La valeur métier pour l'entreprise de la sécurité des imprimantes

Sponsorisé par **HP**

Auteurs :
Angèle Boyd
Keith Kmetz
Matthew Marden

Novembre 2015

L'OPINION D'IDC

Selon les études d'IDC, 80 % des entreprises que nous avons interrogées considéraient que la sécurité des systèmes informatiques est importante pour leurs processus métiers. Pour autant, seulement 59 % jugeaient la sécurité des imprimantes cruciale pour leurs processus métiers. La direction générale est près de 40 % plus impliquée dans la prise de décision concernant la sécurité des systèmes d'information que pour celle des impressions. Nous pensons que ces résultats témoignent d'un manque d'attention portée à la sécurité des impressions qui peuvent exposer les entreprises à des risques. Les études d'IDC ont révélé que les entreprises ont des raisons plus qu'évidentes d'accorder une plus grande importance à la sécurité des imprimantes, en raison des avantages financiers et informatiques importants obtenus en protégeant l'environnement d'impression :

» L'enquête d'IDC a révélé que plus de la moitié des entreprises interrogées ont été victimes d'un acte de piratage informatique impliquant les imprimantes au cours des 12 derniers mois.

» L'environnement d'impression/documentaire d'une entreprise présente de nombreuses failles. Ces failles peuvent être dues à des attaques malveillantes provenant de l'intérieur ou de l'extérieur de l'entreprise ainsi qu'à une utilisation négligente des imprimantes. Les actes de piratage des impressions potentiels peuvent se présenter sous la forme d'infiltration des ports réseau des imprimantes, d'interception de documents numérisés/copiés/imprimés, intrusion dans la mémoire vive et les disques durs de l'imprimante/MFP, le vol de documents copiés ou imprimés laissés dans les bacs de sortie ou l'utilisation illégale de supports sécurisés (chèques, ordonnances) etc.

» Les entretiens réalisés par IDC auprès de dirigeants d'entreprises qui protègent leurs flux de documents et d'impressions ont mis au jour l'existence de deux types d'entreprises soucieuses de la sécurité de leurs documents/imprimantes :

- Les entreprises préoccupées par la sécurité et la conformité qui font le choix d'une

infrastructure informatique sécurisée

- Les entreprises motivées par les avantages de coût et de productivité obtenus grâce aux projets en matière de sécurité

» Les entretiens réalisés par IDC auprès d'entreprises qui ont mis en place un programme de sécurité des imprimantes ont révélé qu'elles avaient obtenu les plus gros avantages et la plus grande valeur métier dans trois domaines : renforcement de la sécurité des imprimantes, meilleure productivité des informaticiens et réductions des coûts. Les entreprises interrogées ont fait état d'une longue liste d'améliorations pour leurs environnements de sécurité et d'impression :

- Une division par six en moyenne des actes de piratage des imprimantes après la mise en place de solutions de protection
- Une réduction du temps consacré par les informaticiens à l'entretien et la réparation des imprimantes après la mise en place de solutions de sécurité
- 15 % d'économies en moyenne sur le papier, le toner et l'encre

» La façon avec laquelle les solutions de protection des imprimantes sont déployées influe non seulement sur leur efficacité, mais aussi sur la productivité des salariés. Certaines exigences relatives aux technologies, aux personnes et aux processus doivent être prises en compte pour obtenir le maximum d'avantages.

Dans ce livre blanc

TABLEAU 1

Firmographie des entreprises interrogées — Entretiens approfondis

	Moyen	Médian	Plage
Nombre de salariés	60 300	20 500	200 à 290 000
Nombre d'informaticiens	4 500	610	40 à 25 000
Nombre de personnes utilisant les systèmes informatiques	57 200	19 500	180 à 290 000
Nombre total d'imprimantes	8 800	1 200	4 à 100 000
Nombre d'utilisateurs qui impriment	50 800	9 000	200 à 280 000
Nombre de pages imprimées par an	51 millions	10 millions	10 000 à 300 millions
Industries	Télécommunications, industrie, services financiers, édition, aérospatial, biotechnologie, enseignement et santé		

n = 16 entreprises

Source : Entretiens sur la sécurité des imprimantes d'IDC, 2015

IDC Analyze the Future

Ce livre blanc s'inspire des études primaires et secondaires d'IDC sur la sécurité des systèmes informatiques et des parcs d'imprimantes. IDC a réalisé des entretiens approfondis entre juillet et septembre 2015 auprès de personnes chargées de la mise en place et la gestion des solutions de sécurité des impressions dans 16 entreprises. Les entretiens ont été conçus pour permettre à IDC de mesurer l'impact quantitatif et qualitatif des solutions de sécurité des imprimantes. Les entretiens reflétaient les expériences d'un ensemble divers d'entreprises. Le tableau 1 donne un aperçu des environnements d'impression des 16 entreprises interrogées.

IDC a complété les entretiens en profondeur avec des analyses inspirées du travail d'enquête : Les sondés qualifiés provenaient de plus de 440 entreprises de toutes tailles et occupaient un emploi à temps plein. Les personnes interrogées devaient connaître les imprimantes utilisées dans l'entreprise ainsi que les règles de sécurité des systèmes informatiques.

Description de la situation

L'importance de la sécurité des imprimantes/infrastructures documentaires pour les entreprises

La plupart des entreprises ont érigé la sécurité des SI au rang de priorité. Les raisons ne manquent pas. L'essor fulgurant des technologies de calcul, mobile, *cloud computing* et autres permet de créer un environnement informatique dans lequel les travailleurs de la connaissance exigent et ont besoin d'un accès permanent et en tout lieu aux informations de l'entreprise. IDC constate souvent que les systèmes d'impression et les technologies associées sont rarement pris en compte dans la stratégie de protection des systèmes informatiques d'une entreprise.

L'étude d'IDC a révélé que plus de la moitié des entreprises ont été victimes d'une infraction impliquant la sécurité des imprimantes au cours des 12 derniers mois.

Pourquoi les entreprises changent-elles leur approche de la sécurité des imprimantes et les sécurisent comme elles le font pour d'autres technologies (PC, serveurs, terminaux mobiles, etc.) ? La réponse est qu'une infrastructure d'impression non sécurisée expose l'ensemble des systèmes d'information. Le risque de piratage lié aux imprimantes est plus important que l'on peut le penser et les conséquences financières sont considérables.

L'étude d'IDC a révélé que plus de la moitié des entreprises ont été victimes d'une infraction impliquant la sécurité des imprimantes au cours des 12 derniers mois. Cette faille peut être due à des attaques malveillantes provenant de l'intérieur ou de l'extérieur de l'entreprise ainsi qu'à une utilisation négligente des imprimantes. Les actes de piratage peuvent être commis en infiltrant les ports réseau des imprimantes, en interceptant des

documents numérisés/copiés/imprimés, en infiltrant la mémoire vive et les disques durs de l'imprimante/MFP, en dérobant des documents copiés ou imprimés laissés dans les bacs de sortie ou en utilisant des supports sécurisés (chèques, ordonnances) à des fins frauduleuses, etc. En détail :

- Les ports réseau non sécurisés sont un point d'accès au réseau de l'entreprise et à ses actifs informationnels.
- L'impression de documents confidentiels (par ex. les documents contenant des informations sur les patients ou des transactions financières) sur des imprimantes partagées, où les documents sont laissés sur le bac de sortie, représente un risque de vol de données sensibles et de non-conformité.
- La transmission de données numérisées/imprimées non cryptées est presque une invitation pour les pirates informatiques.

Les failles de sécurité ont un coût. Il existe trois types de conséquence financière :

- **Les ressources de l'entreprise sont utilisées pour remédier aux failles.** Les entreprises qui sont victimes d'un acte de piratage mobiliseront leurs salariés et engageront de grosses dépenses pour résoudre l'incident. Les opportunités génératrices de revenus sont retardées ou annulées pour le résoudre.
- **Amendes/pénalités.** Les entreprises peuvent se voir sanctionner par une pénalité pour non-conformité (ex. HIPAA) ou être poursuivies en justice au titre d'un manquement à l'obligation de protéger la confidentialité des clients.
- **Réputation de l'entreprise.** Une fois l'incident survenu, l'entreprise peut encore subir un préjudice financier qui prend la forme d'une atteinte à sa réputation dans les médias.

Les questions liées à la sécurité de la propriété intellectuelle (PI), des informations confidentielles ou soumises à restrictions, les normes et la nécessité d'une infrastructure informatique sécurisée sont des facteurs clés qui plaident en faveur d'un programme de sécurité des imprimantes.

Les facteurs qui plaident en faveur de la sécurisation des impressions

Sur la base des entretiens réalisés auprès d'entreprises qui ont mis en place différents niveaux de sécurité, nous avons mis au jour les facteurs déclencheurs suivants :

- Préoccupations en matière de sécurité et de conformité (dont la réponse à un acte de piratage)
- Standardisation proactive de la sécurité à l'échelle de l'infrastructure

Les réductions de coûts sont l'un des avantages indirects mais importants de la mise en place d'un plan de sécurité des documents et des imprimantes.

» Réductions des coûts et gains de productivité

Préoccupations en matière de sécurité et de conformité

Les questions liées à la sécurité de la propriété intellectuelle (PI), des informations confidentielles ou soumises à restrictions, les normes et la nécessité d'une infrastructure informatique sécurisée sont des facteurs clés qui plaident en faveur d'un programme de sécurité des imprimantes. Certaines entreprises décident de déployer des logiciels de protection plus efficaces en réponse aux incidents passés.

Selon le témoignage d'un directeur des systèmes informatiques d'une société de services financiers : « La sécurité est un défi de tous les instants et l'imprimante est un appareil accessible au public qui est utilisé pour imprimer des documents confidentiels, soumis à restrictions ou non. Les machines en réseau qui traitent des données confidentielles sont soumises à exigences de conformité, de sécurité et d'audit. Nous étions donc obligés de le faire. »

Standardisation à l'échelle de l'infrastructure informatique

La standardisation de la sécurité sur l'infrastructure informatique tout entière d'une entreprise facilite l'adoption de mécanismes de protection des documents et des imprimantes, ainsi que d'une politique complète pour résoudre les problèmes liés à l'utilisation de ces appareils. Un directeur adjoint des technologies de l'information d'une maison d'édition a expliqué : « Nous cherchions une sécurité fondée sur des règles, la résolution automatique des incidents et la sécurité élémentaire des certificats d'identité [pour les imprimantes] en phase avec notre approche pour les autres services. »

Réductions des coûts et gains de productivité

Toute initiative IT qui permet de réduire les coûts d'exploitation d'une entreprise fera le bonheur de la direction de l'entreprise. Les réductions de coûts sont l'un des avantages indirects mais importants de la mise en place d'un plan de sécurité des documents et des imprimantes. Même si cet avantage n'est pas forcément à l'origine de la mise en place d'un tel programme, son impact a été le principal avantage constaté par un tiers des sondés.

Un DSI expérimenté d'une société de services financiers a expliqué : « La nécessité de protéger la propriété intellectuelle et les impacts financiers potentiels des violations de données ont justifié la mise en place de ces solutions. Nous sommes convaincus que les

contrôles qui limitent les impressions inutiles nous ont permis de réaliser des économies sur le papier et les consommables. »

Les initiatives visant à protéger les imprimantes présentent également d'autres avantages financiers « moins directs ». Plusieurs entreprises ont souligné que les gains d'efficacité obtenus en centralisant et standardisant la gestion de la sécurité et des impressions ont permis de réduire les coûts. En gérant et en sécurisant plus activement les impressions, la fonction informatique peut se consacrer à d'autres priorités technologiques. Le DSI d'une université a expliqué : « Nous cherchions à regrouper le contrôle des coûts et de la gestion centrale sur notre environnement d'impression. »

En moyenne, ces entreprises ont constaté une division par six de la fréquence des infractions à la sécurité depuis le déploiement de solutions de protection.

Valeur de la sécurité des imprimantes pour l'entreprise

Les entretiens réalisés par IDC auprès des 16 entreprises qui utilisent des solutions de sécurité des imprimantes ont révélé que déploiement de ces solutions permet de créer une forte valeur ajoutée. Ces entretiens, dans lesquels IDC a demandé aux entreprises de décrire leur environnement d'impression avant et après le déploiement de solutions de sécurité, ont montré que les entreprises atteignent leurs objectifs de protéger leur parc d'imprimantes, tout en réduisant leurs coûts et en bénéficiant de gains de productivité.

- **Sécurité.** Les parcs d'imprimantes sont désormais plus sécurisés et les coûts liés à la réparation des vols de données et au respect des normes et au contrôle de la conformité ont baissé.
- **Productivité du personnel informatique.** Le temps consacré par le personnel à la gestion et l'entretien des parcs d'imprimantes et à la rédaction, la modification et l'application de la politique a été réduit, ce qui libère du temps pour se consacrer à d'autres projets.
- **Réduction des coûts.** Les coûts liés à l'impression, imprimantes et consommables, ont été réduits grâce à une amélioration de la visibilité et au changement des comportements.

Atténuation des risques : Sécurité et conformité des imprimantes renforcées

Les entreprises interrogées ont rapporté avoir tiré parti des solutions de sécurité des imprimantes pour réduire l'impact des actes de piratage et pour se mettre en conformité

avec les normes à moindre coût.

IDC a interrogé les participants sur la fréquence des infractions à la sécurité des imprimantes et des vols de données et si leur entreprise a été victime de ce qu'ils considèrent comme une infraction grave à la sécurité des imprimantes. En moyenne, ces entreprises ont constaté une division par six de la fréquence des infractions à la sécurité depuis le déploiement de solutions de protection. Le déploiement de solutions de cryptage des impressions, d'authentification des utilisateurs et d'impression à la demande ont permis une traçabilité et une responsabilité qui rassurent et permettent d'éviter les actes malveillants. La sécurité des imprimantes a également permis à certaines entreprises de mener à bien leurs projets de sécurité de l'infrastructure informatique et de venir à bout des failles résiduelles. Les entreprises interrogées ont fourni quelques exemples

TABLEAU 2

Impact des solutions de sécurité des imprimantes sur les actes de piratage — Entretiens

Les actes de piratage en général	
Nombre moyen d'infractions par an - avant la mise en place de la solution de sécurité	9,9
Nombre moyen d'infractions par an - après la mise en place de la solution de sécurité	1,5
Variation du nombre d'actes de piratage	Jusqu'à 6 fois moins
Actes de piratage ayant de lourdes conséquences	
Nombre d'entreprises interrogées ayant été victimes de	5
Nombre moyen de salariés concernés	54
Temps moyen consacré à la résolution (heures)	277
Coût moyen total pour réparer les conséquences d'un acte de piratage (amendes comprises)	521 400 $

n = 16 entreprises

Source : Entretiens sur la sécurité des imprimantes d'IDC, 2015

d'acte de piratage dont elles ont été victimes :

- **Imprimer des informations confidentielles dans le but de les utiliser à des fins frauduleuses.** Le directeur informatique d'une entreprise industrielle a expliqué que sa société a perdu certaines de ses innovations du fait, entre autres, de l'impression par des salariés de documents particulièrement sensibles qui ont fini dans les mains de concurrents.
- **Impression et gestion inappropriée de données sécurisées.** Le directeur informatique d'un établissement financier a expliqué que des salariés de son entreprise exposaient des dessins et d'autres propriétés intellectuelles en les imprimant inutilement ou en laissant les documents imprimés sur l'imprimante.

Les entreprises interrogées ont fourni plusieurs exemples qui montrent comment les solutions de sécurité utilisées leur ont permis de limiter l'impact des actes de piratage :

- **Protection des informations à travers le processus d'impression.** Un directeur adjoint des technologies de l'information d'une maison d'édition a expliqué : « La solution est devenue vitale pour protéger le workflow de documents et de données depuis et vers nos imprimantes en réseau, en garantissant une sécurité sans faille qui nous a permis de limiter les possibilités de commettre un acte de piratage. »
- **Éviter les impressions inutiles.** Le DSI d'une société de services financiers a expliqué : « L'entreprise interdit souvent d'imprimer les documents sensibles destinés à être distribués en interne. Ces solutions nous permettent de limiter les actes de piratage, dont un nombre croissant se produit en interne volontairement ou à la suite d'impressions abusives.

Les entreprises interrogées ont déclaré à IDC qu'en moyenne, leur personnel consacrait deux fois moins de temps à la maintenance des imprimantes depuis la mise en place de solutions de sécurité.

Comme le montre le tableau 2, même si chaque acte de piratage peut avoir des conséquences financières, les entreprises doivent veiller tout particulièrement à éviter les infractions graves en raison des coûts exorbitants qu'elles comportent. Selon les cinq entreprises interrogées qui ont été victimes de ce qu'elles considèrent comme une infraction grave à la sécurité des imprimantes, le coût moyen d'une grave infraction comprend des baisses de productivité pour 54 salariés, 277 heures de travail pour réparer l'incident et un coût direct de 500 000 dollars par infraction, amendes comprises.

Outre la baisse de la fréquence des actes de piratage, pour 10 entreprises sur les 16 interrogées, les solutions de sécurité leur ont permis de remplir plus efficacement leurs obligations en matière d'audit et de conformité. Une sécurité renforcée et une meilleure traçabilité ont leur permis de profiter des avantages suivants :

- **Sécurité renforcée :** Le DSI d'une société de services financiers a expliqué : « La mise en

place de ce système de sécurité présente l'avantage de vous permettre de construire un environnement plus sûr et fiable qui protège les données et garantit la confidentialité des dessins. Le fait de sécuriser l'architecture et les imprimantes nous a permis de mieux faire appliquer nos normes de sécurité. »

- **Traçabilité et visibilité :** Le directeur adjoint des technologies de l'information d'une société du secteur des sciences de la vie a expliqué : « Nous avons pu créer une piste d'audit, éviter que des données ne soient dérobées et limiter l'accès des utilisateurs aux données confidentielles. Notre vérification et nos audits comprennent une identification des risques et une analyse des menaces, ainsi que des solutions recommandées. Nous avons un aperçu complet de l'état du système que nous pouvons surveiller en temps réel. »

Ces améliorations ont également permis d'économiser du temps et de l'argent pour les efforts de conformité et d'audit des entreprises. En moyenne, les entreprises interrogées ont rapporté que les solutions de sécurité des imprimantes ont permis d'économiser plus de 200 heures de travail par an et près de 250 000 dollars par an, dont les coûts d'assistance de sociétés externes pour les audits et la conformité.

Gains de productivité du personnel informatique

Les entreprises interrogées par IDC ont affirmé que les solutions de sécurité leur ont permis de réduire le temps consacré à la gestion et la maintenance de leur parc d'imprimantes. Ces gains ont été accentués par des facteurs tels que la mise en place ou l'extension de solutions de gestion centralisée et l'automatisation, ainsi que la capacité à résoudre plus rapidement les problèmes liés aux imprimantes. Un DSI expérimenté d'une société de services financiers a expliqué : « [L'utilisation de solutions de sécurité des imprimantes] a eu un impact important sur le temps que consacre le personnel à des activités chronophages, en lui permettant de se concentrer sur des activités plus stratégiques. La solution aux problèmes liés aux imprimantes est désormais globale. » Les entreprises interrogées ont déclaré à IDC qu'en moyenne, leur personnel consacrait deux fois moins de temps à la maintenance des imprimantes depuis la mise en place de solutions de sécurité.

Les entreprises interrogées ont déclaré que les solutions de sécurité des imprimantes ont permis d'améliorer la productivité des salariés en charge de leur parc d'imprimantes. Les économies réalisées sur le personnel sont le résultat de changements tels que l'automatisation du support et de la maintenance, dont celle des certificats, ainsi que la mise en place d'autres processus reproductibles. Le directeur adjoint d'une entreprise de services financiers qui appliquent des règles d'authentification des salariés et des certificats uniques

a, par exemple, expliqué que sa société est parvenue à réduire de 60 % le temps consacré par son personnel à la surveillance des équipements : « Nous réduisons le temps passé par nos informaticiens car les profils peuvent être facilement créés et transférés sur de nombreux périphériques en même temps et nous pouvons automatiser la gestion des certificats. »

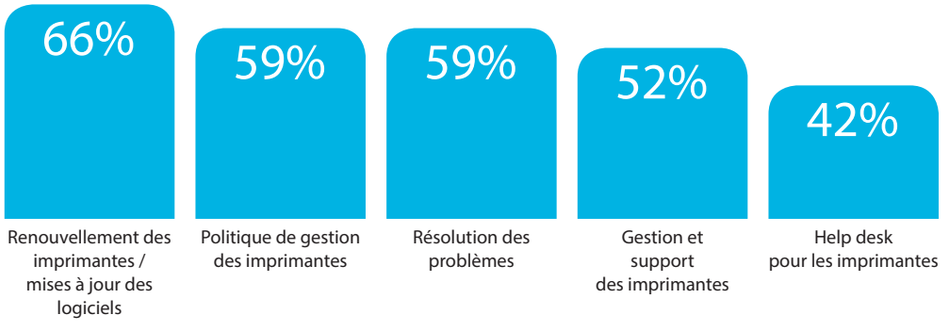
Les entreprises interrogées bénéficient également des gains de temps obtenus grâce aux solutions de sécurité des imprimantes en créant, en appliquant et en modifiant les règles. En moyenne, le personnel de ces entreprises consacre 59 % de temps en moins à la politique de gestion des imprimantes. Outre les gains de temps, une mise en œuvre plus efficace de la politique de gestion des imprimantes présente des avantages en amont, tels que la baisse des probabilités des actes de piratage et la création de directives plus efficaces pour encadrer l'utilisation des imprimantes.

Face aux problèmes, les entreprises interrogées ont rapporté que leur personnel a bénéficié des fonctions des solutions de sécurité des imprimantes, telles que le fait d'avoir (ou de mieux exploiter) des consoles centrales et un accès à distance aux imprimantes. Ces facteurs, outre à l'amélioration de l'efficacité de la politique de gestion, ont permis aux entreprises interrogées de réduire de 59 % et de 42 % en moyenne, le temps consacré à résoudre les problèmes des imprimantes et à répondre aux appels des utilisateurs des imprimantes (voir figure 1). Le directeur adjoint des systèmes d'information d'une maison d'édition qui utilisait des solutions de sécurité comprenant une fonction d'auto-résolution et de gestion de certificats uniques a décrit l'impact sur la capacité de son équipe à gérer la maintenance des imprimantes : « Les problèmes sont désormais moins fréquents et ceux que nous rencontrons prennent moins de temps à résoudre. Les solutions nous ont permis de dégager du temps pour le consacrer à d'autres activités de support et de planification. » Le directeur informatique d'une société de services financiers qui utilise un logiciel de gestion de la sécurité des imprimantes faisait remarquer : « Notre *help desk* possède désormais une vue d'ensemble de la configuration des imprimantes, des autorisations et des problèmes et peut soit intervenir lui-même, soit contacter un service d'impression externe pour le support de niveau 2. »

Les initiatives pour la sécurité des imprimantes ont davantage sensibilisé les employés qui impriment sur l'utilisation qu'ils font des imprimantes et ont permis d'économiser sur les coûts.

FIGURE 1

Gains de temps moyens pour le personnel en charge des imprimantes — Entretiens approfondis



n = 16 entreprises

Source : Entretiens sur la sécurité des imprimantes d'IDC, 2015

Réductions des coûts liées aux imprimantes

Toute initiative informatique essentielle qui s'accompagne également d'une baisse des coûts augmente son attractivité. La capacité des entreprises interrogées à réduire leurs coûts en déployant des solutions de sécurité des imprimantes présente une forte valeur ajoutée. Les pratiques telles que l'authentification des employés et l'impression à la demande (*pull printing*) avaient les faveurs des personnes interrogées (plus des deux tiers des entreprises). Ces solutions préservent la confidentialité des documents et permettent de réduire les coûts en imposant aux utilisateurs des imprimantes de suivre une procédure formelle pour imprimer des documents et en réduisant le nombre d'impressions non demandées ou envoyées par erreur. La capacité des solutions de sécurité des imprimantes à réduire les coûts liés aux imprimantes est telle que plusieurs entreprises interrogées ont constaté que l'optimisation des coûts était la principale raison de la mise en place de ces solutions.

Les entreprises interrogées ont expliqué que les solutions de sécurité leur ont permis de réduire les coûts grâce à :

» **Une réduction des impressions en changeant les comportements des utilisateurs :** Voici le témoignage du trésorier d'une entreprise de l'industrie agro-alimentaire : « L'impression à la demande nous permet d'envoyer à l'impression mais elle impose aux utilisateurs de passer leur badge sur l'imprimante pour vraiment lancer l'impression. Je pense, d'après les derniers chiffres que j'ai pu voir, que cela nous a permis de réduire les impressions entre 21 et 24 %. »

- **Une vue d'ensemble sur l'utilisation des imprimantes :** Le DSI d'une université a expliqué : « Nous pouvons désormais suivre les coûts des pages imprimées pour les répercuter sur les services concernés. » En ayant la possibilité d'attribuer les coûts d'impression à chaque département, l'université peut imposer à chaque département de trouver des moyens d'améliorer l'efficacité des utilisateurs.
- **La mise hors service des imprimantes inutiles ou obsolètes :** Le directeur adjoint d'une société de services financiers a fait remarquer : « Nous réduisons le nombre d'impressions inutiles car les salariés savent que les impressions sont surveillées et nous mettons hors service et remplaçons les anciennes imprimantes qui ne répondent plus aux normes de sécurité de l'entreprise. »

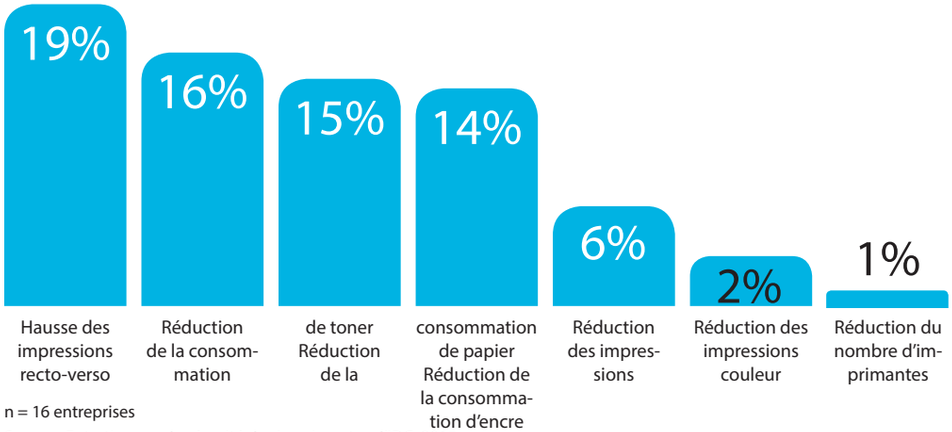
Les initiatives pour la sécurité des imprimantes ont davantage sensibilisé les employés qui impriment sur l'utilisation qu'ils font des imprimantes et ont permis d'économiser sur les coûts. En moyenne, les personnes interrogées ont déclaré que leurs salariés envoient 43 % d'impressions en moins à la mauvaise imprimante. Moins de tâches d'impression sont par conséquent abandonnées ou répétées. Comme le montre la figure 2, ces améliorations ont permis de mieux exploiter les imprimantes, en favorisant une baisse des impressions (6 % en moyenne), une hausse des impressions recto verso (19 %) et une légère baisse des impressions couleur (2 %). Ces facteurs, conjugués à une vue d'ensemble des environnements d'imprimantes, ont permis aux entreprises interrogées de réduire considérablement les coûts de leur parc d'impression, dont le nombre de machines installées et entretenues (1 %, ou 115 imprimantes en moyenne par entreprise), ainsi que les coûts associés au papier, à l'encre et au toner (baisses respectives de 15, 14 et 16 %).

IDC recommande aux entreprises de tester leurs logiciels de sécurité des documents/ imprimantes.

FIGURE 2

Économies et gains d'efficacité obtenus en moyenne sur les parcs d'imprimantes — Entretiens approfondis

(% d'efficacité ou d'amélioration)



n = 16 entreprises

Source : Entretiens sur la sécurité des imprimantes d'IDC, 2015

Défis

Prévoir à l'avance permet d'éviter certaines difficultés. Les difficultés rencontrées par l'échantillon interrogé englobaient les trois stades du déploiement d'une solution de sécurité : planification, mise en œuvre et post-mise en œuvre.

Les entreprises étudiées ont rapporté qu'il était urgent pour elles d'élaborer la stratégie et le plan. Elles doivent consacrer énormément de temps pour obtenir la réduction des charges de travail de la post-mise en œuvre. La mise en conformité des employés doit être en outre un processus automatisé qui englobe les outils de surveillance, un processus d'escalade et des solutions pour réduire les appels passés au *help desk*.

Pour les utilisateurs des imprimantes, les entreprises doivent prendre deux paramètres en considération :

- **Trouver le bon compromis entre la sécurité des imprimantes et l'absence d'impact sur la productivité du personnel.** La sécurité de l'entreprise doit être une priorité, mais une entreprise doit s'efforcer de limiter le plus possible l'impact sur la productivité. Par exemple, certaines entreprises qui font le choix de l'impression à la demande pour renforcer la sécurité de leur parc d'imprimantes peuvent se heurter à la résistance des utilisateurs, désormais contraints de s'authentifier (par la saisie d'un mot de passe) et d'attendre que tout le document soit imprimé. Dans ce scénario, la contrepartie est la protection des informations contenues dans le document (par ex. personne ne peut voir les documents imprimés qui sont laissés dans le bac à papier) au lieu d'attendre que le document soit imprimé (par ex. l'impression n'est lancée qu'après vérification de l'identité de l'utilisateur).
- **Formation des salariés :** Abordant la question de la productivité des salariés, le plan de sécurité des imprimantes doit préciser le processus et le temps nécessaire à la formation des salariés aux nouvelles procédures et politiques. Les entreprises doivent être prêtes à dispenser de nouvelles formations et à utiliser différents formats pour s'adapter aux différences de mode de formation et de générations.

Directive essentielle

IDC a identifié plusieurs arguments incontestables qui plaident en faveur de l'intégration des imprimantes et des *workflows* de documents dans un cadre de sécurité informatique à l'échelle de l'entreprise. L'un des principaux avantages concerne la mise en place d'un

programme complet de sécurité des SI qui englobe les impressions. Ce plan présente également d'autres avantages importants en plus de la sécurité. Les deux principaux avantages sont une réduction importante des coûts et des gains d'efficacité de la fonction informatique.

IDC recommande aux entreprises de tester leurs logiciels de sécurité des documents/imprimantes. L'entreprise doit être consciente que cet objectif ne peut être atteint qu'à la condition de faire participer les individus et les processus à la mise en œuvre du plan.

Technologie

L'intérêt pour une entreprise d'investir dans des solutions technologiques varie en fonction du niveau de sécurité de ses systèmes.

IDC recommande de déployer dès que possible les capacités suivantes au sein de l'entreprise. Le personnel informatique et les fournisseurs d'infrastructure d'impression doivent veiller à ce que les fonctions suivantes soient configurées et actives pour toutes les imprimantes utilisées dans l'entreprise :

» Vérifiez que toutes les imprimantes en réseau possèdent les fonctions suivantes ou que leur *firmware* est au moins mis à jour.

Siège mondial d'IDC

5 Speen Street
Framingham, MA 01701
États-Unis
508.872.8200
Twitter : @IDC
idc-insights-community.com
www.idc.com

À propos d'IDC

International Data Corporation (IDC) est le premier cabinet mondial spécialisé dans les études de marché, les services de conseil et l'organisation d'événements pour les secteurs des technologies de l'information, des télécommunications et des technologies grand public. IDC permet aux professionnels de l'informatique, aux dirigeants d'entreprise et aux investisseurs de prendre des décisions fondées sur des données objectives pour les achats de technologies et la stratégie d'entreprise. Plus de 1100 analystes d'IDC apportent leur expertise mondiale, régionale et locale sur les tendances et les opportunités sectorielles et technologiques dans plus de 110 pays. IDC fourni des informations stratégiques depuis plus de 50 ans pour aider les clients à atteindre leurs principaux objectifs métiers. IDC est une filiale d'IDG, la plus grande société au monde spécialisée dans l'organisation d'événements, les études et les médias ayant trait aux technologies.

IDC Analyze the Future

- Vérifiez que les machines n'utilisent que des protocoles de communication cryptés et désactivez le reste.
- Mettez en place un système qui efface ou détruit les données stockées sur le disque dur dans le cadre de sa mise hors service.
- Prenez en charge au moins une méthode d'authentification des utilisateurs (deux ou trois de préférence) et envisagez la mise en place de l'impression à la demande pour les environnements d'impression caractérisés par un volume important de données confidentielles ou des exigences de conformité.
- Vérifiez que le *firmware* est à jour et qu'une version valable est chargée.
- Veillez à ce que tous les disques durs des imprimantes soient sécurisés (crypter et effacer les données périodiquement).
- Déployez des fonctions inviolables ou utilisez des imprimantes avec des tiroirs verrouillés pour des supports spécialisés si la production de l'organisation le permet. Cela permettrait de sécuriser les impressions qui représentent une cible pour les fraudeurs, comme les chèques, les ordonnances médicales etc.
- Utilisez un logiciel de gestion de flotte pour gérer, surveiller et réparer de manière centralisée l'appareil pour garantir l'application des règles de sécurité. L'entreprise peut ainsi éviter d'avoir à configurer et entretenir chaque machine manuellement. Le logiciel doit simplifier la création et l'administration de la politique de sécurité, détecter lorsque des imprimantes sont ajoutées au réseau, permettre une gestion des certificats de machine uniques et consigner les cas de non-conformité et résoudre les incidents par un processus d'escalade et de résolution. Le logiciel doit pouvoir fonctionner avec des outils de gestion de la sécurité des systèmes de l'entreprise qui surveillent les terminaux pour déceler les non-conformités et les anomalies afin de pouvoir identifier les infractions rapidement.
- Faites en sorte que les impressions et les numérisations des PC de bureau et portables (à distance ou sur site) sont cryptées pour garantir la protection totale des données imprimées. Cela signifie que même les pièces jointes à imprimer doivent être ouvertes et converties en images pour renforcer la sécurité. Un logiciel qui surveille le contenu imprimé et numérisé est un élément clé pour garantir une sécurité maximale et être en conformité avec les politiques de l'entreprise et les normes du secteur.

Personnes

Une entreprise qui prend la sécurité de ses systèmes informatiques au sérieux pour

s'assurer que le département sécurité soit doté en personnel qualifié pour sécuriser les imprimantes et les flux de documents associés. Le service de la sécurité peut être composé de salariés de l'entreprise et/ou de ressources qualifiées externes. L'équipe interviendra pour dispenser des conseils sur la sécurité des imprimantes et des documents et fournir une assistance pour l'intégration d'un plan de sécurité des systèmes.

Pour s'assurer que la protection des imprimantes et des documents imprimés n'altère pas la productivité des salariés, l'entreprise doit recevoir les contributions de certains salariés triés sur le volet dans le cadre de la planification. Il est également recommandé de faire appel à un expert en conduite du changement, notamment si l'ampleur ou la nature des changements requis est important. Cet expert peut également prodiguer ses conseils sur la méthode de déploiement et de formation à utiliser.

La plupart des entreprises ne possèdent pas les compétences nécessaires pour sécuriser elles-mêmes leurs systèmes d'impression et de gestion des documents. Une entreprise doit par conséquent faire appel aux ressources du fournisseur des imprimantes sur lesquelles le service informatique peut s'appuyer. Les ressources englobent les fonctions de sécurité disponibles dans les imprimantes/MFP, les logiciels de sécurité et les services de sécurité (par ex. services professionnels, évaluations de la sécurité, conduite du changement et expertise en matière de réglementation pour certains secteurs).

Principe

Une entreprise doit impérativement démarrer son projet par une évaluation de l'état actuel de son environnement d'impression et la mise en place d'un plan à même de garantir un niveau de sécurité en phase avec celui du reste des imprimantes. Cette initiative doit comprendre une analyse des exigences essentielles en matière de sécurité propres au secteur de l'entreprise ainsi qu'un plan pour surveiller, faire remonter, résoudre et appliquer ces politiques.

Le plan doit être réévalué régulièrement sur la base des données recueillies au cours de la période afin de procéder, le cas échéant, à des ajustements et tirer les enseignements des infractions commises en dehors de l'entreprise. Les modifications varieront en fonction des données collectées, du niveau de risque et des dépenses de l'entreprise en matière de sécurité.