

# La sécurité des entreprises modernes : enjeux et solutions

Le défi de l'environnement de travail flexible



Les entreprises modernes doivent pouvoir accéder, déplacer et partager les informations à une vitesse et une échelle plus grande que jamais. Vos collaborateurs s'attendent à des façons de travailler plus flexibles, efficaces et collaboratives. Puisque l'environnement de travail s'étend au-delà des murs de votre entreprise, votre information doit être aussi mobile que vos collaborateurs.

De nos jours, la grande majorité des entreprises est confrontée à ces scénarios et, bien qu'ils offrent de belles opportunités pour la productivité et l'innovation, ils génèrent également des menaces sérieuses pour la sécurité de vos données professionnelles.

Comment trouver le juste milieu entre les attentes de vos collaborateurs et le besoin de sécuriser vos informations ? Ce manuel de stratégie explore le défi de mettre en place un environnement de travail numérique flexible, mais sécurisé, détaille les risques de sécurité à considérer et propose quelques solutions concrètes pour les résoudre.

**RICOH**  
imagine. change.



## La situation

### Vos collaborateurs veulent un environnement de travail flexible et une plus grande mobilité

Grâce aux moyens technologiques, les employés d'aujourd'hui s'attendent à pouvoir travailler depuis n'importe où.

Même si vous n'avez pas de collaborateurs à distance, la prolifération de la technologie mobile et cloud signifie que votre travail n'est plus limité dans l'espace. Pour les professionnels, l'idéal en termes de mobilité est beaucoup plus que la fonction des e-mails sur smartphone, c'est un accès facile aux documents, données, collaborateurs et clients dès qu'ils en ont besoin et depuis n'importe où. Cette liberté est devenue une attente primordiale, il est donc impensable de la compromettre si vous voulez attirer et retenir des talents.

Cependant, la mise en place d'un environnement de travail véritablement flexible et mobile peut exposer votre entreprise à un nouveau champ de menaces potentielles pour la sécurité de vos données. Que se passe-t-il lorsqu'un PC portable ou un smartphone est perdu ou volé ? Comment gérer la sécurité de vos informations si les employés peuvent y accéder à partir de leurs appareils personnels ? Comment vous protéger des menaces qui vous guettent lorsque vos collaborateurs se connectent à un réseau WiFi public ?



## Les défis

Disposer d'un système inadéquat pour stocker et partager les informations avec vos collaborateurs à l'intérieur et à l'extérieur de vos locaux peut avoir un impact considérable, tant sur la productivité que sur la sécurité.

Lorsqu'ils ne disposent pas des outils nécessaires, vos collaborateurs se tournent vers ce qu'ils connaissent pour combler ce manque. Les fichiers sont envoyés par e-mail sur des comptes personnels et ouverts sur des ordinateurs personnels. Des documents sont stockés et partagés à l'aide de solution cloud grand public. L'adoption non-autorisée de différents services cloud peut rapidement transformer un système informatique bien conçu en un système fragmenté.

Ces solutions de rechange peuvent mener au phénomène de « fuite de données » qui représente indiscutablement une perte de contrôle sur vos informations.

### Des solutions de rechange bien intentionnées menacent vos informations précieuses

84 % des employés utilisent des e-mails personnels pour envoyer des fichiers sensibles.<sup>1</sup>

### L'approche BYOD (Bring Your Own Device) gagne de plus en plus de terrain

Plus de la moitié des sociétés nord-américaines et européennes développent des programmes BYOD en réponse à la demande de leurs collaborateurs.<sup>2</sup>

### De nombreuses violations de données sont accidentelles

En 2017, plus de 28 millions de groupes de données ont été compromis au Royaume-Uni. Parmi ceux-ci, 38 % étaient attribués à une perte accidentelle.<sup>3</sup>

### Le WiFi public est un champ de mines

On estime que seulement 5 % des hotspots WiFi sont cryptés, mais 95 % des personnes les utilisent au moins une fois par semaine pour le travail.<sup>4</sup>

### Vous ne connaissez peut-être pas l'étendue du risque

Plus de la moitié des responsables informatiques manque de visibilité sur le transfert de fichiers et de données au sein de leur organisation.<sup>5</sup>

1. Ipswitch File Transfer, « Are Employees Putting Your Company's Data at Risk? Survey Results Exposing Risky Person-to-Person File Sharing Practices: An eBook report » [www.ipswitchft.com](http://www.ipswitchft.com). 2. [www.forrester.com/Bring-Your-Own-Device-\(BYOD\)](http://www.forrester.com/Bring-Your-Own-Device-(BYOD)). 3. [www.theregister.co.uk/2017/09/20/gemalto\\_breach\\_index/](http://www.theregister.co.uk/2017/09/20/gemalto_breach_index/). 4. [gfi.com/blog/survey-95-6-of-commuters-in-the-us-put-company-data-at-risk-over-free-public-wi-fi/](http://gfi.com/blog/survey-95-6-of-commuters-in-the-us-put-company-data-at-risk-over-free-public-wi-fi/). 5. Rapport sous forme d'e-book d'Ipswitch File Transfer [www.ipswitchft.com](http://www.ipswitchft.com)



# Les solutions

Pour la mise en place d'une mobilité sécurisée, il est nécessaire de comprendre dans un premier temps comment est diffusée, stockée et utilisée l'information au sein de votre organisation. Puisque les données se déplacent dans votre entreprise à travers une myriade de périphériques, elles doivent être protégées par des mesures de sécurité avancées.

## Intégrez vos informations dans le système

Même le meilleur système de synchronisation et de partage de fichiers vous sera inutile tant que les informations dont vous avez besoin se trouvent encore dans un meuble de rangement. Une solution Scan-to-cloud peut envoyer les documents directement au service de votre choix et permettre un stockage sécurisé. **Procédez facilement et en toute sécurité aux opérations de Scan-to-cloud avec la solution logicielle Streamline NX de Ricoh.**

## Sortez-les quand vous en avez besoin

Malgré le côté pratique et la flexibilité des fichiers numériques, il y a un temps et une place pour les copies papier. Assurez-vous que les bonnes informations tombent toujours entre de bonnes mains avec **des solutions d'impression sécurisée telles que la fonctionnalité Print2Me de Ricoh Streamline NX.**

## Adoptez l'impression mobile et l'impression pour invités

Un besoin d'impression urgent du personnel en déplacement ou des invités est souvent comblé par l'envoi de pièces jointes à un contact sur site. Or, cela peut augmenter le risque de virus et de logiciels malveillants transférés par inadvertance. Une communication de pair à pair entre un périphérique et un smartphone et une impression à la demande basée sur le cloud peut atténuer ce risque. **En savoir plus sur l'impression mobile MyPrint de Ricoh.**

## Gérez vos informations

La mise en place d'une solution de gestion documentaire peut garantir que chaque employé dispose du niveau adéquat d'accès aux informations. Elle peut également permettre de gérer comment, quand et par qui les documents sont consultés ou modifiés. **Découvrez comment Ricoh et DocuWare collaborent pour permettre une gestion documentaire sécurisée et efficace.**

Adressez-vous à un expert

Rendez-vous sur [www.ricoh.fr](http://www.ricoh.fr) ou contactez votre représentant Ricoh local pour découvrir comment nous pouvons vous aider dans votre transition vers un environnement de travail numérique, aussi sécurisé que flexible.



Ricoh France SAS  
7/9, Avenue Robert Schuman,  
Parc Tertiaire Silic, 94513 Rungis



0892 01 20 12



[www.ricoh.fr](http://www.ricoh.fr)

**RICOH**  
imagine. change.

Les chiffres et données présentés dans cette brochure sont rattachés à des études de cas spécifiques. Des cas particuliers peuvent avoir des résultats différents. Tous les noms d'entreprise, de marque et de service sont la propriété de leurs détenteurs respectifs et sont déposés. Copyright © 2017 Ricoh France SAS. Tous droits réservés. Cette brochure, son contenu et/ou sa mise en page ne peuvent pas être modifiés et/ou adaptés, copiés en intégralité ou en partie et/ou intégrés dans d'autres travaux sans l'accord écrit préalable de Ricoh France SAS.