

Cafés sans filtre

Les petits-déjeuners débats de Groupe Synergie Globale

Compte-rendu du 30 avril 2009 sur

Les risques liés à l'externalisation et à la sous-traitance de la gestion des données sensibles de l'entreprise

Autour de Jean-Michel Errera, membre du Directoire de la Caisse d'Épargne Ile-de-France en charge de l'informatique, des services bancaires et de l'organisation et d'André Tarrat, Directeur de la sécurité, Deloitte France

Débats coanimés par Eric Denécé, Directeur du Cf2R, notre partenaire ainsi que par Didier Rancher, Directeur général délégué de Groupe Synergie Globale

Un grand nombre d'entreprises externalisent ce qui ne relève pas, selon elles, de leur cœur de métier. Les fonctions externalisées correspondent à des tâches souvent considérées comme subalternes, du moins répétitives et bien formatées, ce qui facilite la rédaction d'un contrat, pièce maîtresse du dispositif d'externalisation.

Il existe un certain nombre d'intérêts pour justifier un processus d'externalisation : gagner en flexibilité, trouver des savoir-faire qui n'existent pas en interne, dégager un gain financier et des gains sur les coûts cachés (réunions, trajets, etc.).

S'il y a des secteurs où l'on ne peut se passer de l'externalisation, il est prudent de garder en tête que l'intérêt financier ne peut être le seul argument. Toutes sortes de risques sont en effet associés à l'externalisation : sociaux, perte de savoir-faire, difficulté à revenir en arrière, qualité, image, etc.

Le suivi notamment s'avère délicat. En termes de risques, la principale vulnérabilité vient de l'humain. Or cette dimension est bien souvent mise de côté lorsqu'il est question de ces fonctions répétitives et les vrais risques sont ceux qu'on laisse de côté sans les voir.

Comment alors limiter les risques liés à l'externalisation et à la sous-traitance de la gestion des données sensibles de l'entreprise ? En matière d'externalisation, il n'existe pas de règles d'or. La réflexion se fait au cas par cas tout en respectant quelques principes de bon sens :

1. Pour bien externaliser une activité, il faut d'abord la **maîtriser en interne**, ne serait-ce que pour être en mesure de contrôler. Bref, on ne se débarrasse pas via l'externalisation d'une activité que l'on ne maîtrise pas. Il est prudent par ailleurs de garder en interne des experts qui auront pour mission d'aller contrôler régulièrement ce qui se passe chez le prestataire externe.
2. L'externalisation ne peut se concevoir qu'avec une **vision long terme**. Elle se prépare comme un projet avec toute une structure projet à mettre en place. Elle se conçoit également comme une action de partenariat et doit donc être gagnante pour les deux parties.
Dans un contexte marqué par le court terme et les quick wins, il faut s'efforcer de prendre le temps de la réflexion et éviter la précipitation.
Externaliser nécessite donc un investissement très lourd, tant en ressources humaines qu'en moyens ou en temps.
3. **S'appuyer sur les normes**. Au-delà des risques classiques qui pèsent sur une gestion de projet insuffisamment préparée, l'externalisation implique des risques non conventionnels de toutes sortes et il n'est pas toujours aisé d'en convaincre les dirigeants en dehors de l'occurrence d'un quelconque accident.
Dans ce contexte, les normes ont un rôle à jouer : on ne peut d'ailleurs en faire l'économie lorsque l'on parle de contrôle qualité. A minima, on s'inspire de celles qui existent dans le monde industriel (normes ISO) auxquelles se sont ajoutées très récemment des normes sur la sécurité des systèmes d'information (exemple : norme 27005). Ces dernières permettent de passer d'une culture de la conformité (la *compliance* des anglo-saxons) à la culture du risque car elles obligent à se projeter dans l'avenir pour imaginer une menace ou une vulnérabilité.
Parler « norme » représente donc déjà un progrès. Les normes permettent aussi de fixer une limite droite et une limite gauche, ce qui permet de réduire les risques liés au fait que chacun à son poste n'a pas la perception du risque, il pense toujours que c'est le problème du voisin.
4. Dernière précaution utile : envisager chacun des risques liés à l'externalisation de façon très **concrète** : « risque image », par exemple, « chez nous, qu'est-ce concrètement ? ». Lorsqu'Alcatel Lucent annonce qu'il va externaliser une partie de son informatique, comment a-t-il prévu de se prémunir contre la possibilité pour des concurrents, des sectes..., de placer leurs pions en amont chez ses éventuels futurs sous-traitants ?

En conclusion, il faut souligner que dans un contexte de crise économique et sociale aigue comme celle que nous traversons actuellement, les risques liés à l'externalisation et à la sous-traitance de la gestion des données sensibles de l'entreprise augmentent proportionnellement à la fébrilité des Etats majors. Mauvaise conseillère, la précipitation peut conduire à faire appel à des externes sans respecter un minimum de précautions.