pour tous les professionnels.

Contactez nos équipes pour un audit gratuit de votre infrastructure réseau. Nos techniciens se déplacent gratuitement pour évaluer la sécurité de vos systèmes d'informations.

Nos systèmes de sauvegardes sont proposés sur mesure et évolutifs dans le temps.

Iconet

Société basée à Courbevoie – 92400

Siren: 808520621

Tel: 09 53 00 25 36

contact@iconet.fr

<http://iconet.fr>