Internet : TÃ©lÃ©travail, un risque pour la sÃ©curitÃ© informatique des PME.
Internet
PostÃ© par : JerryG
PubliÃ©e le : 22/10/2013 14:00:00

Une Ã©tude dâ□□Iron Mountain suggÃ¨re que prÃ¨s des deux tiers des employÃ©s enÂ Europe pourraient trÃ¨s bien travailler de chez eux Ã temps plein ou partiel. 3 %Â des employÃ©s lâ□□envisageraient une fois tous les deux ou trois mois et 15 %Â estiment pouvoir travailler de chez eux Ã plein temps.

Le scÃ©nario est quasiment toujours le mÃªme : entre 9 heures et 18h, ces employÃ©s font le mÃªme job quâ□□au bureau, mais chez eux, assis Ã un bureau ou Ã la table de la cuisine, face Ã un ordinateur ou au tÃ©lÃ©phone, en lien permanent avec leurs documents de travail et leurs collÃ¨gues. Leur employeur sait oÃ¹ les trouver et ce quâ□□ils font.

La plupart des employeurs mettent en place lâ□□infrastructure IT et des mÃ©canismes pour protÃ©ger Ã la fois le tÃ©lÃ©travailleur et les donnÃ©es de lâ□□entreprise. Ces mesures englobent lâ□□accÃ¨s sÃ©curisÃ© au rÃ©seau de lâ□□entreprise, la mise Ã disposition dâ□□Ã©quipements IT protÃ©gÃ©s par mot de passe, ainsi que des consignes claires des types dâ□□information qui peuvent Ãªtre sortis de lâ□□entreprise et selon quelles conditions. Il devient Ã©vident que la belle clÃ´ture blanche qui symbolise le pÃ©rimÃ¨tre de sÃ©curitÃ© de lâ□□information des entreprises doit dÃ©sormais Ãªtre Ã©tendue au domicile des tÃ©lÃ©travailleurs, Ã leur jardin et mÃªme Ã leur voiture.

A lâ□□instar dâ□□autres Ã©tudes, celle-ci rÃ©vÃ¨le que les employÃ©s de bureau interrogÃ©s sur le tÃ©lÃ©travail Ã©voquent dâ□□instinct les tÃ¢ches quâ□□il est convenu quâ□□ils rÃ©alisent dans leur journÃ©e de travail, mais de chez eux, connectÃ©s Ã Internet. Nul doute quâ□□ils ont raison, mais on en vient alors Ã occulter un aspect du fonctionnement des employÃ©s de bureau qui se vÃ©rifie de plus en plus. Cette tendance est commune Ã ceux que lâ□□on appelle les tÃ©lÃ©travailleurs â□□invisiblesâ□□ : ceux qui emportent du travail avec eux Ã la maison, en dehors de leurs horaires contractuels et souvent sans que ces conditions de travail soient rÃ©gies par un quelconque contrat.

Le tÃ©lÃ©travailleur invisible est celui qui ramÃ¨ne avec lui ce quâ□□il nâ□□a pas eu le temps de finir pour le faire dans la soirÃ©e ou pendant les week-ends. Ainsi, en fin de journÃ©e, câ□□est toute une armÃ©e dâ□□employÃ©s qui sort des documents sensibles et des informations confidentielles de leur entreprise en sâ□□affranchissant des rÃ¨gles de sÃ©curitÃ© Ã©lÃ©mentaires ; le tout avec les meilleures intentions du monde. Et il y a de grandes chances que ces tÃ©lÃ©travailleurs de lâ□□ombre nâ□□aient pas un accÃ¨s sÃ©curisÃ© Ã lâ□□intranet de lâ□□entreprise, ni mÃªme dâ□□Ã©quipement IT validÃ© par lâ□□entreprise et encore moins dâ□□accords Ã©crits et signÃ©s. Les risques auxquels sâ□□exposent les tÃ©lÃ©travailleurs rÃ©guliers sont encore intensifiÃ©s dans ce cas.

Parmi les risques pour lâ□□information, citons lâ□□utilisation dâ□□un compte de messagerie personnel pour envoyer et recevoir des documents de travail (notre Ã©tude confirme que câ□□est une pratique courante de 50 % des tÃ©lÃ©travailleurs rÃ©guliers), le fait de laisser des documents de travail chez soi, Ã la vue de tous (29 % des tÃ©lÃ©travailleurs interrogÃ©s), ou encore de jeter des documents dans la poubelle de la cuisine sans les dÃ©truire (19 %). Un petit nombre (11 % des tÃ©lÃ©travailleurs interrogÃ©s) admet mÃªme sortir des infos internes de chez eux pour aller travailler dans des lieux publics, des cafÃ©s par exemple, et 7 % reconnaissent envoyer et recevoir des documents via un rÃ©seau WiFi public non protÃ©gÃ©. Tous exposent lâ□□information Ã des

risques et Ã des attaques, avec ce que cela suppose de consÃ©quences dÃ©sastreuses pour leur entreprise si elle devait Ãªtre victime dâ□□une violation de donnÃ©es.

Quelles mesures peut donc prendre une entreprise pour mieux apprÃ©hender et encadrer ces pratiques de tÃ©lÃ©travail invisible ?

La premiÃ¨re Ã©tape, et la plus importante, est de comprendre qui apporte du travail Ã la maison, quel type dâ□□information exactement et pourquoi. Et ce nâ□□est pas seulement un problÃ¨me de risque pour lâ□□information, mais aussi une question dâ□□encadrement du personnel. Lâ□□interdiction de sortir des documents de lâ□□entreprise ne fonctionnera jamais face Ã des salariÃ©s qui se sentent incapables dâ□□assumer leur charge de travail dans les temps, qui ne savent pas bien gÃ©rer leur temps ou qui doivent sâ□□exÃ©cuter dans des dÃ©lais extrÃªmement courts. Ceux de vos salariÃ©s qui travaillent les soirs et les week-ends sont probablement les plus dÃ©vouÃ©s, ambitieux ou combatifs ; ils mÃ©ritent quâ□□on les soutienne et non quâ□□on les censure.

La seconde Ã©tape consiste Ã instaurer des consignes claires de manipulation responsable de lâ□□information, communiquÃ©es Ã lâ□□ensemble du personnel, et non uniquement Ã ceux qui sont officiellement autorisÃ©s Ã travailler de chez eux.

Ces mesures RH doivent sâ□□appuyer sur une infrastructure robuste dâ□□administration IT et de gestion documentaire, englobant les documents Ã©lectroniques et papier. En effet, lâ□□information peut Ãªtre vÃ©hiculÃ©e et fuiter par e-mail, sur des ordinateurs portables, sur des clÃ©s ou des unitÃ©s de stockage, ou imprimÃ©e sur des feuilles A4 : vous devez gÃ©rer lâ□□ensemble des risques que supposent ces canaux de communication de lâ□□information.

Certains dossiers trop confidentiels, sensibles ou stratÃ©giques ne peuvent tout simplement pas quitter lâ□□entreprise ; pour ceux-lÃ , des restrictions dâ□□accÃ¨s incontournables sâ□□imposent.

Enfin, les dirigeants des entreprises doivent comprendre que la responsabilitÃ© de la protection de lâ□□information, tout en maintenant sa libre circulation dans lâ□□entreprise Ã©tendue, ne relÃ¨ve pas uniquement des services IT, des archivistes ou mÃªme des RH, mais bien que chacun doit se sentir concernÃ©, Ã commencer par eux-mÃªmes.

Il revient aux cadres supÃ©rieurs et membres de la direction de dÃ©finir quels comportements et quels processus sont acceptables et lesquels doivent Ãªtre proscrits, mais câ□□est aux collÃ¨gues, aux responsables et aux supÃ©rieurs directs de veiller Ã ce quâ□□aucun salariÃ© ne demeure invisible, oÃ¹ quâ□□il travaille, surtout ceux qui donnent leur maximum pour ne pas se laisser submerger par leur charge de travail.