

Trois employés présentant des risques élevés compromettent la sécurité de l'entreprise

Protéger une entreprise contre la fuite de données (par malveillance ou par accident) nécessite une combinaison de techniques, de politiques, de contrôles physiques et de contrôles sur les personnes. Avec l'augmentation de la mobilité des employés, les entreprises ont été contraintes de revoir leur stratégie pour assurer la sécurité des données. Un domaine important et dont on se soucie trop peu est la confidentialité visuelle – la protection des données affichées à l'écran. L'explosion de la présence des appareils mobiles et le passage à des solutions basées sur le nuage, où les données sont accessibles partout et en tout temps, font en sorte qu'un grand nombre d'écrans affichent des données sensibles – souvent dans des lieux publics tels que les cafés et les avions. L'implémentation d'une approche fondée sur les risques pouvant contrevenir à la protection de la confidentialité visuelle de l'entreprise est essentielle à toute stratégie de sécurité des données. Le présent document décrit une approche pour classer les employés et pour appliquer les outils, les politiques et la formation appropriés visant à réduire les risques de fuite de données visuelles.

Le fait de classer les employés en groupes de risque peut aider à établir une stratégie opérationnelle en matière de confidentialité visuelle. La clé est de déterminer les groupes d'employés qui accèdent à des renseignements sensibles et qui les affichent à leur écran, et de connaître la fréquence à laquelle les employés travaillent à l'extérieur des bureaux. Les groupes clés dont il faut tenir compte sont les suivants :

Les cadres : Les cadres n'ont généralement pas accès aux numéros de sécurité sociale ou aux numéros de cartes de paiement des clients, mais les renseignements auxquels ils ont accès peuvent avoir des conséquences beaucoup plus graves en matière de fuite de données visuelles. Les documents traitant de futurs plans non publics conçus par l'entreprise, de la santé de l'entreprise (y compris les finances de l'entreprise) et les renseignements sensibles de l'entreprise, y compris les aspects entourant les ressources humaines, les renseignements sur les fusions et les acquisitions et les secrets commerciaux, peuvent avoir des conséquences graves lorsqu'ils sont exposés. Ces renseignements sont particulièrement à risque lors de la modification ou de l'affichage de fichiers comme des diapositives PowerPoint puisque le contenu d'un fichier PowerPoint est généralement créé pour être lu à distance.

Le service des finances : Au sein d'une entreprise, le service des finances travaille avec des renseignements particulièrement sensibles. Si elles sont exposées, ces données peuvent avoir des conséquences graves pour l'entreprise, telles que des fuites qui peuvent faire l'objet d'examen par la Securities and Exchange Commission (SEC). Le risque est particulièrement grave pour les entreprises cotées en bourse, car les données financières dérobées peuvent être utilisées pour faire des échanges commerciaux.

Le service des ventes : Même si les différents aspects liés aux ventes ne sont peut-être pas considérés comme sensibles ou confidentiels, les listes de clients, qui peuvent inclure des données hautement réglementées comme les numéros de sécurité sociale et les numéros

de carte de crédit, les listes de prospection, les offres en attente et les chiffres d'affaires sont certainement les renseignements les plus sensibles qu'une entreprise peut détenir. Le personnel du service des ventes d'une entreprise est généralement très mobile; il travaille bien plus dans les avions, dans les aéroports et dans les cafés qu'au bureau. Le personnel du service des ventes doit être sensibilisé au risque de fuite de données visuelles et pour ce faire, il faut miser sur la formation.

Il est important que les responsables de la sécurité de chaque entreprise évaluent sérieusement les groupes et les individus qui travaillent régulièrement à l'extérieur des bureaux pour connaître exactement le type de données auxquelles ils ont accès, afin d'obtenir une image précise du risque de fuite de données visuelles. Le risque dépend à la fois de la sensibilité des données traitées et de la fréquence à laquelle l'employé travaille à l'extérieur du bureau. Outre les groupes décrits précédemment, les techniciens sur le terrain, les travailleurs médicaux sur le terrain, les conseillers juridiques, les responsables des RH, les travailleurs à horaire souple (employés qui travaillent régulièrement à l'extérieur du bureau), le personnel responsable du marketing et les ingénieurs peuvent poser un risque considérable en raison de leurs habitudes de travail et de leur accessibilité aux données.

En matière de contrôle de sécurité, les filtres de confidentialité jouent un rôle critique dans la protection des données pouvant être dérobées par des initiés non autorisés, ainsi que par des observateurs qui ne font pas partie de l'entreprise. La Visual Data Breach Risk Assessment Study – une étude réalisée par People Security et commandée par 3M, fabricant des filtres de confidentialité – indique que, pour être efficace, une mesure visant à fournir des outils tels que les filtres de confidentialité aux employés à risque doit être combinée à une politique en matière de sécurité. Un sondage mené auprès de 800 professionnels révèle que les deux tiers (67 %) des répondants affirment avoir eu accès à des données sensibles en dehors du lieu de travail, y compris des renseignements réglementés et confidentiels. En bloquant la vue de côté, les filtres de confidentialité peuvent contribuer à réduire le risque d'exposition des données sensibles.

La clé est d'éduquer tous les employés à risque grâce à des modules d'enseignement, en leur fournissant les outils appropriés pour protéger les renseignements sensibles tels que l'obscurcissement d'écran planifié ou les filtres de confidentialité, ainsi qu'en établissant des politiques qui encadrent la consultation des données sensibles et l'utilisation de ces outils.

46 %

des utilisateurs de nuage informatique indiquent qu'ils ont utilisé des applications infonuagiques principalement parce qu'ils veulent être en mesure d'accéder à leurs données, peu importe l'endroit où ils se trouvent et l'appareil qu'ils utilisent.¹

Pour en savoir plus, consultez le 3M.ca/ProtégerMonÉcran

¹Privacy and Data Management on Mobile Devices, <http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/>