Sécurité de l'information : positionnement et profil du RSSI

Daniel Lang, Jean-Luc Pillet

Sécurité de l'information : positionnement et profil du RSSI[1]

Daniel LANG
Enseignant chercheur en Systèmes d'Information
Institut TELECOM
TELECOM Ecole de Management
9 rue Charles Fourier
91011 EVRY Cedex
Tel : 01 60 76 41 67
Fax : 01 60 76 44 93
daniel.lang@it-sudparis.eu

Jean-Luc PILLET
Adjoint Scientifique
UNI Mail - HEC Genève
40 Bd du Pont-d'Arve,
1211 Genève
Tél. : +41 22 379 81 35
HEG Fribourg
4 chemin du Musée – 1700 Fribourg
Tel +41(0)76 501 80 70
jeanluc.pillet@free.fr

Résumé :

L'évolution des technologies informatiques impacte les pratiques sécuritaires qui doivent faire face à des nouvelles menaces. Le rôle et la fonction du RSSI d'aujourd'hui s'adaptent pour répondre aux besoins de l'entreprise. L'objet de notre recherche est d'analyser les tâches d'un RSSI au quotidien et de déterminer ses nouvelles compétences organisationnelles et techniques. Ce document relate toutes les réponses apportées par une enquête effectuée par le CLUSIS[2] et l'Université de Genève en octobre 2009.

Mots clefs : RSSI, pratique sécuritaire, organisation, positionnement, tâches

Abstract :

To protect information Systems from increasing levels of cyber-threats, enterprises are compelled to institute information security policies. This paper investigates the evolution of information security and competencies of its responsible. In this study, we attempt to evaluate the information security maturity level and provide thoughtful analysis of the information security landscape, particularly about his responsible, the CISSO[3]. A survey questionnaire is utilized to gauge the security landscape and to further understand qualities and competencies of his leader.

Keywords : security policies, competencies, CISSO, evolution

[1] Responsable de la Sécurité des Systèmes d'Information
[2] Association Suisse de la sécurité des systemes d'information
[3] Chief Information System Security Officer

1. Introduction

Aujourd'hui, l'entreprise est soumise à une pression considérable du marché. Elle doit comprendre et s'approprier les nouvelles tendances technologiques. Elle doit également faire évoluer sa gouvernance de manière à pouvoir répondre aux enjeux de la performance et aux principes d'une qualité sans défaut. En conséquence, les collaborateurs d'une entreprise sont directement impactés par ces nouvelles pratiques managériales. Dans ce contexte, nous nous intéressons plus particulièrement à l'évolution d'un « métier » RSSI (Responsable de la Sécurité des Systèmes d'Information) en déterminant son champ d'action actuel. Nous cherchons également à déterminer les formations possibles qui permettent de répondre à ce besoin de nouvelles compétences. Globalement pour notre étude, nous voulons répondre à sept questions :

1. Le poste RSSI : une fonction ou un métier ?
2. Quel est le rôle du RSSI ?
3. Peut-on répertorier des tâches communes relatives à un ensemble de collaborateurs d'entreprises RSSI et distinguer également les fonctions plus techniques, organisationnelles, managériales ou basées sur les métiers ?
4. Est-il possible d'évaluer l'autonomie d'un RSSI ?
5. Peut-on connaître le niveau de sécurité de l'entreprise en relation avec les tâches quotidiennes d'un RSSI ?
6. Quelles sont les qualités d'un RSSI idéal ?
7. Quelles sont les formations «Sécurité SI» adaptées au RSSI ?

La réponse à ces questions constitue la trame de notre recherche.

2. Les enjeux de La sécurité des systèmes d'information

L'informatique est omniprésente dans notre société, au sein de laquelle Internet et les autres réseaux sont devenus incontournables. Tous les objets de notre quotidien sont ou seront bientôt équipés de puces. Ces technologies peuvent communiquer entre elles en s'appuyant sur une même transformation fondamentale : la numérisation. De nombreux domaines sont concernés : les communications (téléphones portables), les transports (GPS), le commerce, la médecine (imagerie, assistance robotisée) et environnement (gestion des moteurs de voitures) (Kaczmarek, Marion, 2010).

Cependant, dès lors que l'information a pu être stockée ou transmise, sa protection a été nécessaire et ce depuis des siècles. Pour mémoire, le moyen cryptographique de Jules César pour transformer un texte lisible en document chiffré en est une parfaite illustration[4]. Or, la criminalité a toujours essayé de contourner ces moyens de protection et s'est toujours adaptée aux différents espaces (terrestre, maritime, aérien). Aujourd'hui, c'est l'espace informationnel générée par les T.I.C. qui entraine une nouvelle forme de délinquance : la cybercriminalité. Les conséquences peuvent être particulièrement sérieuses pour les

[4] L'algorithme utilisé était une clé de 3 qui transforme une lette **a** en **d** en tenant compte de l'alphabet. Ainsi, un texte en clair : attaquer devient dwwdtxhu

entreprises, les états et les citoyens. Une enquête annuelle effectuée par le CSI/FBI[5] montre les diverses menaces dont doivent se préoccuper les collaborateurs, entreprises et administrations.

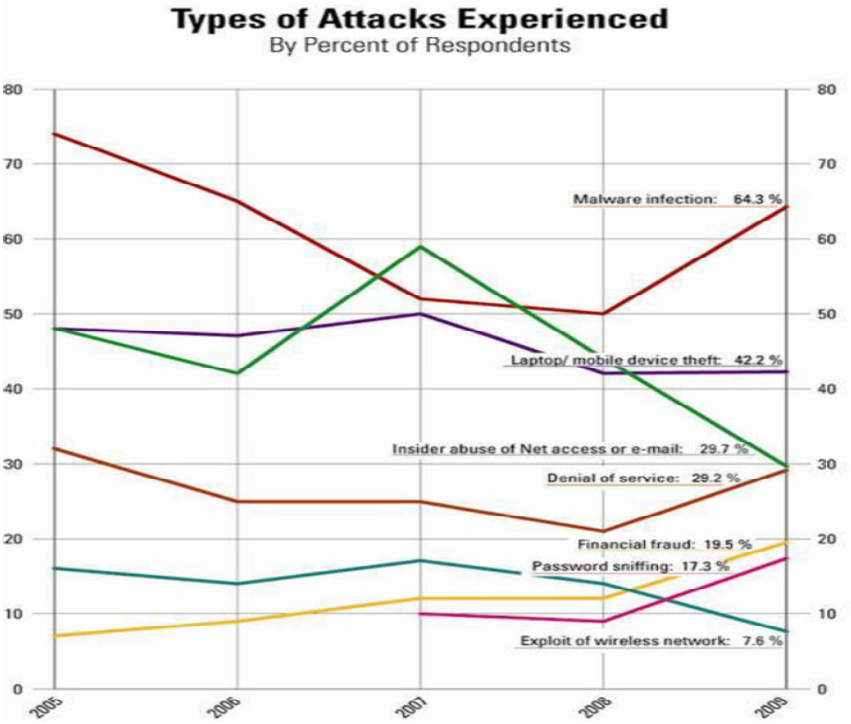


Figure 1 : l'enquête annuelle du CSI / FBI concernant les types d'attaques informatiques

En parallèle, le profil des attaquants a évolué du bandit de grand chemin, en passant par le passionné de technologies voulant démontrer ses exploits en contournant un processus d'authentification, jusqu'au hacker professionnel visant le vol d'informations confidentielles pour obtenir des gains financiers. Aujourd'hui, le concept de cyber-guerre n'est plus un sujet de prospective mais bien une réalité (Larcher, 2009). Ce sont des groupes très organisés qui intentent des attaques au niveau d'un état.

Ces infractions ne se limitent pas aux intrusions et vol de données (virus, escroquerie en ligne) mais concernent également leur contenu (insulte, xénophobie, pédophilie) si bien que l'on doit considérer également le respect du droit d'auteur et de la propriété intellectuelle (ouvrages, musique, vidéo, logiciels). De plus, les risques ne se limitent pas à des intentions de fraude mais également par des accidents divers : mauvaises utilisations, évènements naturels divers (incendie, tremblement de terre). Les dysfonctionnements peuvent résulter d'une combinaison des trois composantes principales du système d'information (Willcocks &al, 1995), (Champenois, 1997), à savoir :

- les infrastructures et compétences techniques (serveurs, réseaux, matériels…),
- les aspects logiciels (« applicatif »),
- les appropriations et usages des utilisateurs.

C'est donc l'ensemble des menaces potentielles qui doit être considéré car chaque type de menace peut affecter le système d'information de l'entreprise. Par exemple, une inondation dans une salle machines va rendre inutilisable le serveur qui héberge une application

[5] 14th Annual CSI Computer Crime and Security Survey, december 2009

comptable. Face à la dépendance croissante des organisations vis-à-vis de leurs systèmes d'information, les entreprises sont contraintes de se soucier des risques induits (Dlamini&al, 2008), (Kraemer&al, 2009) car un dysfonctionnement partiel ou total du Système d'Information peut ébranler une organisation. Certaines données, qu'elles concernent ses employés, ses fournisseurs ou ses clients, sont confidentielles, et toute perte ou altération de celles-ci peut entrainer des préjudices très sérieux. En outre, dans un contexte de forte compétitivité, l'information représente une valeur qui peut donner lieu à des convoitises et induire des vols.

En conséquence, les entreprises mettent en œuvre des stratégies de sécurité adaptées pour protéger leur capital informationnel. En effet, ce dernier est devenu une matière première sans laquelle les activités des entreprises ne peuvent être exercées. Initialement, les processus de sécurisation étaient souvent perçus comme des solutions relevant d'outils techniques, donc délégués à des entités technologiques de l'entreprise (Schneier, 2000). Cependant cette vision très restrictive est en train d'évoluer, d'autant que les risques impliqués ne concernent pas uniquement les aspects matériels, mais aussi le droit et la légalité (Tudor, 2000), la perte de confiance ainsi que les répercussions financières (Mc Adams, 2004). Il est dorénavant reconnu que l'implication des Directions est fondamentale dans la mise en place d'une culture et d'une politique de sécurité (Solms & Solms, 2004), (Anderson, 2008). Contrairement aux idées préconçues, la sécurisation ne consiste pas uniquement en la mise en œuvre d'une solution technique. Il s'agit essentiellement de développer une politique de sécurité en considérant les trois composantes suivantes : les humains, les processus, la technologie.

Certains experts affirment que le niveau de sécurité recherché doit être proportionnel à la valeur de l'information, et aux pertes financières qu'un dysfonctionnement du capital informationnel entraînerait (Peltier, 2002). Il faut apporter une nuance à cette affirmation en tenant compte du secteur d'activité d'une entreprise. Ainsi, la charte d'un hôpital précise que son objectif premier est de soigner en priorité ses malades et de gérer ensuite ses flux financiers. Cependant, dans tous les cas, la sécurité de l'information est un problème stratégique qui doit être géré par des décideurs qui doivent définir sa mission, ses buts et ses objectifs.

Solms & Solms (2004) mettent en exergue que les organisations doivent considérer la protection de l'information comme un problème organisationnel et non pas uniquement technique, dont les composantes sont les éléments suivants : gouvernance d'entreprises, politique organisationnelle, éthique, juridique, humain, technologie, audit, maturité, conscience. En effet, un principe fondamental dans la mise en œuvre d'une politique de sécurité concerne la perception individuelle des acteurs impliqués par ce sujet : les risques perçus par ces acteurs (Ezingeard, 2003) et la façon dont ils considèrent ce qui constitue une barrière de sécurité (Musekura, 2003). Une façon d'améliorer cette perception consiste à investir dans la formation et à sensibiliser l'ensemble des employés en vue de développer une culture de la sécurité dans l'organisation. Enfin, des méthodes (EBIOS, CRAMM, OCTAVE, MEHARI) doivent être utilisées en vue de mettre en œuvre des règles de conformité édictées par les divers standards (ISO 2700x, Bâle II, Sox).

Dans ce contexte, des ressources humaines compétentes sont essentielles pour cette mise en œuvre. C'est dans ce sens que l'on a assisté à l'apparition de nouveaux métiers comme le RSSI il y a environ 10 ans. On note une classification des fonctions dans un organigramme en distinguant le niveau le plus stratégique de la sécurité d'entreprise représenté par le CSO (Chief Security Officer) de notre RSSI affecté à des tâches plus opérationnelles (responsable de la sécurité de l'informatique et des réseaux). Le schéma ci-dessous permet d'en distinguer les divers composants (De Blasis, 2008) :

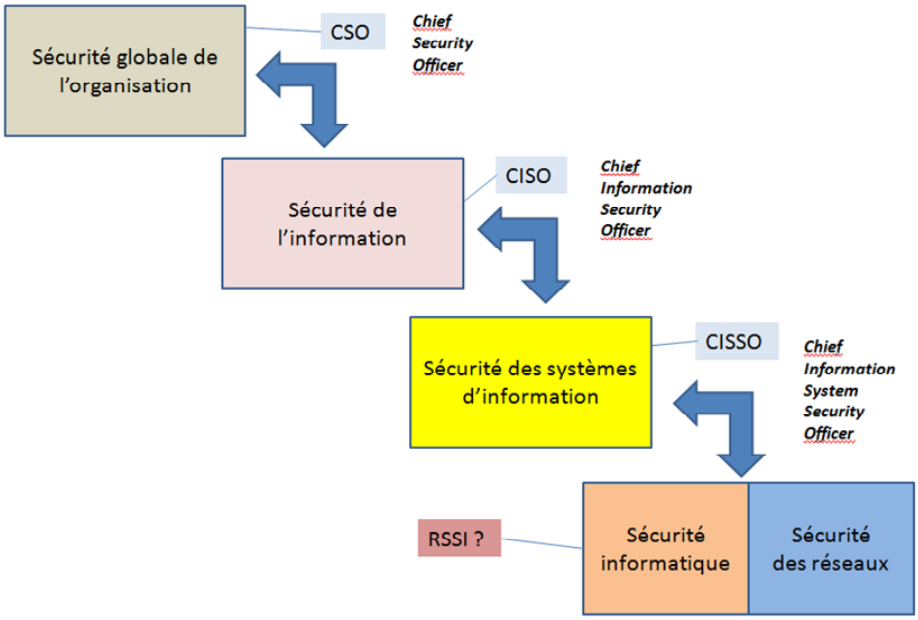


Figure 2 : la position hiérarchique du RSSI dans l'organigramme de l'entreprise

Ainsi, l'objet de notre recherche est de comprendre le positionnement actuel d'un RSSI. Quel est son rôle exact ? Doit-il être considéré comme un pur technicien ou doit-il avoir également une fibre managériale ? Est-il autonome en termes budgétaires ? Quelles sont ses fonctions précises ? Doit-il être un communicateur ? Notre enquête a pour but de répondre à toutes ces questions.

3. Les données de l'enquête

Le questionnaire a été envoyé en octobre 2009 auprès d'environ 500 entreprises localisées en Suisse Romande. Nous avons reçu 41 documents en retour, soit environ 8% de taux de réponses. L'ensemble des réponses permet un découpage en tenant compte des secteurs d'activité suivants :

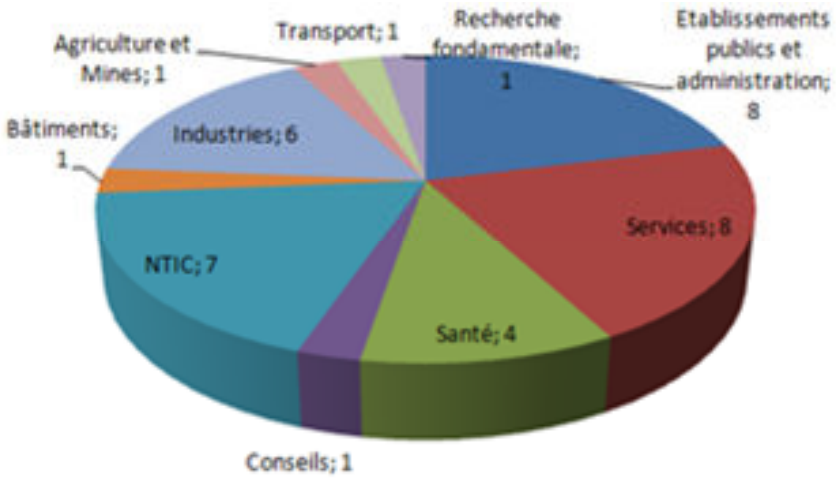


Figure 3 : les divers secteurs d'activité

On peut remarquer que l'ensemble des secteurs d'activité est représenté à l'exception du secteur agro-alimentaire. On peut également constater qu'un poste RSSI reste en grande majorité l'adage des grandes entreprises. En effet, le classement des entreprises par nombre d'employés montre une proportion très importante de sociétés de plus de 1'000 employés (environ 22 sur un total de 34 réponses). Cette absence de PME dans notre échantillon confirme le fait que le statut de RSSI n'est pas formalisé dans une petite structure multi tâches.

Nombre d'employés	[0-100[	[100-500[	[500-1'000[	[1'000-5'000[	[5'000-10'000[	[10'000-25'000[	[25'000 et plus
Nombre d'entreprises	5	4	3	9	5	5	3

Tableau 1 : la taille des entreprises et l'existence d'un poste RSSI

4. Le concept de métier ou de profession

4.1 L'adaptation du modèle théorique de (Beynon-Davies, 2002) pour le poste RSSI

Le terme de profession ou métier, utilisé dans un contexte général et quelquefois galvaudé, s'approprie une certaine valeur lorsqu'il est porteur d'un statut, en d'autres termes, lorsqu'il est symboliquement labellisé (Brint, 1993). Adapté au monde de l'informatique, nous tenons compte de modèles pour formaliser notre approche. Le tableau ci-dessous nous en montre les principales composantes :

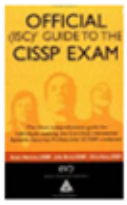
Modèles	***traditionnel***	***fonctionnaliste***	***statutaire***	***interprété***
Concept général	Référence à une liste d'attributs commun	Attaché à un groupe qui contribue à l'évolution du processus professionnel	Protection par une réglementation juridique	Procédé d'interprétation pour faire émerger une image professionnelle en regard avec un type d'activité
Adapté au RSSI	Classification du Cigref CIGREF	Lien entre l'évolution des risques sécuritaires et les avantages que peuvent en tirer les agents économiques	Nécessité de négocier et de statuer pour obtenir une légitimation juridique 	Positionnement du métier «RSSI» *C'est quoi, un RSSI ?*

Tableau 2 : les diverses composantes d'un métier adaptées au RSSI

Le modèle traditionnel : on y trouve une description des tâches qui doivent être effectuées par le collaborateur en poste. Le cahier des charges formalise cette description[6].

Le modèle fonctionnaliste : l'actualité brulante liée la sécurité informatique et les risques associés contribue à influencer notre RSSI pour qu'il prenne les mesures appropriées. C'est donc la pression du marché qui s'impose à notre collaborateur. De plus, il doit tenir compte des nouveaux standards (par exemple Bâle II ou ISO 2700x) et s'y conformer.

Le modèle statutaire : certaines professions bénéficient d'organes professionnels, administratifs et juridictionnels qui défendent et régulent un métier. On pourrait citer le conseil national de l'ordre des médecins en France[7] ou le conseil de l'ordre des avocats dans le Canton de Genève[8]. Au contraire, le métier RSSI n'a jamais été labellisé. Cette profession est un corps parcellisé entre des activités liées à l'analyse de risque, la politique de sécurité, les architectures techniques ou les audits et le contrôle. Cependant, on peut noter la volonté de certaines formations spécialisées d'inclure un code éthique au métier du responsable sécurité (ISC)[9].

Le modèle interprété : c'est l'image d'une profession qui est colportée par le grand public**.** Malheureusement, le nombre des spécialisations avec des nouveaux contenus (Lemaire et Valenduc, 2005) et de nouvelles spécialisations répertoriées par le Cigref en 2009[10] contribuent à donner une perception très floue de l'informaticien pour des néophytes. On est loin aujourd'hui du spécialiste généraliste des années 70, bénéficiant de l'aura d'une nouvelle profession, qui était écouté de manière respectueuse par des utilisateurs. Aujourd'hui, l'informatique s'est banalisée. Elle est utilisée de manière instinctive par une tranche d'âge beaucoup plus jeune qui baigne dans cet univers. De ce fait, l'attrait de cette

[6] http://securit.free.fr/ressources/organisation.htm
[7] http://fr.wikipedia.org/wiki/Conseil_national_de_l'ordre_des_médecins
[8] http://www.odageneve.ch/index.php?option=com_content&task=view&id=23&Itemid=113
[9] http://www.isc2.org/ethics/default.aspx
[10] Cigref, (2009) «*Nomenclature 2009 : les emplois métiers du SI dans les grandes entreprises* »

profession ne fait plus rêver puisqu'elle fait partie du quotidien. Il a été constaté lors d'une enquête en 2008[11] une baisse de fréquentation importante (environ 50%) des étudiants dans les filières informatique des hautes écoles en Suisse (EPF, HES et Universités) entre 2001 et 2006. Or, la fonction RSSI nécessite une bonne compréhension des aspects techniques (systèmes et réseau).

4.2 Être RSSI : est-ce une fonction ou une profession ?

Certains auteurs optent pour la terminologie «fonction RSSI». D'autres penchent plus spécifiquement pour une profession à part entière. Il est vrai que selon le type et la taille des entreprises, la sécurité informatique peut être affectée à un collaborateur qui doit également effectuer d'autres tâches bien différentes. Dans ce cas, on pourrait estimer que la sécurité est une fonction. Sinon, le terme profession devrait être utilisé pour notre collaborateur RSSI. Les réponses 18 et 19 de notre enquête sur l'ensemble de nos répondants permettent d'apporter un éclairage sur ce sujet :

Temps complet 57%	**Temps partiel 43%**

Tableau 3 : un poste RSSI à temps complet ou partiel

Ainsi, un poste RSSI correspond à une profession pour environ 57% des RSSI.

4.3 Les compétences TIC[12] et non TIC du RSSI

Le RSSI d'aujourd'hui doit évoluer en tenant compte de ses compétences techniques, mais également en regard d'une logique professionnelle. De notre point de vue, il s'agit donc de distinguer les compétences « cœur de métier » des autres logiques liées à l'existant de l'entreprise et à l'organisation du travail. En effet, peut-on réellement comparer une analyse de risques effectuée dans un milieu hospitalier en regard avec les risques perçus dans le secteur bancaire ? Les diverses situations par rapport à une compétence TIC ou non TIC sont reprises par les chercheurs du LENTIC, laboratoire de l'Université de Liège. Le schéma ci-dessous permet d'illustrer les diverses composantes :

[11] http://www.lesquotidiennes.com/travail/lindustrie-suisse-en-pénurie-dinformaticiens-se-tourne-vers-les-femmes

[12] Technologie de l'Information et de la Communication

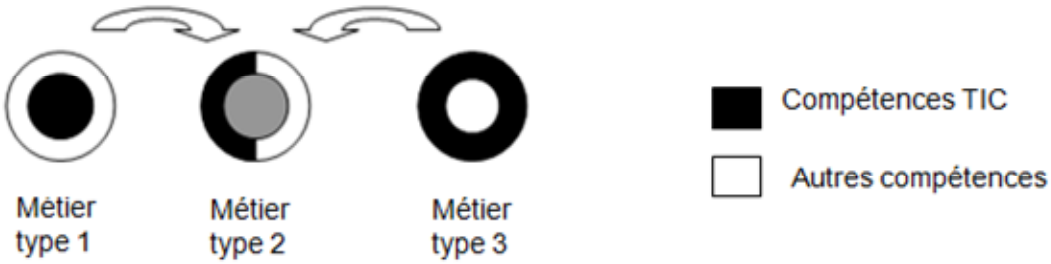


Figure 4 : les types de métiers associés aux compétences TIC et non TIC

Le métier de type 1 met en évidence un cœur de compétence bâti sur des TIC (couleur noire), complété en périphérie par des compétences non TIC. Il s'agit essentiellement des logiques professionnelles traditionnelles de l'informatique. Dans le cadre de la sécurité des SI, les compétences techniques réseaux, applicatives et matérielles sont fondamentales.

Le métier de type 2, objet de notre recherche, caractérise les nouveaux métiers liés aux développements des TIC. Pour nous, les aspects métiers d'une organisation impacte directement sur la politique de sécurité, y compris dans les mesures de protection techniques à élaborer pour réduire les risques au sein d'une entreprise.

Le métier de type 3 : cette composante rassemble les métiers dont la compétence TIC est secondaire. On pourrait s'intéresser aux processus métiers qui sont gérés quotidiennement en entreprise et avec lesquelles le RSSI doit interférer périodiquement. Les résultats de l'enquête (question 21) montrent tous les services et/ou départements cités en relation avec la fonction RSSI :

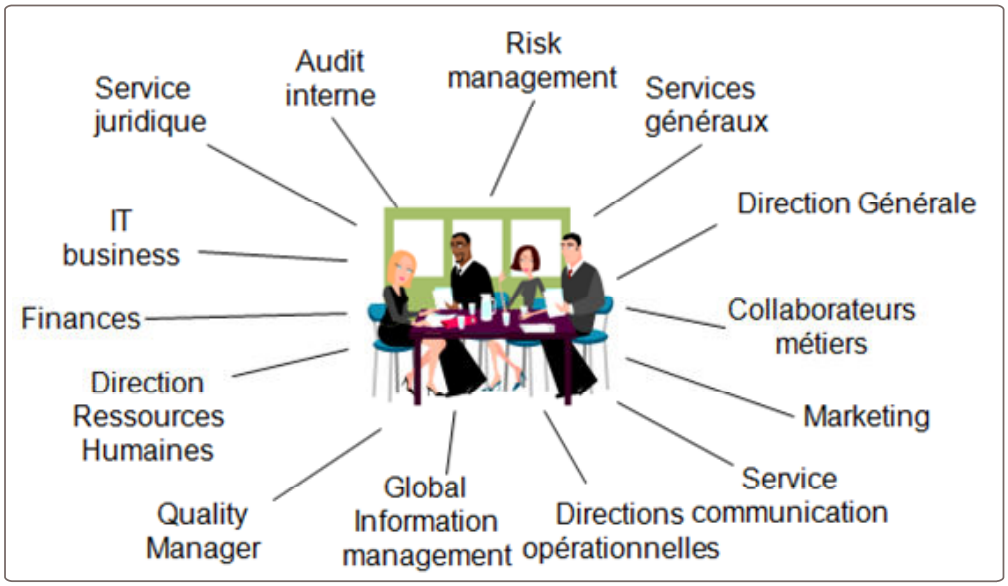


Figure 5 : les divers départements ou services en relation avec le RSSI

En conclusion, le poste RSSI correspond bien à un métier de type 2.

5. La mission et les tâches d'un RSSI

5.1 L'importance d'un sigle

Lorsque l'on s'intéresse à l'évolution des organigrammes d'entreprise, il a été constaté un changement d'une appellation « Département Informatique » ou EDP[13] pour évoluer vers un intitulé « Organisation Informatique » ou « Systèmes d'Information ». Dans le domaine plus spécifique de la sécurité, nous nous sommes focalisés sur le sigle RSSI (Responsable Sécurité des Systèmes d'Information). Cependant, on peut noter l'existence d'autres dénominations concernant le même type de poste. Ainsi, les répondants aux questions 15 et 16 proposent « Global Information Security Officer » (1), « Responsable Sécurité et Disaster Recovery » (2) ou encore « Information Security & Risk Management Lead » (3). Ici, on insiste plus sur les aspects globaux (1), la continuité des affaires (2) ou le management des risques (3) du poste.

5.2 La mission du RSSI

La mission et les tâches inhérentes au RSSI vont permettre de compléter le modèle théorique de la typologie des métiers exposé au paragraphe précédent. On peut citer les définitions suivantes concernant la mission d'un RSSI :
Selon le (Cigref, 2009), le RSSI doit :

- définir la politique de sécurité du système d'information et veiller à son application,
- assurer un rôle de conseil, d'assistance, d'information, de formation et d'alerte. Il peut intervenir directement sur tout ou partie des systèmes informatiques et télécoms de ***son entité***.

Une autre définition (Foray, 2007) apporte une perception différente à cette première approche :

- définir, mettre en œuvre, et contrôler la politique technique de sécurité basée sur la politique de sécurité interne,
- le domaine concerné : ***toutes les entités de la DSI*** ainsi que ***certaines unités opérationnelles*** de la société avec un focus particulier sur les infrastructures techniques.

Ainsi, on peut noter une différence importante lorsque l'on examine le périmètre d'intervention du RSSI. La première définition estime que le champ d'investigation se limite aux systèmes informatiques et aux télécoms de son entité. La deuxième définition élargit le domaine d'activité du RSSI puisqu'il peut intervenir sur les entités de la DSI mais également sur certaines unités opérationnelles. Cette différence de conception montre bien l'évolution d'un métier. Les deux approches s'opposent : l'une reste traditionnelle, l'autre tient compte du business appliqué à la sécurité des SI.

[13] Electronic Data Processing

5.3 Les tâches affectées au RSSI

Dans le cadre de sa mission, il faut également déterminer les tâches de nature opérationnelle ou managériale. Les résultats de l'enquête montrent les tâches communes suivantes en tenant compte du nombre de répondants :

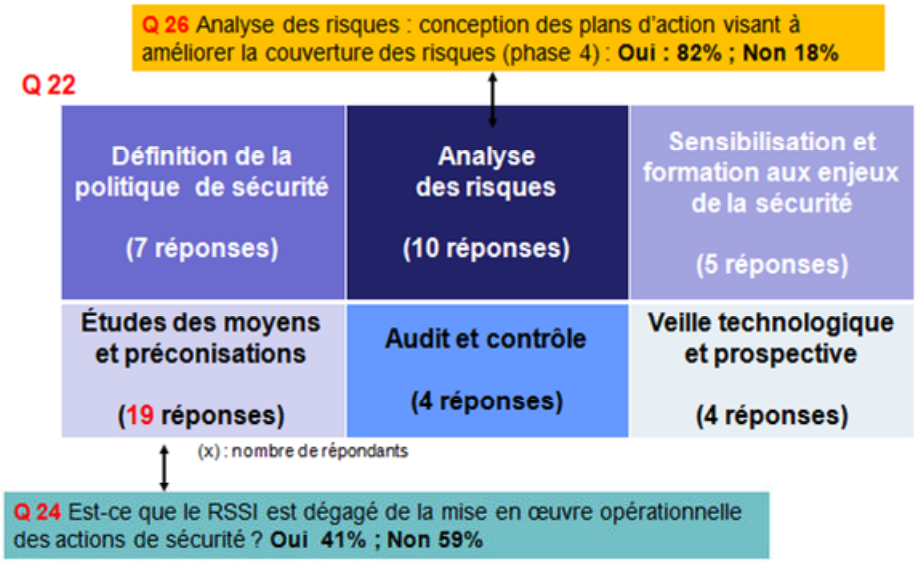


Tableau 4 : le rôle et les responsabilités d'un RSSI

Ainsi, les réponses apportées à la question 22 illustrent bien l'affectation de certaines tâches de nature opérationnelle ou d'exploitation (audit et contrôle, sensibilisation et formation des utilisateurs, mise en œuvre des actions de sécurité). D'autres tâches concernent davantage la partie étude et analyse (analyse des risques, veille technologique, études des moyens et préconisations). Enfin, notre RSSI prédispose d'une responsabilité d'ordre managériale dans l'élaboration d'une politique de sécurité. Il est intéressant de constater également que 82% des répondants sont en phase 4 d'une analyse de risque (question 26), soit la phase ultime de cette analyse qui se traduit par l'élaboration d'un plan d'action pour répondre à des menaces potentielles. Cependant, il est fort probable que cette situation découle du fait que beaucoup de nos répondants travaillent dans de grands groupes, avec des budgets qui peuvent être consacrés à ce type d'étude. En conséquence, la nature du travail affectée au RSSI est forcement dépendante d'une spécificité liée à la taille de l'entreprise ou à son secteur d'activité (questions 5 et 6). La question 28 précise justement cette différentiation des tâches par ordre d'importance, même si la mission générale d'un RSSI est bien perçue et appliquée par l'ensemble des entreprises. Le tableau ci-dessous en donne une illustration :

Q 28	La plus importante	Moyennement importante	Importante
R1	Gestion des risques (30%)	Sensibilisation (15%)	Audit et contrôle (15%)
R2	Opérationnel (20-40%)	Analyse (10-20%)	Conseils techniques (10-20%)
R3	Politique de sécurité et suivi (50%)	Reporting (20%)	Formation (10%)
R4	Maîtrise d'ouvrage sécurité logique (40%)	Continuité des activités (40%)	Maîtrise d'ouvrage sécurité physique(10%)
R5	Gouvernance (60%)	Contrôles – formation (20%)	Veille (10%)

Tableau 5 : la différentiation des tâches au quotidien

Ainsi, le répondant R5 consacre 60% de son temps pour la gouvernance. Inversement, le répondant R2 doit gérer l'opérationnel entre 20-40% de son temps. Cet échantillonnage parcellaire de ces cinq RSSI montre bien la variété des tâches à effectuer selon la typologie de l'entreprise.

6. La maturité des entreprises en matière de sécurité

Il est constaté une évolution du niveau de sécurité des entreprises selon un classement en trois temps : le temps de la maturité technologique (temps 1), celle de l'organisation (temps 2) et enfin celle du pilotage et de la mise en conformité (temps 3). Le travail du RSSI va bien sûr dépendre de cette évolution du niveau de sécurité en entreprise. Les réponses apportées sur le schéma suivant (question 38) permettent d'établir un état de situation en matière de sécurité :

Q 38	La sécurité physique et logique (infrastructures techniques) (1)	La réponse aux audits en termes de processus et d'organisation (2)	La mise en conformité aux diverses normes (3)
	11 réponses	10 réponses	16 réponses

Figure 6 : le niveau de maturité des entreprises

Ainsi, plus de la moitié des entreprises (16) consacrent des projets dans le pilotage de la sécurité et de la conformité. Ce taux de réponses très important en phase 3 est corrélé à de grandes entités.

7. Les compétences et les qualités idéales pour un RSSI

Au-delà des tâches exécutées au quotidien, il est intéressant de pouvoir déterminer les qualités requises pour ce poste. Les réponses apportées à la question 30 permettent d'apporter des éléments de solution. Les nombreux commentaires de nos répondants ont été systématiquement répertoriés sur une grille d'analyse d'évaluation des compétences. Le référentiel de compétences «CompéQ» (Menthonnex, 2006) suivant permet d'apporter la synthèse suivante :

Q 30		Poids
Compétences Personnelles **Poids total : 26**	Compétences personnelles de base *(esprit d'analyse et de synthèse)* Engagement ciblé *(respect du cahier des charge, autonomie)* Comportement responsable *(persévérance, être intègre)* Transformation et innovation *(créativité et flexibilité)* Maintenir son employabilité *(esprit d'ouverture et évolution)*	9 2 10 2 3
Compétences sociales **Poids total : 34**	Aptitudes à communiquer *(en équipe, par oral et écrit)* Orientation client *(avoir le sens du service)* Aptitudes à coopérer et à travailler en équipe *(négocier et défendre ses idées)*	19 2 13
Compétences en organisation **Poids total : 11**	Gestion et promotion du personnel *(gérer une équipe, être diplomate)* Gestion des affaires *(élaborer une vision d'avenir)*	3 8
Compétences professionnelles **Poids total : 11**	Compétences professionnelles générales *(maîtrise des principaux outils informatiques nécessaire à la fonction)* & compétences spécifiques au métier	10 1

Tableau 6 : les qualités requises pour un poste RSSI adapté par le CompéQ

Le poids donné à chaque référence de qualité correspond aux nombre de répondants qui s'identifient justement à cette référence. On remarque que les compétences sociales sont mises en pole position devant les compétences personnelles. Ainsi, l'aptitude à communiquer (19 réponses) et à négocier (13 réponses) montre bien les liens avec les corps métiers. Il doit défendre ses idées devant différents services qui n'ont pas forcement une préoccupation sécuritaire comme objectif premier.

8. L'autonomie d'un RSSI

La position hiérarchique du RSSI et son autonomie budgétaire sont des indicateurs qui peuvent montrer une certaine indépendance vis-à-vis du DSI. Des experts dans le domaine de la sécurité précisent leur point de vue sur ce sujet[14] :

« *Le RSSI intervient de manière transversale sur l'ensemble du système d'information de l'entreprise, d'un point de vue organisationnel et technique, en synergie avec les différentes*

[14] http://securit.free.fr/ressources/organisation.htm

directions. Il est généralement convenu que le RSSI, pour des questions d'indépendance et d'efficacité, doit être rattaché à un niveau hiérarchique élevé (ex. rattachement au niveau Direction Générale) et disposer d'un budget spécifique».

Les résultats de notre enquête ne semblent pas confirmer cette tendance puisque 54% des répondants n'ont pas de budget spécifique à la sécurité informatique (question 20). Le tableau ci-dessous montre la position hiérarchique des RSSI :

Q 20 La position du RSSI est dépendante de :

Direction de l'entreprise	Direction des systèmes d'information	Comité de groupe de sécurité	CSO (Chief Security Officer)	Autres
11	16	2	3	5 •Département organisation •Responsable infrastructure •Control & Compliance Manager •Unité Systèmes de Management, dans une direction Droit & Risques

Tableau 7 : la position hiérarchique du RSSI

On peut constater que 16 RSSI sur un total de 37 répondants dépendent d'une DSI, soit 43% des réponses. En conclusion. La situation actuelle ne permet pas de constater une autonomie réelle d'un RSSI (seulement 11 réponses sont en dépendance directe avec la Direction de l'entreprise).

9. Les formations possibles pour un RSSI

L'objet de notre contribution est d'apporter des éléments de réflexion sur l'évolution des compétences dans le domaine de la sécurité informatique en tenant compte de la nécessité de « coller » aux nouvelles tendances techniques, d'en percevoir les nouveaux dangers mais également de comprendre les liens Business et les échanges entre organisations (Lasfarges, 2003). Le graphique ci-dessous permet de schématiser notre approche (Rockart et Short, 1995) :

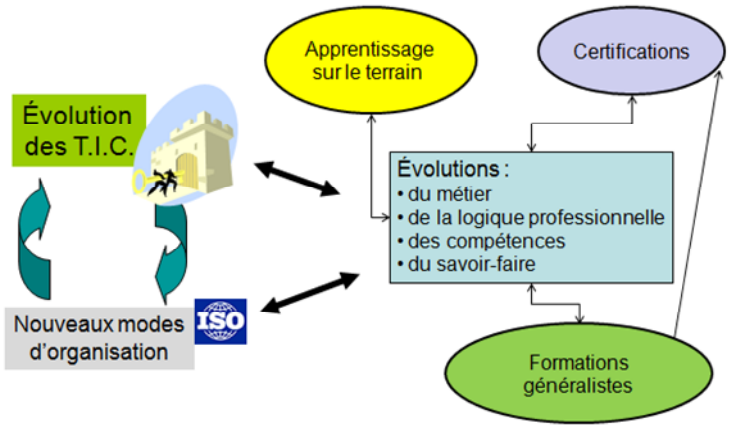


Figure 7 : le lien entre l'évolution des TIC, les nouvelles organisations et les compétences

Depuis la fin des années 70, il y a principalement deux modèles (Paradeise et Lichtenberger, 2001) qui posent la question du passage du modèle de la qualification à un modèle de la compétence. La classification des métiers correspond à un type de qualification. Cependant, l'évolution de l'organisation du travail tend vers plus de souplesse et ne répond plus à un régime de certifications statufiées. La compétence est considérée comme une combinaison de connaissances, savoir-faire, expériences et comportements (Reynaud, 2001).

Le cas de l'informatique est un exemple du modèle de la compétence (Pichault, Rorive, et Zune, 2001). Pour ces auteurs, l'acquisition des TIC s'effectue sous un mode cumulatif et également supplétif. Dans ce contexte, il est difficile de vouloir qualifier de manière formelle toutes ces évolutions. Cependant, le débat n'est pas clos : les constructeurs de matériels et logiciels informatiques cherchent à promouvoir leurs produits par des certifications (CCNA[15] de Cisco, MCSE[16] de Microsoft). Le domaine de la sécurité n'est pas en reste de cette tendance. Les formations généralistes de type MBA ont pour objectif d'apporter un socle de base durable sur le fond. Cependant, l'évolution du niveau sécuritaire nécessite également l'apport de formations plus spécialisées, moins pérennes dans le temps. Ainsi, la certification CISSP[17] n'est homologuée que pendant 3 ans[18]. Le CISM[19] propose un nombre d'heure de «maintenance» obligatoires pendant les 3 années qui suivent la certification[20].

Dans le contexte de notre enquête, les diverses réponses n'ont pas permis de dégager une préférence entre les formations généralistes et les spécialisations pointues à court terme. Il n'existe pas non plus la formation idéale en la matière puisque le management des diverses entreprises ne précisent pas formellement un passage obligé par une formation précise et attitrée. Le schéma suivant illustre bien ce constat :

Figure 8 : la réputation et le contenu des diverses formations

[15] Cisco Certified Network Associate
[16] Microsoft Certified System Engineer
[17] Certified Information Systems Security Professional
[18] http://en.wikipedia.org/wiki/Certified_Information_Systems_Security_Professional
[19] Certified Information Security manager
[20] http://www.isaca.org/Template.cfm?Section=Certification&Template=/ContentManagement/ContentDisplay.cfm&ContentID=51252

Ainsi, les réponses à la question 33 montrent une "non préférence" entre les formations généralistes (11 réponses) et spécialisées (10 réponses). Le «Non défini» (11 réponses) appuie très fortement cette incertitude. Concernant l'évolution des domaines utiles (question 35), les tendances confirment bien notre analyse au paragraphe 2 puisque les domaines qui doivent être étudiés (le management, organisation, le juridique, l'économie, la finance, …) doivent permettre de mettre notre RSSI dans une position où il peut comprendre les contraintes des divers services et départements.

10. Conclusion

Nous constatons que le métier RSSI est en pleine mutation. Au-delà d'une maîtrise technique généraliste, le RSSI doit être un communicateur et faire accepter la nécessité sécuritaire auprès des divers départements ou services sans avoir le statut du pouvoir managérial d'un «Top Executive». Pour mieux convaincre ses collègues et responsables métiers, il doit connaître le business de l'entreprise en profondeur. Un RSSI n'est pas un chef d'orchestre, c'est un homme orchestre. Comme le précise Pierre-Luc Refalo il y a déjà quelques années : « *Le RSSI apparaît aujourd'hui tout à la fois un manager et un expert, un stratège et un chef de projet, un veilleur et un éducateur, voire parfois un administrateur ou un enquêteur* » (Refalo, 2003). Les réponses à notre enquête confirment bien les propos de cet auteur.

Dans le cadre d'une prospective à court/moyen terme, il serait intéressant d'effectuer une enquête plus ambitieuse dans le cadre de l'Europe. En plus d'une nouvelle participation du CLUSIS, des associations sœur telles que les CLUSIx[21] peuvent être intéressées par cette démarche. Les résultats permettraient alors de constater des similitudes ou des différences par régions ou pays.

[21] Ces associations ont été crées pour répondre aux besoins de sécurité en entreprise : CLUSIF pour la France, CLUSIT pour l'Italie, CLUSIB pour la Belgique.

11. Bibliographie

Anderson R (2008) "Security engineering: aguide to building dependable distributed systems", Wiley Publishing

Beynon-Davies, P (2002) *Information Systems – An Introduction to Informatics in Organisations*, Palgrave

Brint S. (1993) "*Eliot Freidson's contribution to the sociology of Professions*" Sage, Thousand Oaks

Champenois A. (1997) "*Infogérance : externalisation des Systèmes d'Information*", Interéditions, Paris

Cigref, "*Nomenclature 2009 : les emplois-métiers du SI dans les grandes entreprises*", octobre 2009

De Blasis, J.-P. (2008), « Sécurité et qualité dans l'organisation des SI – 2ème et 3ème partie : aspect du management de la sécurité du S.I.», Module 1-4b, Cours Dssi, septembre 2008

Dlamini MT, Eloff JHP, Eloff MM, (2008) "Information security: the moving target", Computers and Security 2008

Ezingeard JN, Bewen-Schire M (2003) "Information security: a strategic issue" etude conjointe Hanley Management College (UK) et Dataföreningen (Sweden)

Foray, B. (2007), "*La fonction RSSI – Guide des pratiques et retours d'expérience*", Dunod

Kaczmarek, M. et Marion J.-Y. (2010), « Boulevard du cybercrime », Dossier pour la science, N° 66, janvier-mars 2010, p. 78

Kraemer S, Caryon P, Clem J, (2009) "Human and organizational factors in computer and information security: pathways to vulnerabilities," Computers and Security 2009

Lasfargue, Y.: *Halte aux absurdités technologiques*, Editions d'Organisation, 2003

Larcher, S. (2009), « La cyber-guerre a commencé », l'Informaticien, N° 79, décembre 2009

Lemaire, L. Valenduc, G. (2005) « Métiers, emplois et offres de formation dans les TIC – en Wallonie et à Bruxelle », *MéTIC*, Fondation Travail-Université

McAdams AC (2004) "Security and risk management: A fundamental business issue", Information Management Journal, 36-44 july/aug

Menthonnex, J. (2006), « COMPÉQ, un référentiel de compétences pour aider à structurer et à piloter ses apprentissages », 7e colloque européen sur l'Autoformation « faciliter les apprentissages autonomes » Enfa, Auzeville - 18 –19- 20 mai 2006

Musekura JB., Ekh R (2003) "Information security issues – difference between perception and practice in organizations", Orebro University, Sweden

Paradeise, C. Lichtenberger, Y. (2001) « Compétences, compétences », *Sociologie du travail*, N°1

Peltier TR (2002) "Information Security Policies, procxedures and standards: guidelines for effective information security management", 1st ed. CRC Press

Pichaul, F., Rorive, B. et Zune M. (2001) « Etude TIC et métiers en émergence », DiGITIP

Refalo, P-L. (2003), « La fin du RSSI », L'informatique Professionnelle, 215 – juin-juillet 2003, p41

Reynaud, J-D. (2001), « Le management par les compétences : un essai d'analyse » in *Sociologie du travail*, N°1, vol. 43

Rockart J.F. et Short, J. E. (1995), L'entreprise compétitive au futur, « *L'organisation des réseaux et le management de l'interdépendance* », les éditions d'organisation

Schneier B (2000) "Secrets and lies – Digital security in a networked word", Wiley Computer Publishing

Solms B, Solms R, (2004) "The 10 deadly sins of information security" Computers and Security

Tudor JK (2000) "Information security archtecture – an integrated approach to security in an organisation" London, Auerbach

Willcocks LP., Fitzgerald G., Feeny D. (1995) "*Outsourcing IT: The strategic implications*", Long Range Planning, vol 28, n°5, pp 59-69

12. Annexe : Le questionnaire proposé

	Renseignements généraux (réponses facultatives)	
1.	Nom	
2.	Prénom	
3.	Fonction	
4.	Nom de votre organisation	
5.	Secteur d'activité principal de votre organisation	
6.	Taille de votre organisation	
7.	Votre organisation est-elle : • une PME (1) • le siège social d'un groupe (2) • une unité décentralisée d'un groupe (3) • autre (4)	
	Adresse de votre entreprise	
8.	Rue	
9.	NPA (code postal)	
10.	Localité (ville)	
11.	Téléphone	
12.	Fax	
13.	e-mail	
14.	Adresse Web	
	Le poste RSSI	
15.	**Existe-t-il dans votre organisation une fonction RSSI en tant que telle avec cette dénomination ?** *(répondez par OUI ou NON)*	
16.	Si oui, sous quelle dénomination (si autre que RSSI) ?	
17.	Autre	
18.	**Est-ce un poste à plein temps?** *(répondez par OUI ou NON)*	

19.	Si non, quel est le pourcentage d'activité de ce poste ?	
20.	**La position du poste RSSI est-elle dépendante hiérarchiquement ?** • de la direction de votre entreprise (1) • de la direction des systèmes d'information (2) • d'un comité de groupe de sécurité (3) • du CSO (Chief Security Officer) (4) • autre(s) *(merci de préciser)* (5)	
21.	**Quelles sont les autres fonctions avec lesquelles le RSSI est en interaction dans votre entreprise ?**	
22.	**Quel est le rôle (la responsabilité) du RSSI dans votre entreprise ?**	
23.	**Dans votre entreprise, le RSSI est-il dépendant ou indépendant des fonctions opérationnelles ?** *(répondez par OUI ou NON)*	
24.	**Est-ce que le RSSI est dégagé de la mise en œuvre opérationnelle des actions de sécurité ?** *(répondez par OUI ou NON)*	
25.	**Est-ce que le RSSI dispose d'un budget autonome ?** *(répondez par OUI ou NON)*	
26.	**Parmi les missions du RSSI listées ci-dessous, lesquelles sont concernées par celles définies dans votre entreprise ?** • la gestion de l'analyse des risques liés à l'information (1) • la définition des moyens organisationnels, techniques, juridiques et humains requis (2) • le contrôle de leur mise en place et de leur efficacité (3) • la conception du/des plan(s) d'actions visant à l'amélioration de la couverture des risques (4)	
27.	Autre	
28.	**Quelles sont les 5 tâches les plus importantes par ordre décroissant dont vous vous occupez quotidiennement comme RSSI ?** (en pourcentage de vos journées de travail)	• la plus importante : _____% • importante : _____% • moyennement importante : _____% • ponctuelle : _____% • insignifiante : _____%
29.	Autre	
30.	**Quelles sont les qualités requises par le RSSI ?**	

	Le parcours professionnel du RSSI	
31.	**De quel(s) horizon(s) provient le RSSI de votre entreprise ?**	
32.	**Comment avez-vous acquis votre expérience en sécurité de l'information ainsi qu'une connaissance approfondie du secteur d'activité de votre entreprise (cœur de métier) ?**	
33.	**S'il est défini, quel est le parcours professionnel (niveau de formation, type de diplôme(s)) requis pour le poste RSSI dans votre entreprise ?**	
34.	**Quelles sont les formations que vous avez suivies pour accéder à ce poste ?**	
35.	**Pour accéder au poste de responsable sécurité (fonction de RSSI), quelles sont les formations utiles d'après vous ?**	
36.	**Quelle(s) formation(s) supplémentaire(s) (formation continue) suivez-vous ou avez-vous suivi ces 3 dernières années ?**	
37.	**Quel(les) est(sont) le(s) réseau(x)/association(s) professionnel(les) implanté(es) dans la sécurité au(x)quel(les) votre entreprise fait partie ?**	
	Le niveau de sécurité de votre entreprise	
38.	**De manière générale, vos projets concernent-ils davantage ?** • la sécurité physique et logique (infrastructures techniques) (1) • la réponse aux audits en termes de processus et d'organisation (2) • la mise en conformité aux diverses normes (3)	
39.	Autre	
40.	**Dans ce cadre, les processus utilisés correspondent à quel niveau de maturité de la SSI (réf : Clusis, Claude Maury – janvier 2005) ?** • **méconnaissance** (procédures élémentaires de backup/restore de l'information) (phase 1) • **délégation** (seul le périmètre informatique est sécurisé) (phase 2) • **prise de conscience** (un plan de sécurité informatique est existant) (phase 3) • **engagement total** (un plan de continuité des activités est en place) (phase 4)	
41.	Autre	