Impression de documents : un faux sentiment de sécurité ?

Pourquoi les entreprises doivent sécuriser leur environnement d'impression

Février 2013

Au cours des dernières années, de nombreuses entreprises ont été confrontées à la perte, au vol ou à la divulgation de données internes confidentielles. Ces risques pèsent aujourd'hui sur les organisations du monde entier, quel que soit le secteur d'activité.

Des incidents majeurs, tels que la divulgation de millions de documents top-secret par WikiLeaks ont montré à quel point les données les plus confidentielles, y compris des informations gouvernementales, militaires et diplomatiques, étaient vulnérables.

Bien que souvent négligée, l'impression fait partie des activités à prendre en compte en matière de sécurité. De plus en plus d'entreprises optent pour un environnement d'impression partagé. Mais une fois imprimés sur des multifonctions, les documents sont exposés aux regards indiscrets et peuvent, intentionnellement ou non, tomber entre de mauvaises mains. Dans le cadre d'une stratégie efficace de gestion des impressions, les documents doivent être accessibles uniquement aux utilisateurs autorisés. Cette approche tend à se généraliser dans le domaine de la sécurité documentaire.

Mais la technologie, à elle seule, ne suffit pas.

Pour déployer une stratégie efficace de prévention contre la perte de données (ou DLP, pour « *Data Loss Prevention* »), les responsables IT doivent appréhender plusieurs aspects des données traitées : leur valeur, leur emplacement, ainsi que les utilisateurs qui peuvent y accéder. Si elle n'est pas associée à une évaluation des risques, même la technologie de DLP la plus puissante ne peut offrir une solution viable.

La perte ou l'utilisation abusive de données personnelles ou confidentielles peut porter gravement atteinte à la réputation d'une entreprise et à la confiance que lui portent ses clients. Mais au-delà du préjudice d'image, ces incidents peuvent avoir des conséquences financières considérables, et même déboucher sur des sanctions pénales.

Les besoins de protection d'un volume d'informations sans cesse croissant font peser une pression toujours plus forte sur les entreprises. En même temps, elles doivent répondre aux demandes d'accessibilité de leurs employés, partenaires et clients. Au cours de leur vie, une grande partie de ces informations seront disponibles sur l'un des supports les moins sécurisés qui soient : le papier.

Avec les environnements d'impression en réseau adoptés par plus en plus d'entreprises, des documents confidentiels imprimés sur des multifonctions peuvent facilement tomber entre de mauvaises mains, accidentellement ou pas.

Pourtant, la sécurisation des multifonctions reste souvent négligée. Une étude menée par Quocirca révèle qu'à peine 22 % des entreprises ont mis en place un environnement d'impression sécurisé. Comme 63 % des entreprises qui déclarent avoir subi des fuites de données dues à des documents imprimés, les entreprises s'exposent à de sérieux problèmes de confidentialité.

Ce rapport présente les avantages d'une technologie d'impression sécurisée en matière d'authentification, d'autorisation et de suivi, et explique comment les entreprises peuvent améliorer la sécurité de leurs documents et se conformer aux exigences réglementaires.

Il repose sur une étude menée par Quocirca sur 150 entreprises de plus de 1000 salariés, au Royaume-Uni, en France et en Allemagne.

Louella Fernandes
Quocirca Ltd
Tél. : +44 7786 331924
Email : Louella.Fernandes@Quocirca.com

Bob Tarzey
Quocirca Ltd
Tél. : +44 7900 275517
E-mail : Bob.Tarzey@Quocirca.com

Pourquoi les entreprises doivent sécuriser leur environnement d'impression

De nombreuses entreprises s'exposent à un risque élevé de fuite de données parce qu'elles n'ont pas mis en place les contrôles de sécurité adéquats sur leurs imprimantes et multifonctions en réseau. Les documents imprimés par leurs utilisateurs sont souvent oubliés dans les bacs de réception, où ils peuvent tomber entre les mains de personnes mal intentionnées. Face aux répercussions financières et juridiques que peuvent avoir de telles fuites de données, les entreprises doivent agir. Pour protéger leurs informations sensibles, préserver la confidentialité de leurs employés et de leurs clients et respecter les exigences réglementaires, elles doivent impérativement sécuriser leurs multifonctions. Pour les aider dans cette tâche, les entreprises peuvent déployer une technologie d'impression sécurisée.

Multifonctions et imprimantes de réseau : des périphériques à risques	Les multifonctions sont de plus en plus répandus dans nos bureaux. Mais les risques qu'ils font courir en matière de sécurité sont souvent négligés. Ces périphériques sont généralement accessibles au personnel, aux sous-traitants et même aux visiteurs. Les documents imprimés qui restent dans les bacs de réception sont ainsi exposés aux regards les plus indiscrets. Les fuites de données sont le plus souvent dues à une négligence des salariés. Aussi, pour ne pas engendrer un risque supplémentaire, les imprimantes et multifonctions doivent être sécurisés.
Les entreprises sous-évaluent les risques de fuite des données	Une nouvelle étude[1] de Quocirca révèle que peu d'entreprises se préoccupent de la sécurité de leurs documents imprimés. Même si les résultats varient selon le secteur d'activité, à peine 22 % d'entre elles considèrent cet aspect comme essentiel. Alors qu'une majorité des organismes financiers considèrent que la protection des documents est essentielle, moins de 10 % des administrations publiques affichent cette préoccupation. Un résultat surprenant, au vu du volume et de la nature des documents papier traités par ces établissements.
Un processus d'impression sécurisé limite les risques	Un système d'impression sécurisée (ou impression en mode « pull ») impose aux utilisateurs de s'authentifier à l'aide d'un code d'accès, d'une carte ou d'un système de reconnaissance biométrique pour pouvoir récupérer leurs travaux d'impression. Ce procédé réduit également les gaspillages en éliminant les impressions qui ne sont jamais récupérées, et offre une solution idéale pour les utilisateurs mobiles qui peuvent libérer leurs impressions depuis n'importe quel périphérique d'impression du réseau.
Une parfaite conformité réglementaire, grâce à des audits d'utilisation	De nombreux outils d'impression sécurisée offrent des fonctions d'audit et de création de rapports qui permettent de suivre avec précision les activités d'impression, de copie, de numérisation et de télécopie. Grâce à l'authentification des utilisateurs, il est possible de savoir qui a imprimé quel document, à quel moment et sur quel périphérique. Les pistes d'audit ainsi obtenues permettent d'identifier les sources potentielles de gaspillage ou d'utilisations abusives.
Les logiciels indépendants : la solution pour les environnements mixtes	Pour répondre à leurs besoins d'impression, les entreprises ont souvent recours à une multitude de périphériques de marques différentes, allant de la simple imprimante pour groupe de travail au multifonction haut de gamme adapté aux grands volumes. Parce qu'elles sont indépendantes des fabricants de multifonctions, les solutions d'éditeurs tiers offrent une approche universelle aux problèmes de suivi et de sécurisation au sein d'un environnement mixte.
Le besoin d'une stratégie de protection globale des informations	Pour être efficace, tout système de sécurisation des impressions doit s'inscrire dans une stratégie globale de protection des informations, qui prévoit notamment un contrôle et une classification des données confidentielles. La technologie, et notamment l'impression en mode « pull », peut offrir des réponses concrètes. Mais la protection des données doit également reposer sur la formation et la responsabilisation des employés.

Conclusion

Les fuites de données sont de plus en plus fréquentes, et les exigences réglementaires en matière de protection des informations ne cessent de se renforcer. Aussi, les entreprises qui négligent la sécurisation de leurs impressions s'exposent à des risques considérables, aussi bien en termes d'image que d'impacts financiers. Comme les employés sont souvent à l'origine de fuites de données, et que les entreprises manipulent des informations toujours plus sensibles, il est crucial qu'elles appréhendent le rôle majeur que l'impression occupe dans la chaîne de sécurité des données.

Introduction

Les incidents impliquant des fuites d'informations ne cessent d'émailler les pages des journaux. Et c'est sans compter les nombreux cas qui n'arrivent jamais à la connaissance du public. La perte de données demeure une préoccupation majeure des entreprises, aussi bien dans le secteur privé que public. Ces incidents peuvent avoir de terribles conséquences pour les entreprises. Outre les répercussions désastreuses en termes d'image et de confiance des clients, les amendes et sanctions pénales peuvent être particulièrement sévères. Après le piratage Zappos, portant sur 24 millions de comptes clients, Tony Hsieh, Président directeur général de la société, a déclaré : « Il nous a fallu 12 ans pour remporter la confiance de nos clients. Mais un seul incident a suffi pour réduire tous nos efforts à néant ». Les données sensibles et confidentielles sont souvent stockées sous forme électronique, sur des ordinateurs, des smartphones, des tablettes, des clés USB, ou encore dans des e-mails. Cependant, au cours de leur vie, une grande partie de ces informations figureront sur l'un des supports les moins sécurisés qui soit : le papier.

En effet, à l'ère des smartphones et autres tablettes, l'impression de documents reste pourtant une procédure très courante dans de nombreux secteurs d'activité, notamment les services financiers et juridiques, ainsi que les organismes publics. Les multifonctions sont aujourd'hui de véritables plateformes qui assurent l'impression, la copie, la télécopie et la numérisation de documents, et même leur envoi par e-mail. Ils ont apporté des améliorations considérables à notre environnement professionnel, tant en termes de confort que de productivité. Mais cet environnement centralisé et partagé a fait naître de nouveaux risques. Les multifonctions sont généralement installés à des endroits faciles d'accès. Et en l'absence d'une stratégie de contrôle adéquate, les documents confidentiels laissés dans les bacs d'impression peuvent être récupérés par des utilisateurs non autorisés, intentionnellement ou accidentellement.

À plusieurs reprises, des organismes de réglementation ont infligé de lourdes sanctions à des entreprises qui ne protégeaient pas assez leurs documents imprimés contenant des données sensibles. En novembre 2012, la municipalité de Plymouth, en Angleterre, a été condamnée à une amende de près de 70.000 euros par le Commissariat à l'information, pour avoir envoyé au mauvais destinataire des informations sur un cas de maltraitance d'un enfant. Un employé s'était « simplement trompé de documents dans le bac de l'imprimante ».

Les amendes encourues pour ce type d'incidents tendent à s'alourdir, depuis que la Commission européenne a demandé aux autorités de sanctionner les entreprises à hauteur de 5 % de leur chiffre d'affaires annuel en cas de fuites de données pour négligence. Depuis que le rapport « Cost of Data Breach Study »[2], publié par Ponemon Institute, a clairement identifié les négligences internes comme première cause de fuites de données en 2011, les entreprises ne peuvent plus se permettre la moindre complaisance en matière de sécurité des impressions.

Ce rapport souligne pourquoi il est essentiel de renforcer la sécurité des impressions, et comment une stratégie de sécurisation couplée à des méthodes d'authentification, d'autorisation et de suivi peut renforcer la protection des documents. Il repose sur une étude menée par Quocirca sur 150 entreprises de plus de 1000 salariés, au Royaume-Uni, en France et en Allemagne.

Un faux sentiment de sécurité

Alors que l'impression de documents demeure une pratique courante dans de nombreuses entreprises, la sécurité des impressions reste souvent négligée. D'après une étude de Quocirca, à peine 22 % des entreprises considèrent cet aspect comme essentiel.

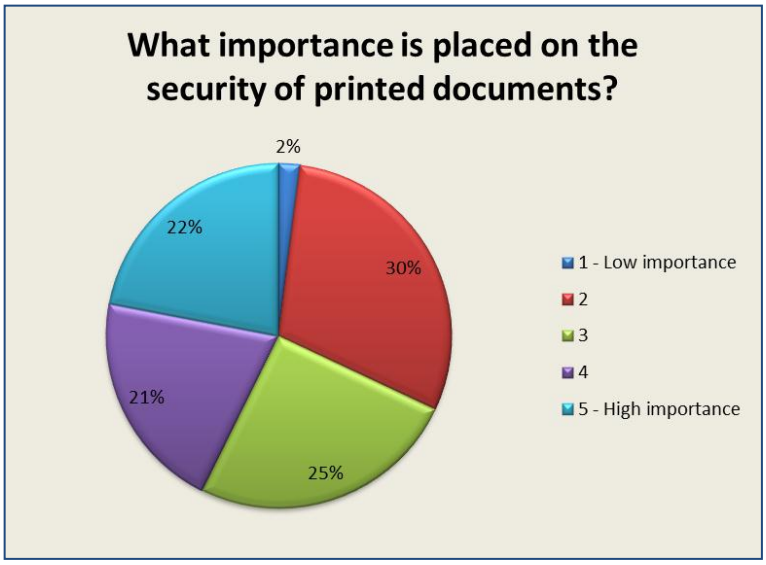


Figure 1. Importance accordée à la sécurité des documents imprimés

Les résultats varient considérablement selon le secteur d'activité. Les organismes financiers sont ceux qui se soucient le plus de la sécurité des documents imprimés. Ceci est peu surprenant au vu des contrôles rigoureux auxquels ils sont soumis. En revanche, malgré le volume et la nature des documents papier qu'ils manipulent, les organismes publics affichent un score d'à peine 2,6 (voir Figure 2). Ainsi, seulement 6 % des établissements publics interrogés donnent une note de 4 à 5 à l'importance du niveau de sécurité des documents imprimés, contre 100 % des organismes financiers.

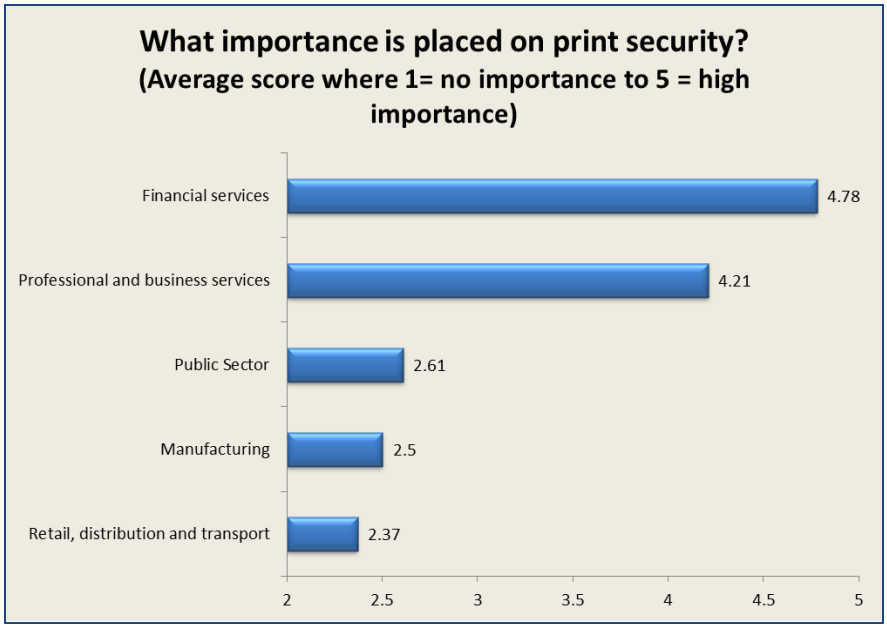


Figure 2. Importance accordée à la sécurisation des impressions (par secteur d'activité)

Ce laxisme a d'importantes répercussions : 63 % des entreprises interrogées déclarent avoir déjà subi un incident de sécurité lié à l'impression de documents. Les organismes financiers semblent tirer les leçons de leurs erreurs : alors que 66 % d'entre eux ont déjà connu un incident de ce type, seulement 16 % en ont connu plusieurs. En comparaison, 90 % des entreprises du secteur public ont subi un incident de sécurité, et 35 % d'entre elles en ont subi plusieurs. (Figure 3)

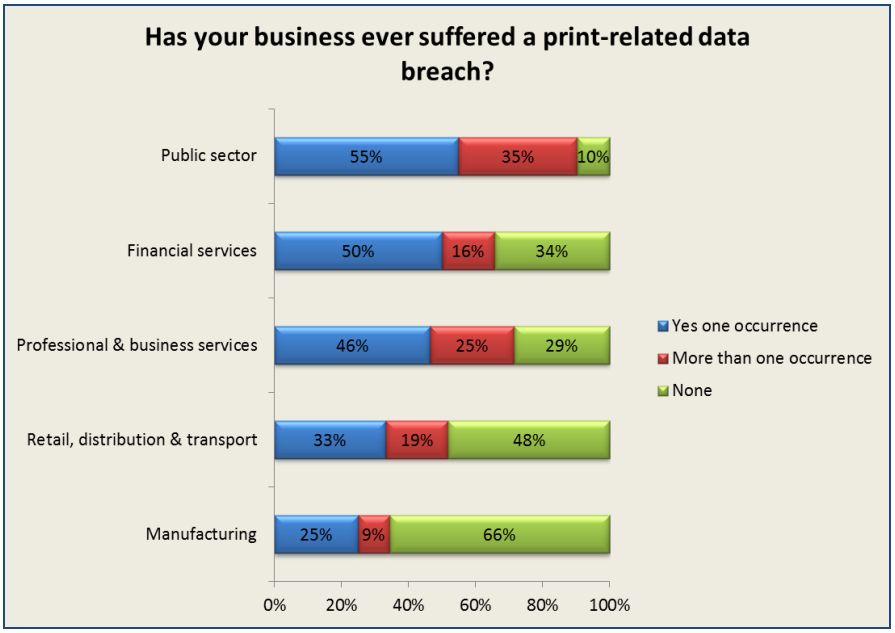


Figure 3. Fuites de données liées à l'impression de documents (par secteur d'activité)

Il apparaît clairement que les actions prises par les entreprises pour protéger leur environnement d'impression sont insuffisantes. Elles s'exposent ainsi à des conséquences financières et juridiques potentiellement désastreuses. Même si les entreprises déploient des efforts considérables pour protéger les données électroniques stockées sur leurs PC, ordinateurs portables, périphériques mobiles, clés USB, ou dans leurs e-mails, la fuite de données reste une menace réelle dès lors que des informations sensibles ou confidentielles sont imprimées et accessibles à des personnes non autorisées.

La nécessité de sécuriser les impressions

L'étude menée en 2011 par Quocirca souligne les trois principales raisons pour lesquelles les entreprises n'adoptent toujours pas de réel système de protection des impressions : faible priorité (92 %), méconnaissance des avantages (71 %) et absence de stratégie de sécurité des impressions (65 %). Aujourd'hui encore, de nombreuses entreprises semblent ignorer les risques inhérents aux multifonctions, et l'existence de solutions pour les limiter.

Pour la plupart d'entre elles, la gestion des activités et des coûts d'impression se limite au simple contrôle des dépenses en papier, toners et autres consommables. À l'exception de l'effacement des disques durs avant l'élimination des imprimantes et des multifonctions, la sécurité des impressions reste négligée. Ainsi, considérant à tort le bureau comme un espace protégé, rares sont les entreprises capables de détecter et d'empêcher les utilisations non autorisées de leurs imprimantes et multifonctions.

La sécurisation des multifonctions impose plusieurs défis aux entreprises :

- **Contrôler l'accès aux multifonctions et aux imprimantes.** Il s'agit de s'assurer que les périphériques sont uniquement utilisés par les utilisateurs autorisés, ou que des groupes et individus définis ne peuvent accéder qu'à des fonctions spécifiques, selon leur fonction et leurs responsabilités.
- **Sécuriser l'impression mobile.** De plus en plus de travaux d'impression sont lancés à partir de périphériques mobiles, tels que des smartphones et des tablettes, obligeant les entreprises à déployer des solutions d'impression mobile. Pourtant, ces travaux d'impression peuvent échapper à tout contrôle s'ils sont envoyés directement à des imprimantes ou multifonctions non sécurisés.
- **Suivi et audit des activités.** À des fins de conformité, les entreprises doivent être en mesure d'indiquer quels utilisateurs ont accédé à quel périphérique, ainsi que les documents qu'ils ont imprimés.

Principaux avantages de l'impression sécurisée

- **Protection renforcée des informations :** l'accès est réservé aux seuls utilisateurs autorisés
- **Mobilité et productivité accrues :** les utilisateurs peuvent imprimer des documents à tout moment, où qu'ils se trouvent
- **Réduction des gaspillages :** les documents non réclamés ne sont pas imprimés, d'où des économies de papier, d'encre et de toner
- **Suivi amélioré :** l'utilisation des périphériques fait l'objet d'un suivi détaillé, à des fins d'audit

Les imprimantes et multifonctions non sécurisés représentent une faille sérieuse en matière de sécurité des données. Il est plus facile - et moins coûteux - de prévenir les pertes de données que d'avoir à gérer leurs conséquences. La mise en place d'un environnement d'impression sécurisé implique un investissement relativement faible par rapport aux répercussions financières et juridiques d'une fuite de données. En outre, un tel environnement peut contribuer à réduire les coûts d'impression, tout en renforçant la transparence des activités.

Limitation des risques

Heureusement, il existe des moyens efficaces pour sécuriser les documents imprimés. Les systèmes d'impression sécurisée (en mode « pull ») tendent à se généraliser. Ils imposent aux utilisateurs de s'authentifier pour pouvoir libérer leurs impressions, et permettent de produire des pistes d'audit sur l'utilisation des périphériques.

Ces systèmes reposent sur deux approches : l'utilisation de fonctionnalités intégrées ou la centralisation sur un serveur. Dans le premier cas, les utilisateurs doivent s'authentifier sur le multifonction à l'aide d'un code d'accès pour pouvoir libérer leurs impressions. De nombreux périphériques offrent aujourd'hui cette fonctionnalité. Ce type de protection très simple permet d'éviter que des personnes non autorisées accèdent à des données sensibles. Il s'agit d'une approche économique, idéale pour les petites entreprises dont le parc de périphériques se compose d'équipements de la même marque.

Dans le second cas, lorsqu'un utilisateur lance un travail d'impression, celui-ci est envoyé à un serveur d'impression, où il est conservé dans une file d'attente jusqu'à sa libération (voir Figure 4). Le serveur peut bénéficier du système de sécurité du centre de données, ce qui garantit une parfaite protection des documents en attente d'impression. Le travail d'impression peut alors être libéré sur n'importe quel périphérique géré par le serveur, après saisie d'un code d'accès ou d'un mot de passe, ou utilisation d'une carte magnétique ou d'un système de reconnaissance biométrique. Les utilisateurs peuvent libérer leurs travaux sur le périphérique de leur choix, quand ils le souhaitent, ce qui leur garantit qu'aucun autre utilisateur ne récupérera leur document à leur place. Les travaux non réclamés sont automatiquement supprimés de la file d'attente après un laps de temps défini.

Cette méthode étant indépendante de la marque des périphériques, elle convient aux entreprises qui possèdent un parc d'équipements étendu et hétérogène, et qui ont des exigences élevées en matière de sécurité. Outre l'authentification standard des utilisateurs, les outils serveur offrent généralement les fonctionnalités avancées suivantes :

- **Authentification sur le réseau :** intégration aux systèmes d'identification réseau existants, y compris de type LDAP et Active Directory.

- **Comptabilisation des travaux :** un suivi précis de l'utilisation des multifonctions (au niveau des documents et des utilisateurs) est essentiel, aussi bien pour la protection des données que pour la conformité aux exigences réglementaires. Des outils d'audit permettent de consigner, suivre et restreindre les interactions impliquant des documents électroniques ou papier. Les administrateurs peuvent utiliser ces outils pour déterminer quel document a été copié, imprimé ou numérisé, par qui, à quel moment, sur quel périphérique et combien de fois. Le contrôle d'accès et le suivi de l'utilisation des périphériques permettent d'identifier rapidement toute anomalie ou comportement suspect et, par conséquent, de prévenir les incidents.

- **Gestion intelligente des impressions.** Grâce aux autorisations basées sur des règles, l'accès aux fonctions d'impression peut être limité selon les utilisateurs ou les applications. Il est ainsi possible de prévoir que seuls les utilisateurs autorisés peuvent accéder à certains périphériques, ou imprimer en couleur. La fonctionnalité de redirection automatique des travaux optimise également l'utilisation des périphériques. Un travail d'impression couleur pourra par exemple être automatiquement redirigé vers le multifonction plus économique.

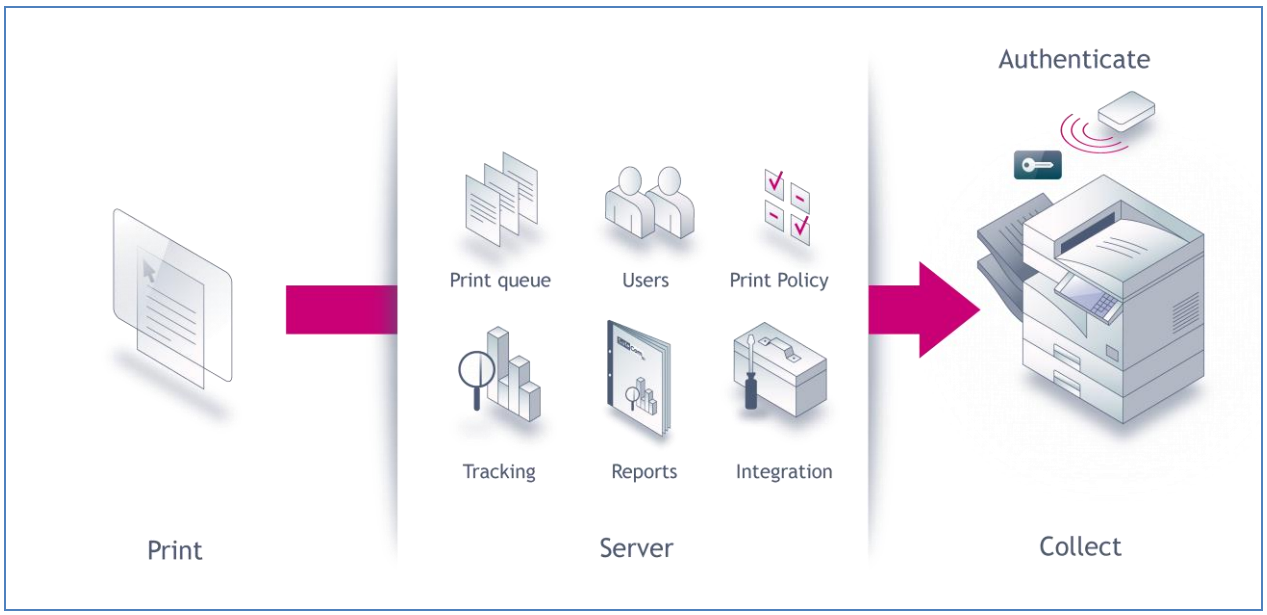


Figure 4. Libération sécurisée des impressions (source : Nuance)

La dernière étude de Quocirca révèle que 21 % des entreprises ont déjà déployé une solution d'impression en mode « pull », et que 22 % en envisagent la possibilité (voir Figure 5). Si ce résultat est encourageant au vu des risques de fuites de données liées aux impressions, trop d'entreprises tardent encore à envisager cet investissement pourtant essentiel. Les organismes financiers indiquent, pour 56 % d'entre eux, avoir déjà déployé une solution d'impression en mode « pull », suivis par 46 % des autres fournisseurs de services. Dans le secteur public, aucun des établissements interrogés n'avait déployé ce type de solution, même si 26 % d'entre eux déclaraient l'envisager. Les entreprises allemandes sont celles qui affichent le plus grand intérêt à l'égard des systèmes d'impression en mode « pull ».

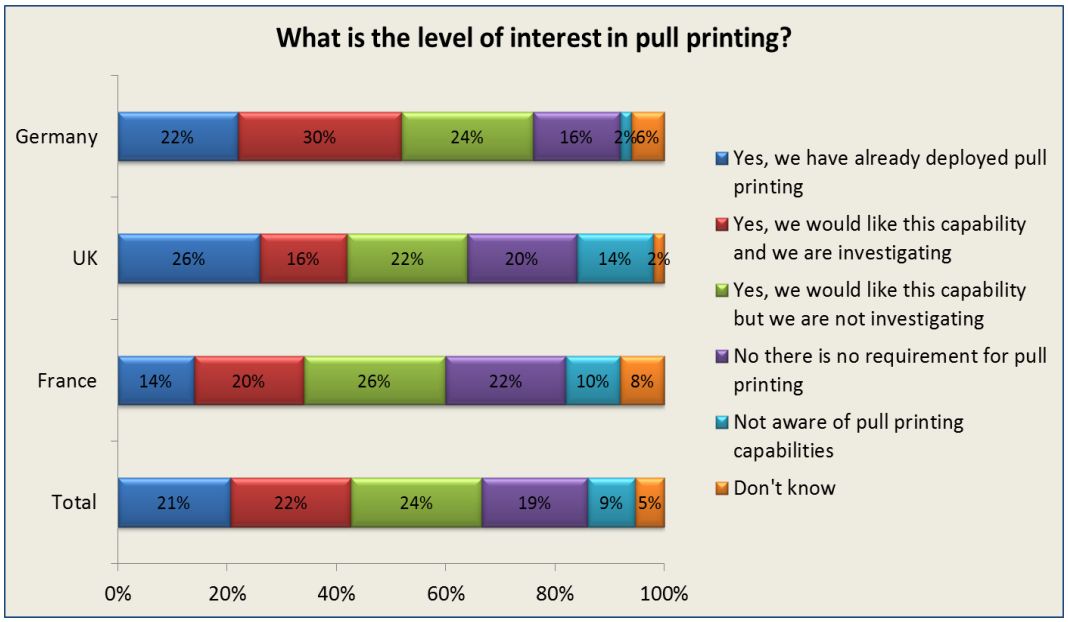


Figure 5. Intérêt à l'égard de l'impression sécurisée

Études de cas

Services financiers et impression sécurisée

La banque suisse Graubündner Kantonalbank propose des services bancaires et d'investissement aux particuliers et professionnels. Elle compte plus de 1000 employés, répartis sur 73 agences.

Les besoins
La banque Graubündner Kantonalbank souhaitait moderniser son parc d'imprimantes, et ce, sur l'ensemble de ses agences, en vue de mettre en place une plateforme homogène et centralisée, et de réduire ses coûts d'impression. Son parc comptait 854 périphériques pour un total de 1116 employés, ce qui représente un taux particulièrement élevé d'imprimante par utilisateurs. Le projet visait à moderniser l'infrastructure d'impression en vue d'optimiser les processus existants et de réduire le nombre total d'imprimantes à l'échelle de l'entreprise, via le partage des équipements. Des données sensibles, notamment des informations financières personnelles et des données professionnelles, sont quotidiennement transférées entre les différents services de l'entreprise. La banque recherchait une technologie d'impression sécurisée capable de répondre à ses exigences en matière de protection des données confidentielles.

Le produit choisi
Pour renforcer la protection des informations imprimées, la banque a choisi Nuance Equitrac et ses fonctionnalités d'authentification et de contrôle d'accès. Parmi ces fonctions, Follow-You Printing® oblige les employés à s'authentifier à l'aide d'un badge ou d'un code d'accès pour pouvoir libérer des travaux d'impression.

Cette fonction de libération sécurisée est compatible LDAP, une exigence fondamentale pour la banque. Aujourd'hui, plus aucun document ne reste sans surveillance dans un bac de réception, ce qui réduit considérablement le risque d'accès aux documents confidentiels par des personnes non autorisées. Les employés peuvent libérer leurs impressions sur le périphérique de leur choix, au siège de la banque, ou dans n'importe quelle agence.

Nuance Equitrac assure notamment une comptabilisation détaillée des opérations effectuées sur les multifonctions, pour permettre leur facturation aux services concernés. Les employés peuvent consulter des rapports d'utilisation les concernant, et connaître les coûts liés à leurs activités de copie, d'impression, de numérisation et de télécopie.

Secteur public et impression sécurisée
Fondé en 1889, le conseil du comté du Lancashire est l'autorité locale en charge du quatrième plus vaste comté d'Angleterre, avec plus d'un million d'habitants et 35.000 entreprises.

Les besoins
Le conseil souhaitait optimiser son infrastructure d'impression, non seulement en remplaçant ses périphériques existants, mais également en essayant de faire évoluer la culture de son personnel en matière d'impression, et ce, sur plus de 600 sites. Jusqu'alors, les responsables locaux pouvaient acheter autant d'imprimantes qu'ils le souhaitaient, tant que le budget le permettait. Au final, le comté possédait pas moins de 2900 imprimantes en réseau, réparties sur plus de 600 bureaux.

Le produit choisi
Dans le cadre d'un contrat de services de gestion d'impression, le conseil a consolidé son parc de périphériques en remplaçant les imprimantes et photocopieurs et en limitant le nombre d'imprimantes à une par site (alors que le rapport était jusque-là d'une imprimante pour sept utilisateurs). Les bureaux de plus grande envergure disposent toujours de plusieurs périphériques. Depuis la mise en place de la solution Nuance SafeCom Pull Print, les travaux d'impression sont placés dans une « imprimante virtuelle », située sur le serveur d'impression. Ils peuvent être récupérés par l'utilisateur sur n'importe quelle imprimante du réseau, après authentification à l'aide d'un code personnel.

Les avantages
Nuance SafeCom Pull Print permet également une plus grande souplesse de travail, dans la mesure où les employés n'ont plus à revenir à leur bureau pour imprimer des documents. Ils peuvent les récupérer sur n'importe quel périphérique de n'importe quelle agence locale, ce qui leur épargne des déplacements et leur permet de réaliser des économies de carburant. En outre, la réduction du nombre d'imprimantes et de copieurs a permis de libérer beaucoup d'espace.

Grâce au système d'authentification, les travaux d'impression sont libérés uniquement lorsque l'utilisateur se trouve devant le périphérique, d'où une sécurité renforcée. Ce procédé d'impression polyvalent améliore les flux de production documentaire et simplifie la gestion de l'environnement d'impression. En effet, il est possible de savoir qui a imprimé quel document et sur quel périphérique, en consultant le site intranet du conseil.

Recommandations

Même si elle ne répond que partiellement aux besoins de sécurité des entreprises, la mise en œuvre d'un système d'impression sécurisée reste essentielle. L'effort consacré à l'amélioration de la sécurité des impressions implique un réel investissement et le soutien des équipes dirigeantes. De nombreuses fuites de données sont dues à des négligences humaines. Aussi, pour tirer pleinement parti des avantages d'une solution d'impression sécurisée, les utilisateurs doivent impérativement être formés.

Quocirca recommande la mise en place des pratiques suivantes :

1. **Définir une stratégie d'impression sécurisée.** L'environnement d'impression doit s'inscrire dans une stratégie globale de protection des informations. Outre la technologie et les exigences en matière de ressources et de formation, cette stratégie doit intégrer des règles, des normes et des procédures. Chaque entreprise a des exigences spécifiques en matière de sécurité. Il convient donc d'adopter une approche progressive, en commençant par une protection de base, puis en évoluant vers des fonctionnalités avancées, en phase avec les besoins de l'entreprise.
2. **Envisager un service d'impression géré.** Lorsqu'il s'agit de consolider une infrastructure d'impression obsolète, la mise en œuvre d'un environnement d'impression géré représente souvent une étape clé. Les fournisseurs de services de gestion d'impression et revendeurs de solutions de sécurité peuvent être d'excellent conseil et aider les entreprises à opter pour une technologie qui répond précisément à leurs besoins. La sécurité des impressions peut être améliorée moyennant un investissement raisonnable, dans la mesure où les entreprises possèdent déjà souvent les équipements requis.
3. **Sécuriser les périphériques.** Les multifonctions sont dotés de disques durs, d'une mémoire et d'un microprocesseur. Ils peuvent même utiliser des systèmes d'exploitation courants, tels que Windows et Linux. Par conséquent, selon le niveau de protection recherché, de nombreuses pratiques de sécurité applicables aux périphériques réseau peuvent être déclinées aux multifonctions, notamment le blocage de connexions réseau, le cryptage des disques durs, l'écrasement de données des disques durs, l'ajout de filigranes sécurisés, etc. Des conseillers spécialisés peuvent aider les entreprises à déterminer les mesures les mieux adaptées au niveau de sécurité souhaité.
4. **Activer l'impression en mode « pull » sur tous les périphériques.** Optez pour des produits tiers offrant une expérience homogène sur tous vos équipements en réseau, et garantissant que tous les travaux d'impression, de copie et de numérisation peuvent être suivis et contrôlés sur l'ensemble de vos périphériques.
5. **Contrôler régulièrement l'infrastructure d'impression.** Assurez un contrôle permanent à l'aide d'outils d'audit et de suivi des impressions.

Conclusion

Les entreprises qui consolident leur parc d'imprimantes optent très souvent pour des environnements partagés. Inévitablement, le risque de voir des documents tomber entre de mauvaises mains s'accroît. Dans le cadre d'une stratégie de sécurité des impressions, les entreprises doivent pouvoir contrôler l'accès à leurs multifonctions et disposer de fonctionnalités de contrôle et d'audit permettant un suivi des activités par périphérique et par utilisateur. L'efficacité d'une stratégie de protection des informations est toujours limitée à son maillon le plus faible. L'impression de documents demeure une pratique courante pour de nombreuses entreprises, mais celles-ci ne peuvent plus se permettre la moindre négligence en matière de sécurité. Même si l'impression en mode « pull » offre un moyen efficace pour lutter contre la perte de données, elle doit s'inscrire dans une stratégie globale, intégrant formation des utilisateurs, définition de règles et intégration de technologies complémentaires.

Références

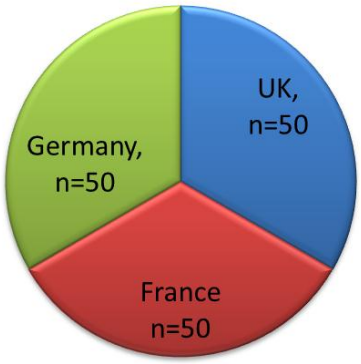
[1] ***Étude Quocirca sur l'usage des imprimantes et multifonctions (2012).*** 150 entreprises interrogées au Royaume-Uni, en France et en Allemagne.

[2] ***« Cost of Data Breach », étude menée par Ponemon Institute (2011).***

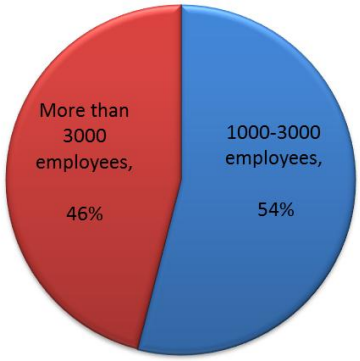
Profil des entreprises interrogées

Les graphiques suivants illustrent le profil des 150 entreprises interrogées, par pays, par taille et par secteur d'activité.

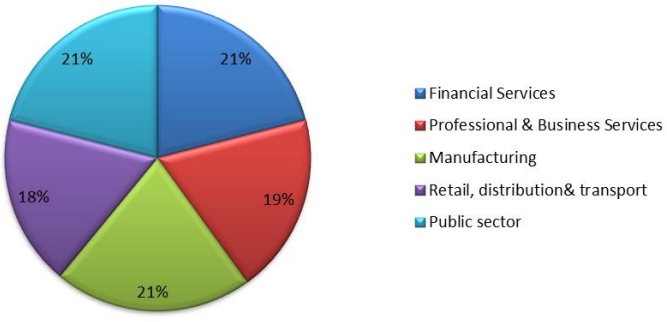
Respondents by Country



Respondents by Organisation Size



Respondents by Industry



À propos de Nuance
Nuance Communications, Inc. est leader sur les marchés des solutions d'imagerie numérique et de reconnaissance et de synthèse vocales destinées aux professionnels. Les technologies, applications et services Nuance optimisent le travail des utilisateurs en révolutionnant la manière dont ils interagissent avec les informations et créent, partagent et utilisent leurs documents.

Nuance fournit des solutions vocales avancées pour un large éventail de sociétés et de clients dans les secteurs des technologies mobiles, de la santé et des centres d'appel. La société compte parmi sa clientèle européenne des entreprises leaders comme Audi, Barclays, BMW, BT, Deutsche Bank, National Healthcare Systems (NHS), Office of Irish Revenue et Vodafone. L'activité imagerie de Nuance inclut des solutions de gestion des impressions n°1 sur le marché, telles qu'Equitrac et SafeCom, ainsi que des solutions de gestion documentaire et d'OCR, telles qu'eCopy ShareScan et OmniPage, qui bénéficient de solides partenariats avec de grands fabricants, tels que Canon, Ricoh, HP, Konica Minolta et Xerox.

Basé dans le Massachusetts (États-Unis), Nuance emploie aujourd'hui plus de 12.000 personnes, avec des bureaux répartis dans 35 pays.

Pour plus d'informations, rendez-vous sur www.nuance.fr

À propos de Quocirca

Quocirca est un cabinet d'étude et d'analyse de premier plan, spécialisé dans l'impact des technologies de l'information et de la communication (TIC) sur les entreprises. Offrant une couverture en langue nationale, Quocirca est une société d'envergure internationale qui fournit une analyse approfondie des opinions des acheteurs et des « influenceurs » dans les grandes, moyennes et petites entreprises. Son équipe d'analystes chevronnés est composée de spécialistes du terrain possédant une expérience directe des TIC, qui étudient en permanence le secteur pour mettre en évidence l'utilisation réelle de ces technologies sur les marchés.

Au travers de ces recherches, Quocirca met en évidence les véritables obstacles à l'adoption des technologies que sont les aspects individuels et politiques de l'environnement professionnel, et la nécessité de démontrer une valeur ajoutée dans toute mise en œuvre. Cette capacité à déceler et analyser les perceptions des utilisateurs finaux sur le marché autorise Quocirca à livrer des recommandations sur les réalités, et non les promesses, de l'adoption des technologies.

Les études réalisées par Quocirca sont toujours pragmatiques et axées sur l'entreprise, tout en s'inscrivant dans un cadre beaucoup plus large. Les TIC ont le pouvoir de révolutionner l'entreprise et ses processus métier, mais force est de constater qu'elles échouent le plus souvent dans ce rôle. Quocirca s'est fixé pour objectif d'aider les entreprises à optimiser l'intégration de leurs processus, grâce à un meilleur niveau de compréhension et à l'adoption opportune des technologies.

Quocirca a mis en œuvre un programme d'études proactif de premier ordre, basé sur des sondages réguliers menés auprès des utilisateurs, acheteurs et revendeurs de produits et services TIC, au sujet des technologies en phase d'émergence, de développement ou de maturité. Au fil du temps, Quocirca est parvenu à esquisser les tendances des investissements à long terme, fournissant ainsi de précieuses informations à l'ensemble de la communauté TIC.

Quocirca travaille en étroite collaboration avec des fournisseurs internationaux et locaux de produits et services TIC, afin que ces derniers tiennent leurs promesses vis-à-vis des entreprises. Les clients de Quocirca incluent les sociétés Oracle, IBM, CA, O2, T-Mobile, HP, Xerox, Ricoh et Symantec, ainsi que d'autres grandes et moyennes entreprises - fournisseurs, prestataires de services et sociétés spécialisées.

Pour plus d'informations sur les activités et les services offerts par Quocirca, rendez-vous sur le site : http://www.quocirca.com