La France mauvais élève de la certification ISO ?

Réunis par le Clusif (Club de la Sécurité de l'Information Français), responsables sécurité, RSI… ont abordé la question des stratégies en matière de management de la sécurité de l'Information (**SMSI**) et de leur prolongement, la certification **ISO 27001**.

La norme créée en 2005 traitant des politiques de gestion de la sécurité connaît un **manque d'intérêt** dans les organisations quel que soit leur secteur d'activité. Pour preuve, à l'heure actuelle, **seulement un poignée d'entreprises françaises (10) l'ont adopté** à en croire l'Organisation internationale de normalisation.

Car si les professionnels ne rechignent pas, en général, à établir un véritable plan pour assurer la sécurité de leur Information, rares sont celles qui franchissent le pas vers la norme ISO. Fouad Echaouni, Adjoint RSI de Maroc Telecom résume la situation : « *la norme ISO 27001 a le but simple d'**éviter que les informations stratégiques ne s'ébruitent ou ne se perdent**. Il s'agit donc d'une étape presque obligatoire pour les sociétés. Cela nous assure une **confiance supplémentaire** de la part de nos clients mais aussi de nos collaborateurs*« .

Un constat que confirme Stéphane Duproz, Directeur Général de TelecityGroup, société spécialisée dans les centres d'hébergement. Il se confirme que l'intérêt entre une politique sérieuse de sécurité et une certification réside dans l **'image qu'elle va donner**. Le dirigeant s'explique : « *ISO 27001 nous confère un gain en matière d'image. Un gage de sérieux qui nous donne un **avantage stratégique** certain alors que le coût à la marge entre SMSI et ISO est faible*. Il poursuit, *un moindre coût qui nous fait **économiser maintenant sur les audits externes***« .

Dès lors, par quel chemin arriver à la certification ? Tous s'accordent sur un réel « **plan d'attaque**« , ou plutôt un plan annuel de contrôle des processus qui vont servir à analyser les risques en matière de sécurité informatique de chaque métier. Ce contrôle *a priori*de tout ce qui constitue la société va alors être plus consistant à mesure de l'avancée dans le plan. Une entreprise va alors pouvoir prendre plusieurs mois à plein temps pour tout contrôler. Un délai qui peut sembler trop étendu pour certains comptes.

Laurent Bellefin, directeur des opérations sécurité chez Solucom, spécialisée dans les audits de sécurité témoigne du manque de **maturité des entreprises françaises** : « *bien définir le périmètre, c'est-à-dire quels sont vos besoins sont les maîtres mots. Cela dit **ISO ne garantit pas un bon niveau de sécurité**. Cela ne doit pas être une fin en soi. Une donnée qu'à mon avis peu de responsables ont encore compris*« .

Si encore peu de société françaises ont fait le pas vers ISO 27001, les choses pourraient changer puisqu'une **nouvelle norme** concernant les données bancaires voit le jour sous le terme de **PCIDSS**. Un nouveau défi dont on verra s'il est relevé par les dirigeants.