

D mission d un salari , attention aux risques de fuites de donn es.
S curit 

Post  par : JPilo

Publi e le : 30/6/2014 13:00:00

Na vet  et confiance mal plac e composent un cocktail potentiellement dangereux dans le monde de l entreprise. C est encore plus vrai en ce qui concerne la gestion des risques pour l information. Une  tude r cente r v le que 87 % des entreprises en Europe ne pensent pas que leurs employ s emportent des informations quand ils quittent la soci t .

Pour 81 % des personnes interrog es, cette confiance s explique par l adoption de mesures strictes : faire signer des contrats de confidentialit , bloquer l acc s aux r seaux IT de l entreprise des anciens salari s, emp cher que l on puisse copier des donn es sur des disques ou des cl s USB, escorter   l ext rieur ceux qui occupent des postes   risque d s l instant o  ils remettent leur d mission. Bon, tout va bien alors...

Sauf que les trois quarts des r pondants n ont jamais v rifi  que ces mesures suffisaient effectivement   emp cher toute fuite d information. Une autre  tude  , qui s int resse cette fois-ci aux pratiques vis- -vis de l information des employ s qui quittent une soci t , d peint d ailleurs un tout autre tableau.

Elle montre en effet qu ils sont nombreux   n  prouver aucun scrupule   emporter des documents sensibles ou hautement confidentiels avec eux. La plupart n y voit aucun mal.

Ils sont deux tiers   reconna tre qu ils emporteraient volontiers des informations qu ils estiment avoir contribu    produire, ou   l avoir d j  fait, et 72 % estiment que ces informations pourraient leur  tre utiles   leur nouveau poste.

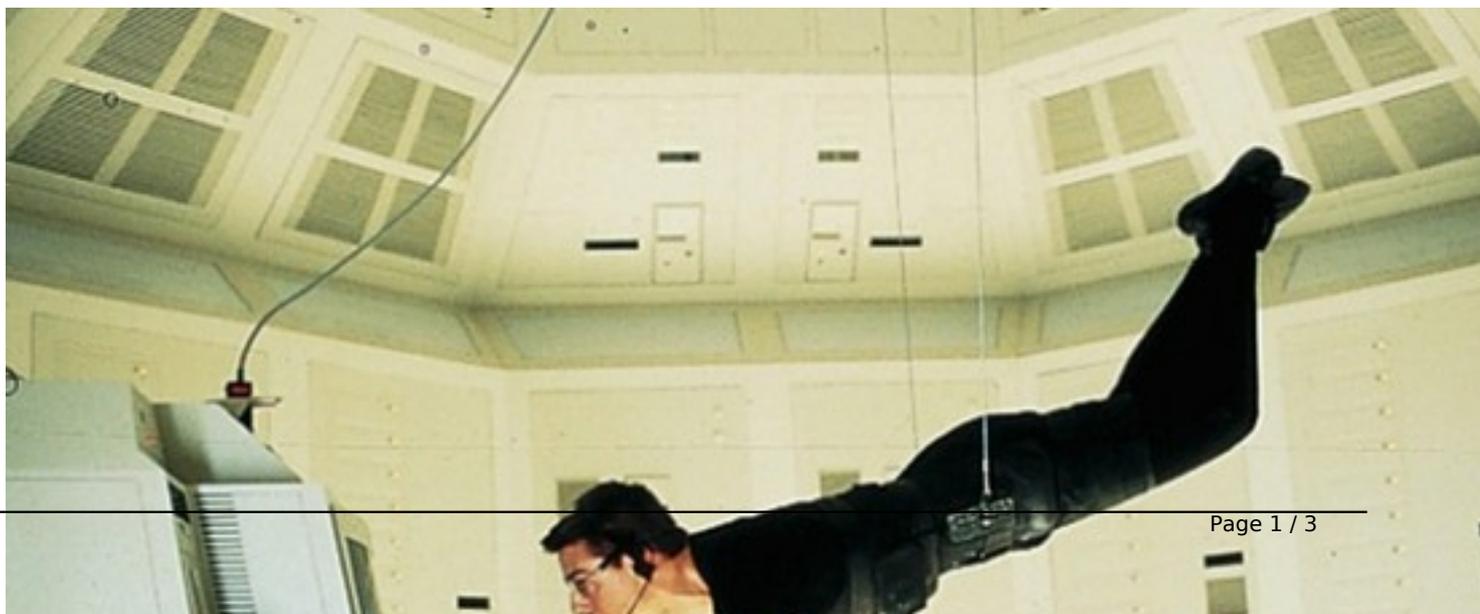
En Europe, les employ s de bureau qui ont d j  emport  des informations reconnaissent avoir quitt  leur entreprise en ayant sous le bras des pr sentations [46 %], propositions [21 %], plans strat giques [18 %] et feuilles de route de produits/services [18 %].

Plus inqui tant encore, la moiti  (51 %) se servent directement dans les bases de donn es client confidentielles, en d pit des lois de protection des donn es en vigueur.

 

 

 



  
  
  
  
  

Et si les mesures qui bloquent l'acc  s aux informations se d  clenchent d  s l'instant o   l'employ   remet sa d  mission, alors il y a de grandes chances que les documents soient subtilis  s juste avant.

La confiance exprim  e par les employeurs appara  t donc en total d  calage. Surtout quand on mesure la valeur de l'information pour les professionnels interrog  s pour l'activit   : cabinets juridiques, services financiers, assurances, fabrication industrielle, g  nie civil et industrie pharmaceutique.

Il est extr  mement important que les employeurs appr  hendent l'ampleur du risque. Qu  ils r  alisent que mettre en place des proc  dures dissuasives pour g  rer le risque pour l'information que posent les salari  s ne suffit pas, encore faut-il contr  ler leur efficacit  .

Autrement dit, supprimer l'acc  s au r  seau interne de l'entreprise le jour-m  me o   la personne d  missionne rel  ve certes d'une bonne intention, mais   a ne rime    rien si, la semaine qui pr  c  de, l'employ   a pu imprimer en toute tranquillit   des documents sensibles ou s  nvoyer des bases d'infos clients sur son adresse e-mail priv  e.

Le tableau n'est pas non plus totalement noir. Deux tiers (67 %) des employeurs disent mesurer le risque que constituent les d  parts de salari  s pour la s  curit   de l'information. La plupart estiment qu'ils ont pris les mesures qui s'imposaient. Que pourraient-ils donc faire de plus ou de mieux ?

La r  ponse se trouve dans l'information et la sensibilisation des employ  s. Il est essentiel qu'ils comprennent ce que sont les informations confidentielles et qu'ils mesurent les cons  quences l  gales ou les pr  judices de r  putation que peut occasionner une fuite de donn  es.

Une conclusion tr  s int  ressante ressort de l'activit   2012 : le comportement des employ  s est directement li      l'existence ou non d'une politique de protection des donn  es dans l'entreprise et    la mani  re dont elle leur est communiqu  e.

Par exemple, 80 % des sond  s allemands disent comprendre les consignes vis-  -vis des informations qu'il est ou non possible de sortir de l'entreprise, contre une moyenne europ  enne de 57 % et un tiers seulement a d  j  mport   des documents qu'ils avaient produits eux-m  mes, contre une moyenne europ  enne de 56 %. Conclusion, les employ  s qui connaissent les r  gles agissent en cons  quence.

En ce qui concerne les donn  es les plus sensibles et confidentielles, des mesures de s  curit   suppl  mentaires sont envisageables, comme d  emp  cher les employ  s d'enregistrer des donn  es sur leur PC.

Il est possible   galement de limiter l'acc  s en lecture seule, et sur demande exclusivement, aux donn  es conserv  es dans un r  f  rentiel central (les dossiers de patients ou les statistiques de recherches, par exemple). Cette derni  re pratique est d  j  largement adopt  e

dans le secteur de la santé.

Le message est clair. Pour garantir la protection des données en continu et non seulement au moment du départ, c'est une culture de responsabilité vis-à-vis de l'information qu'il faut instaurer, fondée sur la confiance et le respect de la valeur de l'information, électronique et sur papier, doublée de mesures de sécurité strictes, termine Marc Delhaie, Président-Directeur Général Iron Mountain France et Suisse.