

Tome IV

Octobre 2007

# LIVRE BLEU

Quels pouvoirs en sécurité  
des SI ?

réalisé par

 **Hapsis**  
Education

pour


 07  
**Les Assises**  
L'Événement Européen de la Sécurité et des Systèmes d'Information



# Prenez de l'altitude avec **Le cercle**

**Le Cercle Européen de la Sécurité et des Systèmes d'Information  
rassemble les utilisateurs et décideurs en sécurité informatique**



 Parce que cybercriminalité et cyber-terrorisme sont devenus des menaces actuelles pesant sur l'activité des entreprises et des services de l'Etat autant que sur la vie des citoyens, la Sécurité des Systèmes d'Information est, aujourd'hui, un enjeu vital. Il est plus important que jamais de s'informer, de se protéger, de se connaître et de partager expériences, solutions et enjeux.

Constitué de Responsables, de Directeurs de la Sécurité des Systèmes d'Information, d'Experts en sécurité ainsi que de personnalités reconnues, le Cercle compte déjà plus de 300 adhérents actifs appartenant à des entreprises privées et à des organisations gouvernementales européennes.

Ses objectifs visent à fédérer une communauté de professionnels, à participer à l'élargissement des compétences, à échanger sur tous les enjeux liés aux risques, solutions et moyens de protection des patrimoines numériques stratégiques des entreprises et institutions. Accompagner les initiatives privées et gouvernementales, favoriser l'acquisition de connaissances et la détection de projets, développer l'esprit établi par une « communauté de compétences » pragmatique et disposant des mêmes valeurs de référence et de citoyenneté, voici le programme du Cercle Européen de la Sécurité et des Systèmes d'Information.



**Le cercle**

Européen de la Sécurité et des Systèmes d'Information



Pour plus d'informations contactez-nous au **01 41 93 09 12**  
par courriel [contact@lecercle.biz](mailto:contact@lecercle.biz) ou sur notre site web [www.lecercle.biz](http://www.lecercle.biz)



# SOMMAIRE

1. Introduction .....	2
2. Préambule : notions de pouvoirs .....	3
2.1. Aspects juridiques.....	3
2.2. Aspects pratiques.....	4
2.3. Adaptation au RSSI.....	4
2.4. Résultats de l'enquête du Cercle 2007.....	5
3. Les pouvoirs de la fonction SSI.....	6
3.1. D'abord une affaire de délégation : obtenir l'autorité.....	6
3.2. Ensuite une question de champ d'activité : gagner la légitimité.....	7
3.2.1. Une européanisation qui s'accélère.....	7
3.2.2. Les enjeux « Sécurité » se recentrent.....	8
3.2.3. Un pilotage « transverse » qui ne se normalise pas réellement.....	9
3.2.4. Recentrage ou segmentation des fonctions clés ?.....	10
3.2.5. Légitimité et crédibilité dans l'action politique.....	11
3.2.6. La légitimité en pratique ou le conflit permanent ?.....	13
3.2.7. Influence clé auprès des métiers ou « usurpation de pouvoir » ?.....	15
3.2.8. Le pouvoir de dire « non » en question.....	16
3.2.9. Des administrateurs au « pouvoir absolu » ?.....	17
3.3. Capacité réelle et limitation des moyens.....	18
3.3.1. Une insuffisance avouée.....	18
3.3.2. Des ressources humaines qui s'internalisent.....	19
3.3.3. Le pouvoir de contrôle des collaborateurs.....	19
4. Les facteurs externes du pouvoir en SSI.....	21
4.1. L'environnement général du RSSI.....	21
4.2. Le rôle des prestataires.....	22
4.3. Un poids encore limité de la certification.....	23
4.4. Pour un rééquilibrage des zones d'influence.....	25
4.4.1. Aspects législatifs et réglementaires : des impacts organisationnels.....	26
4.4.2. Aspects économiques et marketing.....	27
4.4.3. Aspects éducatifs et culturels.....	28
4.5. Les acteurs clés du Pouvoir en Sécurité SI.....	30
5. Conclusion.....	31
6. Annexe : le panel.....	32
6.1. Secteurs d'activité.....	32
6.2. Entité organisationnelle des répondants.....	32
6.3. Expérience en SSI.....	33
6.4. Ancienneté dans le poste actuel.....	33
6.5. Rémunération.....	33



# 1- INTRODUCTION

Depuis 2004, les enquêtes du Cercle Européen de la Sécurité ont établi des radioscopies des responsables / managers de la Sécurité des Systèmes d'Information (SSI) sur leurs rôles et leurs activités.

Elles ont aussi tracé des perspectives d'évolution pour la fonction :

- sur l'importance d'un management stratégique des cyber-risques (2004)
- sur l'usage d'indicateurs et de tableaux de bord en SSI (2005)
- sur les grands défis qui attendent les professionnels de la Sécurité SI (2006)

Nous avons eu au fil des années, de nombreuses confirmations statistiques qui font apparaître deux « profils types » de RSSI (le pilote et l'opérationnel).

Mais nous avons aussi mis en évidence pas mal de questionnements sur l'avenir d'une activité qui ne sera pas demain ce qu'elle est aujourd'hui.

C'est notamment le cas dans le domaine des « pouvoirs » dévolus aux professionnels de la SSI. Au-delà du « qui sont-ils ? » et « que font-ils ? », pourquoi ne pas chercher à comprendre « que peuvent-ils faire ou ne pas faire ? ».

Le thème de l'année « Quels pouvoirs en Sécurité des SI ? » n'est pas simple à aborder. D'une part parce que le terme même de « pouvoir » renvoie à des considérations philosophiques et juridiques complexes. D'autre part, parce qu'appliqué à la sécurité ou aux risques, il s'adresse à un domaine où le compromis et l'équilibre sont des principes de base.

Néanmoins, il nous est apparu pertinent d'investiguer ce domaine avec ambition, en nous appuyant comme les années précédentes, sur les résultats de l'enquête annuelle du Cercle Européen de la Sécurité et des Systèmes d'Information.

Le propos s'appuie en effet sur des chiffres qui n'ont de valeur que par la qualité d'un panel qui s'est progressivement élargi passant de 40 personnes en 2004 à 104 en 2007. Des européens francophones en font désormais partie mais aussi des RSSI opérationnels, certains moins expérimentés, souvent plus acteurs de terrain que managers.

Cette évolution n'est pas sans influence sur certains résultats de cette année.

Des variations assez importantes sont apparues et elles trouvent leur explication à la fois dans l'évolution structurelle de la fonction SSI et dans l'élargissement voulu du panel. Nous avons pu aussi effectuer des « zooms » pour 2 secteurs d'activité disposant d'un nombre significatif de répondants : Banques / Assurances et Administrations / Services Publics. Les chiffres intéressants sont alors mis en évidence.

Nous remercions chaleureusement tous ceux qui oeuvrent à cette démarche, chez DG Consultants, au Cercle, mais aussi tous les participants anciens et nouveaux. L'analyse des chiffres est aussi renforcée par les avis d'une dizaine de professionnels qui doivent aussi être remerciés.

Et nous espérons surtout que ce 4ème volet des Livres Bleus des Assises vous éclairera dans vos activités quotidiennes.

Pierre-Luc REFALO, Hapsis Education



## 2 - PRÉAMBULE : NOTIONS DE POUVOIRS

Le RSSI <sup>1</sup> possède-t-il un pouvoir ? Si oui lequel ? Dans quel domaine ?  
Si non, est-ce parce que cela n'a pas de sens ? Ou parce qu'un (d') autre (s)  
acteur (s) s'en charge (nt) ?

Ces questions ne sont pas si simples qu'il y paraît. Lors de nos entretiens avec des RSSI expérimentés, à qui la question a été soumise, nous avons pu mesurer à quel point, la notion de « pouvoir en SSI » était souvent réduite à la question de l'autorité ou du pouvoir de décision pour le RSSI lui-même.

Or, notre objectif est de traiter le sujet au-delà du RSSI, que ce soit dans son entreprise mais aussi dans l'environnement général de la profession. Vaste sujet !

Nous ne pouvons pas, dès lors, aborder la question sans rappeler quelques définitions essentielles..

### 2.1. Aspects juridiques

« **Le pouvoir** est la **capacité** dévolue à une autorité ou à une personne d'utiliser les moyens propres à exercer la **compétence** qui lui est attribuée soit par la Loi, soit par un **mandat** dit aussi "procuration". » <sup>2</sup>

« **La capacité** est l'aptitude définie par la Loi de conclure un acte juridique valable ayant pour conséquence d'engager la responsabilité de celui qui le souscrit dans le cas où il n'exécuterait pas les obligations mises à sa charge par le contrat et qui, en conséquence, engage son patrimoine. »

Bien qu'il faille distinguer le pouvoir et la **compétence**, la pratique ne fait pas toujours cette distinction, parce qu'il est évident que sans pouvoir pour l'exercer, la compétence ne serait pas déléguée.

« Le mot "pouvoir" est également utilisé pour désigner la convention écrite ou verbale par laquelle la personne qui mandate convient avec une autre, le mandataire, de lui donner une compétence pour réaliser un acte juridique à sa place. On dit "pouvoir", "mandat" ou "procuration". » On désigne ainsi, à la fois le pouvoir et le document par lequel ce pouvoir est transmis.

*Le mandat peut être verbal. Il prend le plus souvent l'aspect d'un texte écrit. »*

L'ensemble du propos de ce Livre Bleu 2007 doit être abordé en gardant à l'esprit l'essence juridique du « mandat » attribué à un RSSI.

---

<sup>1</sup> Nous désignerons par RSSI tout professionnel en charge de la définition et / ou de la mise en œuvre d'une Politique Sécurité dans son entreprise.

<sup>2</sup> Dictionnaire juridique en ligne

## 2.2. Aspects pratiques

Au-delà des aspects juridiques, le pouvoir s'exerce dans la pratique de multiples façons. Certaines ont d'ailleurs donné lieu à des expressions très significatives : pouvoir absolu, abus de pouvoir, séparation des pouvoirs, pouvoir de l'ombre, contre-pouvoir, etc.

Concrètement, le pouvoir trouve généralement son application dans trois domaines :

- L'exercice de l' « autorité » (ou la souveraineté)
- Les pratiques d' « influence » (ou des relations informelles)
- L'expression de la « puissance » (ou la capacité)

Ils ne sont pas exclusifs les uns des autres.

De leur côté, les chercheurs attribuent à l'expression du pouvoir par une autorité, quatre formes distinctes selon qu'elles sont issues :

- D'un **pouvoir formel** : il découle du pouvoir que détient une personne sur d'autres (pouvoir de maîtriser, de dominer, de forcer, de faire plier les autres et de les amener à agir contre leur gré.)
- De l'**expérience** ou d'une formation : ce type d'autorité découle de l'expérience d'une personne, de son savoir, de sa formation, de ses aptitudes, de sa sagesse, de son éducation.
- D'un **titre** ou d'une position hiérarchique : c'est la reconnaissance des tiers qui facilite une décision acceptable pour tous.
- D'**ententes informelles** : l'autorité obtient sa puissante influence de l'engagement personnel sur lequel elle est fondée.

## 2.3. Adaptation au RSSI

Appliqués au RSSI, ces concepts peuvent laisser perplexes car il n'y a pas de modèle absolu de la fonction. Chacun peut ne pas se reconnaître du tout dans ces propos, mais peut-être plus ou moins, dans l'une ou l'autre des formes d'expression du pouvoir.

Si l'on s'appuie sur l'origine juridique du pouvoir, comme expression de la Loi, force est de constater que le RSSI (Manager) détient **UNIQUEMENT** son pouvoir de l'attribution qui lui est faite formellement et / ou oralement de définir la Politique de Sécurité de son organisation (comme une réglementation interne).

Indépendamment de ses moyens, humains et financiers, le reste de ses capacités d'agir relève d'une légitimité tirée :

- De son titre ou de sa position : directeur ou non, rattaché à la DSI ou non etc.
- De son expérience : interne ou externe à l'entreprise, informaticien, consultant ou militaire, etc.
- De ses capacités d'influence : force de persuasion, charisme, pédagogie, etc.

Ces trois points, tout en étant essentiels au quotidien, mettent en évidence la vaste étendue des potentialités et des différences de « pouvoirs » pour les RSSI, lorsqu'on ajoute encore le critère de son organisation (taille, secteur d'activité etc.).



## 2.4. Résultats de l'enquête du Cercle 2007



L'enquête du Cercle 2007 a été exploitée dans l'optique d'éclairer la notion de « pouvoirs » en Sécurité des SI. Les 104 réponses aux 28 questions proposées permettent d'apporter des éléments de réponse à l'expression des pouvoirs dans notre domaine. Mais tous les aspects n'ont pas été abordés (rôle de l'Etat, du marché, des associations, etc.). Ils le seront cependant dans la conclusion.

Nous reprenons ici quelques positions de fond exprimées anonymement par le panel sur le pouvoir des RSSI et plus généralement en SSI.

### Sur le RSSI :

- « Le RSSI est un soutien auprès de la Direction générale. »
- « Il a assez peu de pouvoir ! Le RSSI élabore les règles, et les autres ne les suivent pas ... »
- « Le RSSI n'a pas de délégation de pouvoir. Il y a un pouvoir d'influence proportionnel à son expertise et à ses capacités d'initiatives. »
- « Le RSSI use d'un pouvoir de conviction plus que d'une autorité formellement octroyée. »
- « La décision est financière. Le RSSI exécute et contrôle. »

### Sur le management en SSI :

- « Il n'y a pas de notion de pouvoir. Il y a des projets, des analyses de risque et une décision de la direction après consultation de l'ensemble des éléments. »
- « La SSI n'a pas besoin d'autre pouvoir que celui d'alerte vis à vis de la DG. »
- « Le "pouvoir" est assuré par le Directeur Général Adjoint pour les décisions et les arbitrages stratégiques. Le pouvoir de contrôle est assuré par le RSSI et les organismes de contrôle externes. »
- « Le pouvoir financier n'est qu'un moyen ! Le pouvoir hiérarchique est efficace mais rare ! Le droit de veto est rare et délicat à utiliser ! L'accès à la direction générale est nécessaire ! »
- « Le pouvoir s'exprime d'abord par les processus de validation SSI (conformité politique et analyse des risques), Puis sous la forme de dérogation avec l'acceptation des risques associés. »
- « Le pouvoir s'exerce en démontrant l'utilité et l'efficacité pratique des outils/conseils mis en oeuvre. »
- « Le pouvoir existe via des actions de lobbying sur la gouvernance et la production de métrique ad hoc permettant aux membres de direction la mise en oeuvre de la stratégie visée par le RSSI. »
- « Le pouvoir s'exprime par le rattachement à un membre du directoire qui valide les plans d'actions SSI et budgets proposés par la direction de la sécurité. »
- « Le RSSI et le Directeur sécurité identifient les risques et enjeux et ont mandat de faire faire des audits. »

### Sur le rôle de la DSI :

- « Le pouvoir repose sur le tandem DSI – RSSI qui propose à la DG et aux Métiers. »
- « Le DSI a le pouvoir absolu, ce qui pose la question du positionnement hiérarchique de la sécurité. »
- « Le pouvoir s'exerce par celui qui détient le budget : la DSI. »
- « Le pouvoir s'exprime par la mise en oeuvre d'un Comité de Sécurité mensuel. »
- « Le pouvoir en SSI repose sur une Politique Sécurité validée par la DG et des arbitrages au sein du Comité Sécurité. »

### 3 - LES POUVOIRS DE LA FONCTION SSI

#### 3.1. D'abord une affaire de délégation : obtenir l'autorité

Dans toute organisation, le pouvoir réel ne s'exerce qu'à travers le transfert de responsabilités d'une autorité, légale ou économique, à une autre.

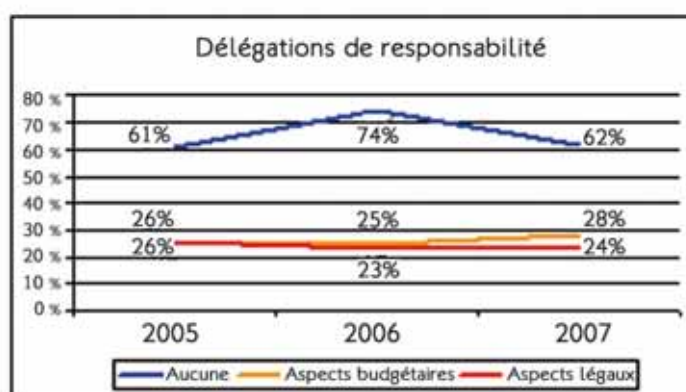
Dans le domaine de la sécurité des SI, les aspects juridiques sont au coeur de la problématique ne serait-ce qu'au travers de la cryptographie, du secret des correspondances, de la propriété intellectuelle ou de la protection des données personnelles. Le RSSI est-il garant du respect de la législation touchant la « SSI » dans son entreprise ? Pour les trois quarts du panel, la réponse est non.



Plus largement, on constate que la très grande majorité des RSSI demeure sans pouvoir officiel et réel (y compris au plan économique). Nous avons déjà ici un élément de réponse essentiel :

**Les professionnels de la SSI n'ont généralement pas de réel pouvoir en termes d'autorité ou de souveraineté.**

Cette situation est stable depuis que nous organisons les enquêtes du Cercle. Ce qui est surprenant au regard de l'importance que prend la fonction SSI dans les organisations.

Elle est d'ailleurs, généralement acceptée par la plupart des RSSI « managers » qui considèrent leur rôle avant tout comme un « pilote » voire un « médiateur ». N'est-ce pas la meilleure manière de se faire accepter ?



		
aucune délégation	63%	50%
délégation budgétaire	27%	39%
délégation légale	23%	31%

Zoom : Les professionnels de la SSI du secteur public possèdent une plus grande autorité qu'elle soit légale ou budgétaire.

Vue comme une fonction « support », la Sécurité des SI apporte aux dirigeants et aux métiers un conseil, une expertise, une assistance. Cette vision ancienne demeure d'actualité, alors que les moyens désormais alloués à la SSI ont très profondément évolué.



La phrase « type » légitimant l'action « politique » d'un RSSI peut se résumer par :  
« Définir et contrôler la Politique Générale de Sécurité des différentes directions. »

### 3.2. Ensuite une question de champ d'activité : gagner la légitimité

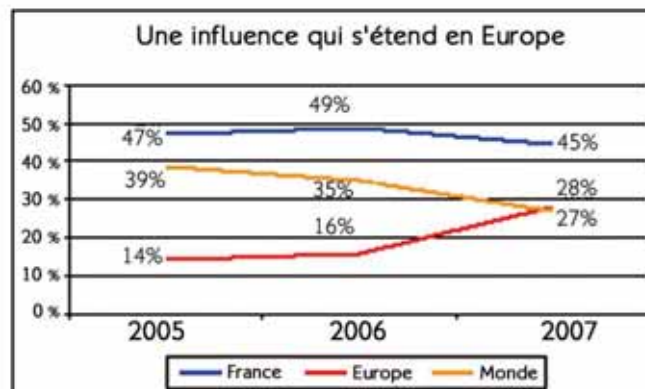
Autre aspect du pouvoir : l'influence. Pas question ici de « capacité » ou de « souveraineté ». Obtenir sa légitimité via ses domaines d'action et d'intervention est déjà un beau challenge pour un RSSI. C'est en particulier remarquable lorsqu'on cherche à supprimer un « S » à RSSI et devenir « Responsable Sécurité de l'Information ».

Les anglophones utilisent assez largement désormais le CISO (Chief Information Security Officer) qui au-delà du fait d'avoir un statut de Directeur, est plus centré sur le contenu que sur le contenant. En France en particulier, le concept de Sécurité du Système d'Information reste très présent alors qu'il est évident désormais que l'enjeu est bien de protéger les informations qu'elles soient stratégiques ou personnelles.

#### 3.2.1. Une européanisation qui s'accélère

Le panel 2007 s'est élargi en Europe francophone. La moitié des répondants demeure franco-français, mais l'autre moitié oeuvre dans le contexte international avec une part grandissante en Europe.

La zone d'influence n'est pas centrée sur un site ou une entreprise, mais s'ouvre à des filiales, sous-traitants, partenaires qui élargissent le champ d'action des professionnels de la SSI.

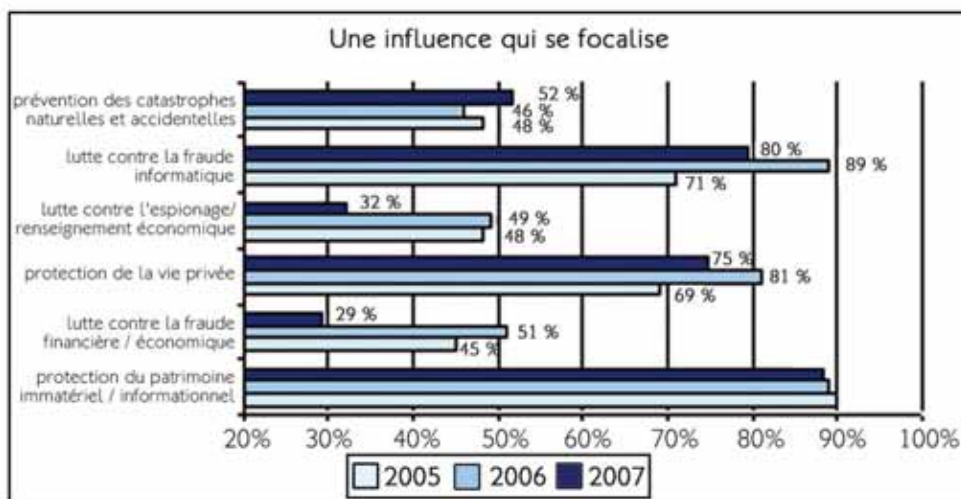




Cette influence se concrétise souvent dans un titre comme « CISO – EMEA », « European IT Risk manager » par exemple.

Et l'Europe de la SSI est en marche depuis de nombreuses années. La Commission Européenne s'est emparée du sujet au début des années 90 et n'a cessé de multiplier les initiatives à tous les niveaux. En 2005, la création de l'ENISA (European Network and Information Security Agency) est là pour nous rappeler que de nombreux enjeux, historiquement la cryptographie, puis les données personnelles ou encore la cybercriminalité ne peuvent trouver de réponse au plan strictement national.

### 3.2.2. Les enjeux « Sécurité » se recentrent

Nous considérerons ici les 6 enjeux entrant plus ou moins directement dans le cadre de la Sécurité des SI. Depuis 2004, nous avons pu mesurer l'importance qu'ils avaient pour les professionnels de la SSI. En général, entre la moitié et 90% du panel abordaient l'un ou l'autre dans son management.



		
protection du patrimoine	87%	89%
protection de la vie privée	77%	85%
lutte contre la fraude informatique	97%	73%

Zoom : La protection de la vie privée est plus importante dans le secteur public, tandis que les RSSI de la Banque/Assurance placent la lutte contre la fraude informatique comme l'enjeu N°1.

**Un phénomène de concentration semble s'opérer sur la protection du patrimoine immatériel et des données personnelles.**

En 2007, des changements sont remarquables.

La baisse significative des questions de lutte contre l'espionnage économique / industriel et contre la fraude financière démontre que ces thématiques s'éloignent du cadre stricte de la SSI. Elles sont prises en charge par des fonctions dont c'est le métier. Mais cela ne signifie pas que les professionnels de la SSI ne soient pas concernés.

L'évolution du panel est une 2<sup>ème</sup> explication possible.

En tout état de cause, l'action semble se focaliser et nous constatons encore que la « Protection » est privilégiée à la « Lutte » et que le Patrimoine informationnel est la clé de la démarche.

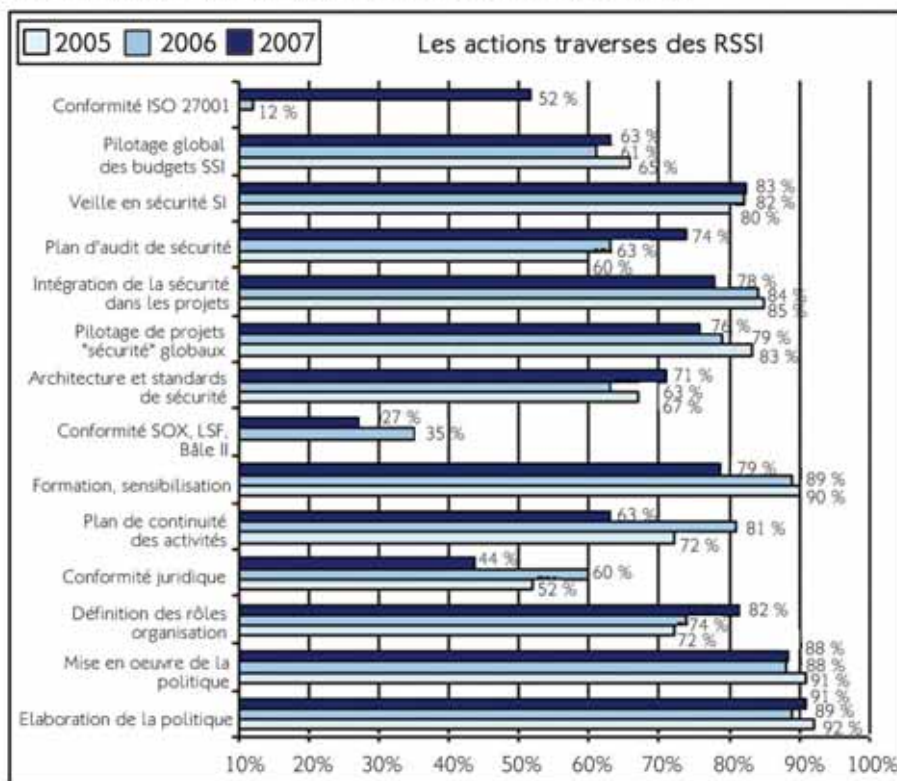




### 3.2.3. Un pilotage « transverse » qui ne se normalise pas réellement

Le RSSI a un rôle essentiel dans le pilotage. C'est là qu'il trouve sa véritable légitimité, quand bien même il lui est demandé de plus en plus des « résultats » (via des tableaux de bord), d'être aussi acteur (voir plus loin, les « fonctions clés »). Inutile d'insister ici sur la dimension « politique » comme le soulignent les missions attribuées aux RSSI.

Cette année, des évolutions remarquables doivent être mentionnées :

- La conformité prend de l'importance mais simplement dans le domaine de la SSI avec l'impact des normes ISO27000. Elle faiblit dans les domaines purement réglementaires et financiers. Il y a sans doute un phénomène de cause à effet associé à la mise en place dans les grands groupes de Directions de la Conformité.
- Les questions d'organisation, d'audit et d'architecture progressent. Ces trois aspects s'inscrivent dans une logique de « mise en œuvre effective » de la politique SSI. Le RSSI doit plus que jamais démontrer que l'écrit, la loi, peut devenir une réalité concrète.
- Cette progression semble s'opérer au détriment de la formation / sensibilisation et des plans de continuité qui avaient bien progressé les années précédentes.



		
élaboration politique	93 %	82 %
mise en œuvre politique	83 %	85 %
formation / sensibilisation	80 %	93 %
veille	80 %	85 %

Zoom : La formation / sensibilisation (globalement en baisse) demeure un enjeu majeur dans le secteur public tandis que les RSSI Banque/Assurance se situent dans la moyenne du panel.

Les questions de conformité ISO 27000 (et non de certification) ainsi que d'organisation progressent fortement dans une logique de « gouvernance » au détriment de la formation / sensibilisation.

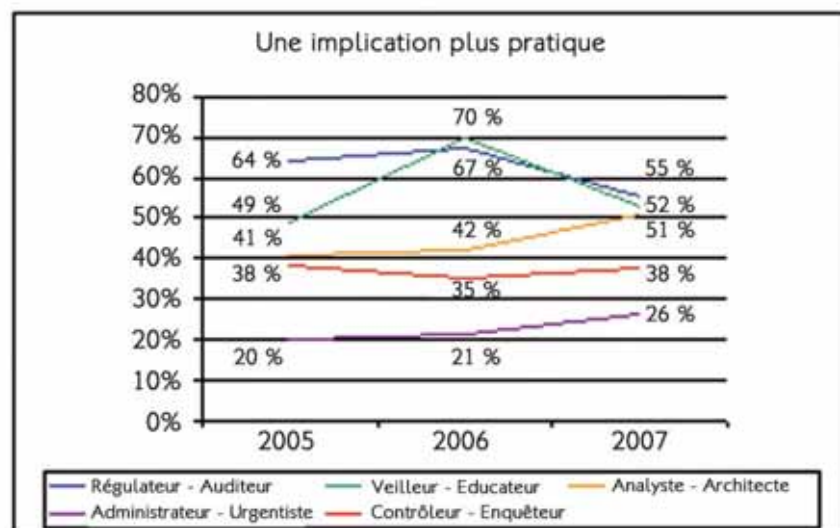
### 3.2.4. Recentrage ou segmentation des fonctions clés ?

Les rôles des membres du panel évoluent aussi considérablement cette année. On peut penser que l'évolution des répondants en est la principale raison. C'est néanmoins cohérent avec le constat des actions de pilotage. Cette tendance au « 50% » pour les trois fonctions clés associées au RSSI « Manager », laisse aussi à penser qu'il y a bien 2 grands types de RSSI :

- Les managers : Régulateur-Auditeur + Veilleur-Educateur
- Les opérationnels : Analyste-Architecte + Administrateur-Urgentiste

Les premiers ne sont pas nécessairement situés au sein de la DSI, les autres plus certainement. L'analyse du panel 2007 montre d'ailleurs que comme les années précédentes, environ deux tiers (65%) des répondants appartiennent à la DSI.

Il faudrait vraiment, et enfin, leur trouver des titres différents ! On distingue fréquemment le RSSI du RSI (Responsable Sécurité Informatique). C'est une solution mais qui ne s'applique pas partout.



analyste - architecte	69%	46%
régulateur - auditeur	35%	46%

Zoom : Les RSSI Banque/Assurance s'impliquent plus fortement au plan méthodologique et technique donnant au terme de « politique sécurité » une connotation plus opérationnelle que réglementaire. Dans le secteur public, les RSSI se situent encore plus au niveau opérationnel.

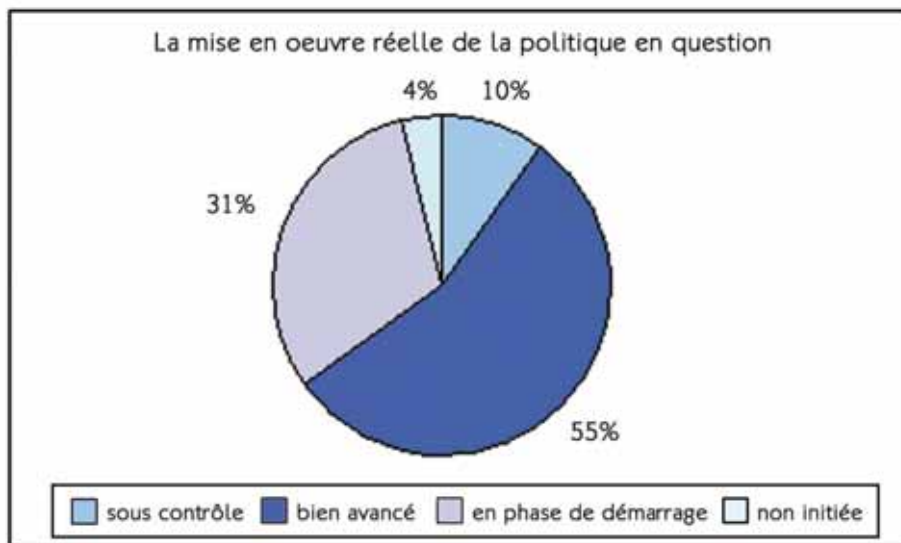
**Le RSSI « Pilote » et le RSSI « opérationnel » tendent-ils à devenir réalité ?  
Lorsqu'ils co-existent, comment parviennent-ils concrètement à répartir leurs rôles ?**



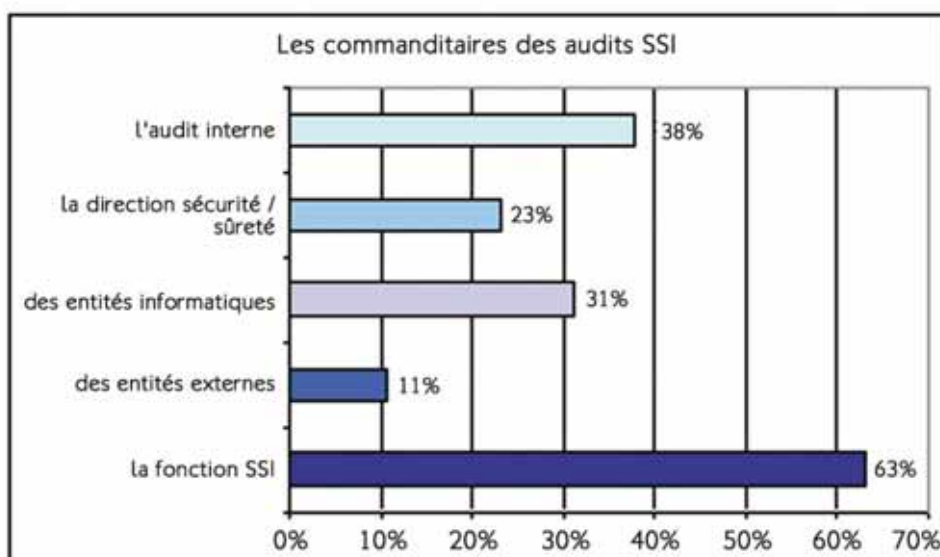
### 3.2.5. Légitimité et crédibilité dans l'action politique

Après la légitimité, la crédibilité s'acquiert en prouvant que le texte ne reste pas lettre morte. C'est ici que des liens forts se nouent avec le marché. On constate que l'état d'avancement de la mise en œuvre des politiques est assez limité. Seulement 10% du panel la positionnent « sous contrôle ».

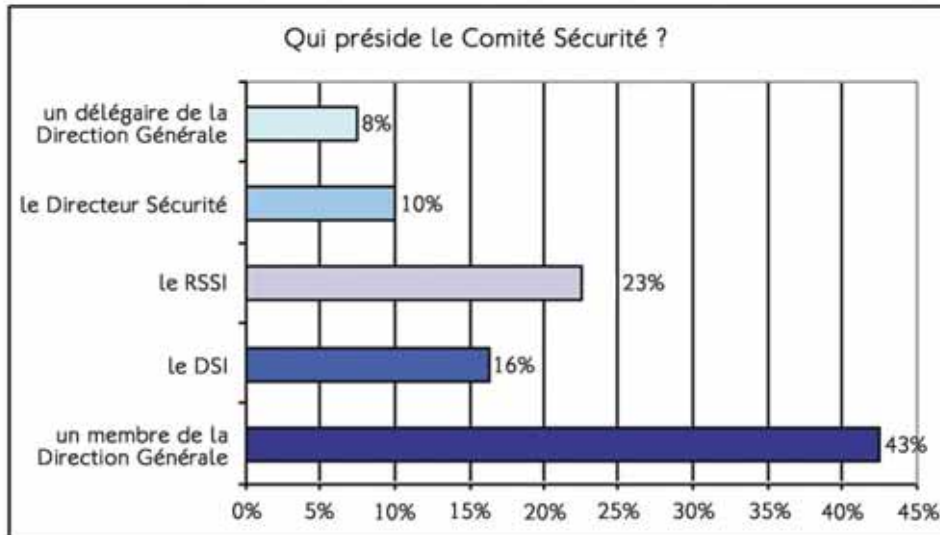
Pour un tiers du panel, la mise en oeuvre effective de la politique est en phase de démarrage. Ce chiffre est à corrélérer avec la structure du panel où l'on remarque que 41% des répondants sont en poste depuis moins de 3 ans.



Seuls les audits parviennent à démontrer la mise en oeuvre effective des référentiels. A ce titre, la fonction SSI se doit de garantir l'indépendance des intervenants lors des audits. Celui (un prestataire) qui conçoit ou réalise ne doit pas intervenir dans un plan d'audit. Or la réalité est bien différente.



Pour conclure cette dimension règlementaire et ses impacts organisationnels, nous souhaitons mettre en évidence l'importance de la mise en place d'un Comité Sécurité. Seul 78 % du panel l'ont fait. Il est ici à remarquer que la majorité en confie la présidence à un acteur non SI et non SSI. Ce lieu de décision collégial doit être développé au sein de l'entreprise, dans lequel le RSSI influe sur les décisions mais ne les impose en aucune manière.



As du compromis et de l'équilibre, le RSSI peut certainement exercer une véritable influence en terme de décision dans un Comité Sécurité, et ce d'autant mieux qu'il n'en assure pas la présidence.



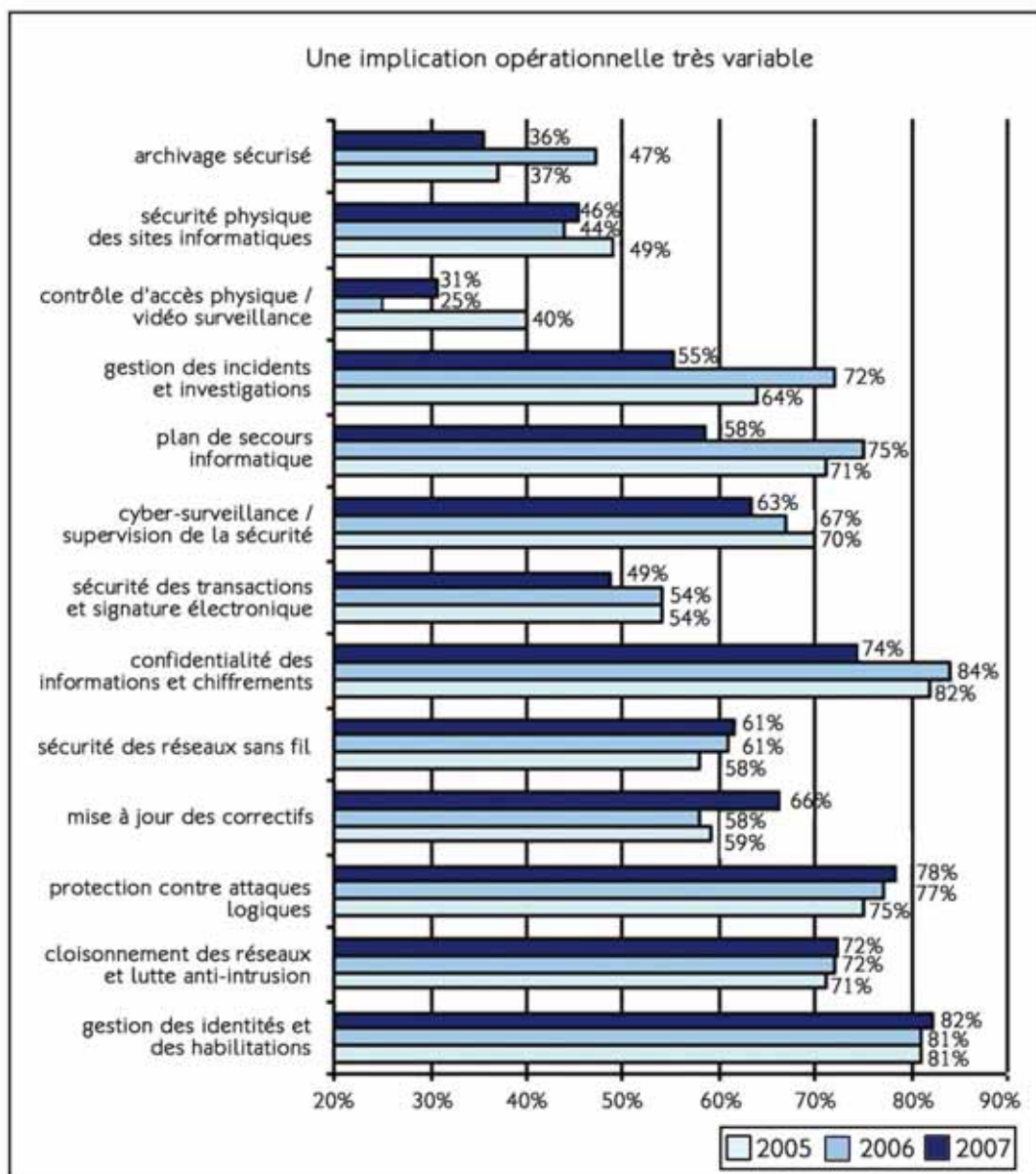
### 3.2.6. La légitimité en pratique ou le conflit permanent ?

Les compétences techniques ou le passé informatique du RSSI ont longtemps été son « sésame » pour se faire accepter par les équipes IT. Au début des années 2000, souhaitant gagner en indépendance et se placer au niveau du pilotage, certains RSSI n'ont plus eu besoin de rechercher cette légitimité, d'autant plus que les évolutions technologiques rapides ne lui permettent pas de tout connaître, comprendre, voire maîtriser.

Nombreux aujourd'hui sont ceux qui parviennent à mettre à profit cette absence de compétence technique en donnant ainsi plus de crédit aux équipes informatiques sur les questions de Sécurité. Si chacun le comprend, c'est du « gagnant-gagnant ».

Néanmoins, l'implication réelle du RSSI (avec ou sans équipe) dans les projets « métier » et dans la mise en œuvre de processus et d'organisation est réelle. Naturellement, les « conflits » potentiels sont alors quasi-permanents :

- Avec les métiers : pour faire accepter les mesures et les coûts couvrant les risques réels
- Avec les informaticiens : pour bâtir les meilleures solutions avec les technologies adéquates
- Avec l'ensemble des parties : pour développer des plans d'audit cohérents



Ce schéma démontre la très vaste couverture « technique » des actions SSI. Les fortes variations à la baisse semblent ici encore démontrer que les répondants se focalisent sans doute plus que par le passé (réponses multiples). Les années précédentes, certains thèmes étaient sans doute « exploratoires ». Ils ont disparu pour certains ou se sont renforcés par des projets concrets pour d'autres.

Nous noterons uniquement l'évolution du classement des 6 premiers thèmes (les plus consensuels) : le plan de secours et la gestion des incidents / investigations disparaissent au profit de la gestion des correctifs et la supervision / cyber-surveillance.

La stabilité des 3 actions primordiales indique d'une part que le défi est permanent et que les solutions, outils, processus se doivent d'évoluer, mais aussi d'autre part, que LA solution n'existe pas, ou du moins que sa mise en oeuvre est longue, fastidieuse, voire quasi impossible, parfois... pour certains.

	2005		2006		2007	
1 <sup>er</sup>	Confidentialité et Chiffrement	82%	Confidentialité et Chiffrement	82%	Gestion identités et Habilitations	82%
2 <sup>ème</sup>	Gestion identités et Habilitations	81%	Gestion identités et Habilitations	81%	Protection attaques logiques	78%
3 <sup>ème</sup>	Protection attaques logiques	75%	Protection attaques logiques	77%	Confidentialité et Chiffrements	74%
4 <sup>ème</sup>	Plan de secours	71%	Plan de secours	75%	Cloisonnement du réseau	72%
5 <sup>ème</sup>	Cloisonnement du réseau	71%	Cloisonnement du réseau	72%	Gestion des correctifs	66%
6 <sup>ème</sup>	Supervision et Cyber-surveillance	70%	Gestion d'incidents et investigations	72%	Supervision et Cyber-surveillance	63%

Ceux qui sont les plus avancés dans leur démarche, peuvent piloter ces activités sans en avoir une réelle responsabilité opérationnelle. Ceux-là concentrent leur pouvoir sur de l'influence interne (métiers et équipes informatiques) et externe (offreurs et prestataires) dès lors que les processus sont mis en place et exploités au bon niveau, en amont et en aval, notamment au sein de la DSI.

Nombreux sont ceux qui pensent que cela fait beaucoup pour une seule personne ! Peut-être, sauf si celle-ci parvient à s'organiser en conséquence et à s'appuyer sur les bons acteurs (voir plus loin).

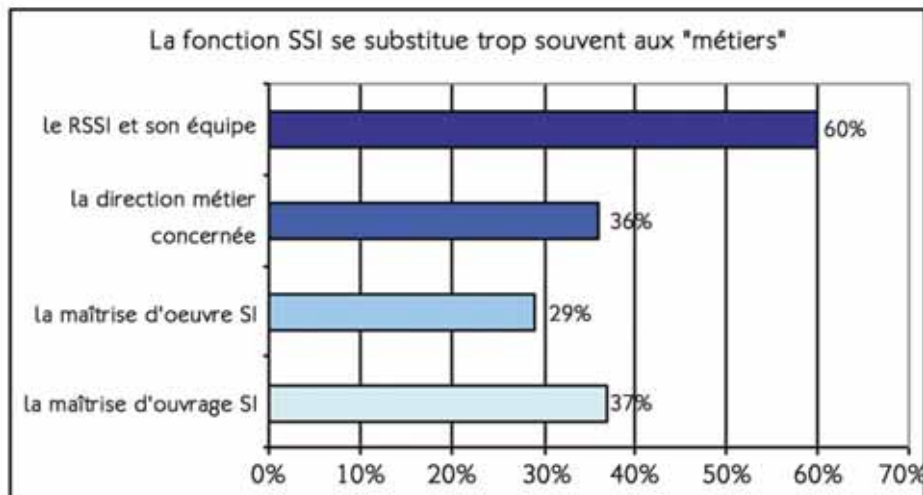
**Une plus forte concentration des efforts semble s'opérer.  
Pour gagner en efficacité ou parce que les moyens se réduisent ?**





### 3.2.7. Influence clé auprès des métiers ou « usurpation de pouvoir » ?

Une des clés de l'action des RSSI est de parvenir à obtenir une expression de « besoins » ou plutôt des exigences de sécurité au cours d'une analyse de risques. Cette étape fondamentale demeure un défi permanent. C'est ici que s'exprime le véritable « pouvoir » de décision dans le domaine.

Pour 2/3 des répondants, on est en situation potentielle d'usurpation de pouvoir ! Car seulement un tiers des répondants citent soit la Direction Métier, soit la Maîtrise d'ouvrage SI comme l'acteur qui exprime ses besoins de sécurité.



		
le RSSI et son équipe	93 %	78 %

Zoom : Les RSSI Banque/Assurance et du Secteur public se situent très au-dessus de la moyenne du panel dans leur implication auprès des « métiers » et entités utilisatrices. C'est particulièrement important dans la Banque/Assurance.

Il reste qu'il faut positiver ces chiffres. Il vaut mieux que le RSSI fasse son métier ou plutôt son devoir, quitte à se substituer aux véritables responsables, ou influencer très fortement les décisions de mettre en oeuvre, ou non, telle ou telle action.

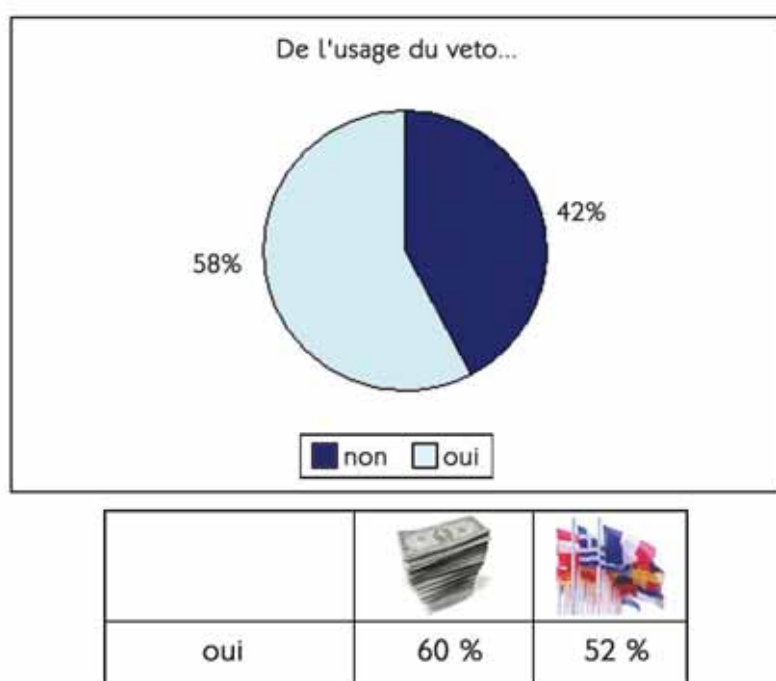
**L'éducation des « métiers » reste un défi à relever. Le RSSI doit prendre en charge l'ensemble du processus « exigence / solution / audit » ...A ses risques et périls !**

### 3.2.8. Le pouvoir de dire « non » en question

Allant plus loin, la question d'un « droit de veto » propre à la fonction SSI est régulièrement posée. Il ressort de l'enquête qu'il est une réalité, même si le fond de la question, très direct, mérite d'être modulé.

Les entretiens font ressortir qu'il faut davantage parler d'arbitrage parfois collégial, lorsque des divergences trop fortes apparaissent entre les exigences de sécurité et les capacités à mettre en œuvre les solutions adaptées au sein de l'entreprise.

On touche ici aussi, un des rôles clés des RSSI en terme d'influence : parvenir à positionner clairement les enjeux pour les métiers et à responsabiliser les acteurs pertinents, sans endosser, lui (ou elle), la décision de faire ou ne pas faire.



Zoom : L'usage du « veto » semble peu ancré dans le secteur public et tend à indiquer que c'est plus fréquemment le cas pour le reste du panel.

**Le droit de veto est une réalité mais il doit demeurer exceptionnel, en lui préférant des arbitrages argumentés.**



### 3.2.9. Des administrateurs au « pouvoir absolu » ?

Autre aspect essentiel du pouvoir en SSI, les capacités d'action des administrateurs apparaissent en pleine lumière lorsqu'on aborde la cyber-surveillance ou le devoir de contrôle de l'entreprise sur ses salariés.

Il ne faut pas être naïf et reconnaître que les administrateurs ont et auront toujours le pouvoir d'accéder aux répertoires, bases de données, boîtes aux lettres ou fichiers de traces. La question est : quand, comment et dans quelles conditions ?

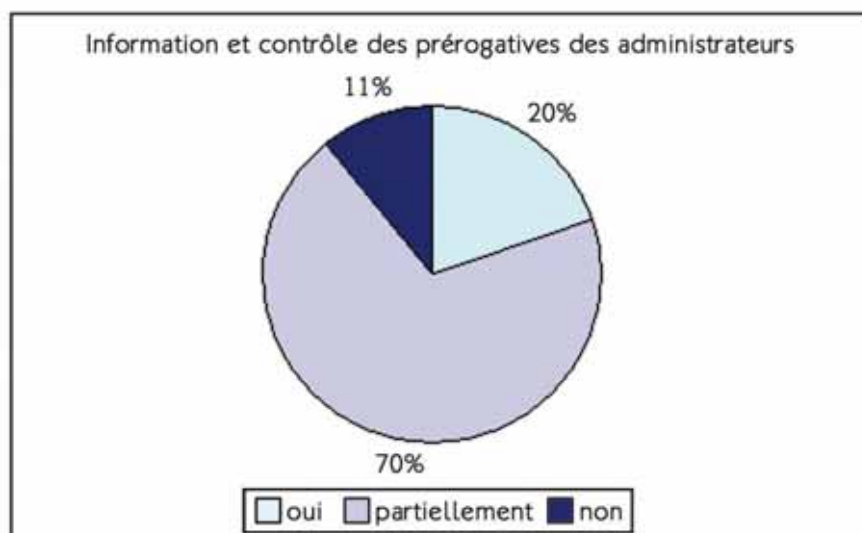
Dès lors qu'une charte d'usage et de sécurité du Système d'Information est en vigueur au sein de l'entreprise (éventuellement sous la forme d'une annexe au Règlement Intérieur s'il existe. Ce qui n'est pas le cas dans la fonction publique), la première étape consiste à informer et former ces équipes à leurs droits et devoirs en la matière au regard de 3 textes fondamentaux :

- La protection des données personnelles
- Le secret des correspondances
- La fraude informatique (accès et maintien non autorisés)

La seconde vise à les responsabiliser réellement, en élaborant une charte spécifique et en la faisant signer individuellement.

L'enquête montre une situation très mitigée dans la mesure où seulement 20% affirment que les actions nécessaires ont été menées. Une des grandes difficultés ici réside dans l'externalisation, parfois hors des frontières, de ces professions.

Le rôle de contrôle du RSSI doit alors être rappelé ici. En terme de processus, il doit systématiquement être informé des accès exceptionnels (hors procédure) des administrateurs et de façon permanente, avoir le pouvoir de « surveiller les surveillants ».



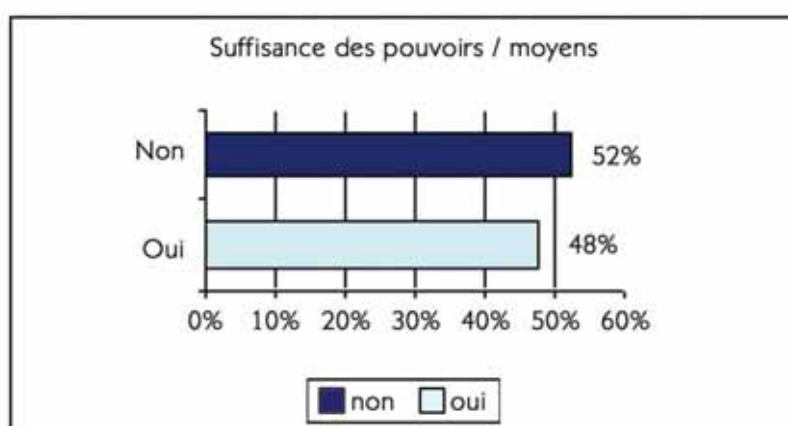
**Ceux qui possèdent les « clés du royaume » doivent en accepter les contre parties.  
Plus facile à dire qu'à faire ?**


### 3.3. Capacité réelle et limitation des moyens

#### 3.3.1. Une insuffisance avouée

Toute fonction en entreprise se doit de disposer des moyens utiles à l'accomplissement de sa mission. Le danger serait d'être vu ou considéré comme un Don Quichotte, aux ambitions nobles et légitimes, mais se battant en permanence contre des moulins à vent, peu enclins à s'orienter dans le sens de la protection du patrimoine informationnel.

La moitié du panel considère ne pas disposer « de moyens suffisants pour accomplir sa mission ». Il peut s'agir de légitimité, sans doute pour une bonne part (souvent mal positionnée dans un organigramme), mais aussi de ressources humaines ou financières, notamment dans les plus petites structures.



		
oui	57 %	33 %

Zoom : Les écarts sont significatifs dans l'appréhension des moyens utiles à la mission. La Banque-Assurance est au dessus de la moyenne, le secteur public, largement en dessous.

**La moitié des RSSI sont satisfaits de leurs moyens.  
Mais le secteur d'activité influence beaucoup cette appréhension.**



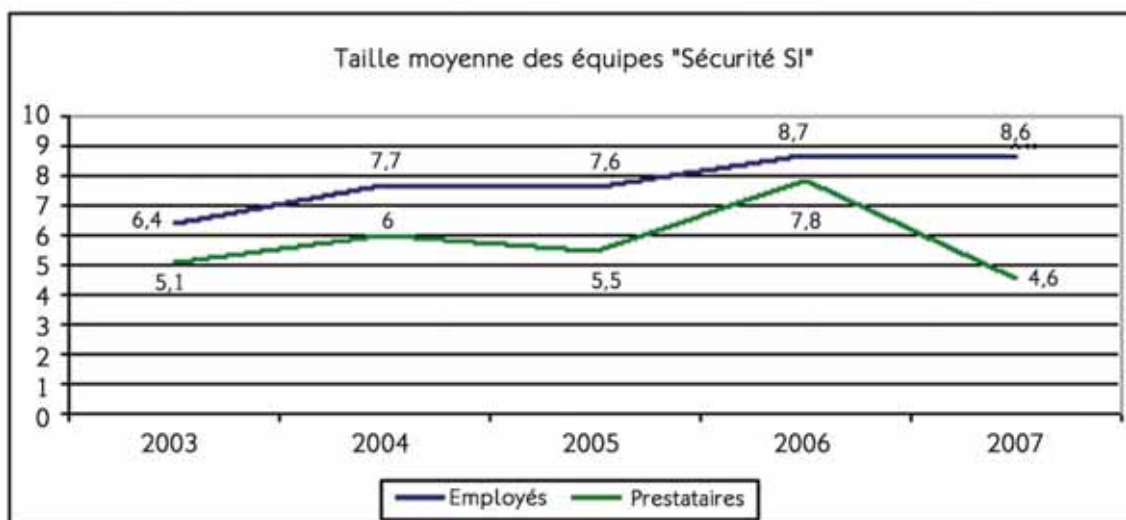
### 3.3.2. Des ressources humaines qui s'internalisent

Nous abordons ici un des indicateurs clés des enquêtes du Cercle. Une majorité de répondants sont des RSSI solitaires, sans équipe, mais s'appuyant sur des consultants si besoin.

Ceux qui disposent de ressources internes voient leur équipe progresser significativement depuis 2003 (+ 42% soit environ 10% / an).

La capacité d'action, notamment parce que la légitimité progresse avec, s'en trouve renforcée.

Mais cette croissance des équipes internes s'effectue en tenant compte de l'apport des consultants. En 2007, le recours à des experts externes s'est considérablement restreint alors qu'il avait beaucoup progressé l'année dernière.



La croissance des équipes SSI internes est de l'ordre de 10% / an.

### 3.3.3. Le pouvoir de contrôle des collaborateurs

La fonction SSI évolue de plus en plus vers le contrôle et la surveillance et parfois l'investigation (91% des répondants).

C'est une réalité qui confère à la SSI un « pouvoir » qui ne peut s'exercer sans capacité adéquate. Celle-ci demeure à conquérir pour 69% du panel répondant « partiellement » à la question : « La fonction SSI a-t-elle des pouvoirs formels et des moyens adéquats dans les domaines du contrôle / de la surveillance de l'utilisation du SI ? »



Une conquête en cours pour les RSSI : quelle implication et quels moyens dans le contrôle de l'usage du SI par les collaborateurs, en relation avec une charte, claire, transparente et comprise.



## 4. LES FACTEURS EXTERNES DU POUVOIR EN SSI

### 4.1. L'environnement général du RSSI

L'essence de la fonction RSSI est, ou devrait être, de nature juridique / réglementaire. Cet aspect est bien appliqué dans la fonction publique (Fonctionnaires SSI rattachés au Haut Fonctionnaire de Défense, Autorités qualifiées, Agents SSI), dans la banque (CRBF-97-02) ou les télécoms (Licences Opérateurs).

Le RSSI n'existe (rait) idéalement que par une **exigence réglementaire « externe »** qui impose la mise en œuvre d'une organisation et de processus de protection des SI ou des informations (au titre du secret en général : bancaire, médical, défense, des correspondances).

Plus récemment, la désignation des Correspondants Informatique et Libertés répond à cette même exigence (bien qu'elle ne soit pas obligatoire).

Or, dans de nombreuses entreprises, et si l'on oublie la question des plans de secours informatique, la fonction prend ses racines (au milieu des années 90) dans la gestion de **menaces externes** issues d'Internet (virus, sabotages, intrusions).

Pour réussir dans sa mission, le RSSI, souvent seul à ses débuts, s'est entouré de consultants, a fait largement appel au marché et aux offreurs de solutions, pour bâtir méthodes et architectures.

Des **collusions d'intérêt**, sans être voulues et recherchées, n'ont pas manqué d'apparaître : de l'assureur au fournisseur de plan de secours, du hacker en quête de reconnaissance à l'éditeur d'anti-virus adepte du marketing de la peur, de l'intégrateur de SSO ou de PKI visant de gros projets, à la presse spécialisée avide de sensationnel ou en recherche de financement publicitaire, etc.

Inévitablement, des « pouvoirs » notamment économiques sont apparus, le tissu associatif s'est développé, des groupes de réflexion professionnels ont émergé. Le pouvoir économique a joué son rôle, pendant que les pouvoirs publics suivaient l'émergence d'une Société de l'information qui touchait d'abord les grandes entreprises, plus que l'Etat et les citoyens.

Désormais, tous les acteurs sont concernés, certes à des degrés divers et face à des menaces très complexes et variées.

D'autre part, l'importance des **normes**, sous influence anglo-saxonne, ne cesse de s'accroître, et elles tendent à promouvoir la **certification « Sécurité de l'Information »** qu'elle s'applique à une organisation ou à un individu.

Dans un marché qui reste peu mature car jeune et en perpétuelle innovation, la promotion de cadres de références internationaux et des démarches « qualité » de la SSI, doit être encouragée. Mais inversement, ce marketing de l'offre ne doit pas se bâtir au détriment des entreprises, voire sans leur implication.

L'Etat et l'Europe, pour leur part, font pale figure, malgré des progrès certains depuis quelques années. La **coopération public-privé** reste balbutiante en dehors du cadre de la Défense. La **multiplication de textes** non appliqués : une fâcheuse habitude. L'**absence d'indicateurs fiables** sur la cybercriminalité : un serpent de mer. L'**empilement de structures** : source d'opacité et d'inefficacité.

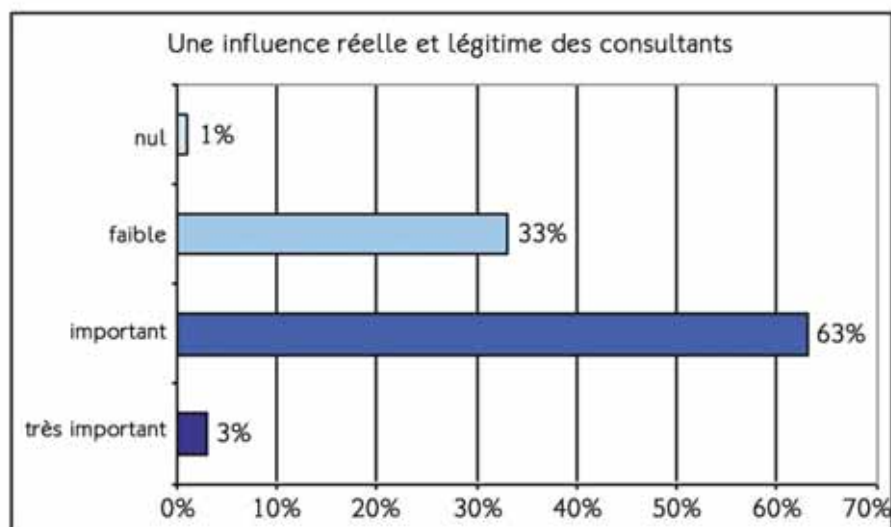
Désormais, face aux menaces portant sur la protection de la vie privée et au développement d'un marché de l'insécurité sans état d'âme, des forces de pression doivent se développer. Mais lesquelles ?

Ainsi, au-delà des facteurs de pouvoirs internes à une organisation, il ne faut pas oublier toutes ces sphères d'influence qui méritent quelque attention. Ce sera l'objet de la conclusion du Livre Bleu 2007, sous la forme d'une ouverture pour discussion plus que d'un bilan exhaustif et de recommandations.

## 4.2. Le rôle des prestataires

L'enquête du Cercle Européen de la Sécurité et des Systèmes d'Information a abordé la question du poids des prestataires auprès des RSSI. Aspect sans doute le plus simple de la problématique.

Seule la moitié du panel fait appel à une assistance externe. Pour 2/3 des répondants, l'influence des prestataires est jugée importante. Le RSSI, seul, ne peut réussir dans sa mission et risque de se scléroser. L'apport de connaissances et de compétences externes est essentiel. Tous les métiers d'une entreprise font appel à des experts (finance, RH, marketing, SI). Le RSSI est souvent seul, rappelons le aussi !

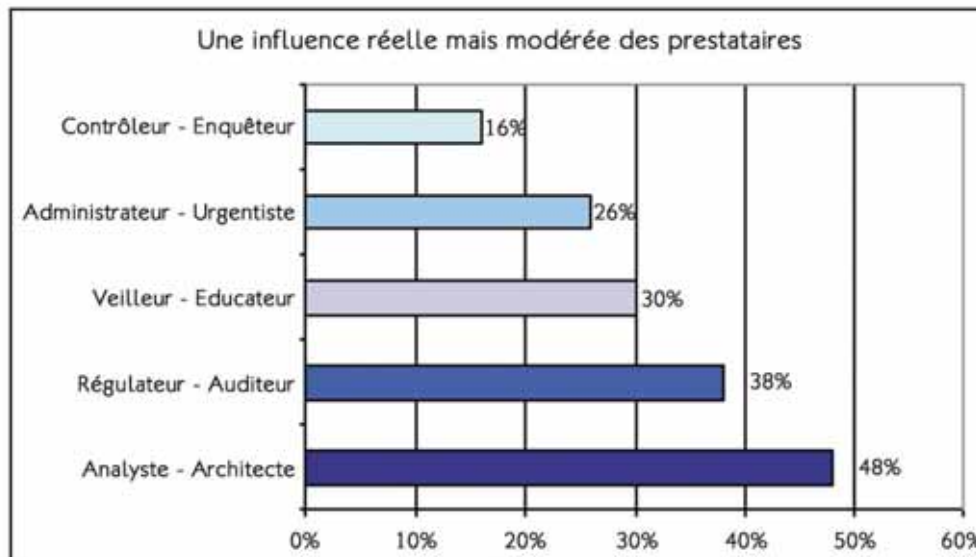


On insistera néanmoins sur le fait que cette année le recours aux prestataires semble se réduire en volume par rapport à 2006.

L'important demeure d'évaluer dans quels domaines cette influence s'exerce. Il s'avère que, sans surprise encore, c'est au plan des analyses de risques et des conceptions d'architecture qu'elle est la plus importante, juste devant la mise en place des référentiels (approche politique et démarche d'audit). C'est-à-dire à des niveaux plus décisionnels qu'opérationnels.

**Les prestataires en SSI se doivent aujourd'hui d'atteindre l'excellence au plan méthodologique et technologique. L'apport des certifications individuelles respectant la norme ISO 17024 est un enjeu d'avenir certain.**





### 4.3. Un poids encore limité de la certification

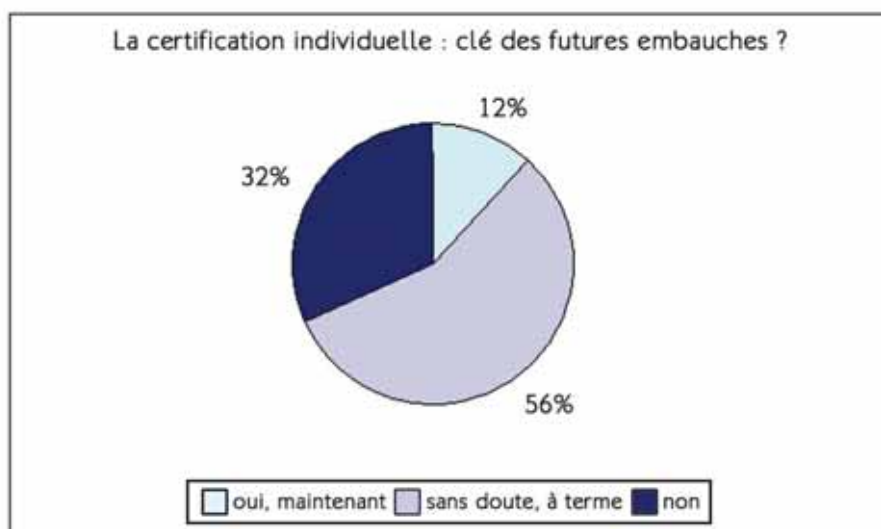
Le panel demeure majoritairement français et la certification en SSI reste un sujet de discussion parfois passionné.

A la question « *La certification des prestataires spécialisés en SSI devrait-elle être obligatoire ?* », 42% du panel répondent « oui » contre 37% en 2005. La progression est limitée et l'engouement demeure aussi minoritaire. Il convient de préciser ici que malgré son développement modéré en Europe, la certification individuelle en SSI recouvre en 2007 de nombreux processus : CISA et CISSP pour les plus anciens, CISM ou ProCSSI et ISO27001 pour les plus récents.



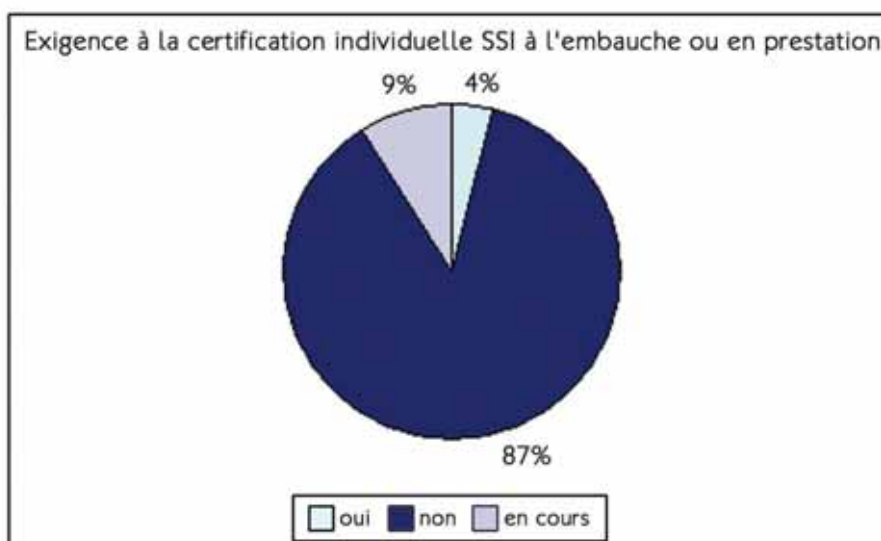
Bien sûr, rien ne remplace l'expérience et le terrain mais les normes et la certification apportent incontestablement un plus. Après la certification d'auditeur ISO 27001, apparaît celle pour le responsable de la mise en œuvre ISO27001.

Néanmoins, la certification, malgré ses limites, possède des intérêts qu'il ne faut pas ignorer. On constate dans le graphe ci-dessous, qu'un professionnel sans certification individuelle pourrait avoir, à terme, des difficultés pour trouver un emploi.



Mais restons lucides, les évolutions seront lentes. Pour 87% des entreprises du panel, les achats de prestation ou les embauches actuelles n'exigent pas de certification individuelle.

Rappelons qu'il y aurait en France de l'ordre d'une centaine de CISSP, quelques dizaines d'auditeurs ISO27001. La grande majorité appartient à des sociétés informatiques américaines, de SSII ou de cabinets de conseil en SSI. Alors qu'on dénombre environ 10 000 professionnels SSI, quelque soit leur métier.



Même si elle paraît inéluctable, la certification des professionnels en SSI reste lente à devenir une réalité, comprise et crédible.



## 4.4. Pour un rééquilibrage des zones d'influence

Elargissons maintenant le cadre de l'enquête pour positionner plus globalement les grands domaines d'exercice du pouvoir ou de l'influence.

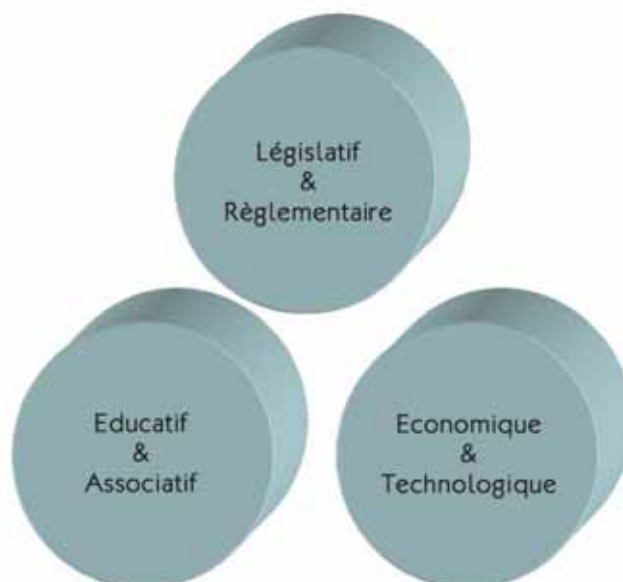
Tout part, en théorie, d'un **cadre législatif et réglementaire**. Or, il n'existe pas à proprement parlé dans la Sécurité des SI. Celui-ci regroupe - ou plutôt interfère avec - de nombreux textes aux origines et champs d'application très variés (du commerce en ligne à la vie privée, de la lutte contre la cybercriminalité à la propriété intellectuelle, etc.).

On notera simplement que la réglementation se doit d'être plus incitative que répressive, plus facilitatrice que contraignante, plus claire et transparente aussi. C'est à cette condition que la coopération public-privé peut se mettre en œuvre.

L'exemple des luttes d'influences ayant secoué les leaders de l'Internet comme Google cet été, au regard de la protection de la vie privée en est un exemple flagrant (vs durée de conservation de données de connexion). Les polémiques liées aux risques d'utilisation des PDA Blackberry pour échanger des données sensibles également (vs gestion des flux et des clés cryptographiques).

Dans la pratique, nous savons que les textes suivent et s'adaptent à leur environnement. En Sécurité des SI, l'action n'attend pas – toujours – la règle. La pression technologique, la réalité des menaces, plus ou moins avérées et un marketing efficace poussent à la mise en œuvre de processus ou de solutions.

Pour que l'ensemble soit cohérent, un tiers, indépendant de l'Etat / de l'Entreprise (de la décision) ou du Marché (de l'action) doit intervenir, certes en étroite relation avec les deux autres. C'est le rôle, au plan macroscopique, du secteur de l'Education et des Associations mais aussi, pourquoi pas, des médias, du moins de certains.



Les 3 domaines d'exercice du pouvoir

Nous allons indiquer dans les chapitres suivants, quelles sont les pistes de réflexion qu'il nous a semblé important de souligner en guise de conclusion.

#### 4.4.1. Aspects législatifs et réglementaires : des impacts organisationnels

L'Etat et désormais l'Europe demeurent des acteurs incontournables du domaine de la SSI. Le rapport du Député Pierre LASBORDES - « La Sécurité des SI : un enjeu majeur pour la France », remis au Premier Ministre le 13 janvier 2006, insistait largement sur les questions d'organisation générale en SSI intégrant le secteur industriel.

Au plan national, il faut donc insister sur l'importance d'une Direction Centrale à la SSI rattachée via le SGDN au 1er Ministre. Son rôle est vaste et stratégique, pour la protection des SI de l'Etat (rôle de veille, de conseil et d'audit) mais aussi au plan de la législation et de la normalisation. L'influence que peut jouer le Bureau conseil dans la mise au point de la série de Normes ISO2700x (notamment ISO 27005 sur l'analyse des risques) ne doit pas être négligée. La question est désormais d'une part de regrouper et renforcer le secteur stratégique et de le séparer clairement de l'opérationnel. Vaste mais fondamental chantier !

La CNIL est l'autre instance sur laquelle nous devons insister. Son rôle est fixé par décret depuis 1978 et consacre son indépendance. Depuis 2004, son action s'est élargie à la labellisation de produits et de procédures. Contrairement à la DCSSI, la CNIL a le pouvoir d'imposer. La CNIL fait partie de ces organisations incontournables, communes à toutes les démocraties. Sans parler de « contre-pouvoir », elle doit assumer un rôle essentiel d'équilibre entre des intérêts souvent divergents au sein même des organisations et de l'Etat.

Tout le monde s'accorde à reconnaître que toutes deux manquent de moyens humains (en les comparant à leurs homologues étrangers). Les efforts de renforcement de ces pouvoirs essentiels ne se mesureront pas uniquement dans des rapports ...

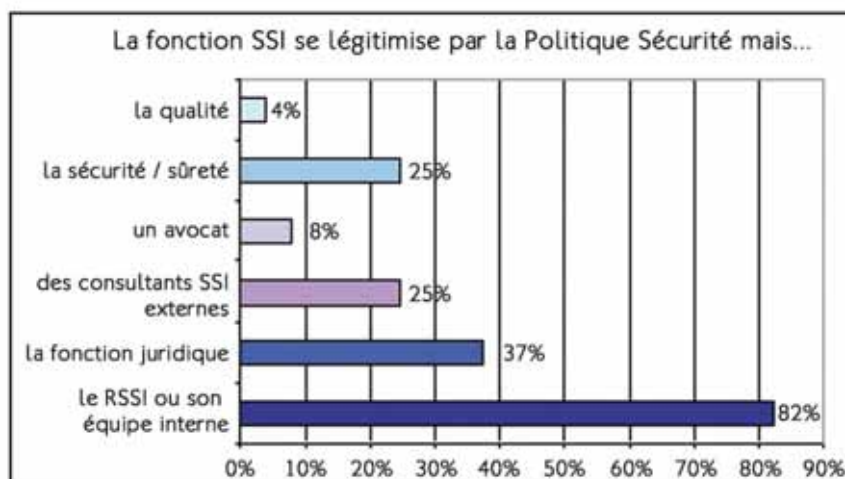
Car, il y a deux ans, le Député Pierre LASBORDES mettait en exergue les failles organisationnelles de la France :

*« La multiplication des acteurs publics dont les missions se chevauchent et dont les textes fondateurs sont peu précis, donnent une impression générale de confusion et d'éparpillement des moyens et des hommes. Dans cette nébuleuse, l'acteur public dédié, le SGDN et plus précisément la DCSSI, souffre d'un manque d'autorité et parfois de crédibilité auprès des publics concernés. Ces deux facteurs, l'éparpillement de moyens et le manque d'autorité du SGDN, nuisent à l'efficacité de l'Etat dans la définition et la mise en œuvre de la politique globale de SSI. »*

Nous ne saurions que trop ré-insister sur le besoin d'une entité « forte », de nature stratégique, au sein de l'Etat.

Revenons aux entreprises / administrations et à l'enquête 2007. Indépendamment d'un cadre réglementaire sectoriel qui « pousse à agir » (comme dans la Banque, les Télécoms, la Défense ou la Santé), le RSSI (supposé le décideur en SSI) tient son autorité de sa mission visant à établir la Politique Sécurité. Mais il n'y parvient pas seul comme l'atteste le schéma ci-dessous. Sa sagesse est de savoir fédérer autour de lui les acteurs (internes comme les juristes ou externes comme les consultants), pour bâtir un référentiel de qualité qui traduit l'importance de la question pour son organisation et qui guidera son action pendant des années.





Cette légitimité acquise dans le formalisme d'un document de référence sera le sésame du RSSI. Car quelque soit l'autorité accordée par un dirigeant à un RSSI, sous quelque forme que ce soit, le plus dur reste à faire.

Le constitutionnaliste reconnu, Guy Carcassonne, n'a pas manqué de souligner dans le magazine LE POINT du 5 juillet 2007 :

*« Que les plus hauts responsables soient aidés dans leur tâche par des soutiens précieux est normal, naturel et n'est un secret pour personne. Que les intéressés y acquièrent un pouvoir, parfois très important, est inévitable et n'a rien de choquant, puisque c'est le titulaire de la fonction qui, en exerçant seul la responsabilité de celle-ci, peut donc s'organiser comme il l'entend. [...] Le plus fiable et le plus influent des collaborateurs mérite la confiance que son patron lui fait et le poids réel qui en résulte, mais l'un et l'autre, doivent se rappeler toujours que si le pouvoir peut, en partie, se déléguer, ce n'est pas le cas de la légitimité. »*

Que les Responsables en charge des questions de SSI, au sein de l'Etat et des Entreprises soient alertés par cet « excès » toujours possible.

Car dans la pratique, il faut encore et toujours démontrer que son « autorité » est exercée. Dans la mise en œuvre de la Politique SSI, le panel apparaît « au milieu du gué ». Or, pour certains, l'ancienneté dans le poste peut être déjà ancienne (cf. annexe).

**Peut-on imaginer que les fonctions SSI (plutôt « protection des informations ») soient un jour légitimées par une Loi ou doit-on se résoudre à les voir évoluer au bon gré de leurs dirigeants et du marché ?**

#### 4.4.2. Aspects économiques et marketing

Une chose semble certaine : le marché continuera d'évoluer avec un marketing de l'offre efficace. Que les technologies « sécurité » soient ou non, un jour, intégrées dans les produits de « consommation » ne change rien à la question. On vendra de l'insécurité.

*« L'insécurité est un phénomène bien réel, mais elle est en même temps insaisissable, diffuse, mouvante, inassignable à un lieu. En conséquence, elle se prête à toutes les manipulations : on peut la minimiser, l'exagérer et, au final, la canaliser dans le sens d'un bénéfice politique et commercial maximal. [...] Cette polarisation a deux avantages. Tout d'abord, elle permet*

*de détourner l'attention du public des facteurs d'insécurité sur lesquels les gouvernements agissent peu quand bien même ils en ont les moyens. [...] A l'inverse, elle met en lumière non seulement les décisions spectaculaires de gouvernements qui entendent être crédités du souci qu'ils ont des angoisses de leurs concitoyens, mais aussi les ripostes individuelles de citoyens qui, avec le concours des marchands, se délivrent de l'énergie négative de l'anxiété en prenant leur sécurité en main. Résultat : les causes profondes de l'insécurité ne sont pas traitées et la fabrique de la peur ne ralentit pas. L'insécurité est un marché prometteur. »*

Ainsi s'exprime Zygmunt BAUMAN, sociologue britannique d'origine polonaise, dans le magazine LE POINT du 26 juillet 2007. Cette vision s'inscrit dans le cadre de son ouvrage « La vie liquide » (Rouergue/Chambon 2006) analysant une mondialisation qui se liquéfie, cédant aux marchés une liberté absolue, généralisant l'incertitude et désagrégeant les solidarités.

Loin d'être décalées par rapport à notre sujet, et sans nécessairement souscrire totalement à la vision de cet intellectuel, les idées sous-tendues par cette analyse s'inscrivent parfaitement dans la dialectique du Livre Bleu 2007.

Le pouvoir parfois excessif de l'économie s'exprime totalement dans notre secteur d'activité et les professionnels doivent prendre garde au poids phénoménal que prend le marketing de la peur.

Evidemment, les entreprises continueront de faire évoluer leurs systèmes d'information et leurs outils de communication. Bien sûr, il est illusoire d'imaginer de supprimer les outils de sécurité. Mais force est de reconnaître que la balance a jusqu'à présent profité aux vendeurs, plus qu'aux entreprises.

1. Quelle a été l'efficacité réelle des sondes anti-intrusion déployées par centaines, milliers, dizaines de milliers ?
2. A-t-on encore besoin d'anti-virus (sur les postes de travail en réseau) alors que s'imposent les anti-spywares ?
3. Comment comprendre que l'industrie informatique n'ait jamais réussi à bâtir un standard de contrôle d'accès synchronisant les mots de passe entre systèmes hétérogènes ?
4. Nous rappellerons encore une fois que la part des dépenses des entreprises dans le domaine de la formation / sensibilisation en SSI est de l'ordre de 5%.

D'aucuns diront que les effets positifs des TIC compensent ses effets négatifs. Sans doute, mais il ne faut pas rester aveugle à certains excès.

#### **4.4.3. Aspects éducatifs et culturels**

Pour conclure, nous devons aborder les domaines d'où, à terme, tout doit (re) partir. Ce sont ceux de l'éducation et de la culture. Ici se joue l'avenir de domaines qui doivent gagner en maturité. Le champ est vaste et les initiatives ne manquent pas. Mais il mérite une attention particulière tant ses capacités d'influence, positives et négatives, sont grandes.

L'OCED a communiqué en 2002 sur le « développement de la culture sécurité de l'information ». La Commission Européenne a réalisé un inventaire des cursus de formation en SSI. L'ENISA publie un rapport annuel sur les actions des Etats membres dans le domaine de la Sensibilisation en sécurité. La France lance des projets d'envergure comme le site [www.protegetonordi.com](http://www.protegetonordi.com).

Le rapport du Député Lasbordes a fixé un cadre d'évolution structuré au sein de l'Etat.

Mais il semble toujours manquer un maillon à la chaîne. Pourquoi ?

N'est-ce pas une question de comportement individuel, quasi « génétique », tout simplement ?

Il faudrait donc, d'une part gérer le quotidien, mais aussi se projeter à l'échelle d'une génération.

Quelques idées / questions de bon sens méritent d'être rappelées ou mentionnées :

1- Comment intégrer dès le collège, voire avant, les dangers de l'utilisation des SI, de la messagerie et d'Internet, des communications mobiles ? On le fait bien pour le traitement des déchets et la sécurité routière.

2- Comment renforcer le tissu associatif, sans doute pléthorique, trop absent en termes d'influence réelle. La coopération publique-privée doit s'établir dans une enceinte indépendante que peut incarner une organisation comme le CLUSIF, au niveau national, et ses homologues en Europe. Mais pour cela, organisation et modes de fonctionnement doivent évoluer ...

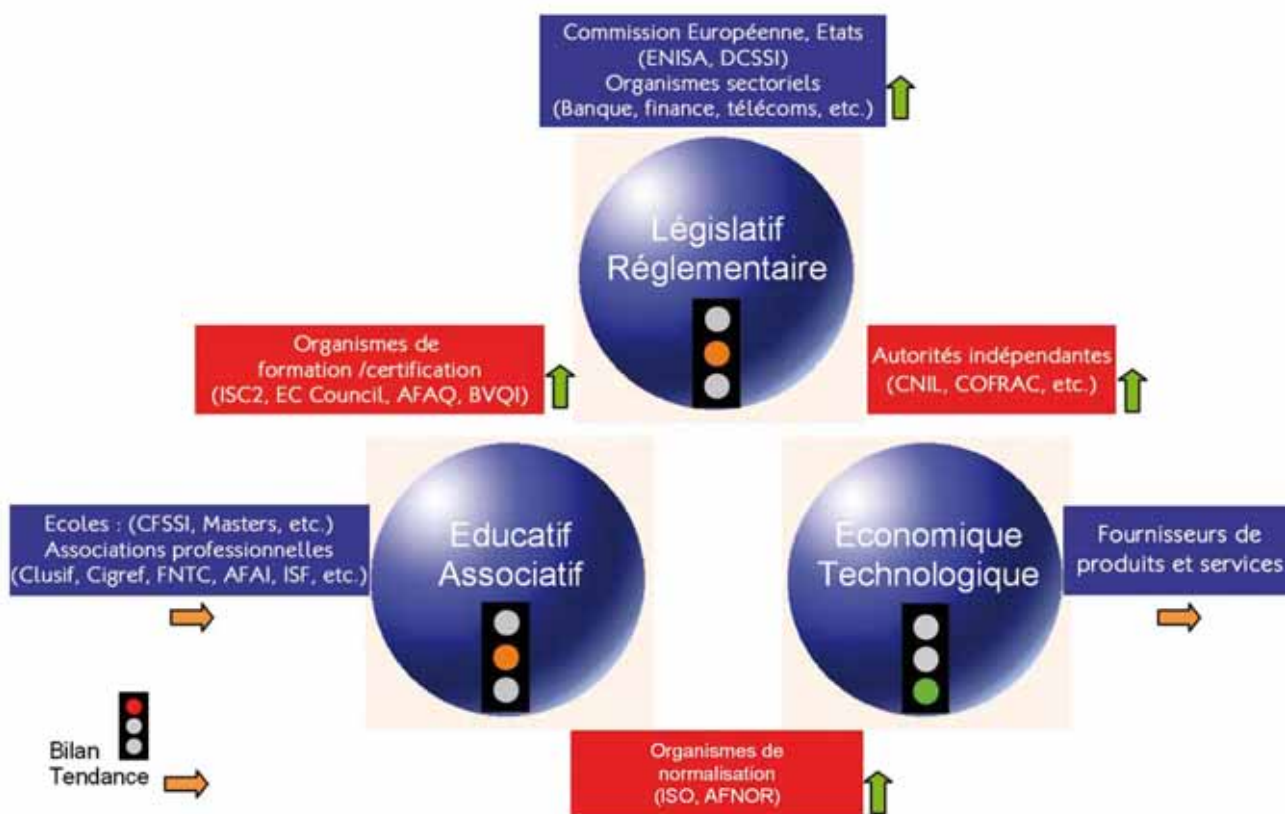
3- Comment renforcer l'influence des RSSI (au sens « acheteurs ») vis à vis des fournisseurs et prestataires ? Leur poids devrait se renforcer, au travers de groupes de pression, associatifs ou non, éventuellement sous la forme d'un « syndicat » représentatif de cette profession.

4- Quels sont les médias spécialisés ou non qui parviendront à informer sans manipuler, sans influencer dans le sens voulu par les annonceurs ? Le nombre de revues et de sites web consacrés à la Sécurité des SI devient pléthorique mais aucun ne traite avec sérieux de la dimension « humaine » du risque informatique et informationnel.



## 4.5. Les acteurs clés du Pouvoir en Sécurité SI

Nous proposons ci-dessous un schéma de synthèse, sans doute partiel, mais éclairant, sur les sphères d'influence externes à l'entreprise et à la fonction SSI. Leur connaissance peut être utile, la compréhension de leur rôle, nécessaire parfois.



Les sphères d'influence externes se modifient

Nous pouvons simplement remarquer que les acteurs des trois sphères de base ne présentent pas d'évolution structurelle majeure. Mais les acteurs « inter-sphères », dont l'indépendance doit être soulignée, semblent prendre une importance accrue.

Nous laissons ce schéma à l'analyse des lecteurs !

D'autres instances, beaucoup plus informelles, existent mais n'apparaissent pas. Elles regroupent des « utilisateurs » comme le Forum des compétences ou l'Information Security Forum.

Mais certaines, dont fait partie le Cercle Européen de la Sécurité et des Systèmes d'Information, sont mixtes et représentent des lieux de rencontre orientés « business ». Ce qui n'exclut pas les discussions de fond, des travaux et des échanges parfois structurants.

## 5. CONCLUSION

Nous proposons ici en forme de synthèse, les idées forces présentées et analysées dans le Livre Bleu 2007. Certaines sont évidemment connues de beaucoup, mais elles méritent d'être rappelées. D'autres nécessitent sans doute discussions et approfondissements. Ce que nous ne manquerons pas de faire dans l'enceinte du Cercle.

1- Les RSSI ne tiennent leur autorité que d'une mission qui leur assigne l'élaboration et le contrôle de la mise en œuvre d'une Politique Sécurité.

2- Les RSSI possèdent des capacités (potentielles ou réelles) d'influence interne extrêmement vastes et variables en fonction de leur profil. C'est ici qu'ils trouvent leur véritable « pouvoir » et surtout une légitimité parfois fort utile (ex : relations avec les pouvoirs publics, implication dans l'Intelligence Economique ou la protection des données personnelles par exemple).

3- Les RSSI doivent s'organiser pour gagner en influence sur le marché sans doute via le tissu associatif. Le marketing de l'offre, s'il est utile, doit être associé à une plus grande exigence de la part des utilisateurs et des acheteurs.

4- L'implication du management (via un membre de la Direction Générale) au sein d'un Comité Sécurité est un élément majeur de prises de décisions collégiales. Le RSSI trouve ici un moyen de légitimité très forte de son action.

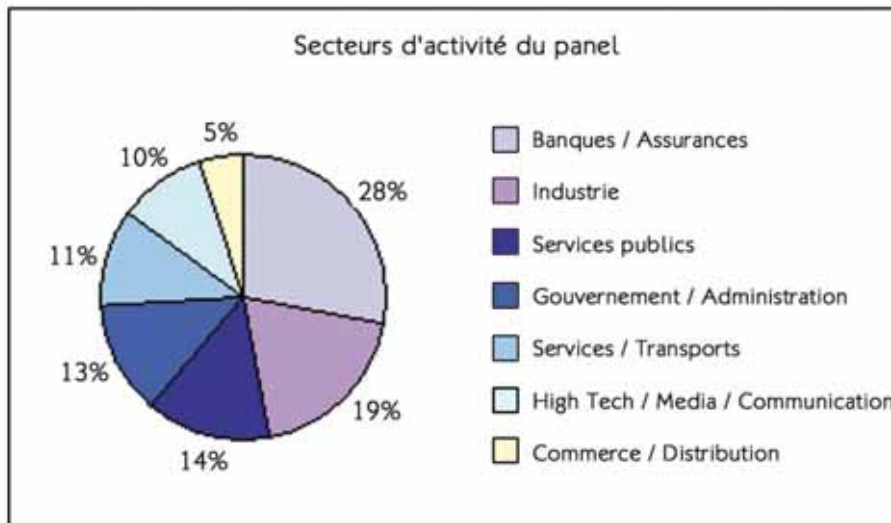
5- La professionnalisation des prestataires SSI se renforce sous l'impact des certifications individuelles de type ISO 27001 (mise en œuvre et audit) conférant aux acteurs de la formation / certification une importance essentielle sur le marché.

6- L'Etat (la DCSSI) doit renforcer ses moyens d'influence externe au plan européen et international. La mise en oeuvre des recommandations du rapport du Député P. Lasbordes mérite une attention particulière.

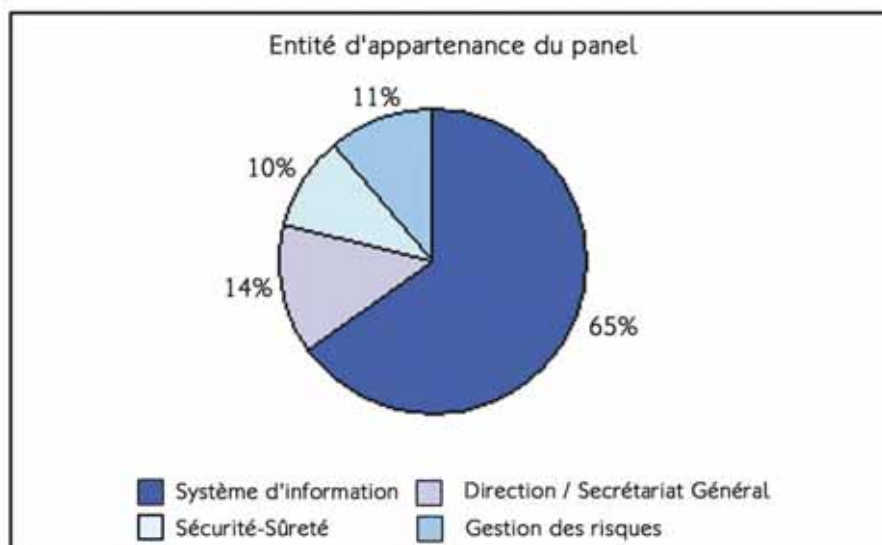
7- Des instances connexes aux métiers de la SSI commencent à posséder de réels pouvoirs mais souffrent d'un manque crucial de moyens : la CNIL, le COFRAC.

## 6. ANNEXE : LE PANEL

### 6.1. Secteurs d'activité

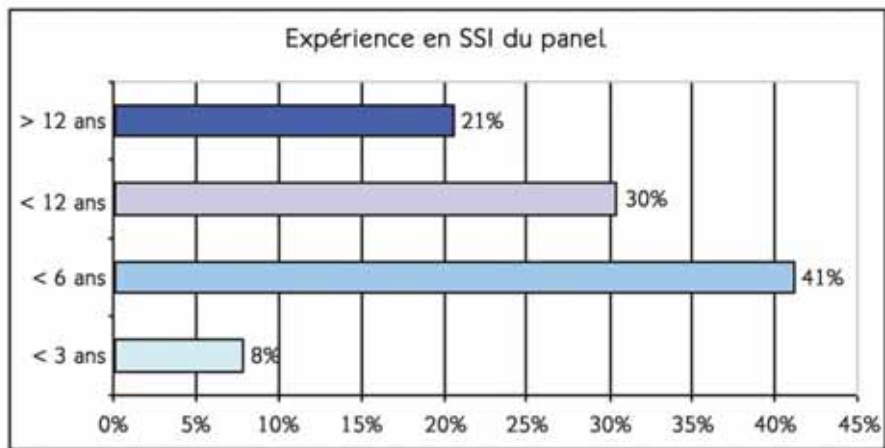


### 6.2. Entité organisationnelle des répondants

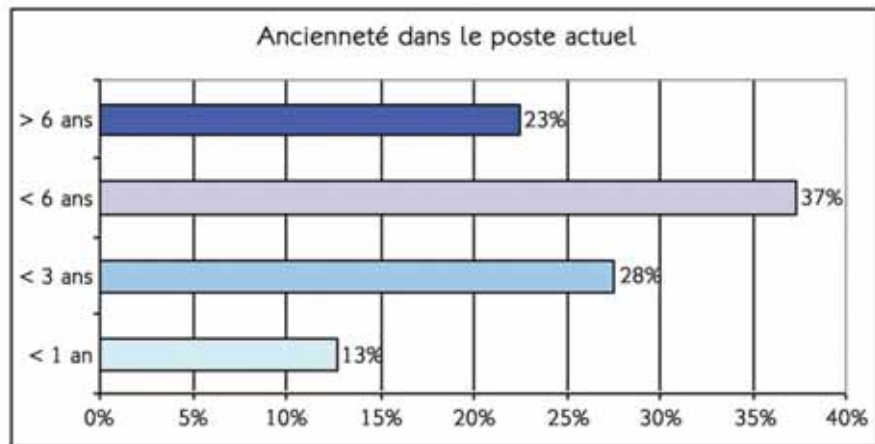




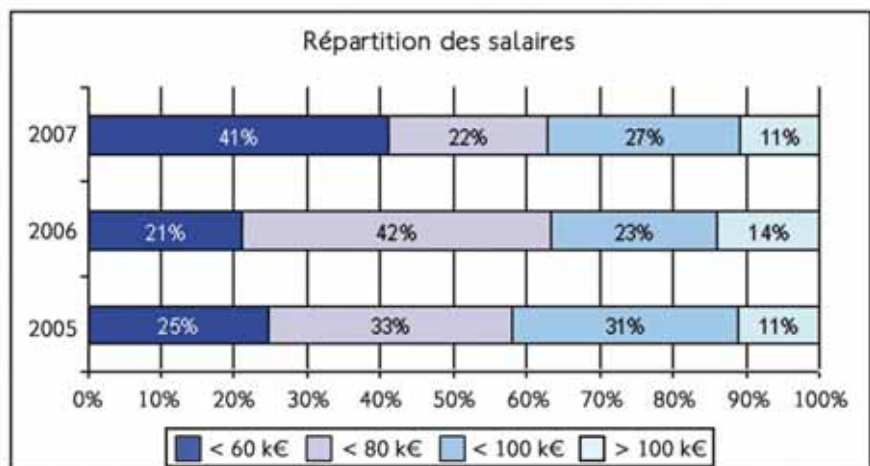
### 6.3. Expérience en SSI



### 6.4. Ancienneté dans le poste actuel



### 6.5. Rémunération



**Monaco**

10-13 octobre 2007

7<sup>e</sup> édition

## L'événement européen de la Sécurité et des Systèmes d'Information

### Les chiffres parlent d'eux-mêmes\*

- **950 participants** RSSI, DSI, Risk Managers, experts et acteurs majeurs de la sécurité, en 2006.
- **97 %** affirment avoir amorcé ou concrétisé des accords au cours de l'événement.
- **98 %** enrichissent utilement leur relationnel avec les prestataires présents.
- **99 %** jugent les informations obtenues pertinentes et très précieuses.
- **100 %** envisagent de participer de nouveau aux Assises en 2007.

**En 2007, les Assises seront plus que jamais la grand-messe annuelle  
des professionnels de la Sécurité et des Systèmes d'Information.**

*\*Enquête de satisfaction - novembre 2006*



# Nos partenaires



INFOCLAS - NETWORKS BUSINESS

# Avec la participation de



un événement

 Pour plus d'information téléphonez au 01 41 93 07 07  
[www.lesassisesdelasecurite.com](http://www.lesassisesdelasecurite.com)



**Prix de l'Innovation  
des Assises 07**  
 L'événement Français de la Sécurité et des Systèmes d'Information



**Le cercle**  
 European de la Sécurité et des Systèmes d'Information



# A vos agendas !

## L'Événement Européen de la Sécurité et des Systèmes d'Information



### Monaco

### 15-16-17-18 octobre 2008

### Bloquez les dates !



## Les Assises

L'Événement Européen de la Sécurité et des Systèmes d'Information



Pour plus d'information, contactez-nous au 01 41 93 07 07  
ou sur [www.lesassisesdelasecurite.com](http://www.lesassisesdelasecurite.com)

un événement

