WHITE PAPER DES ASSISES 2011

La fonction Sécurité des Systèmes d'Information
Visions des dirigeants de grands comptes français

Paris / Monaco, le 5 octobre 2011

1. La fonction Sécurité des SI doit s'adapter à la complexité de son environnement

Depuis 2004, les enquêtes du Cercle Européen de la Sécurité ont permis de clarifier les rôles et les activités des Responsables de la Sécurité des SI (SSI). Elles ont en particulier mis en évidence l'existence de ***2 profils types*** appelant immédiatement à une distinction (non concrétisée) au niveau du titre de la fonction.

Certains sont clairement en charge du pilotage des activités « SSI » en se focalisant avant tout sur la Politique Sécurité SI (PSSI) et sur le contrôle de sa mise en œuvre dans une optique de « maîtrise des risques ». Ils apportent en particulier une assistance méthodologique et technique aux métiers et aux projets. En ce sens, ils sont aussi sollicités pour les moyens à mettre en œuvre.

Les autres, souvent au sein d'un service informatique, apportent une expertise essentiellement technique et mènent une mission opérationnelle. Dans le cadre d'une PSSI, ils garantissent la protection des SI face aux menaces et aux attaques informatiques.

Plus globalement, les professionnels de la Sécurité des SI ont des ***origines très variées***, et d'évidence il n'existe pas de parcours type (formation initiale, activités quotidiennes et parcours professionnels, etc.). Les filières de formation de RSSI restent embryonnaires. Coexistent ainsi : des informaticiens (développeurs, exploitants, chefs de projet), des experts (anciens policiers, militaires ou consultants), des managers issus des métiers. Les plus anciens d'entre eux sont venus à la SSI par pur hasard (dans les années 80), ensuite sans doute par opportunisme (dans les années 90 et l'émergence d'Internet), puis par fort intérêt (dans les années 2000 avec l'explosion du marché et la pression des réglementations et des normes). Aujourd'hui, comme pour les gendarmes ou les pompiers, voire les médecins, la question de la vocation mérite d'être posée …

N'oublions pas enfin que la sécurité informatique historique a progressivement évolué d'abord vers la sécurité des SI avant d'être englobée par la sécurité de l'information. Ces trois formes de sécurité s'intègrent désormais plus largement à l'univers de la **cyber-sécurité** (dématérialisation et globalisation) et aussi au concept de ***sécurité globale*** (Infrastructures vitales).

Ce constat, quelque peu nombriliste, est cependant fondamental. D'une part, il s'appuie sur les enquêtes du Cercle dont l'approche a été de nature quantitative (production d'indicateurs statistiques) et qui on été menées auprès des RSSI eux-mêmes. D'autre part, il montre que l'univers de la SSI dépasse largement le cadre des SI des entreprises et des administrations et des risques qui leur sont liés. Les professionnels évoluent désormais dans ***un monde de plus en plus complexe***, lui-même source de risques, non pas pour les SI proprement dits mais pour les dirigeants et les métiers pour qui ***le SI devient alors un élément critique de la stratégie et des activités***.

Ainsi, les travaux du Cercle Européen se devaient d'être complétés par une analyse plus qualitative de la fonction SSI. Pour ce faire, il fallait s'adresser, non plus aux RSSI eux-mêmes, mais à leurs responsables hiérarchiques et aux dirigeants.

Ce white paper[1], produit par un Groupe de travail du Cercle Européen de la Sécurité, présente la synthèse des entretiens menés auprès d'une vingtaine de dirigeants (voir en dernière page la méthodologie de l'étude).

Deux questions ont été posées aux dirigeants interviewés :

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

Nous reprenons ci-après (en encadré) des *verbatim* des dirigeants interviewés afin d'apporter des éléments concrets à la synthèse proposée.

2. Une fonction clé devant gérer des compromis avec une bonne communication et surtout en apportant des solutions

De l'avis unanime, la fonction SSI apporte incontestablement une vraie valeur ajoutée qui ne peut s'exprimer sans de grandes qualités de communication. Elle se situe aujourd'hui au cœur de problématiques clés de l'évolution des entreprises / organismes : dématérialisation, externalisation, gestion des risques, globalisation, etc. Pour un des dirigeants, ***« c'est une fonction sans fin et une fonction clé pour notre activité. »***

> *« Le RSSI est le poisson pilote de la gestion des risques. »*

> *« La fonction SSI est clairement une fonction majeure qui doit apporter ouverture au monde. »*

> *« La fonction rend accessible la sécurité des SI aux métiers ; ce n'est pas que l'affaire des experts… mais celles des utilisateurs, des métiers. »*

Au-delà de ces positions de principe, les dirigeants consultés n'oublient pas de fixer des obligations opérationnelles et concrètes. Il faut dépasser la posture liée à la fonction. L'action est essentielle.

> *« Il faut avoir un plan d'action qui ne soit pas déconnecté de la réalité. »*

> *« Elle [la fonction] doit trouver un terrain pour concilier les conflits d'intérêt et trouver les compromis. »*

Renforçant ces points, les dirigeants interviewés sont cependant aussi conscients que le RSSI se trouve parfois dans des situations délicates à gérer. Elles peuvent être liées à son positionnement comme à sa mission. Mais elles peuvent aussi concerner des aspects très pratiques sur la qualification d'un risque (qui n'arrive jamais) ou sur un incident majeur (que le RSSI n'avait pas prévu).

Pour l'un des interviewés, ***« C'est la qualité de la personne qui fait toute la différence dans cette fonction. ».*** Renvoyant aux questions de communication, n'est-ce pas ici plus de pédagogie et d'intégrité dont il faudrait faire preuve ?

[1] White paper rédigé par Pierre-Luc REFALO (Associé HAPSIS) et validé par le Groupe de travail.

« La fonction a permis d'identifier des sujets qui étaient sous estimés par rapport à l'analyse de risque. La fonction est génératrice d'inconfort utile. »

3. Une fonction qui va se renforcer, gagner en indépendance et devenir plus pragmatique et ouverte

Bien-sûr, la gestion de l'incertitude est aujourd'hui intégrée à toute pratique de management. Qui sait ce qui va se passer dans 6 ou 12 mois ? Il est cependant utile de questionner l'échantillon de dirigeants sur les évolutions possibles de la fonction à court ou moyen terme.

La tendance la plus forte mise en évidence concerne le renforcement de la fonction qui semble inéluctable et qui doit être associé à une exigence d'indépendance.

L'environnement de plus en plus complexe des entreprises / administrations (technologies, organisations, modèles économiques, évolutions du marché) et leur dépendance de plus en plus forte vis-à-vis des SI (« entreprise numérique ») génèrent des risques que la fonction SSI doit intégrer à sa démarche, plus stratégique.

« La complexification du SI et la dépendance aux SI va nécessiter un renforcement de la sécurité. »

« C'est une fonction qui va prendre de l'importance. »

« La fonction devra s'assurer d'une indépendance de vue. »

Ce nouveau champ de responsabilité apporte(ra) mécaniquement une plus grande transversalité essentielle dans le cadre de la gestion des risques et de la sécurité globale. Cependant, le danger est alors grand de se retrouver déconnecté des réalités opérationnelles liées aux SI des activités et des métiers. Clairement, le RSSI doit largement dépasser le cadre de l'élaboration de la Politique SSI et du contrôle de sa mise en œuvre. Mais comment ?

Sans implication opérationnelle, aucune chance de succès. Place aux exigences « business » dans une approche beaucoup plus pragmatique.

« La fonction doit apporter hauteur et recul mais aussi pragmatisme. »

« La fonction évoluera plus proche des métiers sur des notions de Risk Management d'entreprise et se confondra avec la sécurité métier. »

« 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 ! »

Cette tendance au pragmatisme est un point essentiel de l'évolution de la fonction. 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 se professionnalise et devient facilitateur de projet, voire décisionnaire autour du triptyque opportunités « business » / risques « SI & métiers » / coûts « outils & services ».

4. Synthèse et perspectives

La restitution des entretiens proposée démontre l'importance croissante de la fonction pour les dirigeants rencontrés. Les perspectives mises en évidence concernent potentiellement tous les professionnels de la Sécurité SI.

Les entreprises / administrations, leurs dirigeants, leurs DSI et RSSI disposent ici d'une cible qui n'a rien d'inaccessible. Il est bien connu que les pays anglo-saxons, mais aussi asiatiques, ont renforcé et considérablement professionnalisé les activités de la SSI. Cependant, les MBA et les certifications individuelles contribuent-ils à une plus grande reconnaissance des RSSI / CISO sur le marché ?

Par ailleurs, les points abordés lors des entretiens mettent aussi en évidence des manques majeurs. Certains sont positifs et favorables, d'autres moins.

On pourra s'étonner par exemple :

- De l'absence de considération des questions économiques et budgétaires. Un RSSI sans budget demeure-t-il une perspective crédible ? Ou 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 ?
- 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 sont :

- 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 pour ces dirigeants.
- Aucune exigence de remise en cause de la fonction. Des évolutions ou 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.

Pour conclure, les enseignements de cette étude qualitative auprès d'un échantillon de dirigeants de grandes entreprises françaises sont cohérents avec celles d'une étude du Gartner Group[2] publiée en août 2011. Elle indique que l'évolution et le développement des compétences des professionnels de la sécurité de l'information sont devenus un enjeu majeur. L'étude positionne 6 axes de progression exprimés ainsi :

« *Effective information security practice requires skill sets that adapt to changing business and technology circumstances. Information Security managers must take appropriate action to develop and maintain skills in the following areas:*

- *Integrated risk management*
- *Architecture*
- *Communication*
- *Business*
- *Relationship management*
- *Process management »*

[2] Develop the Key Competencies Required by the New Security Team (Gartner Group - August 2011)

5. METHODOLOGIE DE L'ETUDE

Groupe de travail : Le Groupe de travail du Cercle Européen est constitué de 5 RSSI et un DSI.

- Pascal BASSET (Responsable Sécurité et Conformité – PMU)
- Eric DOYEN (Responsable Sécurité des SI / CISO – GENERALI)
- 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 – SNCF)

Il est piloté par :

- Caroline APFFEL (Associée – Cabinet Heidrick & Struggles)
- Pierre-Luc REFALO (Associé – Cabinet HAPSIS)

Le Groupe de travail s'est réuni lors de 8 réunions et de plusieurs conférences téléphoniques afin de préparer l'étude 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.

Entretiens : une vingtaine d'entretiens ont été menés auprès d'entreprises / organismes variés.

- Services (publics et privés)
- Industries
- Banques
- Assurances

Les fonctions représentées sont :

- Directeur Général délégué
- Directeur de l'Audit
- Directeur des Risques
- Directeur de la Sécurité / Sûreté
- Directeur des Systèmes d'Information

L'étroitesse de l'échantillon est un choix du Groupe de travail permettant de qualifier les interviewés dans le cadre d'une étude qualitative. Les dirigeants ont démontré qu'ils s'intéressaient à la fonction et avaient des avis à exprimer.

Les entretiens ont été menés par Caroline APFFEL (Heidrick & Struggles) et Pierre-Luc REFALO (Hapsis) en l'absence du RSSI de l'entreprise / organisme concerné.