Bien des questions en suspens pour une profession qui attend des réponses!

L'avis de Charles Delbrassine, IT Works

Qu'est-ce qu'un CSO? Question complexe, qui mérite réflexion... Je pense qu'il est nécessaire de scinder la sécurité en deux profils différents selon le rôle au sein de l'entreprise.

• Un premier, très proche d'un gestionnaire des risques, dont le rôle est de conseiller, recommander, alerter et informer la direction générale à laquelle il est directement attaché. C'est à ce profil que j'appliquerais la dénomination de CSO - Chief Security Officer
• Un second, attaché à la direction informatique, dont le rôle est de veiller à la qualité de déploiement et d'utilisation des outils technologiques sécuritaires veillant à la protection de l'information.

Le CSO a donc une fonction plus transversale et organisationnelle que purement technique. Le fait que le CSO ne dépende pas de la direction informatique lui offre une indépendance nécessaire lors de ses missions de recommandations ou de contrôle de la gestion de la sécurité.

C'est à ce responsable qu'il appartient souvent de convertir un langage «sécurité» habituellement technique en termes représentatifs pour les preneurs de décision. Son rôle est de donner des indicateurs clairs de la sécurité par rapport à des normes reconnues, d'identifier les améliorations possibles et de proposer des solutions d'amélioration de la situation.

C'est en grande partie la qualité de son travail et son habilité qui permettront de justifier des investissements dans le domaine de la sécurité, lesquels seront souvent très bien accueillis par son collègue de la sécurité «technique». La sécurité profiterait donc pleinement d'une étroite collaboration entre les deux profils... mais c'est rarement le cas.

Autre interrogation: la responsabilité. Il est à remarquer que la fonction de CSO s'exerce de plus en plus à l'intérieur et à l'extérieur du système d'information et même de l'entreprise. En effet, quand il s'occupe de la sécurité des cartes à puce, il va au-delà des problématiques informatiques pures et sa responsabilité est directement exposée à l'extérieur de l'entreprise.

Le problème est d'autant plus aigu que la notion de délégation de responsabilité et de cogestion des risques avec la Direction Générale devant les tribunaux n'est pas encore bien définie à l'échelle européenne.

Aujourd'hui, le terme de « CSO » demeure vague, en l'absence de texte. Il faut surtout définir l'objet de la délégation, et informer les directions générales de ce qu'elles délèguent. Le problème essentiel est simple : a-t-il, oui ou non, les moyens d'assumer sa délégation? On pourrait avancer que, s'il démontre qu'il n'a pas les moyens de sa politique, sa responsabilité est désengagée, dans la mesure où il a prévenu la direction générale des risques identifiés.

On peut également s'interroger sur la formation du CSO. Plus particulièrement, quelle certification accorder aux CSO? En 2005, la plupart des personnes qui exercent cette fonction n'ont pas de diplôme spécifique à leur fonction et sont issues de la filière technique. Les examens liés aux certifications doivent pallier ce manque. Mais doit-on en choisir une qui soit reconnue par une norme comme la 17024 de l'ISO; la CISSP (Certified Information Systems Security Professional) d'ISC (International Information Systems Security Certification Consortium)? Bien des questions pour une profession qui attend des réponses.

■