

Quelle organisation pour prendre en compte le risque informatique

Philippe GUARNIERI

Enquête CLUSIR 2008

- 37 % des entreprises ont une fonction SSI (16% temps plein, 21 temps partagé).
- Parmi celles ci :
 - 45 % Direction Générale (39 % en 2006)
 - 32 % DSI (41 %, en 2006)
 - autres 20 % (18 % en 2006)
 - dont :
 - 1 % Direction des risques
 - 1 % sûreté générale.

Les différentes organisations possibles (non-exhaustif)

- SSI au sein de la DSI, le DSI cumule avec la fonction de RSSI
- SSI au sein de la DSI avec RSSI
- SSI au sein de la DG
- SSI au sein du Service AUDIT
- SSI au sein d'une direction métier
- SSI au sein du service qualité
- SSI au sein du Risk Management
- Pas de RSSI

SSI au sein de la DSI, le DSI cumule avec la fonction de RSSI

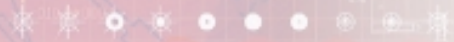
- *Avantages*
 - Le DSI a une vision globale du SI (Sécurité incluse) même si elle reste, le plus souvent, technique
- *Inconvénients*
 - Difficulté de relier la SSI à des processus métiers et donc difficulté pour obtenir les budgets (SI vu comme centre de coût)
 - Le DSI a pour mission de minimiser les coûts et en cas de crise, la SSI en fait les frais.
 - Activité à temps partagé
 - Compétences ?
 - Communication : s'adresser à l'entreprise dans un langage de spécialiste

SSI au sein de la DSI avec RSSI

- *Avantages*
 - Prise en compte de toutes les interactions techniques, adaptée aux démarches de type bonne pratique technique
- *Inconvénients*
 - Pas toujours une prise en compte du risque métier, pas de corrélation automatique et donc rend les projets sécurité difficiles à justifier en terme de ROI
 - Pas de démarche processus naturelle qui permettrait au fonctionnement de l'informatique plus de compatibilité avec le reste de l'entreprise
 - La SSI comme le SI est considéré comme un centre de coût
 - S'adresser à l'entreprise dans un langage de spécialiste

SSI au sein de la DG

- *Avantages*
 - Signifie la prise en compte au plus haut niveau de décision
 - Discours nécessairement compatible avec celui de l'entreprise.
 - Décisions suivies d'actions.
- *Inconvénients*
 - Sauf cas particulier, il vaut mieux associer cette fonction à une autre fonction plus universelle, l'idéal est une direction de l'information au sens large
 - Traiter la sécurité en mode exception, effet balancier



SSI au sein du Service AUDIT

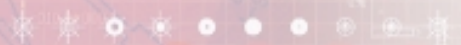
- *Avantages*
 - La SSI devient une fonction qu'il faut auditer comme les autres fonctions de l'entreprise.
 - Position légitime en cas de besoin de certification.
- *Inconvénients*
 - Position faible pour mettre en œuvre le changement

SSI au sein d'une direction métier

- *Avantages*
 - En prise naturelle avec les risques de l'entreprise surtout si le métier choisi est le cœur de métier.
- *Inconvénients*
 - Pas de prise en compte de tous les métiers
 - Démarche de type Risk Management non-assurée du point de vue méthodologique.

SSI au sein du service qualité

- *Avantages*
 - Convergences des méthodes avec la qualité PDCA, indicateurs, processus.
 - Service habitué à pratiquer un mode de management transversal (comme la sécurité) : atteindre des objectifs avec des collaborateurs qui ne sont pas sous votre responsabilité directe
- *Inconvénients*
 - Ne voir la sécurité que comme une méthode, passer à côté des enjeux principaux



SSI au sein du Risk Management

- *Avantages*
 - Au cœur des processus "sensibles" de l'entreprise
 - La démarche risque est naturelle
 - Seule fonction capable de faire de la SSI un avantage concurrentiel
 - L'avenir ?
- *Inconvénients*
 - Compétence ? dépend du profil et du mode de management
 - Il n'existe pas toujours un pôle « Risk Management »

Pas de RSSI

- *Avantages*
 - Si aucun risque n'existe, économie budgétaire
- *Inconvénients*
 - Aucune prise en compte du risque et donc conséquences qui peuvent être graves pour la pérennité de l'entreprise

Conclusion

- *Ce qui est sur :*
 - Sans lien métier pas de politique de sécurité adaptée aux vrais risques informationnels de l'entreprise, pas de vraie légitimité et par conséquent pas pérenne.
 - L'ambition de la DSI est limitée par la nature de sa fonction et de par sa position.
 - CLUSIR 2008 : 30 % des entreprises ont une analyse de risque.
- *Ce qui est possible*
 - Faire participer les métiers à la construction de la politique de sécurité.
 - Dans certains cas, les nouvelles normes de type 2700x peuvent servir de pont avec les autres métiers

L'adoption de telle ou telle organisation est significative de la perception du risque informatique par l'entreprise.