



devoteam
consulting ↑



Enquête internationale
sur la sécurité des Systèmes d'Information 2008

CONNECTING BUSINESS & TECHNOLOGY



Hervé Morizot, ingénieur ESIEA, a intégré le groupe Devoteam en 2004 pour prendre la direction de XP Conseil. En 2007, il devient Directeur de l'entité Information Management et Sécurité de Devoteam Consulting.

Hervé Morizot pilote de nombreuses missions de management de la sécurité des SI (organisation, politique, communication, gestion des risques et audit, tableaux de bord, etc.) pour de grands groupes français. Il intervient en tant qu'animateur de nombreux séminaires sur la sécurité, est chargé de cours à l'Ecole Nationale Supérieure des Télécommunications de Paris et préside le Comité de Programme Eurosec' depuis 2005.



CONTEXTE



Pour la cinquième année consécutive, **Devoteam Consulting** a réalisé son enquête sur les enjeux, l'organisation et les activités liés à la sécurité des Systèmes d'information.

L'enquête 2008, basée sur un questionnaire de 39 questions, a été réalisée auprès d'un panel significatif international de responsables de la sécurité du système d'information (RSSI) : au total 177 personnes y ont participé sur le territoire européen (Autriche, Belgique, Danemark, France, Italie, Norvège, République Tchèque, Royaume-Uni), l'Afrique du Nord (Maroc) et le Moyen-Orient (Arabie-Saoudite).

Les entreprises et administrations ciblées comptent plus de 500 salariés et sont représentatives des différents secteurs d'activités : industrie & services, finance et secteur public.

L'enquête sécurité 2008 reprend certains thèmes abordés lors des précédentes éditions afin de dégager des tendances sur l'évolution du métier et des problématiques liées à la sécurité.

D'autres thèmes ont été ajoutés afin de prendre en compte les nouvelles préoccupations.



RÉSULTATS

L'organisation de la fonction

Le rattachement du RSSI (Responsable de la Sécurité des Systèmes d'Information) dans l'organisation reste bien souvent stable même si ses attributions évoluent :

- La fonction du RSSI reste bien reconnue au sein de l'entreprise pour 72% d'entre eux, même si l'on note une légère baisse par rapport aux années passées (75% en 2007).

24% des RSSI éprouvent ainsi un manque de reconnaissance de leur fonction qu'ils imputent bien souvent au manque de maturité et de sensibilisation des acteurs internes sur les risques liés au système d'information et au fait que leurs actions sont, dans la plupart des cas, « transparentes » pour les utilisateurs.

- La taille globale de l'équipe dédiée à la sécurité des systèmes d'information est variable selon la taille et le secteur d'activité de l'entreprise : 67% des RSSI disposent d'une équipe d'une à cinq personnes, 10% des RSSI ont une équipe dépassant les 20 personnes.

Les secteurs dont le métier repose très largement sur les systèmes d'information sont très consommateurs de ressources orientées sécurité (banque, finance, énergie, etc.).

Le nombre de correspondants sécurité dans les métiers et filiales de grands groupes peut atteindre plusieurs centaines de personnes.

Par ordre de priorité, ces équipes répartissent leurs activités entre la sécurité des infrastructures, la gestion opérationnelle de la sécurité, les aspects liés à la gouvernance et enfin la continuité d'activité (PCA / PRA).

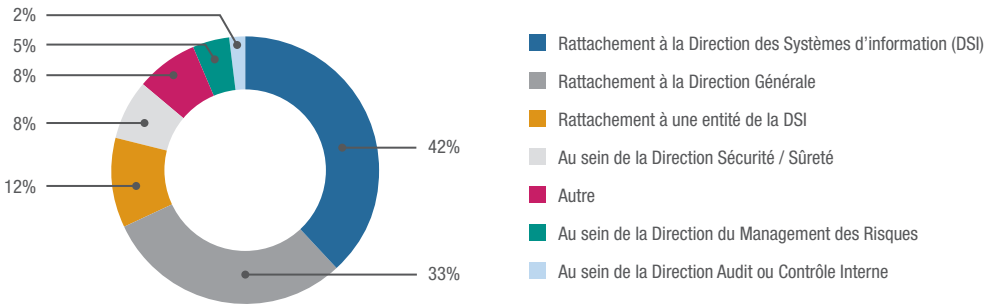
- 33% des RSSI sont rattachés à la direction générale alors que 54% sont rattachés à la DSI (directement à la DSI ou à une entité de la DSI). Les autres sont rattachés à d'autres directions (Sûreté, Gestion des risques, Audit, etc.).

Ce positionnement est souvent lié au métier, ainsi qu'à la taille de l'entreprise : le rattachement à une entité autre que la DSI est souvent observé dans les entreprises ayant entrepris une démarche de pilotage de la sécurité par les risques. Dans les petites structures, le RSSI peut cumuler plusieurs rôles opérationnels (études et développements, pilotage de projets, activités de gestion). Il est alors naturellement rattaché à la DSI.

Seuls 44% des RSSI interrogés sont dédiés à la sécurité des systèmes d'information dans leur entreprise.

- Enfin, les RSSI sont systématiquement consultés pour les évolutions liées au système d'information et l'opinion de 69% d'entre eux est « suivie » lorsqu'ils s'opposent à des évolutions qu'ils jugent contraires aux enjeux de sécurité de l'entreprise.

Rattachement du RSSI dans l'organisation



Les grands chantiers de gouvernance sécurité en 2007

En comparaison des années passées, les sujets relatifs à la gouvernance de la sécurité ont évolué. La priorité a été davantage mise en 2007 sur :

- L'amélioration de la continuité des activités (59% contre 53% en 2006),
- La conformité juridique et réglementaire (40% contre 33% en 2006),
- La sensibilisation et la professionnalisation (43% contre 35% en 2006),
- La gestion globale des risques (41% contre 31% en 2006),

Sur ce sujet 30% des entreprises ont mené une évaluation globale des risques en 2007 et 27% une évaluation des risques sur les processus dits « sensibles ».

39% des entreprises ont engagé cette démarche globale d'évaluation des risques pour respecter les engagements de politique interne, 27% pour respecter des exigences légales.

Enfin 36% d'entre elles réévaluent leurs risques chaque année et 37% occasionnellement, démontrant ainsi une volonté de pérennisation de la démarche d'amélioration continue.

- La lutte contre la fraude impliquant les systèmes d'information reste néanmoins parfois négligée (22% contre 12% en 2006).

23% des RSSI ont mis l'accent en 2007 sur la définition et la mise en place de tableaux de bord de contrôle de la sécurité. 55% d'entre eux disposent de tableaux de bord pour assurer :

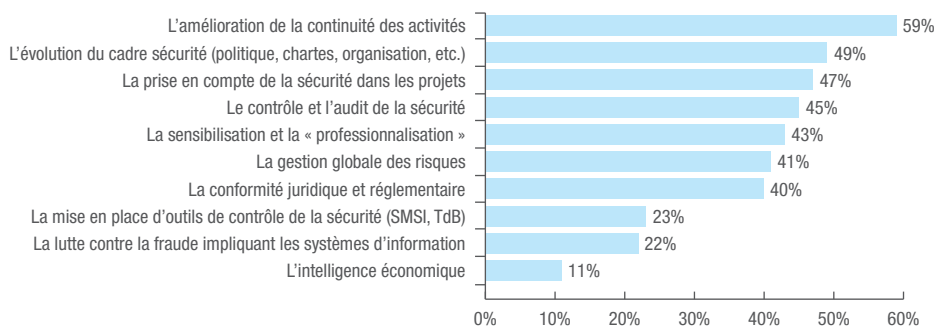
- Le suivi de la sécurité dans les projets (28%),
- Le suivi des attaques, propagations virales (35%),
- Le suivi des déploiements d'outils de sécurité, de patches (35%).

L'Intelligence Economique (IE) a été une priorité en 2007 pour seulement 11% des répondants, ce sujet étant souvent porté par d'autres entités au sein de l'entreprise (stratégie, communication, commerce, etc.).

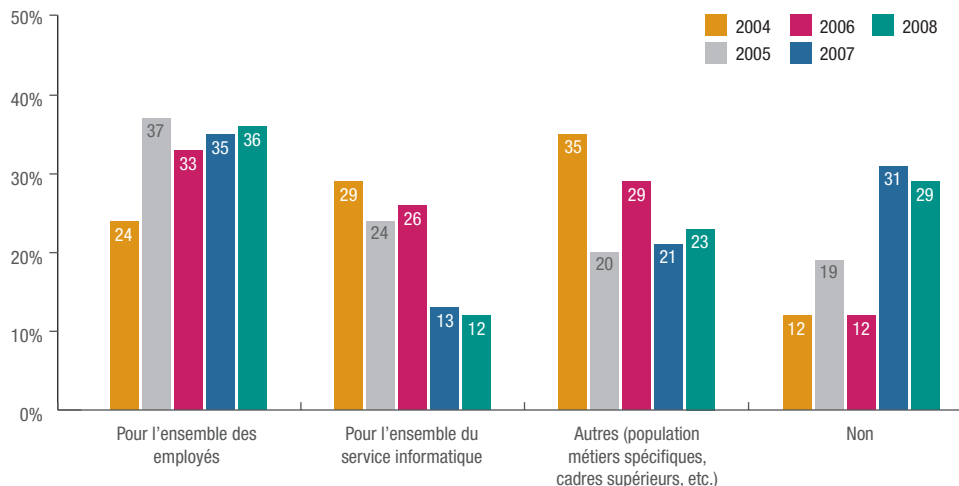
Les sujets de gouvernance traités partiellement, l'ont été par insuffisance budgétaire (39%), par manque de temps (64%), dû au mauvais dimensionnement des équipes (41%), au manque d'implication de la direction générale (26%) et au profit d'autres priorités (24%).

Les entreprises disposent de cellules de veille dédiées à la sécurité : 59% d'entre elles disposent d'une veille technologique (failles, correctifs, etc.) et 41% ont une veille juridique.

Les priorités de niveau 1 liées à la gouvernance de la sécurité en 2007



Votre entreprise organise-t-elle des formations ou des sensibilisations à la sécurité des SI ?



71% des entreprises mènent un programme de formation ou de sensibilisation à la sécurité du SI.

27% des RSSI considèrent que cette action est une démarche continue avec un budget dédié, 40% souhaitent que cette démarche soit renouvelée chaque année et 23% estiment que c'est un exercice ponctuel à effectuer tous les 3 ou 4 ans.

L'évolution démontre que les programmes de sensibilisation sont de plus en plus orientés vers l'ensemble des collaborateurs de l'entreprise, et plus seulement vers les populations informatiques. Les démarches de sensibilisation spécifiques ciblées vers des catégories spécifiques (managers, population métier spécifique) sont de plus en plus envisagées, souvent en complément des programmes de sensibilisation globaux.

Enfin, pour 32% des répondants, chaque nouvel embauché suit un programme de formation dédié à la sécurité des systèmes d'information.

Les chantiers de protection des infrastructures en 2007

Les préoccupations des entreprises pour la sécurisation des infrastructures en 2007 ont été les suivantes par ordre de priorité :

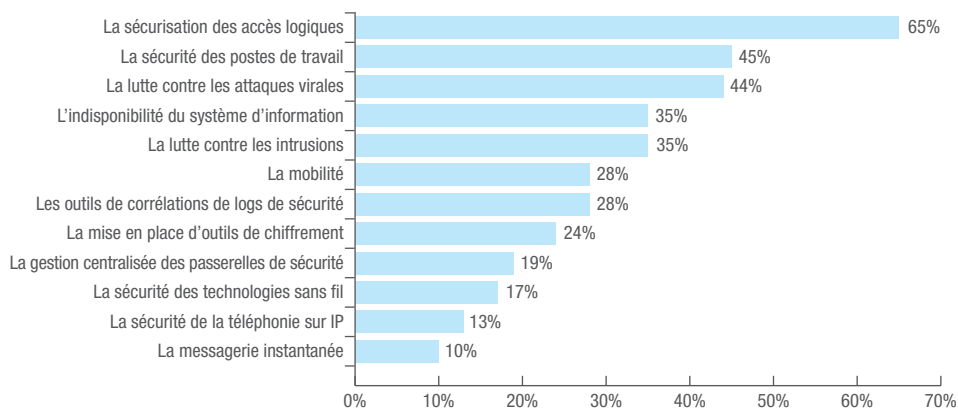
- **La sécurisation des accès logiques** (habilitations, révocations, etc.) occupe la première place comme en 2006 pour 65% des entreprises,
- Viennent ensuite les projets portant sur la sécurité du poste de travail (45%) principalement du fait des premières migrations vers Vista, ainsi que de la convergence sur le marché des éditeurs de sécurité,
- La lutte contre les attaques virales (44%) reste une préoccupation récurrente des entreprises, alors que la lutte contre les intrusions est de plus en plus présente (35% en 2007 contre 12,5% en 2006),
- L'indisponibilité du système d'information préoccupe 35% des RSSI en 2007 (contre 45% en 2006).

Les chantiers liés à la mobilité, les outils de corrélations de log, la mise en place d'outils de chiffrement sont des priorités de niveau 1 pour environ 28% des entreprises.

D'autres thèmes n'intéressent qu'une partie des entreprises qui les placent en priorité de niveau 1 :

- La gestion des passerelles centralisées (19%),
- La sécurité des technologies sans fil (17%),
- La sécurité de la téléphonie sur IP (13%),
- La messagerie instantanée (10%).

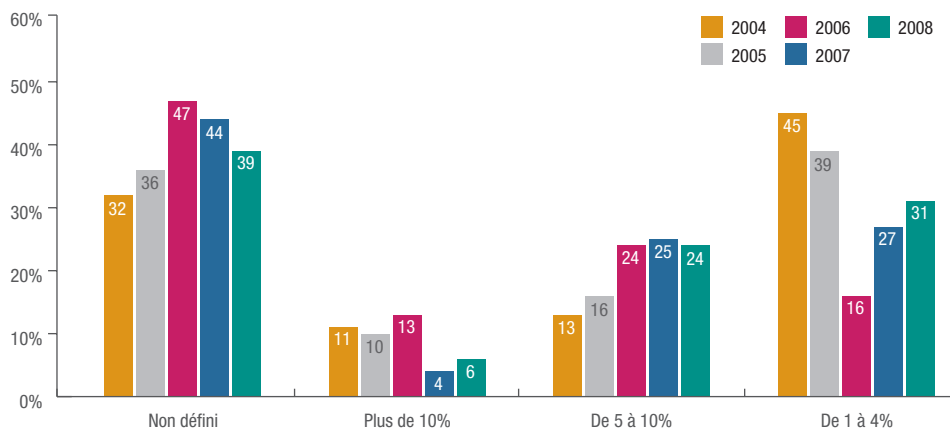
Les priorités de niveau 1 liées à la sécurité des infrastructures en 2007



Evolutions budgétaires

Concernant les évolutions budgétaires, comme pour la précédente enquête sur 2006 / 2007, 85% des RSSI constatent que le budget sécurité de 2008 est soit constant, soit en augmentation par rapport à 2007. Le périmètre de la sécurité reste variable d'une entreprise à l'autre (sauvegardes, PRA, gestion de risques informationnels, etc.) et le budget moyen est d'environ 5% du budget SI.

Quel sera le pourcentage du budget informatique alloué à la sécurité au sein de votre entreprise en 2008 ?



Constats sur les résultats de la mise en œuvre des dispositifs de sécurité du SI

Une amélioration en ce qui concerne les attaques virales :

En 2007, 52% des entreprises interrogées ont été victimes d'attaques virales sans conséquences majeures (contre 57% en 2006), 7% ont subi des conséquences significatives (contre 8% en 2006), et 39% d'entre elles n'ont pas constaté d'attaque (contre 35% en 2006).

Parmi les entreprises victimes d'un problème de sécurité du système d'information (intrusion, vol de données, indisponibilité, virus, etc.), seules 12% ont pu identifier des pertes financières.

D'autre part, 55% des RSSI ne mesurent pas le retour sur investissement de la sécurisation de leur système d'information. Seuls 29% le font.

Les priorités 2008

Les chantiers prioritaires en 2008 en matière de gouvernance sécurité sont de trois natures :

- **Evolution du cadre de sécurité**

En moyenne, 90% du panel possède un référentiel sécurité (politique, directives, charte), mais celui-ci sera intégré dans un processus de maintenance et de contrôle.

- **Déploiement de la norme ISO 27001**

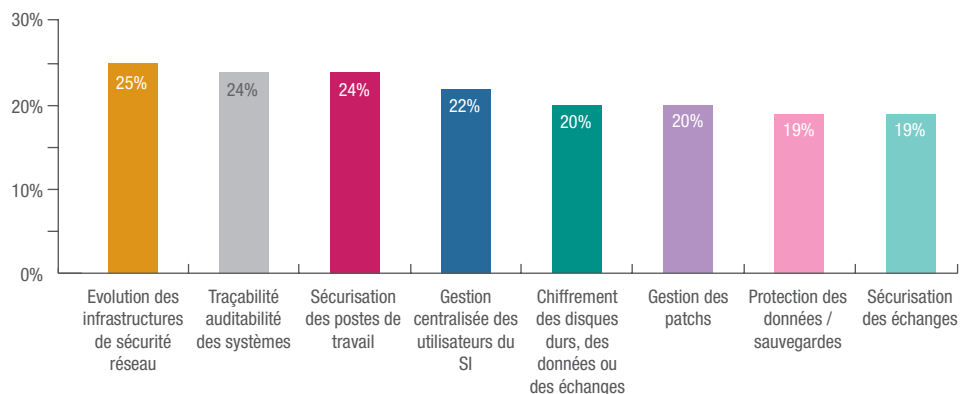
Si la norme apporte en matière de contrôle (axe identifié comme faible en 2007), de nombreuses entreprises visent une conformité à la norme sans certification dans un premier temps.

- **Evaluation des risques**

Cet axe n'est mentionné que par 30% du panel mais l'actualité du début d'année et les perspectives de renforcement des exigences réglementaires laissent présager une accélération prévisible de l'approche risque.

Les chantiers prioritaires en 2008 sont centrés sur les évolutions des infrastructures de sécurité réseau (décloisonnement, renforcement, etc.), la sécurisation du poste de travail et la traçabilité et l'auditabilité des systèmes.

Les thèmes technologiques prioritaires à mettre en œuvre en 2008



La conformité

Réglementaire

La proportion des RSSI impliqués directement ou indirectement dans une démarche réglementaire de l'entreprise est toujours aussi élevée (76%).

Les réglementations applicables sont, au delà de la législation Informatique et Libertés (55% seulement des RSSI y sont impliqués), aux réglementations métier (31%), à la LSF (25%), Bâle II (23%), SOA et CRBF (20%).

Audit interne / externe

65% des RSSI déclarent avoir effectué au moins un audit interne durant l'année et sont en très grande majorité impliqués dans l'élaboration et le suivi des plans d'actions.

62% d'entre eux ont également effectué un audit externe dans l'année pour identifier les faiblesses (40%) et vérifier la conformité réglementaire (15%).

Normes, Référentiels

44% des entreprises utilisent la norme ISO 17799 / 27002 pour rédiger la politique de sécurité (34%) ou pour effectuer un diagnostic du niveau de sécurité (20%).

38% des entreprises utilisent la norme ISO 27001 pour mettre en place un cadre de management de la sécurité des systèmes d'information (SMSI) et 10% d'entre elles préparent déjà une certification, souvent sur un périmètre très restreint.

L'utilisation de référentiels COBIT ou COSO reste cependant assez faible (respectivement 24% et 9%).

devoteam
consulting ↑

86, rue Anatole France 92300 Levallois-Perret
Tél. : +33 (0)1 41 49 48 48
www.devoteam.fr