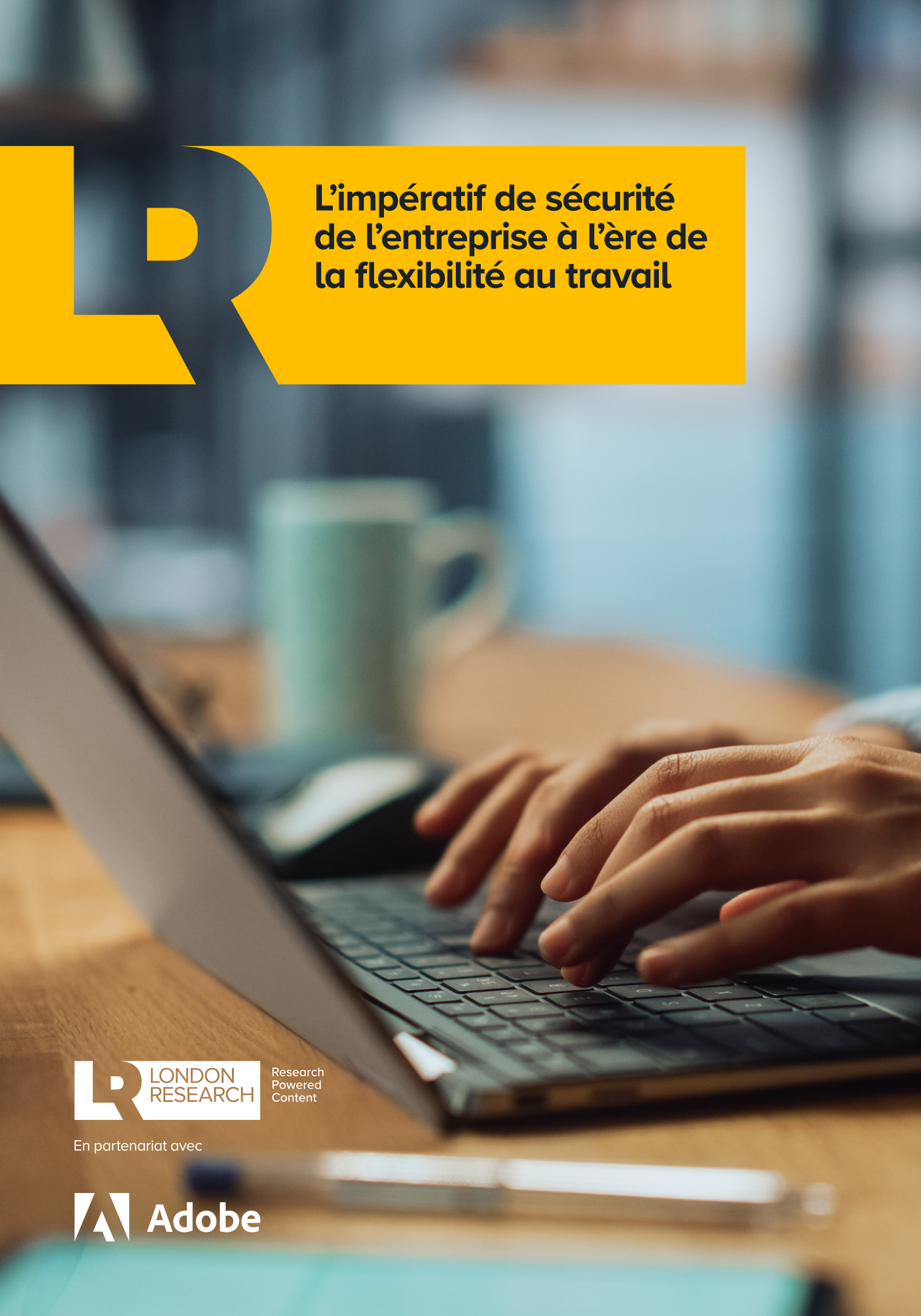
L’impératif de sécurité de l’entreprise à l’ère de la flexibilité au travail



LONDON RESEARCH
Research Powered Content

En partenariat avec

Adobe

Sommaire

Introduction

La sécurité des données a toujours revêtu une importance cruciale pour les entreprises, mais les enjeux sont aujourd'hui plus élevés que jamais. L'une des raisons en est que le coût moyen mondial d'un piratage de données en 2022 s'élevait à 4,35 millions de dollars (5,05 millions de dollars pour le Royaume-Uni, 4,85 millions de dollars pour l'Allemagne et 4,34 millions de dollars pour la France). Mais cela tient surtout au fait que les entreprises doivent soudainement résoudre beaucoup plus de problèmes de sécurité à l'ère de la flexibilité au travail.

Près de neuf cadres IT sur dix (87 %) interrogés dans le cadre d'une étude réalisée par London Research pour le compte d'Adobe affirment que le personnel de leur entreprise est plus nombreux qu'auparavant à travailler à distance. Selon les quatre cinquièmes de ces personnes, cela signifie que leur entreprise est plus vulnérable aux problèmes de sécurité (*Figure 1*).

FIGURE 1

Dans quelle mesure êtes-vous d'accord avec les affirmations suivantes concernant la sécurité des pratiques de travail dans votre entreprise ?

La raison en est simple, mais pas les solutions. Quelle que soit l'habileté dont fasse preuve le service IT pour préserver la sécurité et l'intégrité de l'infrastructure technologique de l'entreprise lorsque l'ensemble du personnel travaille à l'intérieur du pare-feu, sa mission se révèle infiniment plus difficile dès lors que les personnes se mettent à accéder aux ressources depuis des réseaux non sécurisés ou à partir de leurs ordinateurs portables, leurs tablettes et leurs téléphones mobiles personnels.

Les conséquences d'une sécurité insuffisante
Certains des coûts d'une faille de sécurité des données sont évidents. En voici quelques-uns :

- **Versement de rançons**
- **Chute du cours des actions**
- **Manque à gagner imputable aux pannes et dysfonctionnements des systèmes**
- **Préjudice pour votre marque.** La clientèle existante (et potentielle) peut vous juger moins digne de confiance après une faille. Un rapport publié en 2022 par PwC[1] établit qu'au cours des trois années qui ont précédé, 27 % des entreprises à travers le monde ont subi une perte de clientèle et 23 % ont vu leur réputation ou leur image de marque entachée à cause d'un cyberpiratage ou d'un incident préjudiciable à la confidentialité des données. L'atteinte à l'image de marque entraînera également une hausse des coûts RP due aux actions menées pour rétablir votre réputation.
- **Amendes des autorités de règlementation.** Si le piratage aboutit à l'exposition des données personnelles de la clientèle, vous risquez d'enfreindre les obligations légales. Conformément au RGPD[2], les autorités nationales de toute l'Europe en charge de la protection des données sont en droit d'infliger une amende à concurrence de 20 millions d'euros ou de 4 % du chiffre d'affaires mondial de l'entreprise, le montant le plus élevé étant retenu, en cas d'infraction. D'autres sanctions moindres peuvent être prononcées : avertissements et rappels à l'ordre, interdictions temporaires ou permanentes de traitement des données, injonction de mise en conformité, y compris sous astreinte, restriction ou effacement des données et suspension des transferts de données vers des pays tiers.

Mais les répercussions ne s'arrêtent pas là. Les entreprises s'exposent également à d'autres désagréments :

- **Perte de propriété intellectuelle**
- **Majorations tarifaires.** 60 % des entreprises victimes d'un piratage de données n'ont d'autre choix que d'en répercuter le coût sur leur clientèle en augmentant leurs prix, d'après The Ponemon Institute[3].
- **Accès au financement plus difficile et onéreux.** HBR fait également observer que les cyber-risques peuvent entraîner une dégradation de la note de crédit.
- **Mesures correctrices**
- **Frais de procédure et d'audit.** Harvard Business Review[4] indique : « Les frais d'audit facturés à des entreprises consécutivement à des fuites de données peuvent être supérieurs de 13,5 % environ à ceux appliqués à des entreprises non victimes de piratage ».
- **Renchérissement des primes d'assurance**

1 https://www.pwc.com/gx/en/news-room/press-releases/2022/global-digital-trust-insights-survey.html
2 https://www.taylorwessing.com/-/media/taylor-wessing/files/germany/2019/10/german-data-protection-supervisory-authorities-model.pdf
3 https://www.halock.com/summarizing-the-ponemon-cost-of-a-data-breach-report-2022/
4 https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

Résultat : la sécurité des données constitue la principale préoccupation des DTI et DSI en 2023 (*Figure 2*), 86 % de ces cadres allant jusqu'à affirmer qu'il s'agit d'une priorité élevée. Ce pourcentage dépasse celui de domaines souvent plus en vue, tels que la transformation digitale (77 %), l'engagement et la satisfaction de la clientèle (73 %) et le développement durable (56 %). De plus, les trois quarts des DTI/DSI (75 %) déclarent que ce pourcentage est plus élevé qu'il ne l'était il y a un an (*Figure 3*).

FIGURE 2

Dans quelle mesure les domaines suivants constituent-ils une priorité pour votre DTI/DSI en 2023 ?

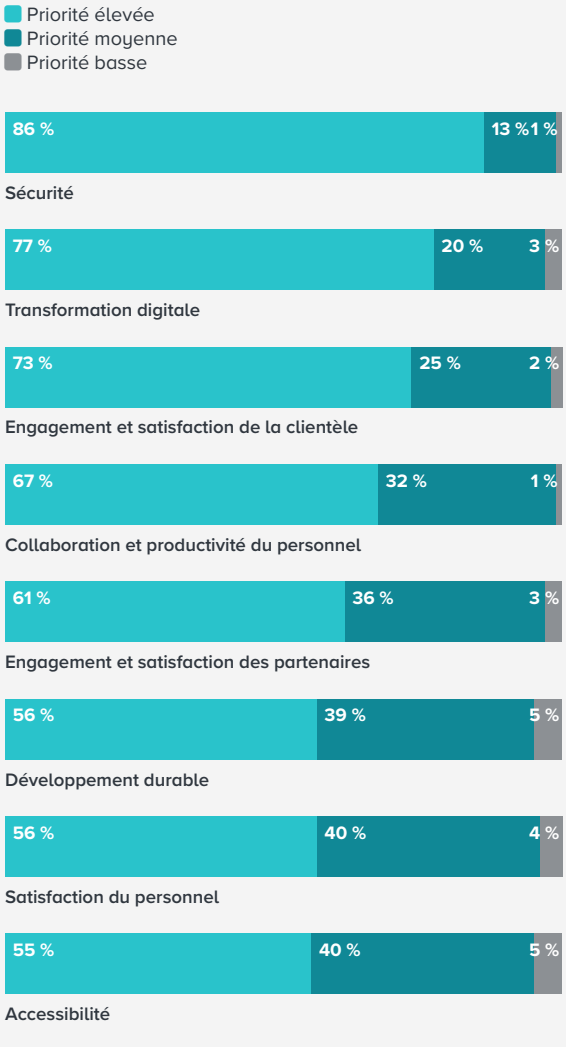
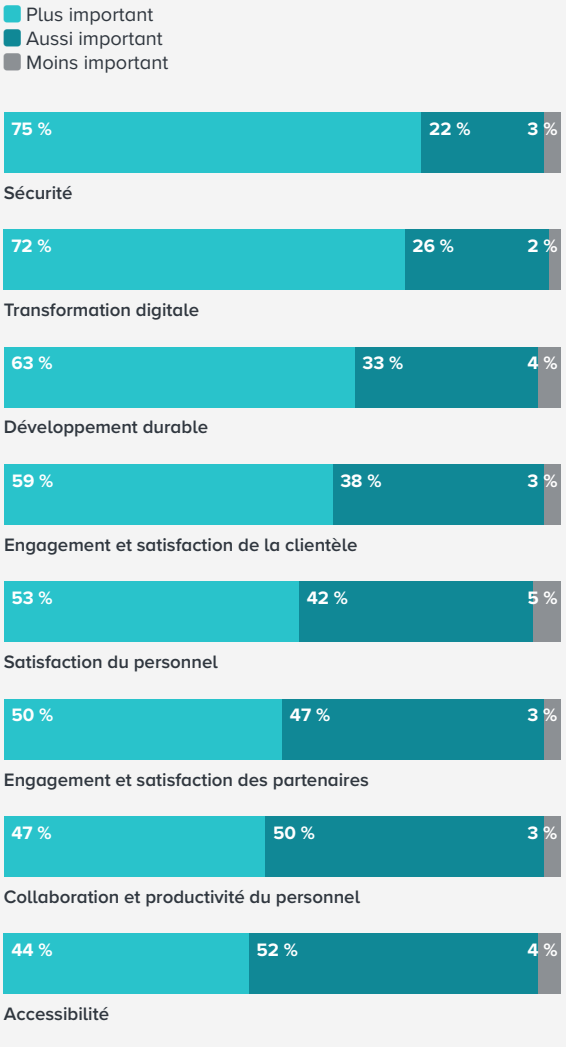


FIGURE 3

Ces domaines sont-ils aujourd'hui plus importants ou moins importants pour votre DTI/DSI qu'ils ne l'étaient il y a un an ?

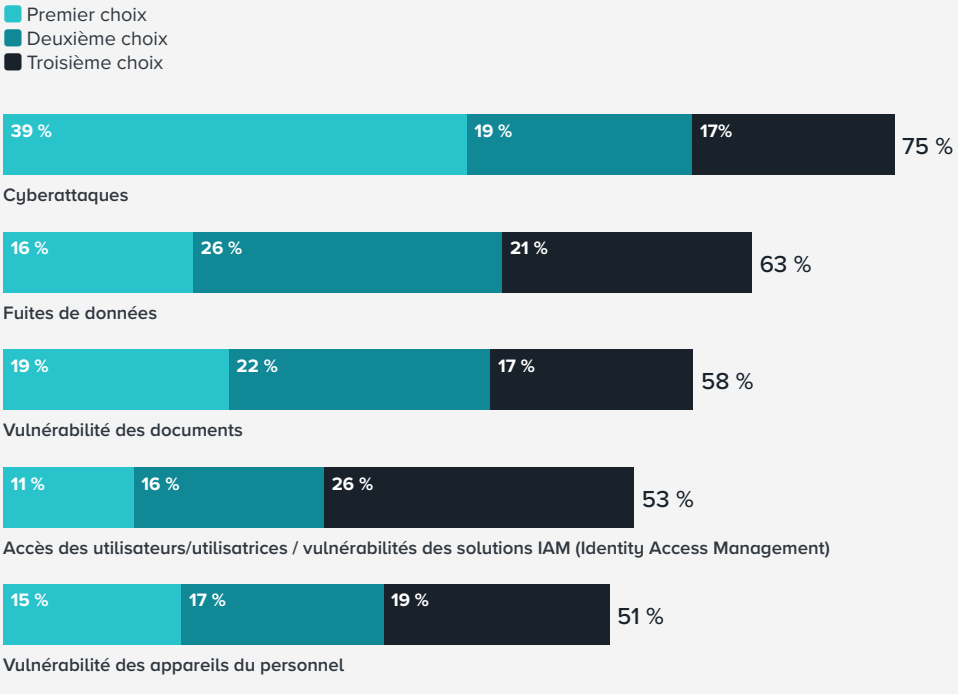


Parallèlement, les entreprises souhaitent profiter des avantages de la flexibilité au travail. D'après le CIPD, « les avantages directs pour l'entreprise incluent une réduction de l'espace de bureau » et « la flexibilité au travail permet également d'établir une meilleure adéquation entre les ressources de l'entreprise et la demande, par exemple avec le service clientèle 24 h/24, 7 j/7 ». Dans le même temps, une étude de la Cranfield University relève « des niveaux de satisfaction professionnelle et d'engagement organisationnel plus élevés chez les membres du personnel flexible que chez leurs homologues non flexibles ».

La gestion documentaire à l'ère de la flexibilité au travail
Il en ressort que la gestion documentaire doit être l'une des priorités des initiatives de sécurité, car le personnel travaille de plus en plus souvent à l'extérieur du pare-feu sur le site de l'entreprise. Lorsque nous leur avons demandé quels défis de sécurité les préoccupaient le plus, une grande majorité de responsables IT a cité les cyberattaques, suivies par les fuites de données, les vulnérabilités liées aux documents, l'accès des utilisateurs/utilisatrices et identités, et les appareils du personnel (*Figure 4*).

FIGURE 4

Parmi les défis de sécurité suivants, lesquels vous préoccupent le plus ?

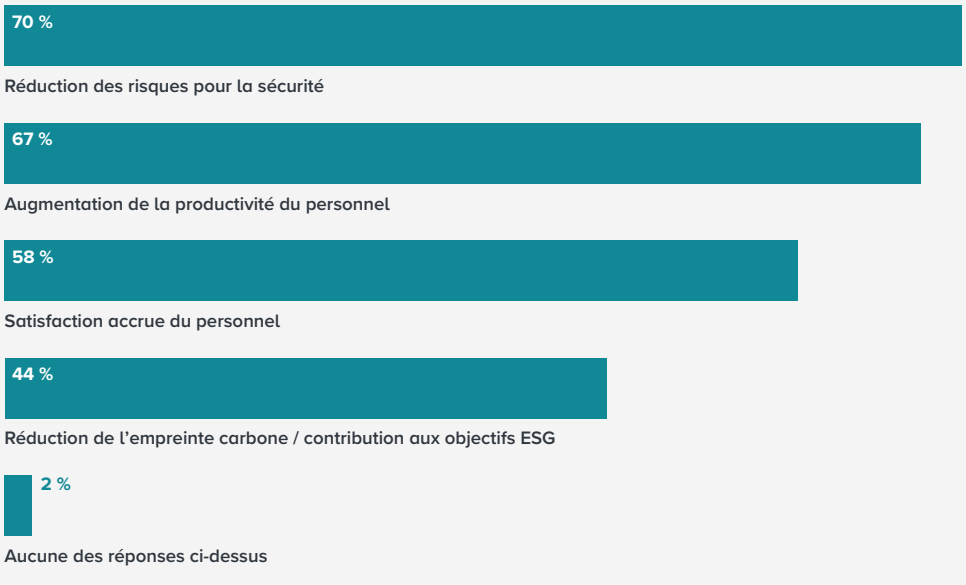


Parallèlement, les entreprises sont confiantes dans le fait d'aller dans la bonne direction. 87 % des responsables IT déclarent que leur technologie de gestion documentaire assouplit et sécurise leurs méthodes de travail. Des doutes subsistent cependant. Moins de la moitié de ces personnes affirment avoir entièrement confiance dans la sécurité de leurs documents, même lorsque ceux-ci ont été créés et sont partagés à l'extérieur du pare-feu de l'entreprise (*Figure 1*).

La réponse à ces préoccupations passe par des investissements supplémentaires dans une technologie plus sécurisée. Plus de neuf responsables IT sur dix (92 %) reconnaissent investir dans une technologie qui les aide à promouvoir des pratiques de travail souples et sécurisées (*Figure 1*). Pour les équipes IT, cet investissement offre deux avantages : la réduction des risques pour la sécurité, et l'augmentation de la productivité et de la satisfaction du personnel (*Figure 5*).

FIGURE 5

Comment votre entreprise mesure-t-elle l'impact de l'investissement dans l'application de gestion documentaire qu'elle utilise ?



Les attentes des utilisateurs et des utilisatrices

Les utilisateurs finaux et les utilisatrices finales de ces nouveaux systèmes de sécurité des documents connaissent parfaitement leurs attentes (plutôt que celles du service IT) vis-à-vis de ces logiciels (*Figure 6*). Ces personnes donnent la priorité à la sécurité et la responsabilité/l'authentification, mais recherchent également l'intégration avec d'autres solutions (ex., Microsoft) et une collaboration efficace (ex., visibilité sur les modifications et contrôle des versions). Cela montre à quel point il est vital pour les services IT de trouver un juste équilibre entre sécurité et facilité d'utilisation.

FIGURE 6

Proportion d'entreprises affirmant que les fonctionnalités de gestion documentaire suivantes sont « très importantes » dans les tâches quotidiennes de leur personnel :

Ces chiffres semblent également indiquer que la sécurité n'est pas nécessairement perçue de la même manière par les utilisateurs et les utilisatrices d'une application que par leurs collègues du service IT. Ils font également état d'un autre problème pour les entreprises qui composent avec des niveaux de télétravail croissants.

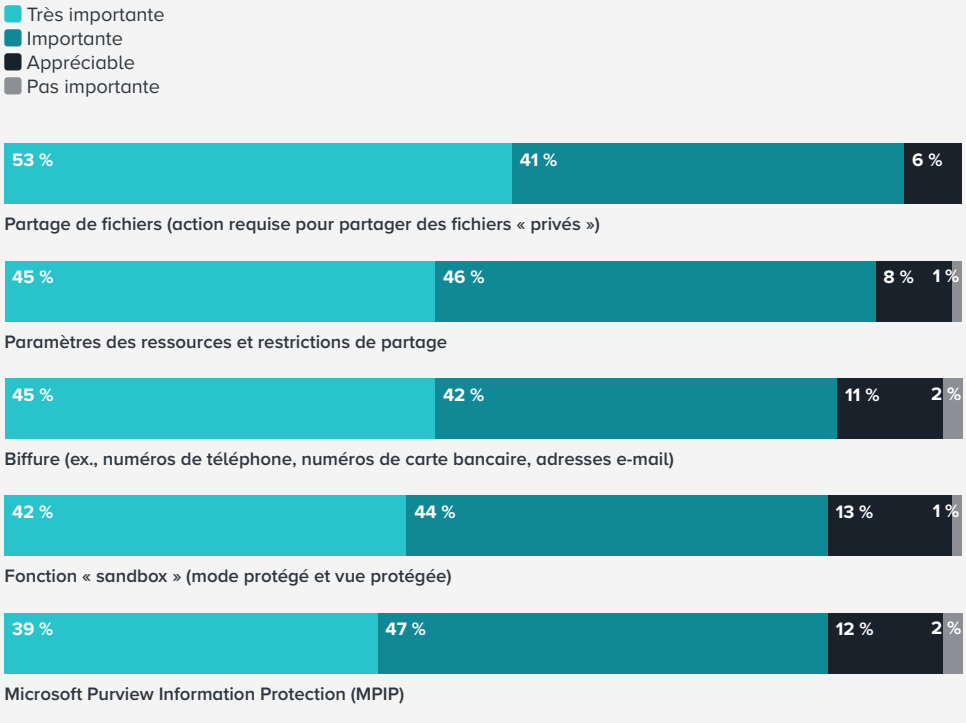
Si les utilisateurs et les utilisatrices reconnaissent volontiers l'intérêt de la sécurité sur le plan théorique, cette conviction ne résiste guère, en pratique, à l'épreuve des délais qui leur sont imposés. La formation joue certes ici un rôle important, mais il est néanmoins préférable de disposer de systèmes « sécurisés par défaut » qui éviteront à ces utilisateurs et ces utilisatrices de s'écarter du droit chemin tout en leur facilitant la tâche.

Les besoins du service IT

Nous avons mis en évidence cette évolution vers la « sécurité par défaut » en demandant aux responsables IT d'établir la liste des fonctionnalités requises pour un système de sécurité documentaire. La nécessité d'effectuer une action pour partager des fichiers « privés », l'exemple parfait de ce mode de pensée, est arrivée en tête de liste (*Figure 7*).

FIGURE 7

Dans quelle mesure les fonctionnalités de gestion documentaire sécurisée suivantes sont-elles importantes pour votre entreprise ?



En outre, de plus en plus d'entreprises recherchent des solutions de gestion documentaire leur permettant de sécuriser d'autres types de documents, tels que des fichiers vidéo, et non simplement des PDF. À juste titre, car un système conçu pour être intégré sera toujours plus sécurisé qu'un autre assemblé à partir de plusieurs solutions.

Nos recommandations aux responsables IT des entreprises

Songez à des méthodes de travail souples et sécurisées.

À quoi bon donner à votre personnel les moyens de travailler n'importe où si, ce faisant, vous vous exposez à des piratages de données et à des cyberattaques ? Sans compter que la sécurité de vos documents est compromise. D'un autre côté, il ne sert à rien de mettre en place des systèmes de sécurité tellement hermétiques que le personnel aura du mal à utiliser les plateformes autorisées. En réalité, c'est même pire car s'il ne parvient pas à emprunter les canaux officiels, il trouvera les moyens de les contourner et il n'y aura alors plus aucune sécurité.

Songez aux solutions intégrées.

La gestion du télétravail à grande échelle est suffisamment complexe sans avoir encore à se soucier de mobiliser plusieurs outils (pour la gestion documentaire, le partage de fichiers et les signatures électroniques) sur de multiples canaux. Plus vous simplifiez la tâche à votre personnel, plus il est productif et plus votre entreprise est prospère.

Songez à la sécurité par défaut.

Ne comptez pas sur votre personnel pour réfléchir à la sécurité : il a d'autres chats à fouetter. Aiguillez-le pour qu'il agisse sans commettre d'impair.

Songez à Adobe.

Renforcez au maximum la sécurité de votre pile technologique et de vos données en travaillant avec les solutions documentaires digitales intégrées d'une société dont toutes les activités sont ancrées et orientées sécurité.

Songez à Adobe

Fiabilité et identité dans Acrobat Sign

Acrobat Sign : la fiabilité pour mot d'ordre

Avec Acrobat Sign, vous pouvez utiliser une signature numérique en toute confiance, car elle repose sur une signature électronique et un certificat numérique. La signature numérique est jugée plus sécurisée et plus fiable qu'une simple signature électronique dans de nombreux pays du monde, y compris aux États-Unis et dans l'Union européenne. Elle utilise la cryptographie pour lier le certificat numérique au document signé afin de prouver que chaque signataire est bien la personne qu'elle ou il prétend être. De plus, un horodatage et un sceau infalsifiable vous aident à avoir confiance dans l'authenticité de votre document.

Centre de données dans l'Union européenne/la zone EMEA

Centres de données régionaux : performances et sécurité au plus près de votre entreprise

Certains de nos centres de données Document Cloud sont situés dans la zone EMEA/l'Union européenne. Ils rapprochent ainsi vos données de votre entreprise, ce qui permet de bénéficier de gains de performances, d'une meilleure collaboration et d'un accès simplifié. En unifiant l'espace de stockage Document Cloud et Creative Cloud, vous pouvez exploiter tout le potentiel et toutes les fonctionnalités des services Document Cloud, dont la création, la modification et le partage de fichiers PDF directement depuis les applications Microsoft 365. Par ailleurs, vous contrôlez mieux la situation, ce qui accélère l'adoption au sein de l'entreprise et optimise l'efficacité du stockage.

Attestation C5

C5 : votre sécurité est notre priorité

Adobe Document Cloud est conforme à la norme C5 (Cloud Computing Compliance Criteria Catalogue), un système d'attestation créé en Allemagne par l'Office fédéral de la sécurité des technologies de l'information (BSI) et soutenu par le gouvernement allemand. L'attestation C5 s'appuie sur des normes de sécurité IT reconnues sur le plan international afin d'offrir un framework de sécurité homogène pour la certification des fournisseurs de services cloud. L'obtention de la certification C5 s'inscrit dans notre engagement à optimiser la sécurité du cloud en garantissant la transparence de la protection des données et en vous donnant l'assurance que vos données seront gérées conformément aux normes de sécurité IT.

Méthodologie

Cet article technique rédigé par London Research pour le compte d'Adobe s'appuie sur une enquête réalisée auprès de 200 décisionnaires IT, responsables des applications de gestion documentaire dans des entreprises implantées au Royaume-Uni, en France et en Allemagne. L'enquête a été réalisée sur le terrain en février 2023. Les entreprises désignent des sociétés réalisant un chiffre d'affaires annuel inférieur à 100 M£.

Qui sommes-nous ?

LONDON RESEARCH Research Powered Content

Fondé par l'ex-directeur d'études d'Econsultancy, Linus Gregoriadis, London Research se consacre essentiellement à la production de contenus basés sur des études à destination d'audiences B2B. Nous sommes basés à Londres, mais notre approche et notre optique se veulent internationales. Nous travaillons essentiellement, mais non exclusivement, avec des agences et des fournisseurs de technologies qui s'efforcent de construire un scénario convaincant à partir d'études solides et de points de données éclairants.

Sous la houlette de Communitize Ltd à laquelle nous sommes rattachés, nous collaborons étroitement avec nos sociétés sœurs Digital Doughnut (communauté d'envergure mondiale rassemblant plus de 1,5 million de responsables marketing) et Demand Exchange (plateforme de génération de contacts), à la fois pour syndiquer nos études et générer des leads de grande qualité.

En savoir plus

Adobe Acrobat

Les entreprises continuent de faire appel aux documents, et leurs équipes veulent pouvoir les manipuler facilement, où qu'elles soient, en utilisant une application fiable et bien intégrée. Conçu par l'inventeur du format PDF, Adobe Acrobat est l'outil PDF et de signature électronique idéal pour les entreprises hybrides actuelles. Avec une solution de renom comme Adobe Acrobat, votre entreprise a toutes les cartes en main pour gérer efficacement ses workflows.

En savoir plus


LONDON
RESEARCH
Research
Powered
Content