

**Dans les PME, on craint plus le vol par des salari s que la cybercriminalit **  
**Internet**

Post  par : JulieM

Publi e le : 13/1/2012 13:00:00

Une  tude r cente, r alis e par **Iron Mountain**, le sp cialiste de la gestion des informations, r v le que **20 %** des entreprises en Europe consid rent que le **risque d un vol par leurs propres employ s** est la menace la plus s rieuse en termes de s curit  de leurs informations.

Elles consid rent que ce risque est encore plus important qu une panne informatique, que la cybercriminalit  ou qu une catastrophe naturelle.

Cette  tude, commandit e par Iron Mountain, sugg re une perte de confiance des employeurs dans leurs salari s et des doutes sur leurs contr les internes.

**Il semble que ce niveau de risque ne soit pas totalement d plac .** Une  tude globale, publi e le mois dernier par le fournisseur d acc s Verizon[2], montre que, bien que seulement 17 % des violations de donn es soient d origine interne, l impact potentiel des vols par des employ s  tait plus  lev  qu une menace venant de l ext rieur, et que le risque de vols de propri t  intellectuelle du fait de salari s  tait trois fois plus probable qu une menace externe.



 « Lorsqu il s agit de la gestion des informations, l  l ment humain est le plus souvent le maillon faible de la cha ne,  » d clare **Florian Kastl**, Directeur International du D partement de la S curit , de la S ret  et de la Continuit  d Activit  de Iron Mountain.  « Les informations sont le c ur de l entreprise, et il est vital que les soci t s mettent en place des contr les stricts leur permettant de r duire, voire de pr venir, le risque de vols par leurs employ s. Cela prot gera leurs employ s, leur activit , leurs clients et leur r putation.  »

**Florian Kastl** recommande de suivre   la lettre les  tapes pratiques ci-dessous pour r duire le risque de vols par des salari s :

 **Ma trisez ce que vous savez.** Identifiez et hi archisez toutes les informations d tenues par votre entreprise   tout, qu il s agisse d  l ments constitutifs de la soci t , de documents l gaux, de propri t  intellectuelle, de donn es financi res, de

prévisions de ventes, de feuilles de route, de données clients ou RH.

❖ **Instaurez des procédures internes robustes** réduisant les occasions de vols, et les contrôles les plus stricts pour les informations les plus importantes ou les plus sensibles. Cela doit inclure un audit précisant quand, où et comment les salariés sont en contact avec des informations circulant dans l'entreprise. Cela vous permettra d'identifier les points de vulnérabilité potentielle nécessitant un accès restreint. Utilisez la technologie adéquate ou un stockage sécurisé hors et sur site, pour verrouiller et protéger vos informations. Affichez une politique claire concernant les violations.

❖ **Vérifiez que les procédures RH** soient en ligne avec votre politique de protection des informations. Des vérifications robustes lors des recrutements, le suivi des changements de comportements et une stratégie formelle en cas de départ de salarié, vous aideront à minimiser les occasions de vols. Il est reconnu que des salariés quittant une entreprise, soit pour un concurrent ou dans des conditions litigieuses, emportent des informations de l'entreprise.

❖ **Vérifiez que vos stratégies** peuvent s'adapter aux changements dans votre activité par exemple dans le cas d'une acquisition ou d'une fusion et sont suffisamment solides pour répondre aux exigences réglementaires, de plus en plus sévères.