WHITE PAPER DES ASSISES 2012

Evolution de la fonction « Sécurité des Systèmes d'Information »

De la vision des dirigeants aux attentes des RSSI

Paris, le 30 octobre 2011

En 2011, des entretiens avec des dirigeants de groupes français ont permis de dégager leur vision et leurs orientations vis à vis de la fonction « Sécurité SI »[1]. Ces résultats devaient être confrontés à la réalité du terrain, au regard des activités concrètes et des aspirations actuelles des Responsables Sécurité SI (RSSI).

Pour ce faire, le Groupe de travail du Cercle Européen de la Sécurité[2] a préparé une enquête menée en juin et juillet 2012 auprès de la communauté des RSSI. Ce 2ème white paper présente la synthèse des résultats[3] en les replaçant dans la dialectique des travaux de 2011. Il s'appuie également sur un atelier des Assises de la Sécurité sur le thème « RSSI : un passage ou une carrière ? », préparé et animé par le Groupe de travail du Cercle.

1. Souvenez-vous l'année dernière : quand des dirigeants définissent la cible et les orientations

En 2011, deux questions avaient été posées à une vingtaine de membres de Comités de Direction :

- ***« Qu'apporte, selon vous, la fonction Sécurité des SI à votre entreprise / organisme ? »***
- ***« Comment la voyez-vous évoluer à court et moyen terme au sein de votre entreprise / organisme ? »***

Globalement, le RSSI incarne désormais ***une fonction clé devant gérer des compromis avec une bonne communication et surtout en apportant des solutions. Elle va se renforcer, gagner en indépendance et devenir plus pragmatique et ouverte.*** Pour l'un des interviewés, ***« C'est la qualité de la personne qui fait toute la différence dans cette fonction. ».*** *« La fonction a besoin de professionnels très ''seniors'' et aptes à travailler en transversal. » « C'est une fonction de ''business enabler'' et pas un empêcheur de tourner en rond ! ».* En clair, la Sécurité des SI doit s'inscrire dans la chaîne de valeur de l'entreprise.

Une forte tendance au pragmatisme avait été mise en évidence. Edicter des règles et veiller à leur application, conseiller une technologie ou un fournisseur, mener des actions de contrôle et d'audit restent les fondamentaux mais ils ne suffisent visiblement plus. Le RSSI qui sert de caution ou de *« garde-fou »*, ou qui passe pour un « gourou » est dépassé. En phase avec la stratégie de son organisation et en lien étroit avec les métiers, il doit se professionnaliser et devenir facilitateur de projet, voire décisionnaire autour du triptyque opportunités « business » / risques « SI et métiers » / coûts « outils et services ».

Nous nous étions cependant étonnés, par exemple :

- De l'absence de considération des questions économiques et budgétaires. Un RSSI sans budget demeure-t-il une perspective crédible ? Le pilotage économique de la SSI doit-il être développé et mis en valeur auprès des décideurs ?
- De l'accent mis sur la fonction SSI ou le RSSI lui-même, sans remarque sur ses compétences, son équipe et ses moyens. L'image du RSSI « homme à tout faire » et sans équipe pourrait-elle se perpétuer pour beaucoup ?

[1] Voir le white paper des Assises 2011 sur www.lecercle.biz
[2] Voir Annexe 2
[3] Voir Annexe 1

- D'un manque de propos sur les objectifs fixés à la fonction. Quels sont les livrables et la valeur ajoutée attendus pour un dirigeant ? Quid des indicateurs et tableaux de bord, voire des certifications « sécurité » ?

A contrario, les points non abordés, concernant des craintes parfois non justifiées des RSSI étaient :

- Aucune remarque sur l' « exaspération » des métiers et des utilisateurs en relation avec les contraintes apportées par la Sécurité SI. La sécurité ne serait ainsi pas perçue comme une contrainte par ces dirigeants.
- Aucune exigence de remise en cause de la fonction. Des évolutions ou des transformations attendues plutôt positives mais sans révolution fondamentale.
- Aucune directive détaillée sur la posture du RSSI, son positionnement précis et ses modes de fonctionnement (à part l'indépendance). Un encouragement implicite au pragmatisme et à l'ouverture rappelant l'exigence de ''séniorité'' et de grande pédagogie pour les RSSI.

Clairement, les dirigeants interviewés encouragent implicitement, sans le dire, les RSSI à encore développer leur crédibilité en se positionnant dans la chaine de valeur de l'entreprise et pas seulement en support de celle-ci, pour gagner la reconnaissance des métiers et du management.

Qu'en est-il en 2012 ? Pour répondre, nous nous appuyons sur l'analyse de l'enquête annuelle du Cercle Européen de la Sécurité (avec 131 réponses de RSSI) et proposons un nouvel éclairage sur l'évolution de la fonction SSI.

2. Quelques confirmations, étonnements et nouveautés

Les résultats obtenus en 2012 (voir annexe pour les résultats détaillés) permettent de dégager des quelques confirmations, des étonnements et des nouveautés.

Globalement, les RSSI conservent une forte composante opérationnelle :

- gestion de projets « SSI » : 64% des répondants
- plan de continuité d'activité : 60% des répondants
- plan de secours informatique : 47% des répondants

Une faible majorité (56%) assure également un véritable management d'équipe, confirmant ainsi l'image du RSSI solitaire ou binôme.

Enfin, les aspects budgétaires et financiers (notamment l'assurance) ne sont traités que par une très petite part de l'échantillon (14%).

A ce rapide constat factuel, nous ajoutons une nouvelle dimension à notre analyse. Au regard des attentes et de la vision des dirigeants, à quoi aspirent les RSSI, en termes d'évolution ?

Globalement seulement 2 RSSI sur 10 n'envisagent pas de changement majeur dans les prochaines années. Mais pour les autres, qui envisagent ou attendent une évolution, aucune tendance forte ne se dégage. En termes structurels, les évolutions se situeraient vers les métiers (46%) comme le risk management (22%) ou la conformité (21%), voire vers la sûreté/défense (14%).

Deux demandes (parmi les plus fortes) corroborent finalement la vision des dirigeants : les RSSI attendent ou espèrent un accès facilité vers les hautes fonctions de l'entreprise (exécutifs) (51%) et des passerelles vers les métiers (37%).

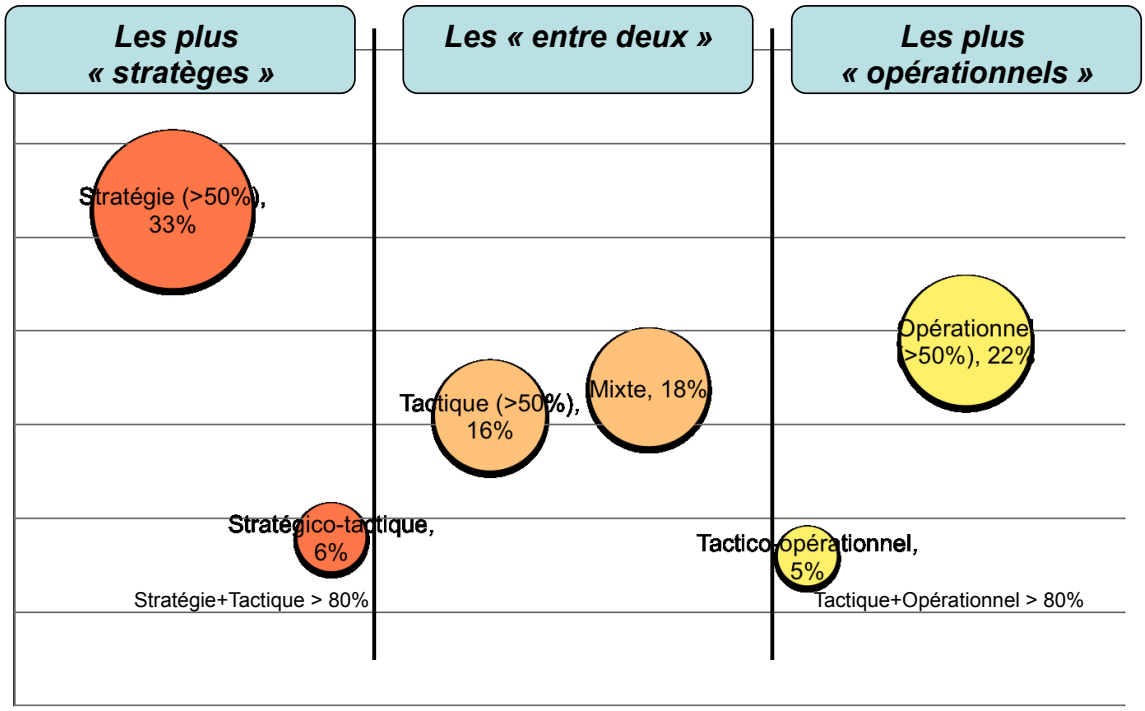
Face à ces constats et à ces aspirations très globales, peut-on dégager des profils « types » de RSSI ? Car on a bien coutume de dire et de constater qu'il y a autant de profil de RSSI que de contexte d'entreprise …

3. Du profil « type » aux 3 « postures » du RSSI

L'exercice n'est pas simple (car il va masquer de grandes disparités) mais nous proposons cette année, au regard des résultats de l'enquête, un profil type en 6 paramètres clés. Ainsi, *« en moyenne »* :

- Un RSSI possède 10 ans d'expérience en Sécurité SI et 4 ans dans le poste.
- Il dispose d'une équipe d'environ 3 collaborateurs internes et de 1,5 experts externes.
- Il tend à être certifié (ISO 27001 et 27005 plutôt que CISM ou CISA voire CISSP).
- Sa rémunération brute globale est de 81 k€.

Lorsque l'on analyse les réponses sur les activités concrètement menées en 2012 (affectation du temps accordé aux différentes activités), nous constatons que 3 grandes *« postures »* se dégagent : les « stratèges » devancent les « entre deux », eux-mêmes plus nombreux que les « opérationnels » (voir schéma ci-dessous et annexe 1).



Répartition des RSSI selon leurs activités en 2012
(temps consacré aux plans stratégique / tactique / opérationnel)

Cependant, quelle que soit l'activité quotidienne en 2012, 6 actions clés permettent de définir la mission d'une très grande majorité de RSSI :

- Définition de la Politique Sécurité SI : 87%
- Pilotage de la mise en œuvre de la Politique Sécurité SI : 88%
- Analyse de risques et classification des actifs : 86%
- Communication et sensibilisation : 79%
- Veille (stratégique, technologique) et relations institutionnelles : 75%
- Contrôle / audit : 66%

Cette répartition des activités ne doit-elle pas aussi évoluer ?

- d'une part en termes « qualitatifs » car faire c'est bien, bien faire, c'est mieux …
- d'autre part en termes de « périmètres » et de « missions » dans une optique « ERM » (Enterprise Risk Management) pour mieux tenir compte des enjeux (pression réglementaire et cybercriminalité),

des risques liés aux nouveaux usages (médias sociaux et mobilité par exemple), et des évolutions technologiques (services proposés par le cloud computing, le big data, etc.).

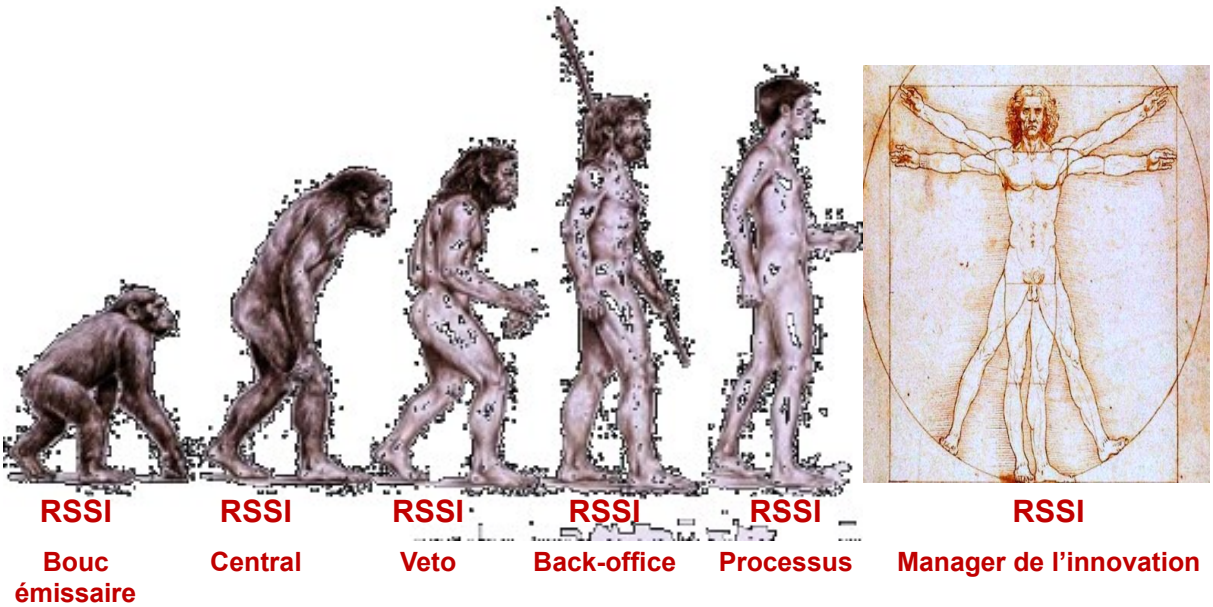
4. DSI / RSSI : une analogie possible

Au delà de ce constat, nous proposons une analyse de la fonction SSI sur les concepts de *« compromis »* (qui sont parfois impossibles : sécurité vs performance et ergonomie, coûts des mesures vs risques à couvrir et budgets disponibles, etc.) et d' *« inconfort utile »* (par exemple : prise de conscience sur des menaces inconnues ou ignorées pour et par les métiers) : une certaine tendance à la schizophrénie qui n'est pas sans rappeler l'évolution des DSI dont les RSSI sont à la fois très proches (dans l'organisation) et très éloignés (dans les missions). Une des clés d'aujourd'hui et de demain, pour la fonction SSI réside (ra) bien dans cette capacité à répondre à des enjeux stratégiques pour les métiers tout en apportant des solutions techniques et très opérationnelles.

Comme le montrent les travaux sur les aspects économiques de la SSI (évaluation des dépenses, budgets), ce n'est pas un point fort de la fonction. Elle dispose finalement de peu de budget en propre et ne s'intéresse quasiment pas au sujet : un accès alors très difficile aux organes de décision où le « ROI » prime et où on n'aborde que « CAPEX et OPEX », « valeur ajoutée », etc. Et même si les salaires de RSSI deviennent significatifs, si certains sont bien positionnés dans les organigrammes, l'atteinte de postes de direction reste très difficile, voire impossible.

Quant à mettre en place une plus grande proximité avec le business et les métiers, c'est facile à exprimer, beaucoup plus délicat à réaliser. Vers qui aller ? Pour faire quoi ? Depuis longtemps, les DSI vivent ça !

Comme le DSI, le RSSI a vécu différentes étapes de son parcours professionnel. Chacun, dans son contexte et selon son profil se situe à l'un ou l'autre des stades de l'évolution (voir schéma ci-dessous).



Darwinisme appliqué au RSSI

(Reproduction avec l'accord de A. Gourevitch - The Boston Consulting Group)

Insistons sur les 4 dernières étapes que certains RSSI connaissent aujourd'hui et que d'autres atteindront peut-être dans les années futures :

- Le RSSI « véto » se caractérise par une forte implication dans la « veille » et des études apportant essentiellement une expertise auprès des projets SI et des métiers. Au risque d'être l'empêcheur de tourner en rond …
- Le RSSI « back office » s'implique plus au plan décisionnel. Il doit argumenter les dépenses à engager et le cas échéant, s'appuyer sur des « benchmarks ».
- Le RSSI « processus » agit au plus prêt des directions. Il doit être capable de démontrer en quoi les mesures de sécurité proposées et mises en œuvre apportent une valeur ajoutée pour les « processus métiers » et pour le développement du « business ».
- Enfin, le RSSI « manager de l'innovation » (englobant sans doute le précédent) aura plus facilement accès aux Comités de direction et d'audit. Il inscrira son action dans le cadre de la stratégie et de la gestion des risques de son entreprise (ex : cartographie et plan de prévention). Sera-t-il cependant encore RSSI ?

Face à ce constat et ces perspectives basées sur l'anthropologie, quelles sont les voies concrètes s'offrant aux RSSI ? Trois peuvent sans doute se dessiner :

- **L'élargissement du périmètre d'action** peut sembler la plus accessible : passer de la Sécurité SI à la Sécurité de l'information au sens large, intégrer aussi la fraude/malveillance dans le cadre de la cybercriminalité dont les impacts atteignent le business, etc.)
- Inversement, **une spécialisation** faisant du RSSI un expert avant tout : la SSI étant devenue tellement vaste et complexe, se concentrer peut aussi être une voie d'évolution y compris en allant vers les fournisseurs qui vont avoir besoin de compétences fortes connaissant l'entreprise.
- Enfin, une troisième voie, plus délicate et lointaine sans doute : **faire évoluer la SSI comme élément de la protection des actifs immatériels** (patrimoine informationnel) dès lors que la valeur de celui-ci est ou sera reconnue par les dirigeants.

Sur ce dernier point, le rapprochement vers les dirigeants et les métiers vu précédemment, sera nécessaire mais sans doute pas suffisant. Connaître les bons acteurs, engager le dialogue et montrer ses apports au quotidien (analyse de risques, bonnes pratiques, solutions) sera utile, mais pour ce faire, il faudra maîtriser leur environnement, connaître leurs méthodes de travail et s'approprier aussi leurs indicateurs de pilotage. Vaste programme …

5. Alors, être RSSI : Un passage ou une carrière ?

Concluons en apportant des éléments de réponse à une question souvent posée : Un RSSI assure-t-il une mission (temporaire) ou peut-il envisager un véritable parcours professionnel dans le domaine ?

Rappelons d'abord quelques éléments clés de l'enquête :

- Si 20% de l'échantillon n'envisagent pas de changement de leur fonction, 8% en espèrent un qui serait « fondamental »
- Les évolutions structurelles se situeraient vers :
  - la gestion des risques (43%)
  - les métiers (20%)
  - la conformité (19%)
- Les évolutions fonctionnelles s'orienteraient vers :
  - du management (46%)
  - de l'aide à la décision (42%)
  - de la communication (25%)

Le Groupe de travail du Cercle Européen ne répond pas réellement à la question posée mais propose ici un argumentaire, positionnant les opportunités et menaces pour chaque scénario.

	RSSI : un passage ?	RSSI : une carrière ?
Opportunités	• Une fonction à forte visibilité sur le marché • Des compétences rares (transversalité, management fonctionnel, aspects techniques et stratégiques / juridiques, etc.) • Des ouvertures réelles vers des métiers proches (contrôle interne, management des risques, etc.)	• Un métier qui évolue en permanence • Un métier que s'adresse à un actif de plus en plus stratégique pour l'entreprise (qui devient « numérique ») • Une fonction qui nécessite une bonne connaissance de son environnement, expertise, légitimité et stabilité
Menaces	• Des « portes de sortie » peu évidentes • Une vision des « RH » concentrée sur l'expertise et la technique • Une visibilité « floue » sur son « profil » • Le frein du salaire qui peut être élevé • L'expertise acquise est le seul bras de levier sur le marché pour évoluer	• Un métier qui pourrait être « cadré » à l'avenir, avec plus de « contraintes » • Une fonction vue comme une « expertise » (non du management de risques) • Une fonction qui peut se « bloquer » dans son entreprise • … Seul un changement d'entreprise permet d'envisager une évolution « forte »

L'ensemble de ces éléments mérite bien sûr d'être contextualisé par chacun et sera sans doute approfondi en 2013 avec une approche plus internationale.

ANNEXE 1 : RESULTATS DETAILLES DE L'ENQUETE

Le RSSI : son profil et ses activités en 2012

	Global	Champ d'action		Secteur d'activité		
		National *(75 réponses)*	*International* *(56 réponses)*	*Banques Assurances (40 réponses)*	*Industries Services (48 réponses)*	*Administrat° Services publics (43 réponses)*
Profil						
Expérience en SSI (ans)	10,2	10,0	10,5	9,8	9,9	10,7
Expérience dans le poste (ans)	3,7	4,1	3,3	3,8	3,6	3,9
Collaborateurs internes (ETP)	2,9	2,6	3,3	4,0	2,5	2,2
Prestataires dédiés (ETP)	1,5	1,2	1,8	1,2	1,9	1,2
ISO 27001 lead implementor	22,9%	26,7%	17,9%	35,0%	18,8%	16,3%
ISO 27001 lead auditor	20,6%	26,7%	12,5%	10,0%	16,7%	34,9%
ISO 27005 risk manager	22,9%	25,3%	19,6%	22,5%	16,7%	30,2%
CISM	6,1%	6,7%	5,4%	12,5%	2,1%	4,7%
CISA	6,1%	7,1%	5,3%	2,5%	6,3%	9,3%
CISSP	13,0%	14,7%	10,7%	10,0%	8,3%	20,9%
Autre	9,9%	12,0%	7,1%	7,5%	8,3%	14,0%
Rémunération moyenne (k€)	81 k€	78,5 k€	84,4 k€	88,3 k€	82,2 k€	73,0 k€
Activités transverses SSI						
Définition Politique Sécurité	87,0%	86,7%	87,5%	87,5%	85,4%	88,4%
Pilotage Politique Sécurité	87,8%	84,0%	92,9%	97,5%	87,5%	79,1%
Analyse Risques / Classification	85,5%	82,7%	89,3%	82,5%	91,7%	81,4%
Veille / Relat° institutionnelles	74,0%	78,7%	67,9%	70,0%	66,7%	86,0%
Management d'équipe	55,7%	57,3%	53,6%	67,5%	45,8%	55,8%
Assurance des risques SI	14,5%	16,0%	12,5%	20,0%	8,3%	16,3%
Communication / Sensibilisation	78,6%	77,3%	80,4%	77,5%	79,2%	79,1%
Audit / Contrôle	74,0%	77,3%	69,6%	82,5%	68,8%	72,1%
Conformité réglementaire	56,5%	52,0%	62,5%	55,0%	56,3%	58,1%
Plan de continuité	59,5%	65,3%	51,8%	50,0%	60,4%	67,4%
Activités orientées « SI »						
Veille techno / menaces	75,6%	72%	80,4%	77,5%	77,1%	72,1%
Gestion projets SSI	64,1%	64,1%	62,5%	72,5%	58,3%	62,8%
Architecture et outils SSI	48,9%	46,7%	51,8%	35,0%	52,1%	58,1%
Mise en œuvre outils / services	37,4%	36,0%	39,3%	30,0%	45,8%	34,9%
Administration outils / services	20,6%	18,7%	23,2%	17,5%	18,8%	25,6%
Gestion identités / accès	24,4%	20,0%	30,4%	25,0%	22,9%	25,6%
Formation des équipes SI	64,9%	66,7%	62,5%	60,0%	60,4%	74,4%
Assistance aux utilisateurs	23,7%	20,0%	28,6%	20,0%	29,2%	20,9%
Gestion du plan de secours	47,3%	56,0%	35,7%	37,5%	41,7%	62,8%
Gestion des incidents SSI	66,4%	57,3%	78,6%	67,5%	75,0%	55,8%
Répartition du temps de travail						
Activités transverses « SSI »	50,3%	48,7%	52,5%	48,5%	52,7%	48,3%
Activités orientées « SI »	49,7%	51,3%	47,5%	51,5%	47,3%	51,7%
Stratégie (politique)	37,1%	39,9%	33,1%	38,0%	36,9%	35,1%
Tactique (projets)	31,6%	31,8%	31,4%	30,0%	28,7%	36,1%
Opérations (processus)	31,3%	28,3%	35,5%	32,0%	34,4%	28,8%

ANNEXE 1 : RESULTATS DETAILLES DE L'ENQUETE

Le RSSI : souhaits d'évolution à 2-3 ans et attentes vis à vis de son management

	Global	Son champ d'action		Son secteur d'activité		
		National *(75 réponses)*	*International* *(56 réponses)*	*Banques Assurances* *(40 réponses)*	*Industries Services* *(48 réponses)*	*Administrat° Services publics* *(43 réponses)*
Evolution globale						
Sans changement fondamental	19,1%	24%	12,5%	27,5%	14,6%	16,3%
Changement radical de métier	6,1%	8,0%	3,6%	5,0%	6,3%	7,0%
Vers un fournisseur	4,6%	5,3%	3,6%	5,0%	4,2%	4,7%
Evolution structurelle						
Vers les métiers	22,1%	17,3%	28,6%	25,0%	20,8%	20,9%
Vers la sûreté / défense	13,7%	8,0%	21,4%	10,0%	22,9%	7,0%
Vers la conformité	20,6%	22,7%	17,9%	25,0%	16,7%	20,9%
Vers la gestion de risques	45,8%	37,3%	57,1%	37,5%	47,9%	51,2%
Evolution fonctionnelle						
Activités plus techniques	3,1%	5,3%	0,0%	0,0%	4,2%	4,7%
plus opérationnelles	10,7%	13,3%	7,1%	7,5%	12,5%	11,6%
plus de communication	27,5%	28,0%	26,8%	17,5%	27,1%	37,2%
plus d'expertise pointue	10,7%	13,3%	7,1%	2,5%	10,4%	18,6%
plus d'aide à la décision	48,1%	46,7%	50,0%	40,0%	56,3%	46,5%
plus de management	43,5%	40,0%	48,2%	47,5%	45,8%	37,2%
Attentes vs son manager						
Validation Politique	31,3%	30,7%	32,1%	32,5%	29,2%	32,6%
Arbitrages en Comité Sécurité	51,1%	54,7%	46,4%	50,0%	54,2%	48,8%
Informations sur stratégie	42,7%	38,7%	48,2%	45,0%	39,6%	44,2%
Accès facilité aux décideurs	51,1%	52,0%	50,0%	45,0%	56,3%	51,2%
Légitimité auprès des métiers	37,4%	38,7%	35,7%	37,5%	33,3%	41,9%
Recrutement de personnel	45,0%	45,3%	44,6%	42,5%	47,9%	44,2%
Augmentat° budget prestations	29,0%	30,7%	26,8%	42,5%	20,8%	25,6%
Augmentat° budget outils	22,9%	18,7%	28,6%	30,0%	18,8%	20,9%

Echantillon : 131 RSSI et équivalent. Enquête publiée en ligne du 15 juin au 31 juillet 2012 auprès des membres du Cercle Européen de la Sécurité.

ANNEXE 2 : LE GROUPE DE TRAVAIL DU CERCLE EUROPEEN

Groupe de travail : Le Groupe de travail du Cercle Européen est constitué de 6 RSSI et un DSI.

- Pascal BASSET (Responsable Sécurité et Conformité – PMU)
- Eric DOYEN (Responsable Sécurité des SI / CISO – Humanis)
- Stéphane JOGUET (Responsable Risques et Sécurité SI – Groupe DAHER)
- Didier GRAS (Responsable Sécurité des SI / CISO – Groupe BNP Paribas)
- Dominique GUIFFARD (Directeur des SI / CIO – CELINE – Groupe LVMH)
- Jean-François LOUÂPRE (Responsable Sécurité / CSO – AG2R La Mondiale)
- Sylvain THIRY (Responsable Sécurité des SI / CISO – Groupe SNCF)

Il est piloté par :

- Caroline APFFEL (Associée – Cabinet SpencerStuart)
- Pierre-Luc REFALO (Associé –HAPSIS)

Le Groupe de travail s'est réuni lors de plusieurs réunions et conférences téléphoniques afin de préparer l'enquête et d'en effectuer l'analyse et la synthèse. Il a produit ce document et le support de présentation de l'Atelier des Assises de la Sécurité 2012.