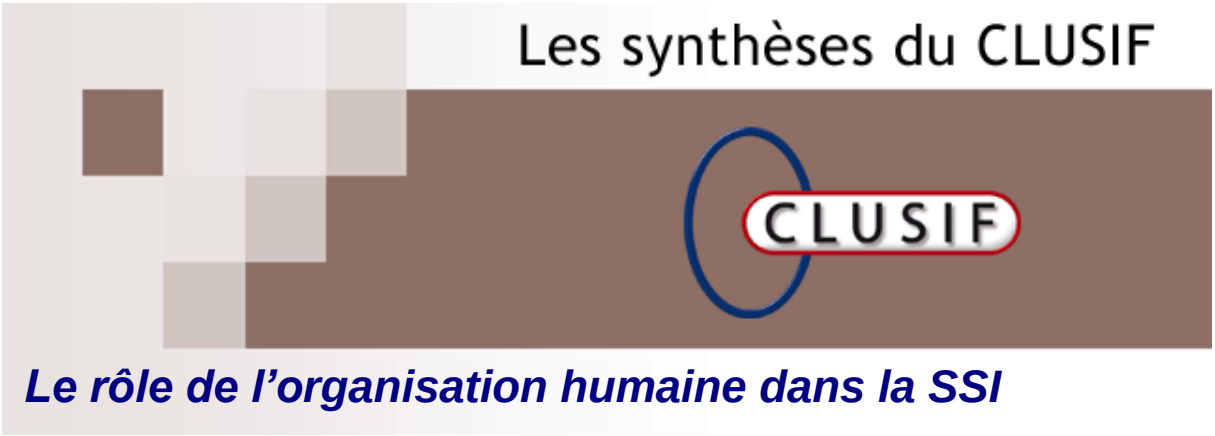


# Le rôle de l'organisation humaine dans la SSI

*Synthèse de la conférence thématique du CLUSIF du 20 juin 2013 à Paris*

Aujourd'hui, la profession de RSSI (responsable de la sécurité des systèmes d'information) est présente dans la majorité des secteurs d'activité. Ce poste existe dans 54% des entreprises interrogées dans le cadre de l'enquête MIPS 2012[1] et dans 32% des collectivités territoriales. Pour autant, la définition et l'exercice de cette fonction diffèrent d'un organisme à l'autre[2]. Sa pertinence dépend de son intégration au sein de l'organisation humaine de chaque entité. Le 20 juin 2013, le CLUSIF a souhaité partager son expérience en la matière, afin de donner **les clefs d'une optimisation de la SSI par l'organisation humaine**. Six orateurs sont intervenus : Thierry CHIOFALO (CLUSIF), Lionel MOURER (Atexio), Eric WIATROWSKI (Orange), Thomas JOLIVET (Harmonie Technologie), Pierre-Luc REFALO (Sogeti) et, en animateur de la table ronde, Eric GROSPEILLER (Ministère de la Santé).

- **Le RSSI doit identifier sa place au cœur de l'« écosystème[3] » de l'organisme**.

Au sein de l'écosystème de l'organisme, la SSI doit permettre d'optimiser les processus de la chaîne de valeur. Ce faisant, elle peut devenir un facteur de maitrise des coûts, voire concourir à la création d'avantages concurrentiels. La diffusion de la SSI se veut générale, chaque acteur de l'écosystème devant regarder dans la même direction. Ainsi, le RSSI doit organiser un véritable « *business model*[4] » et attacher une grande importance à la communication.
Idéalement, le RSSI est rattaché à la direction de l'organisme. Pourtant, ce n'est le cas que dans 32% des entreprises[5]. Les RSSI récemment nommés au sein des PME et PMI sont encore souvent rattachés à la DSI ; un glissement de la DSI vers la Direction Générale (ou autre Direction type « Audit & Contrôle ») pourrait s'opérer (espérons-le…) dans les prochaines années.

- **Le RSSI est un « manager transverse[6] »**.

Le RSSI doit d'abord entretenir des relations avec tous les acteurs de l'organisme. La direction, qui détient le pouvoir décisionnel et les budgets, peut devenir un moteur des projets sécurité. Les directions métier sont des relais précieux vers les utilisateurs, en contact direct avec les enjeux de la SSI. Ensuite, le RSSI est un décideur et un homme de terrain. Auprès de la direction, il établit des stratégies dont l'exécution opérationnelle est un combat de chaque instant. Enfin, le RSSI doit

[1] Enquête relatives aux Menaces Informatiques et Pratiques de Sécurité en France réalisée par le CLUSIF. L'édition 2012 était consacrée aux entreprises de plus de 200 salariés, les collectivités territoriales et les particuliers internautes. Pour plus d'informations : http://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF-Rapport-2012.pdf
[2] Lionel MOURER (Atexio)
[3] Thierry CHIOFALO (CLUSIF)
[4] Thierry CHIOFALO (CLUSIF)
[5] Lionel MOURER (Atexio), enquête MIPS 2012
[6] Thomas JOLIVET (Harmonie Technologie)

intervenir sur tous les fronts pour remplir ses missions. Il doit prendre en compte la sécurité dès les phases projet et organiser une gouvernance de la SSI en amont. Il doit suivre les indicateurs, réaliser une veille et analyser les risques au quotidien. Ponctuellement, il gère les incidents de sécurité.

- **Le RSSI mobilise les « contributeurs[7] » de la sécurité**

Pour une gestion efficiente de la SSI, chaque acteur de l'organisme doit être mis à contribution. Si l'approche varie selon l'organisation de chaque société, certains traits communs se dégagent. La gouvernance de la SSI ne doit pas dépendre d'un seul homme, le RSSI, mais s'appuyer sur une entité stable. Selon la taille de l'organisme, la gouvernance peut reposer sur la direction générale, le Comité de direction, un Comité de direction dédié à la sécurité, voire des comités de sécurité locaux. Une structure pyramidale[8] peut être envisagée. Une telle organisation dépend de l'implication du décideur. Afin de le mobiliser, les contraintes réglementaires et les rapports d'audits internes peuvent être mis en avant et la SSI présentée comme un atout concurrentiel. L'implication de la direction est cruciale pour la certification ISO 27001. Quant aux directions métier, la sécurité leur assure la continuité d'activité opérationnelle. Enfin, les utilisateurs peuvent être mobilisés en intégrant la SSI du côté des ressources humaines (par les fiches de poste, les contrats de travail, le règlement intérieur, la charte informatique ou encore les objectifs personnels). L'implication de ces contributeurs devient un levier pour la SSI.

- **Le RSSI mène une action de sensibilisation permanente**

Si l'humain est souvent présenté comme le maillon faible de la sécurité, une action de sensibilisation bien menée peut en faire un maillon actif permettant la remontée d'alertes SSI[9]. Plusieurs méthodes existent : l'affichage ou la publication sur l'intranet, les campagnes de *mailing*, les clips vidéo, les pièces de théâtre, les conférences, mais aussi de véritables mises en pratique (organisation de simulations d'attaques par hameçonnage ou ingénierie sociale). Ces diverses méthodes se veulent davantage cumulatives qu'alternatives. En effet, pour être efficace, la sensibilisation doit être récurrente. Une évaluation des opérations de sensibilisation est également nécessaire. Là encore, aux simples questionnaires doit s'ajouter une mise en pratique. Pourtant, encore peu d'organismes l'envisagent. Organiser des simulations d'attaques par *phishing* ou *social engineering* se révèle complexe de par des contraintes juridiques et éthiques associées[10].

- **Le RSSI s'adapte aux mutations de la SSI**

La SSI évolue avec les innovations technologiques. Aujourd'hui, le RSSI est notamment confronté aux problématiques du BYOD (« *bring your own device* »), du « *cloud computing* » et de la protection de la vie privée. De nouveaux acteurs influents entrent dans l'écosystème : les « GAFA[11] » et « telcos[12] ». La notion même de sécurité semble muter. La SSI devient un concept global. Son champ d'action s'est étendu. Ainsi, aux attaques informatiques extérieures, s'ajoutent par exemple les fraudes internes, l'espionnage industriel ou la simple perte de matériel. Pour certains, les critères de sécurité deviennent des besoins d'accessibilité, d'identité, de confidentialité et de traçabilité[13]. Enfin, le développement de l'infogérance tend à modifier les missions du RSSI. Progressivement la gestion immédiate de l'incident prend le pas sur l'anticipation du risque, de nombreuses mesures préventives étant intégrées aux produits. Désormais, la SSI comprend donc trois métiers à part entière : la prévention du risque, la gestion des incidents et la protection des données personnelles.

[7] Thomas JOLIVET (Harmonie Technologie)
[8] Eric WIATROWSKI (Orange)
[9] Eric WIATROWSKI (Orange)
[10] Pierre-Luc REFALO (Sogeti)
[11] GAFA : désigne Google, Apple, Facebook et Amazon.
[12] Telcos : désigne les grandes entreprises du secteur des télécommunications.
[13] Pierre-Luc REFALO (Sogeti)

*Retrouvez les vidéos de cette conférence et les supports des interventions sur le web CLUSIF*
*http://www.clusif.fr/fr/infos/event/#conf130620.*