Les Assises de la Sécurité

un événement

LIVRE BLANC

Pour un management stratégique des cyber-risques

Parrainage

Réalisation

octobre 2004

www.nrg.fr

www.e-portal.net

www.demos.fr

Info@dgconsultants.fr

www.cigref.fr

www.netcost-security.fr

www.int-evry.fr

www.utt.fr

www.esiee.fr

Sommaire

- Préambule 7

Le poids des mots

- Volet 1 13

Le RSSI, au cœur du débat

- Volet 2 29

La fonction SSI, sans dessus-dessous

- Volet 3 41

L'intégration perfectible dans l'entreprise

- Volet 4 53

Les ressources humaines, clés de la réussite

- Orientations 67

Des pistes de réflexion, et d'action..

- Annexes 79

Graphisme *(contenu et 1ère de couverture)* : **clette.com**
www.clette.com

Quel plaisir !

Enfin une étude digne de ce nom réalisée auprès, non pas d'un échantillonnage, mais d'un véritable panel représentatif, en nombre et qualité, de l'univers de la Sécurité des Systèmes d'Information.

Vous serez attentifs aux chiffres et résultats figurant dans cet ouvrage mais certainement surpris de découvrir certaines informations (telle la valeur du salaire moyen) qui étaient, à ce jour, des plus "strictement confidentiellles".

Vous serez également ravis de confronter les tendances ; objectifs et contraintes de confrères évoluant tant dans des sphères équivalentes aux vôtres, que de comparer certains critères et processus liés à la sécurisation des systèmes d'information.

Les équipes, sous l'égide de Pierre-Luc, qui ont contribué à ce Livre blanc, méritent nos félicitations sachant que nous souhaitons que cet ouvrage soit pour vous un véritable "outil" de travail et de référence.

Et gageons que ce ne soit que le "1er tome" d'une collection qui s'enrichira des expériences et du vécu des participants aux Assises et au Cercle Européen de la Sécurité.

En conclusion, n'hésitez pas, vous aussi, à faire connaître vos choix et desideratas, et encore un grand merci à Pierre-Luc.

Gérard RIO
Fondateur des Assises
de la Sécurité

Préambule

Le poids des mots

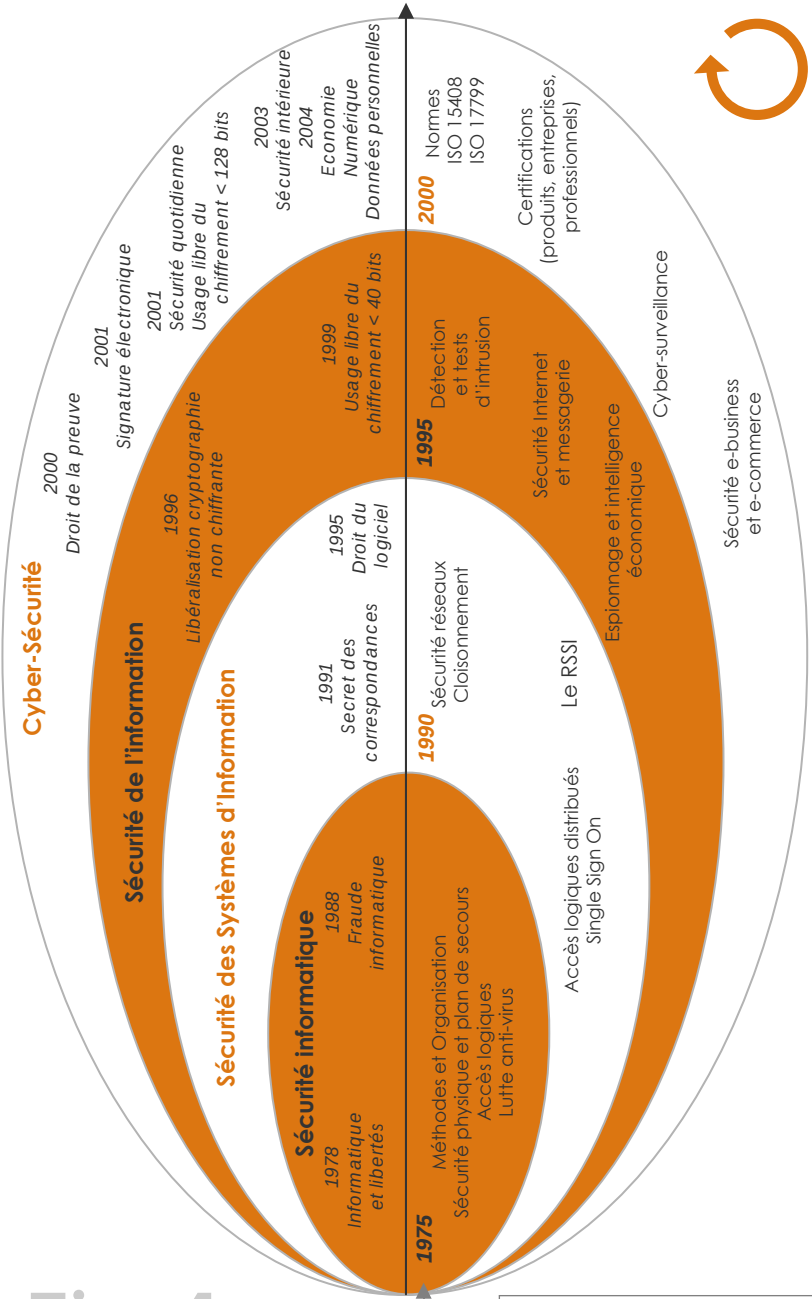


Fig.1

De la Sécurité Informatique à la Cyber-Sécurité

Le poids des mots

Tout a commencé il y a plus de cinquante ans, par la naissance des premiers ordinateurs (à usage essentiellement militaire). Mais tout s'est réellement développé à partir des années 70 avec le développement de l'informatique de gestion en entreprise (banques et assurances). Et tout s'est incroyablement accéléré à partir du milieu des années 90 avec l'usage généralisé de l'Internet et des réseaux par les entreprises et les administrations.

Les nouveaux défis ? La dématérialisation des processus, l'avènement d'une économie "numérique" et le recours à des acteurs dits "de confiance". Dans ce contexte :

- Que représente aujourd'hui la sécurité informatique ?
- Pourquoi entend-on de plus en plus parler de sécurité de l'information ?
- Et que signifie alors la cyber-sécurité qui a fait, elle aussi, son apparition ?

Existe-t-il seulement une définition de **" sécurité informatique"** ? Étymologiquement, elle consiste en *« un ensemble de conditions et de moyens nécessaires à la création d'une* ***situation sans danger pour les ressources matérielles et logicielles*** *composant un système de traitement de l'information. »*

N'est-ce pas par nature un vœu pieux ? Et si c'est bien de **"sécurité des systèmes d'information"** dont la grande majorité des professionnels se réclament, la problématique ne change pas vraiment.

Par contre, on change de dimension lorsqu'on se focalise sur le contenu. La **"sécurité de l'information"** nous ramène aux origines : au secret, à la cryptographie, à la sécurité de défense, etc. La mixité du contenant et du contenu est devenue au fil du temps une des problématiques majeures pour les professionnels.

Mais à l'avenir, la **"cyber-sécurité"** sera certainement le terme qui sera de plus en plus utilisé car le plus fédérateur.

La cyber-sécurité : *« Ensemble des activités techniques, juridiques et humaines permettant de se prémunir des risques de fraude et de piratage utilisant l'informatique et les réseaux de communication et portant atteinte aux intérêts d'autrui. »* C'est une approche globale, portant sur le contenu et le contenant, sur l'interne et l'externe.

La Fig.1, reprise et adaptée du livre "Sécuriser l'entreprise connectée" (Editions d'organisation – octobre 2002), éclaire le positionnement des termes et surtout leur évolution dans le temps.

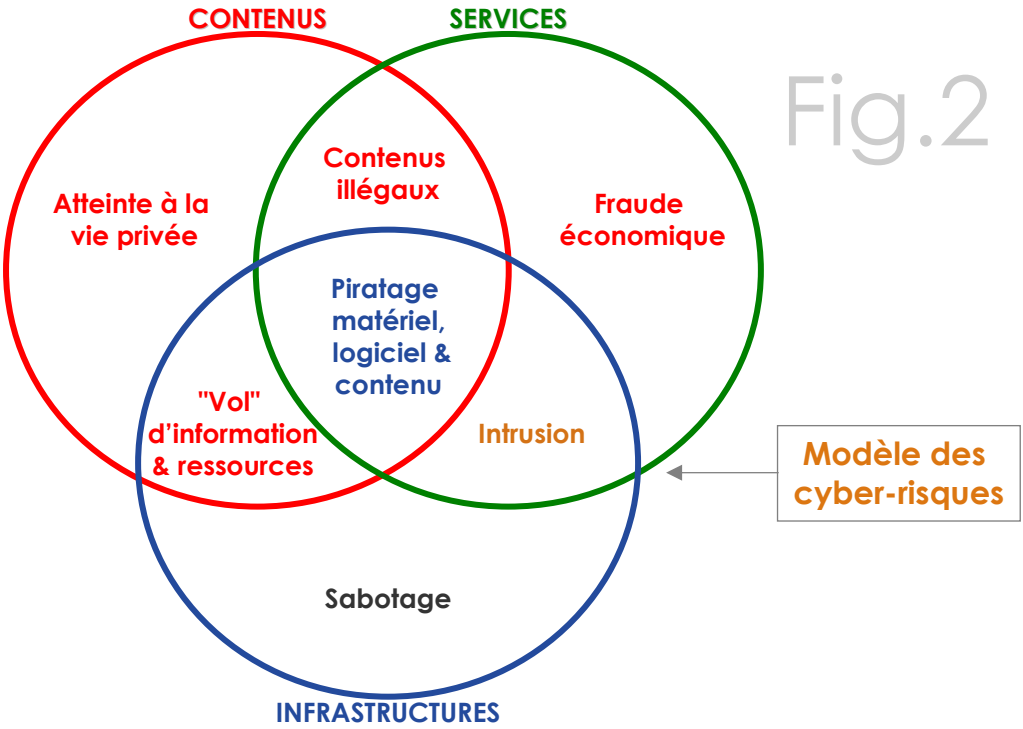

CONTENUS
SERVICES
Contenus illégaux
Atteinte à la vie privée
Fraude économique
Piratage matériel, logiciel & contenu
"Vol" d'information & ressources
Intrusion
Sabotage
INFRASTRUCTURES
Modèle des cyber-risques

Fig.2

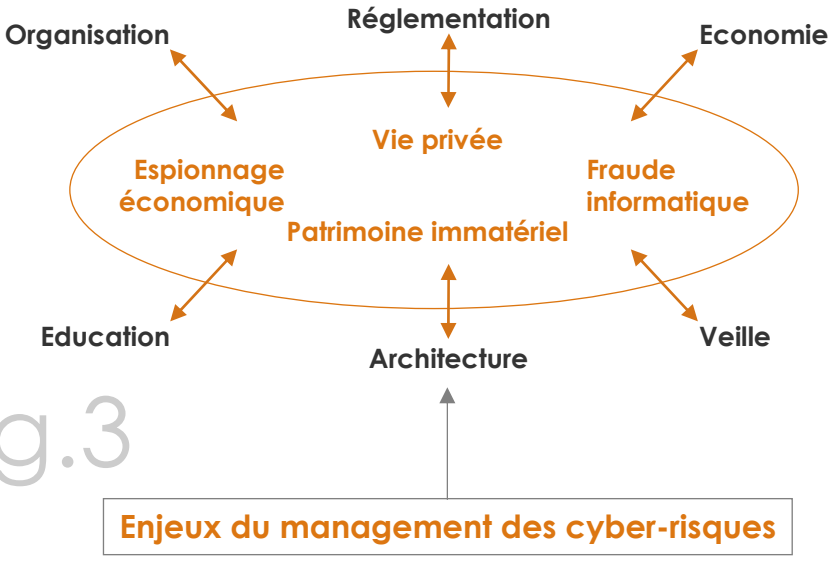

Organisation
Réglementation
Economie
Vie privée
Espionnage économique
Fraude informatique
Patrimoine immatériel
Education
Architecture
Veille
Enjeux du management des cyber-risques

Fig.3

Le poids des mots

Le 1er Livre blanc des Assises présente et commente les résultats de la 2ème enquête du Cercle Européen de la Sécurité sur "Les métiers de la SSI". Mais au-delà du constat, il se doit d'éclairer les professionnels sur leur fonction et leurs activités.

Les exigences de sécurité sont devenues une question essentielle de notre vie quotidienne, personnelle ou professionnelle. Dans le domaine juridique, les questions de "vie privée", de "confiance dans l'économie numérique", de "sécurité intérieure" s'adressent plus que jamais aux systèmes d'information et de communication. Quels en sont et seront les impacts en entreprise en termes d'organisation ?

Quoi qu'il en soit, le management de la sécurité doit systématiquement impliquer trois composantes indissociables :

LE RISQUE : ce principe universel et omniprésent pose la question de son "management" dans son expression la plus noble : la **POLITIQUE**. Celle qui fixe des objectifs, définit un cadre réglementaire et rappelle les principes fondamentaux. Quelles sont les bases "politiques" de la SSI en 2004 ?

LE POUVOIR : cette notion fondamentale se décline de la politique et pose la question des champs de responsabilité (en prévention comme en réaction et en gestion de crise), c'est-à-dire de l'**ORGANISATION**. Elle attribue les domaines de compétence et d'intervention.

LA MESURE : outil indispensable du manager, l'évaluation du risque, des enjeux, des impacts, des coûts est plus que jamais à l'ordre du jour. Car ce qui importe désormais c'est la bonne prise de **DECISION**, juste et équilibrée. L'économie joue ici un rôle essentiel.

Le terme "sécurité" est par ailleurs de plus en plus difficile à employer. Il est parfois porteur d'illusion, souvent trompeur, et ambiguë car plus associé au "répressif" qu'au "préventif".

Le Livre blanc est avant tout un appel à une plus grande reconnaissance des professionnels dont les fonctions restent encore mal définies, parfois mal positionnées, souvent sans réel moyen d'action. Intéressons-nous aux aspects les plus nobles, aux hommes et au "management". Et ayons une ambition :

"Pour un management stratégique des cyber-risques."

Volet 1

Le RSSI, au coeur du debat

Un titre à géométrie variable

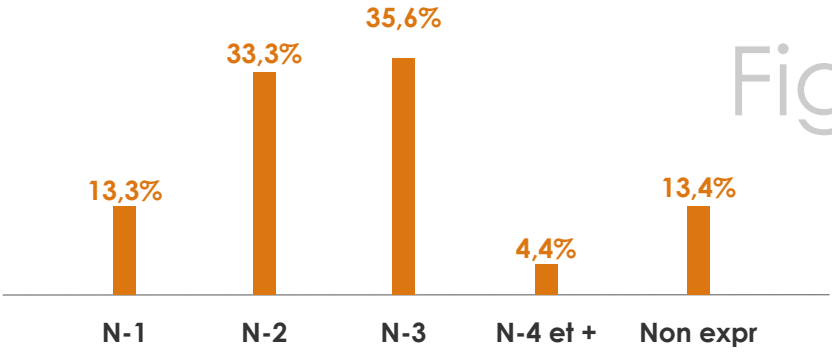


Fig.4

Niveau de rattachement des RSSI en 1998
(source Systèmes et Sécurité – Juin 1998)

Mission	Taux
Sensibilisation	84,4%
Conseil en solutions de SSI	77,8%
Élaboration des référentiels, guides, …	73,3%
Intégration de la sécurité dans les projets SI	64,4 %
Conduite de projets	64,4 %
Audit des dispositifs opérationnels	62,2 %
Analyse des risques du SI	57,8 %
Anticipation des situations à risques	53,3%

Fig.5

Missions assurées par les RSSI en 1998
(source Systèmes et Sécurité – Juin 1998)

1998 : une base de départ

La fonction "Sécurité des SI" (SSI), et en particulier le "Responsable de la Sécurité des SI" (RSSI), est un thème régulièrement traité au sein des associations et par les médias spécialisés. Certains se sont posés la question de savoir si c'était un véritable métier ou simplement une fonction "assumée au mieux" pour tenir compte des nouveaux risques liés d'abord aux systèmes informatiques et aujourd'hui à ceux de la Société de l'Information.

La revue Systèmes et Sécurité a publié en juin 1998 un numéro spécial (Volume 5 – Numéro 3) sur "Le RSSI". Sa lecture est riche d'enseignements car 6 ans plus tard, on constate que l'on se pose toujours les même questions sur : le profil du détenteur de la fonction, la délégation de pouvoir, les liens avec la sécurité globale de l'entreprise, l'externalisation et l'intelligence économique.

Schématiquement, nous pouvons affirmer que les premiers acteurs en charge de la Sécurité des SI étaient avant tout des Responsables Sécurité Informatique (années 80) et qu'ils sont un peu **"tombés dedans par hasard"**. C'est avec l'apparition des réseaux et l'émergence de l'Internet que la fonction prend ses lettres de noblesse (années 90). De nombreux professionnels, souvent – sans que ce soit péjoratif – par **"opportunisme"**, entrent dans la carrière, que ce soit en entreprise ou dans les services.

Dans ses aspects "opérationnels", la fonction Sécurité des SI doit sans doute être, comme pour les autres domaines de la sécurité (civile, militaire, sanitaire, routière, etc.), une **"vocation"** où le don de soi, sans rien attendre en retour, devrait être la règle.

Le début des années 2000 a été marqué par l'éclatement de la bulle Internet et par la tragédie du 11 septembre 2001. Deux événements majeurs qui ne sont pas étrangers à une mutation vers une "quête de sécurité".

Cette base de départ mérite d'être complétée et enrichie car le titre de RSSI cache d'innombrables disparités qu'il convient encore de mettre à jour.

"Je fais un métier très noble car il donne une base d'éthique et de déontologie à l'entreprise. C'est une activité où il ne faut rien attendre en retour, même si l'on donne beaucoup."

Maricela Pélegrin-Bomel

Responsable centrale de la sécurité des biens, Bouygues Telecom.

17

La revue de presse des principaux articles parus depuis 1998 est une source d'enseignements majeurs.

Janvier 1998 – 01 Informatique

"L'indispensable qualité de stratège du responsable de la sécurité"

Le responsable de la sécurité est avant tout un homme de méthode et d'organisation, même s'il doit posséder de solides connaissances en réseaux et systèmes. Il doit être capable de répondre à la fois aux attentes d'une direction générale et à celle des informaticiens.

Février 1999 – Informatique Magazine

" Le responsable sécurité : un super agent"

Le responsable de la sécurité du système d'information redessine l'architecture réseau face aux nouvelles menaces tout en faisant respecter les règles de sécurité de l'entreprise.

Novembre 1999 – Le Monde interactif

"Les gardiens de la sérénité informatique de l'entreprise"

"Traqueurs de hackers"

Un responsable de la sécurité gagne en moyenne 27,5 k€ par an à l'embauche et il peut facilement tripler son salaire en quelques années. La profession devrait, à n'en pas douter, rapidement susciter de nombreuses vocations.

Le curriculum vitae idéal

Âge	25 ans
Formation	Ecole d'ingénieur ou DEA en informatique Spécialisation en sécurité informatique
Compétences	Très bon niveau en informatique (langages de programmation, systèmes d'exploitation) et en réseaux (protocole TCP/IP, etc.). Bonnes connaissances en sécurité des SI (cryptographie, méthodes)
Langues	Anglais obligatoire
Salaire	De 2,3 k € / mois pour un débutant à 5,3 k € après quelques années d'ancienneté

Mai 2000 – 01 Réseaux

"Le RSSI, plutôt chef d'orchestre que premier violon"

A l'heure de l'e-business et alors que les attaques n'arrivent pas qu'aux autres, la sécurité est devenue un enjeu majeur pour l'entreprise.

Le nouveau profil du Responsable Sécurité des SI

Cursus	Diplôme d'ingénieur informatique / télécoms (niveau BAC + 5)
Expérience	5 ans minimum Spécialisation en sécurité informatique
Compétences incontournables	Expertise systèmes et réseaux voire développement logiciel Qualités relationnelles, sens de l'organisation, réactivité
Évolutions	Risk manager, expert ou auditeur sécurité
Compétences utiles	Veille, réglementation, méthodes sécurité physique et logique
Emploi du temps	20% pour les règlements et référentiels, 30% pour la veille et le relationnel, 50% pour la mise en œuvre et le contrôle des procédures
Salaire	De 50 à 100 k € / an

Février 2002 – 01 Informatique

"Le RSSI : maître d'ouvrage des opérationnels"

Le Responsable Sécurité des SI intervient dans des domaines très variés, du droit à la comptabilité.

Décembre 2002 – Le Monde Informatique

"Le RSSI : les douze travaux d'un expert"

La qualification exacte de la fiche de mission du RSSI constitue un réel problème de fond.

Juin 2003 – 01 DSI

"Monsieur Sécurité : politique ou technicien ?"

Bras armé du DSI en matière de risques, le RSSI prend du galon. Né technicien, il a grandi pour devenir manager.

Juin 2004 – 01 Réseaux

"Le métier de RSSI en pleine évolution"

Intelligence économique, veille stratégique, conformité réglementaire … Le RSSI ne se doutait pas, il y a dix ans, quand la fonction a été créée, qu'il serait un jour gestionnaire des risques organisationnels, réglementaires, stratégiques et opérationnels.

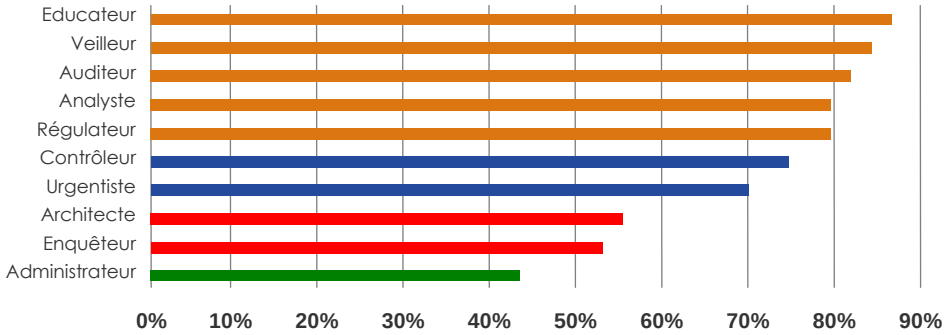


Fig.6

Les rôles assurés par les RSSI
(source Cercle Européen de la Sécurité - 2003)

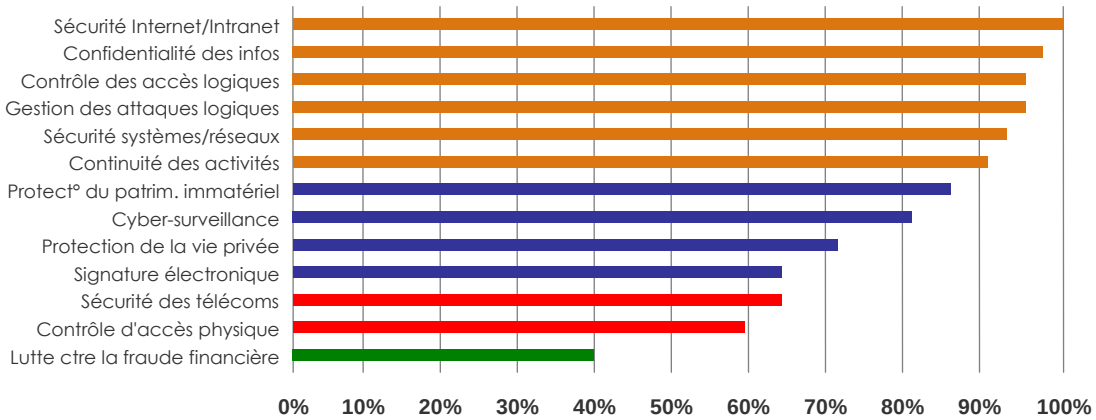


Fig.7

Le champ d'action des RSSI
(source Cercle Européen de la Sécurité - 2003)

Caméléon et "homme à tout faire" ?

L'enquête menée en 2003 par le Cercle Européen de la Sécurité auprès de 40 managers de la SSI a permis de mettre en évidence 2 tendances fortes.

La première est que les rôles assurés par ces professionnels et leurs équipes sont très diversifiés. Sept d'entre eux prédominent et concernent au moins 7 répondants sur 10.

Derrière les 5 fondamentaux du RSSI (qui est d'abord un régulateur-auditeur, un veilleur-éducateur et un analyste), on peut remarquer que les fonctions de "contrôle" et de "gestion d'incident" ne sont pas marginales. Est-il devenu l' "œil de Moscou" ? Ou un "cyber-pompier" ? Que 70 % des répondants de 2003 se sentent investis de ces prérogatives est remarquable (fig.6).

Les fonctions plus opérationnelles, nécessitant des compétences très pointues comme l'architecte, l'administrateur et plus encore l'enquêteur se situent autour de 50 %. Un professionnel sur 2 pouvant être assimilé à un RSSI conserve un rôle de terrain fort utile à sa crédibilité, mais lui enlevant potentiellement le recul nécessaire au décideur.

Ensuite, en ce qui concerne le champ d'action, on constate que les domaines historiques de la Sécurité des SI (en orange sur la fig.7) sont suivis de très près par 4 problématiques à forte connotation juridique (bleu) :

- Patrimoine immatériel
- Cyber-surveillance
- Vie privée
- Signature électronique

C'est une tendance majeure du début des années 2000. Et elle ne devrait pas se ralentir. Dans Mag Securs de Mars 2004, Olivier ITEANU affirmait clairement que ***"le RSSI est coincé entre le marteau et l'enclume de la loi."*** !

Le lien entre la Sécurité des SI et la fraude (financière) apparaît quand à lui, en 2003, relativement restreint. Environ 4 professionnels sur 10 s'impliquent dans cette lutte qui prend un nouveau visage avec les lois Sarbannes Oxley et sur la Sécurité Financière.

Cette photographie initiale du rôle et des domaines d'activité des RSSI va s'éclairer tout au long de ce Livre blanc.

Directeurs et responsables

- Sécurité SI
- Sécurité informatique
- Sécurité de l'information
- Sécurité des données

- Sécurité
- Sécurité et déontologie
- Sécurité des biens et personnes

- Système d'Information
- Informatique
- Technique
- Production informatique

- Prévention des risques informatiques
- Information risk
- IT risk
- Enquêtes et gestion de risques

- Réseaux et sécurité
- Infrastructure et sécurité
- Sécurité et nouvelles technologies

Opérationnels

- Coordinateur
- Contrôleur

- Consultant
- Chargé de mission

- Architecte - Expert
- Architecte – Expert "systèmes / réseaux"

- Administrateur "réseau et sécurité"

Les 25 titres attribués aux professionnels de la SSI

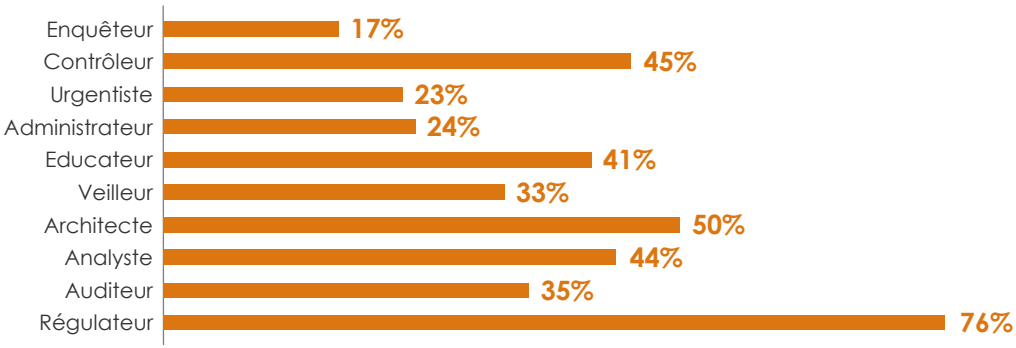


Fig.8

Les rôles assumés par les professionnels de la SSI

Quel est votre métier ?

Les professionnels de la Sécurité ont du mal à se trouver un véritable qualificatif ! Normal, quand une part non négligeable (38%) du panel n'est pas dédiée aux questions de Sécurité des SI. "RSSI" est devenu au fil du temps une aide précieuse, mais trop simplificatrice. Il est important de bien distinguer les fonctions relatives à :

- La sécurité informatique
- La sécurité des systèmes d'information
- La sécurité des données et des informations

Les professionnels dédiés sont "RSSI" ou "DSSI" dans 62% des cas.

Reste à savoir ce que l'on entend pas là et en particulier les rôles qui sont tenus par ces professionnels. A la question, "quels sont les 4 rôles que vous assumez personnellement ?", l'ensemble du panel place largement en tête (76%) le "régulateur". C'est le rôle premier qui montre que la fonction doit déterminer un équilibre :

- Une politique adaptée aux enjeux et à la culture de l'entreprise
- Des moyens cohérents avec les risques encourus
- Un pilotage harmonieux entre aspects techniques, juridiques et humains

Entre 40 et 50 % se trouve tout un ensemble de rôles divers sans qu'il soit possible d'en tirer un quelconque enseignement. "Éducateur", "Analyste" et "Architecte" sont des fonctions "historiques" souvent déléguées à des profils plus "techniques". Et le "Contrôleur" progresse passant de la 6ème place en 2003 à la 3ème en 2004. Certains le nomment d'ailleurs "Superviseur" ou "Inspecteur".

Juste après se situent 2 rôles importants mais ici aussi sans doute délégués par beaucoup : "veilleur" et "auditeur". Nous détaillerons ces rôles dans le 3ème volet relatif à l'intégration de la fonction SSI dans l'entreprise.

Enfin, les rôles de moindre importance mais qu'il convient de remarquer sont "Administrateur", "Urgentiste" et "Enquêteur". Ils ne font pas partie des activités permanentes des membres du panel à quelques exceptions près.

Nota : l'analyse des rôles assumés par les professionnels dédiés à la SSI (temps plein) ne montre pas d'écart significatif (+/- 2 %) par rapport au panel complet.

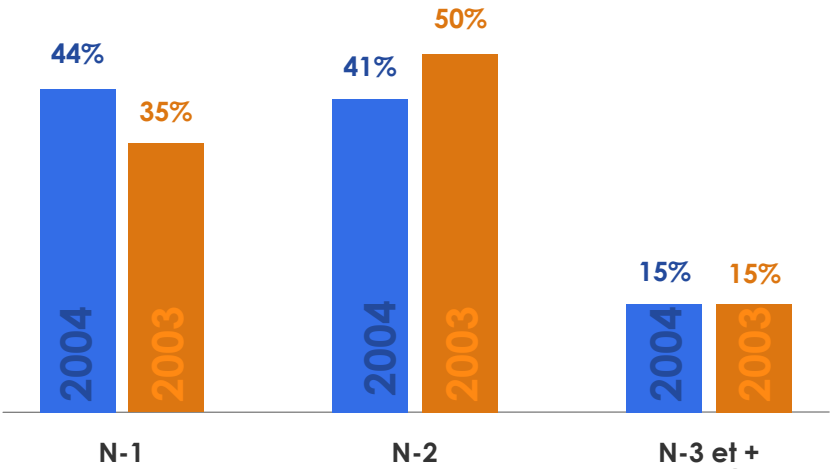


Fig.9

Position par rapport à un Comité de Direction / Exécutif

Rattachement hiérarchique

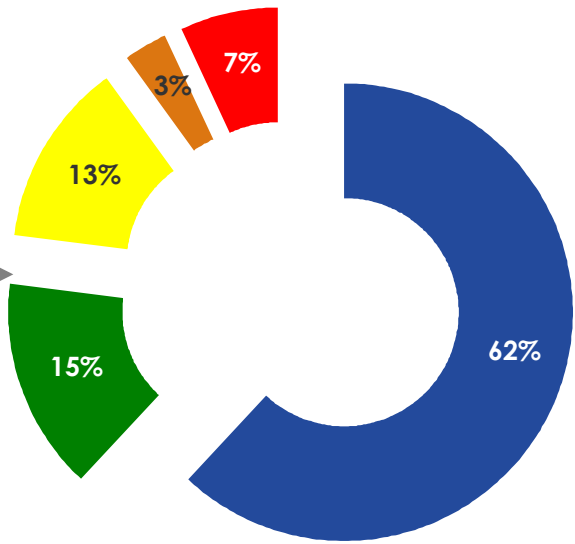


Fig.10

■ Système d'information ■ DG-SG ■ Sécurité - Sûreté ■ Finances ■ Autres

Des acteurs qui prennent du galon

Les professionnels ont considérablement amélioré leur positionnement dans l'entreprise. Le chemin parcouru en 6 ans est considérable (fig.9).

Le rattachement hiérarchique à un membre d'un Comité de Direction progresse donc et deviendra certainement majoritaire dans 1 ou 2 ans pour les RSSI. L'étape suivante, comme cela semble déjà être le cas outre-Atlantique, sera de placer le Directeur de la Sécurité (CSO : Chief Security Officer) ou de la Sécurité de l'Information (CISO : Chief Information Security Officer) au sein du Comité de Direction (Board).

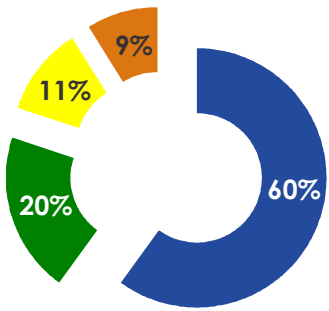
Mais il convient de remarquer aussi que la majorité des professionnels reste attachée à la DSI ! Les RSSI ne profiteraient donc, en quelque sorte, que de l'élévation des fonctions informatiques dans les organigrammes ? C'est sans doute faux. Ils ont plutôt aussi et surtout élargi leur champ d'action à la sécurité générale, aux questions de "gestion de risques". Ou inversement, ils ont intégré la SSI dans leur domaine de compétence initial.

62% du panel de 2004 restent dépendants des fonctions "informatiques" (contre 48% en 2003). C'est sans doute trop. Nombreux sont ceux qui sont désormais dans des Directions "Sécurité/Qualité" ou des Directions des risques, voire mieux au sein d'un Secrétariat général ou d'une Direction financière. Une des alternatives que certains ont trouvée est de définir le IT risk manager, l'Information risk manager, ou pourquoi pas le "cyber-risk manager".

Le positionnement dans une organisation découle finalement de l'ampleur des responsabilités et du champ d'action. Il est d'évidence plus vaste, plus transverse et concerne des préoccupations plus importantes des décideurs.

Enfin, pour mettre en place leur démarche, les entreprises font d'abord appel à la mobilité interne car l'intégration dans les processus et la connaissance des métiers sont fondamentaux. Le marché du "recrutement" en sécurité touche très peu les entreprises comme l'atteste la figure ci-dessous (1/3 des postes environ).

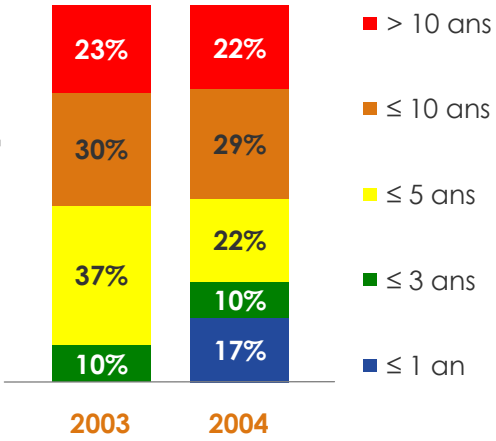
Le mode de recrutement dans le poste



- Mobilité interne
- Annonce
- Chasseur de têtes
- Après prestation

Fig.12

L'expérience en sécurité ou SSI



L'expérience dans le poste

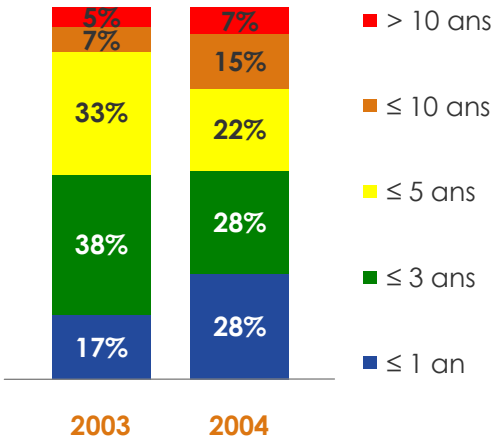


Fig.13

Des gourous aux néophytes

Les professionnels les plus expérimentés sont "entrés dans la carrière" il y a plus de 15 ans. Ils sont bien représentés (10) dans notre panel. Ils sont en quelque sorte les **"gourous"** du métier et sont tous (à 1 exception près) des Directeurs en charge de la SSI ou de la sécurité. La moitié d'entres eux reste néanmoins rattachée au DSI. Les autres se trouvent à la Direction financière, au Secrétariat général ou dans une direction Qualité/Sécurité.

Ils sont suivis par 11 **"challengers"** qui, possédant entre 10 et 13 ans d'expérience, devraient à l'avenir développer leur activité et / ou intégrer de plus fortes responsabilités. Pour les plus jeunes, notamment les "quadras", l'avenir leur appartient !

On retrouve ensuite 32 professionnels qui ont entre 5 et 8 ans d'expérience. Doit-on les qualifier de **"potentiels d'expérience"** ? Ils sont sans doute à une période charnière de leur vie professionnelle. Trouveront-ils des voies attrayantes dans l'entreprise ? Ou devront-ils s'échapper vers d'autres horizons, plus probablement chez un prestataire qu'en entreprise ? Ils sont des candidats potentiels aux certifications individuelles.

En dessous de 5 ans d'expérience se regroupent 29 **"néophytes"** qui doivent encore sans doute faire leurs preuves. Le sujet est suffisamment vaste et complexe pour qu'ils aient encore à apprendre et à investiguer de nombreux domaines qu'ils soient technologiques, juridiques, organisationnels ou méthodologiques. Leurs efforts dans la formation seront cruciaux.

Expérience moyenne en SSI en 2004 = 6,8 ans (8,0 ans en 2003)

La part des professionnels qui sont en poste depuis plus de 5 ans progresse significativement par rapport à 2003 (22% contre 12%) au détriment de ceux qui y sont depuis 3 à 5 ans (22% contre 33%).

La frontière entre plus ou moins 3 ans dans le poste est quasiment identique à celle de 2003 (45% au dessus et 55% en dessous). La question de la mobilité de plus de la moitié du panel est permanente. Néanmoins, il est peu vraisemblable de voir le marché de l'emploi se développer à court terme. L'intérêt et la complexité des projets favorisent une certaine "fidélité" à son entreprise et à sa fonction. Mais les externalisations et la pression budgétaire pourraient impacter certains.

Enfin, 18 professionnels sur 23 en poste depuis un an ou moins ont pris des fonctions à responsabilité (15 RSSI, DSSI, Directeur sécurité) ou innovantes (3 information risk manager, IT risk manager). C'est un signe encourageant.

Expérience moyenne dans le poste en 2004 = 4,0 ans (3,8 ans en 2003)

27

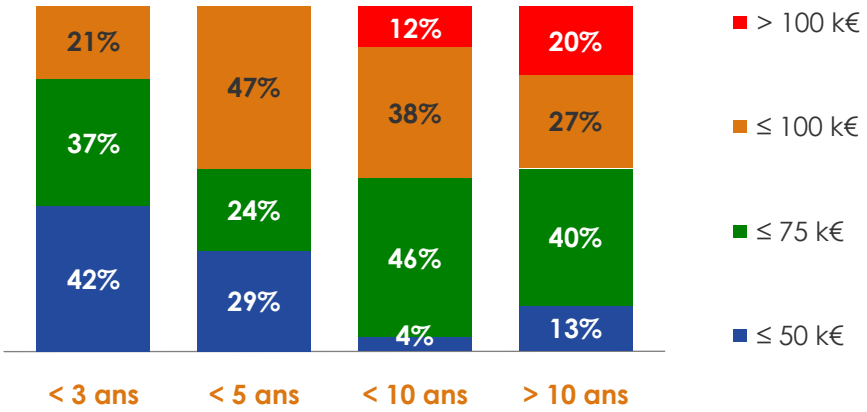


Fig.14

La rémunération et l'expérience en sécurité ou SSI

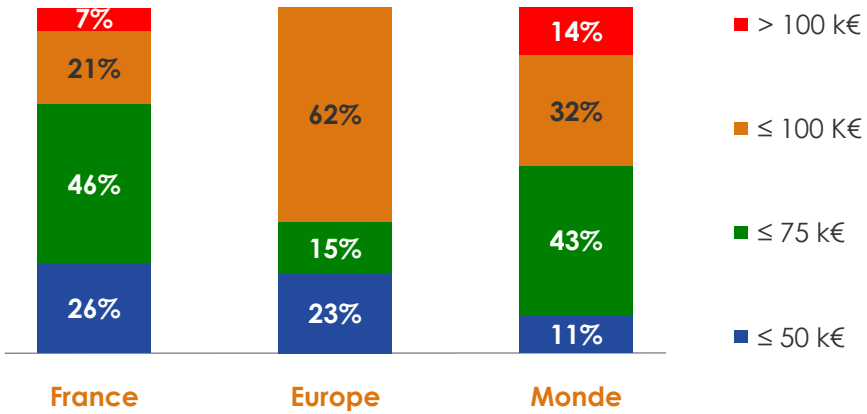


Fig.15

La rémunération et la couverture géographique

La reconnaissance par l'argent ?

La question de la rémunération des professionnels est essentielle. C'est un des éléments qui caractérisent une fonction ou un métier. Aucune étude sur les salaires des cadres ou des informaticiens ne précise réellement la rémunération des RSSI. Souvent la fourchette est large. On lit parfois entre 50 k€ et 100 k€ .

C'est aussi par le salaire que l'on se sent ou que l'on est réellement "reconnu". Et c'est également une mesure simple des coûts de la sécurité. La tendance est forte d'ailleurs de chercher à remplacer des individus par des logiciels qui automatisent des tâches fastidieuses et peu valorisantes.

Les chiffres que nous publions ici sont à prendre avec précaution mais notons quelques points essentiels. La fig.14 montre clairement les proportions de professionnels qui parviennent à obtenir des rémunérations intéressantes sans être très expérimentés. Les plus grosses rémunérations se situent sans surprise dans les grands groupes à dimension internationale.

72% des professionnels n'opérant qu'en France gagnent mois de 75 k € par an alors que 62% de ceux qui couvrent l'Europe gagnent plus de 75 k € par an. Il existe une prime de 10% pour les "européens" et de 18% pour les professionnels oeuvrant à l'international.

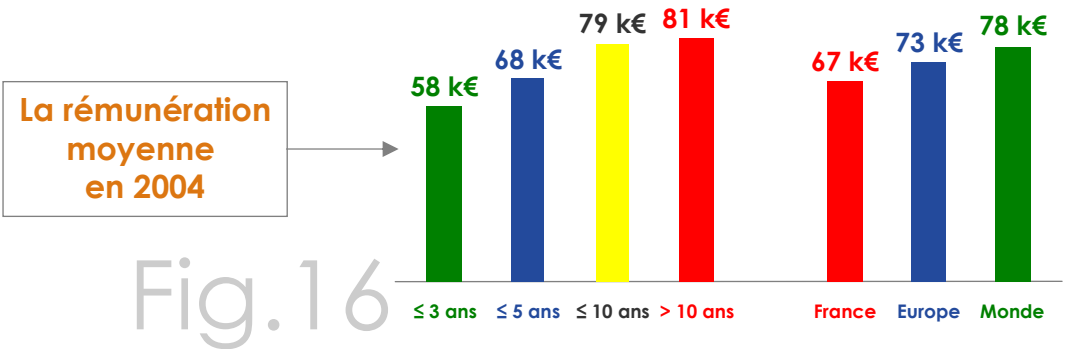


Fig.16

Par exemple, un zoom effectué sur les professionnels du monde banque / assurance met en évidence des salaires moyens supérieurs de 11% à la moyenne globale.

Autre exemple dans le high-tech : les professionnels les moins expérimentés (≤ 5 ans en sécurité) sont rémunérés 7% de moins que la moyenne globale, les plus expérimentés (> 5 ans), 8% au-dessus.

Volet 2

La fonction SSI, sans dessus-dessous

La quête de structuration

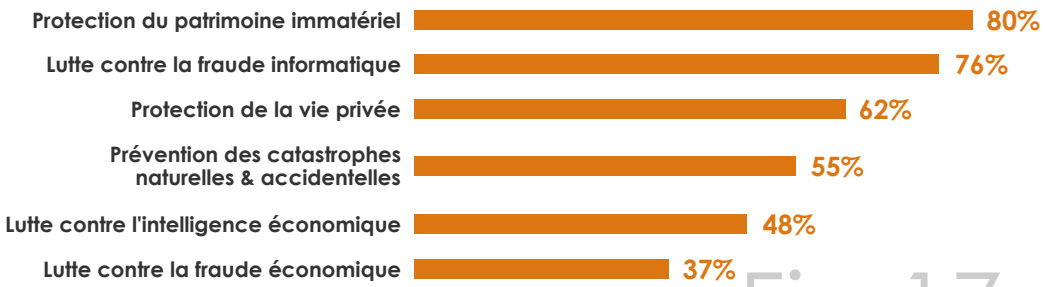


Fig.17

Les enjeux couverts

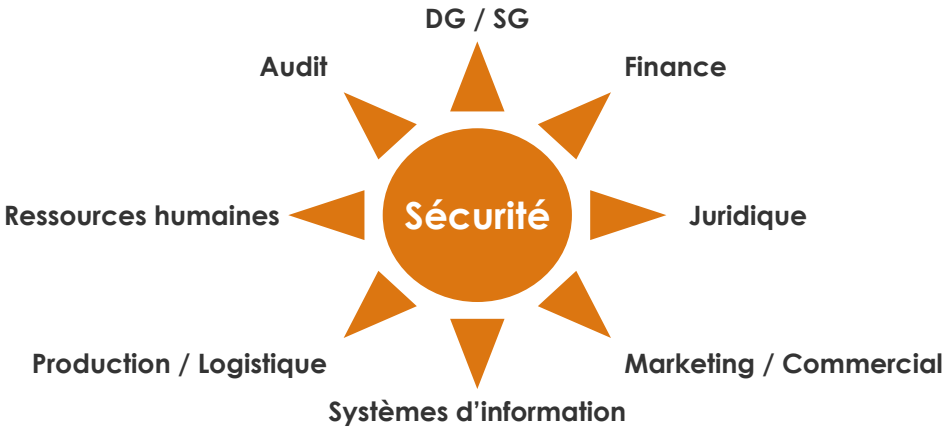


Fig.18

Rayonner sans égocentrisme

La conquête de territoires

Tant que les professionnels s'impliquent dans des questions de sécurité informatique ou de systèmes d'information (lutte anti-virus, plan de secours, étude de risques dans les projets, gestion des accès logiques, etc.), ils offrent un service à leur entreprise, à ses métiers et aux utilisateurs. La dimension "politique" de l'entreprise est finalement peu prédominante. On est d'avantage dans le "processus".

Les professionnels ont parfois à "se battre" pour faire accepter les contraintes de la sécurité. Ils "souffrent" parfois de voir les budgets amputés dans des arbitrages où ils n'ont que peu de place. Mais ils "dérangent" peu. Ils font leur travail, consciencieusement et avec dévouement. Avec les moyens que l'on daigne leur accorder.

Lorsque surviennent les risques liés à l'information elle même, ils prennent une nouvelle dimension. La valorisation du patrimoine et l'intelligence économique, la finance et le monde de la "veille" sont des domaines certes "connexes", et parfois encore éloignés, pour de nombreuses entreprises, des considérations historiques de la sécurité des SI qu'elles soient juridiques ou technologiques.

Lorsque c'est la dématérialisation des processus qui préoccupe, il faut s'impliquer au cœur du fonctionnement des organisations, comprendre les méthodes de travail des métiers, intégrer une dimension économique encore plus forte et parfois parler de "retour sur investissement". Ici, l'expérience des RSSI les plus aguerris dans l'intégration de la sécurité dans les projets leur est fort utile.

On assiste bel et bien depuis 10 ans, à une conquête progressive de territoires qui amène les professionnels de la SSI à s'impliquer bien au-delà du SI lui-même, de ses risques souvent liés d'abord à son infrastructure et aux considérations organisationnelles des projets (fig.17).

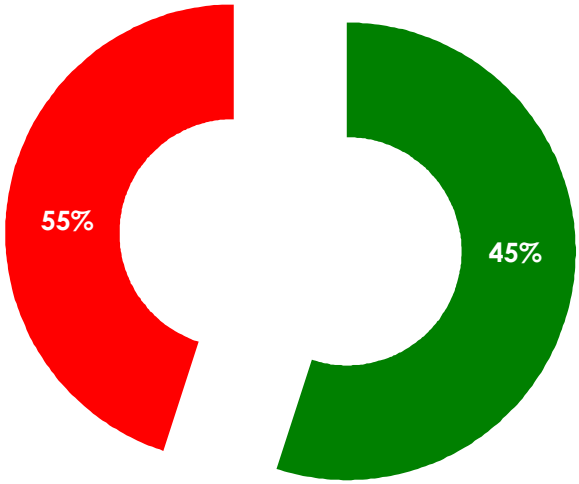
Le danger est alors d'avoir une vision "égocentrique" car les risques et les SI étant désormais omniprésents, la sécurité des SI le serait aussi ! Non, il convient d'être vigilant et de maintenir les métiers de la sécurité dans des rôles de "support" et d' "expertise", certes au sein d'un management, si possible, global et intégré.

La plus belle reconnaissance que peuvent attendre les professionnels, ne réside pas uniquement dans un rattachement hiérarchique ou une ligne budgétaire. C'est dans une implication quotidienne dans des préoccupations majeures des organes de décision. A eux de se faire connaître, reconnaître, accepter, apprécier, recommander. Et de fournir des résultats, … au meilleur coût.

Des zones de friction existeront toujours, ici ou là, en fonction des organisations, des secteurs, des cultures, des hommes. Et si le positionnement au sein d'une DSI ne facilite pas les choses, il ne représente pas un frein incontournable.

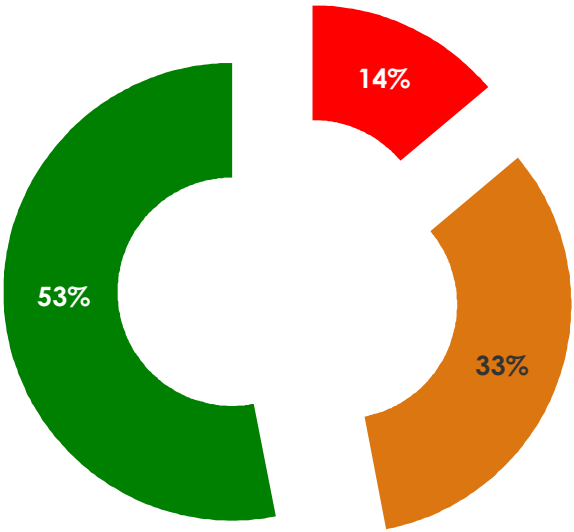
Fig.19

Des délégations minoritaires



Non Oui

La nature des délégations



Pénale Budget Les deux

Fig.20

Un transfert restreint des responsabilités

Supposés "responsables" car dénommés "RSSI", nombre de professionnels n'ont jamais ou très rarement eu les moyens de cette responsabilité. Ces moyens s'entendent dans deux domaines :

- Le juridique : faut-il rappeler la responsabilité civile et pénale des dirigeants au regard de la protection des données personnelles ou du secret des correspondances ?
- Le budgétaire : doit-on rappeler que toute activité "sécurité" n'a de sens qu'associée à un ensemble de mesures techniques et organisationnelles qui s'inscrivent dans des lignes d'investissement et de fonctionnement ?

Nous constatons cette année que la majorité des professionnels (55%) interrogés n'ont aucune délégation de responsabilité formelle. Cette proportion n'est pas liée à la nature du répondant (dédié ou non en SSI). Mais la tendance est apparemment très favorable car en 2003 seuls 17% disposaient d'une telle délégation.

La délégation "pénale" n'est pas une vue de l'esprit. Elle ne peut concerner que des professionnels aguerris. Les secteurs les plus concernés sont l'industrie, la banque / assurance et les télécoms.

En ce qui concerne les budgets, nous tombons ici sur une véritable ambiguïté et un sacré dilemme ! En effet, ce qu'il convient de mettre en place n'est autre qu'un pilotage des dépenses dûment affectées aux bons acteurs. Ces budgets ne pouvant émaner que de décisions au niveau de l'entreprise : c'est-à-dire d'une fonction "régulatrice", indépendante, qui balance l'ampleur des investissements avec les risques mesurés.

Ce régulateur aidé des analystes voire des architectes n'est pas fondamentalement responsable du "comment" seront employés ces moyens budgétaires. Et aussi s'ils seront efficaces, le moment venu. Il sera responsable de les avoir dimensionnés et attribués, puis de contrôler leur usage. Il n'est d'évidence pas Responsable de la Sécurité du SI !

C'est ici que le positionnement des fonctions de "régulateur" et d' "auditeur" au sein de la DSI posera toujours problème. Les coupes budgétaires laisseront peu de marge de manoeuvre si le DSI applique, car on le lui impose, un fâcheux "moins 20 %".

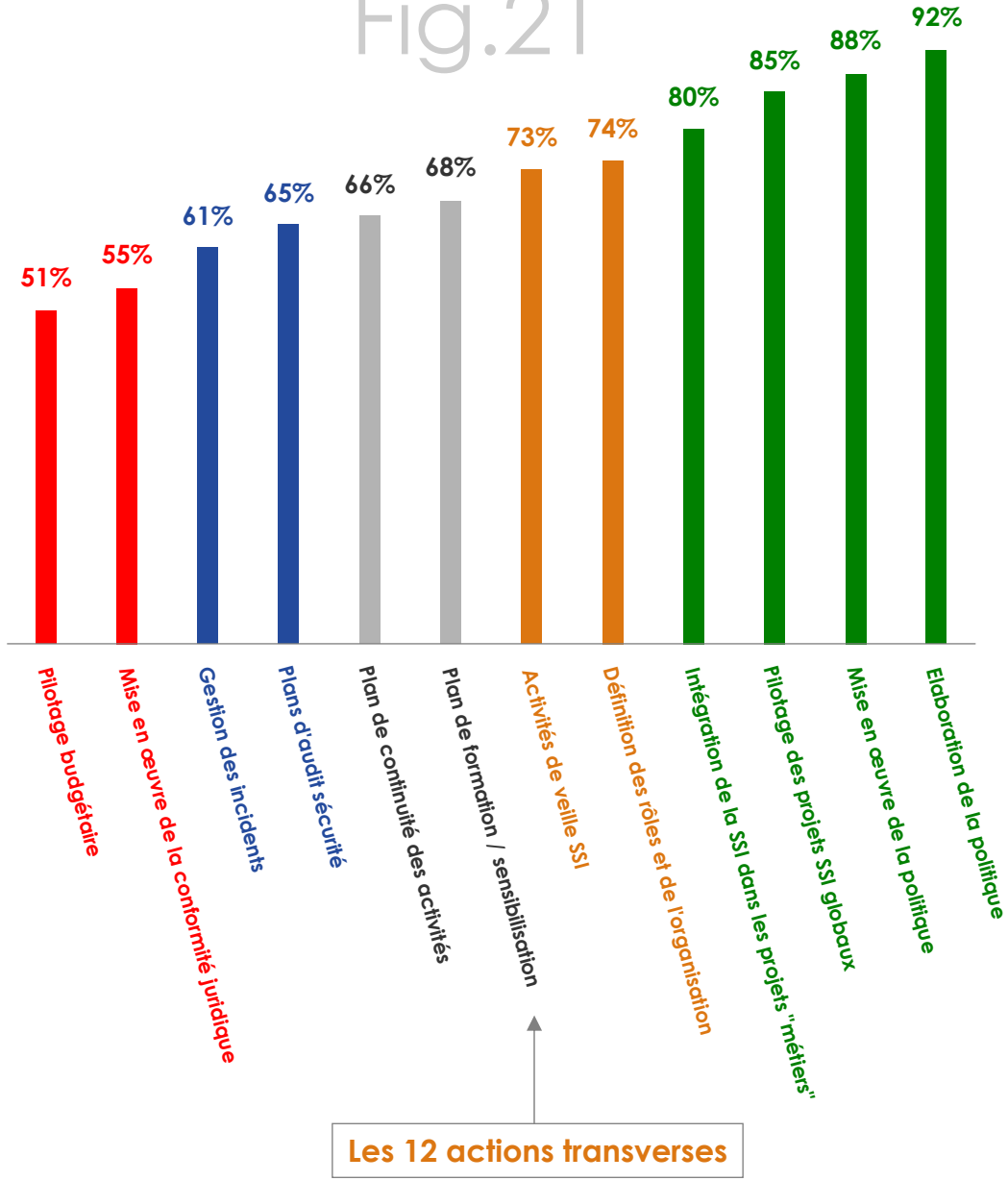
"Je me suis fixé comme priorité de faire comprendre et de concrétiser qu'un budget sécurité ne correspond plus à un centre de coût mais à un centre de profit."

Patrick Langrand

RSSI Natexis Groupe Banques Populaires

35

Fig.21



Les 12 actions transverses

L'importance du pilotage

Le management de la sécurité comporte de nombreux domaines d'activités qui méritent qu'on s'y attarde un peu. Comme nous avons coutume de le dire, il n'y a pas deux RSSI qui se ressemblent. Il s'avère donc utile de mesurer quelles sont les actions "transverses" a priori plus de leur ressort qu'ils assument en 2004. Il va de soi que dans le temps, et en fonction de la maturité et des priorités fixées au sein de chaque entreprise, certaines seront prépondérantes par rapport à d'autres.

En 2004, les dimensions **"politique"** et **"projet"** se placent indiscutablement en tête des activités des professionnels. Avec 80% ou plus des réponses, l'élaboration et la mise en œuvre d'une politique de sécurité ainsi que le pilotage des projets SSI globaux et l'intégration de la sécurité dans les projets métiers sont indiscutablement au cœur de leur fonction où ils tiennent avant tout un rôle de "conseil".

Ces quatre actions (en **vert**) sont suivies par deux autres (en **orange**) où l'attribution des rôles, des responsabilités et la mise en place de processus d'information et de reporting sont essentiels. La coopération avec la fonction "qualité" s'avère ici importante.

Suivent deux actions (en **gris**) impliquant fortement les "métiers" : la **formation / sensibilisation** et la **continuité des activités**. Egalement très proches de la démarche qualité & projets, ces actions consistent à développer une culture et à impliquer chaque acteur au bon moment : avant, pendant ou après un incident.

Nous trouvons ensuite deux actions plus ponctuelles (en **bleu**). Nous analyserons plus loin l'action concrète des professionnels dans ces domaines.

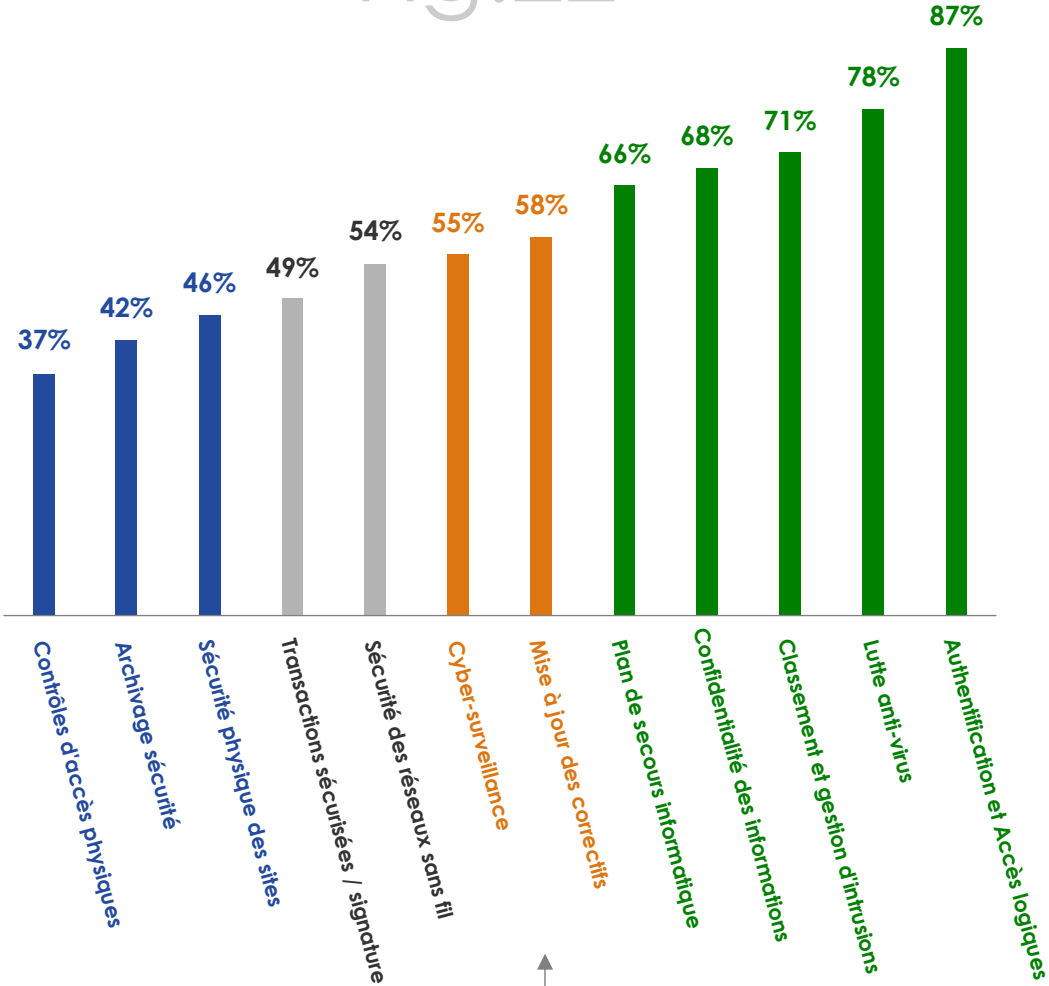
Le pilotage budgétaire et la mise en conformité juridique se situent en queue de peloton avec un peu plus de 50 %. Sans que ce soit une surprise, on constate néanmoins que déjà la moitié du panel s'implique dans une **"démarche juridique et économique"** renforcée. C'est ici qu'apparaît le plus fortement la dimension du "risk management" qui doit s'inscrire dans une chaîne de responsabilités clairement établies et dans une logique économique permanente.

Un professionnel sur 2 s'intègre dans une démarche de "risk management des SI".

Ces 12 actions traduisent l'activité de pilotage de la fonction "SSI". Elles militent d'évidence pour un management global, centralisé, renforcé et efficace. La complexité des problématiques et les difficultés de mise en pratique de concepts aujourd'hui maîtrisés méritent des professionnels compétents et reconnus en interne comme en externe à leur entreprise.

37

Fig.22



Les 12 processus opérationnels

L'action de terrain

Une des grands difficultés des professionnels est de bien positionner leurs actions de pilotage et celles plus techniques où ils sont directement impliqués dans des processus de sécurité. C'est la lancinante question du positionnement des fonctions sécurité au plan de la "stratégie" ou de l' "opérationnel".

7% des professionnels ne sont impliqués dans aucune action opérationnelle.

Il n'est pas aisé de dresser une typologie des processus de sécurité. Nous en avons retenu 12 cette année. Quatre d'entre eux sont assurés par moins d'un professionnel sur deux. Les aspects de sécurité physique sont encore insuffisamment associés aux aspects "logiques" de l'informatique et de l'information. Nous reviendrons plus loin sur l'ampleur et la nature des synergies nouées entre les professionnels de la SSI et les services généraux.

Environ un professionnel sur deux s'implique dans des actions émergentes et critiques pour l'avenir comme la sécurité des transactions et le développement de la signature électronique, la sécurité des réseaux sans fil, la mise à jour des correctifs et la cyber-surveillance. A chacun d'apprécier si c'est encourageant ou pas (notamment pour la signature et la mise à jour des correctifs) tant ce sont des sujets majeurs qui touchent à la "confiance" dans les infrastructures ou dans les échanges dématérialisés.

Les cinq premiers processus sont caractéristiques de la sécurité des SI "historique" et au moins 2/3 des professionnels s'impliquent dans leur mise en œuvre. Remarquons simplement que 66% des professionnels travaillent sur les plans de continuité (qui sont des projets d'entreprise orientés "business") et autant dans les plans de secours informatiques. Ils servent en quelque sorte de lien de "circuit de transmission" entre les exigences des métiers et les capacités de secours de la DSI. Mais remarquons aussi qu'1/3 des répondants ne s'occupe pas de ces sujets.

Les questions de confidentialité des informations deviennent une exigence de plus en plus forte alors que s'animent les débats sur la vie privée et l'intelligence économique. Plus des 2/3 des répondants sont actifs dans ce domaine sur lequel nous reviendrons plus loin.

NOTA : Un filtre appliqué sur les professionnels dédiés à la SSI montre une croissance de 4 à 5% environ des statistiques concernant le panel global avec 2 singularités. La croissance est de 8% environ pour la cyber-surveillance (64 % contre 55%) et la confidentialité des informations (76% contre 68%). Cela tend à démontrer que la fonction "SSI" lorsqu'elle est dédiée s'intéresse à des questions plus "sensibles" et orientées "contenus".

Les activités de veille en SSI

Fig.23

La veille est devenue une des activités essentielles pour les professionnels de la SSI. Elle est surtout assez complexe à structurer, organiser, planifier pour garantir des résultats utiles. On a par ailleurs souvent tendance à ne la considérer que sous l'angle "technologique" (suivi des failles et des correctifs, étude des outils, etc.).

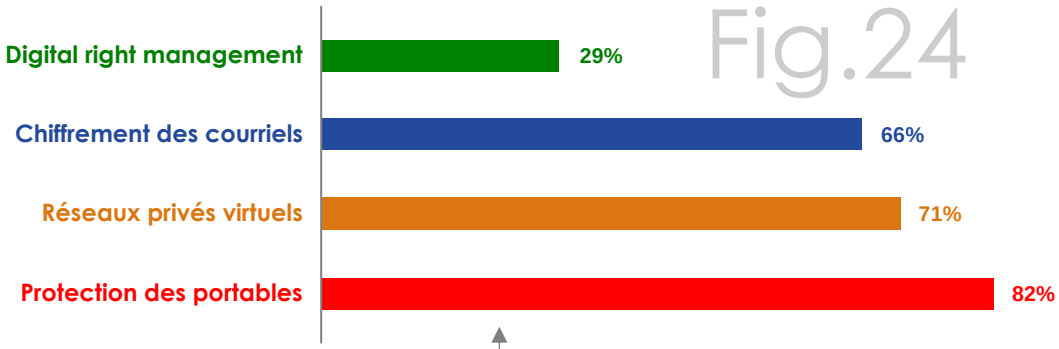
Or, elle s'adresse à au moins quatre grands domaines allant de la menace au cadre légal. Il ne faut pas oublier que les actions de sécurité ne prennent de sens qu'à partir d'une évaluation de risques elle-même issue d'une analyse de la menace et dans un cadre juridique de plus en plus omniprésent et international.

Les professionnels de la SSI ne s'impliquent que partiellement dans ces actions, souvent par manque de temps, par délégation, parfois, auprès d'experts internes ou externes (services spécialisés, associations, presse, sites, web, etc.). Il est réconfortant de constater que la veille sur les menaces est en tête.

Le schéma ci-dessus montre une baisse entre 2003 et 2004 à l'exception de la veille juridique qui progresse. Peut-être un signe de délégation plus importante.

Les questions de plus en plus stratégiques concernant la veille et l' "intelligence" sur la sécurité doivent conduire les professionnels à se poser clairement la question de leurs actions dans ce domaine (cf : rapport du député Bernard Carrayon).

Zoom "confidentialité"



La confidentialité des informations

76 % des professionnels sont impliqués dans des actions de protection des informations confidentielles. Au-delà des mesures physiques et comportementales, nous constatons que les **ordinateurs portables** sont les plus sensibles et qu'ils focalisent l'attention. Combien de dirigeants, de cadres commerciaux ou financiers n'ont pas vu disparaître leur outil de travail, dans un bureau, une voiture, un hôtel, etc. ? Certes la parade technique ne suffit pas, mais il vaut tout de même mieux qu'elle existe, lorsque "le jeu en vaut la chandelle".

NOTA : En 2001, il fut retrouvé en 6 mois 2900 ordinateurs portables, 1300 PDA et 62000 téléphones portables dans les taxis londonniens !

Avec 71% des réponses, les **réseaux privés virtuels** répondent aussi à cette exigence. Néanmoins, beaucoup pensent que les "VPN" répondent d'abord à des questions économiques avant de protéger des informations sensibles. Les professionnels de la SSI s'impliquent très étroitement dans les actions de sécurité des réseaux et il est normal de retrouver les VPN à de niveau.

La **messagerie électronique** est devenue un outil de travail incontournable et elle véhicule de plus en plus de données sensibles, parfois stratégiques. Il est naturel que les professionnels de la SSI se préoccupent, avec les utilisateurs, de la protection de cette application majeure. La protection de la messagerie préoccupe 2/3 du panel.

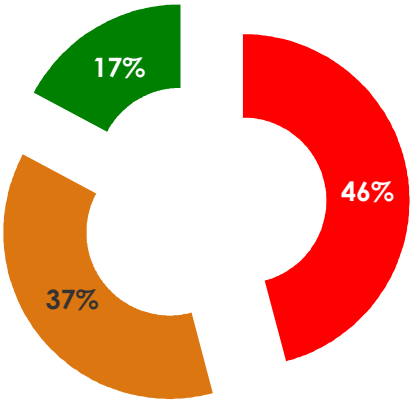
Enfin, nous noterons que 29% des répondants s'intéressent désormais aux mécanismes de **"gestion des droits numériques"** qui ne s'appliquent pas à une "donnée" ou une "transaction" au sein d'une application informatique mais aux contenus quels qu'ils soient : page web, pièce jointe, contenu de courriel, image, fichier vidéo, … C'est un axe de développement majeur du marché où la cryptographie joue un rôle essentiel.

Zoom "investigation"

Fig.25

Les investigations en SSI

- Recherche de preuves
- Evaluation économique
- Les deux



42 % des professionnels sont impliqués dans des investigations liées à des incidents et des attaques. C'est le signe d'une réalité non négligeable mais qui ne permet ici de dire comment aboutit l'investigation. Nous verrons plus loin comment ils les traitent au plan juridique.

Certains professionnels de la SSI se comportent comme des "limiers" apportant des éléments de preuve par de l'analyse et de la corrélation de traces : Qui a fait quoi ? Quand ? Comment ? A partir d'où ? Plusieurs faits relatés dans les médias montrent que des faits de sabotages (dénis de service, mail bombing, etc.), des piratages ou des intrusions ont trouvé des issues favorables aux victimes.

Mais il est remarquable de constater qu'ils doivent aussi tenter de faire une évaluation économique de l'attaque, qui seule permettra d'envisager une poursuite judiciaire et d'éventuels dommages et intérêts.

Cette évaluation permet aussi, a posteriori, de rentrer dans une recherche d'efficacité des moyens financiers mis en œuvre, à supposer qu'on les maîtrise par un pilotage solide et consolidé des budgets.

NOTA : Les enquêtes du CSI/FBI (www.gocsi.com) montrent depuis plusieurs années l'ampleur des cyber-attaques. Depuis 2 ans, les impacts économiques baissent significativement : -56% entre 2003 et 2002, -30% entre 2004 et 2003 pour se fixer à 141 M$.

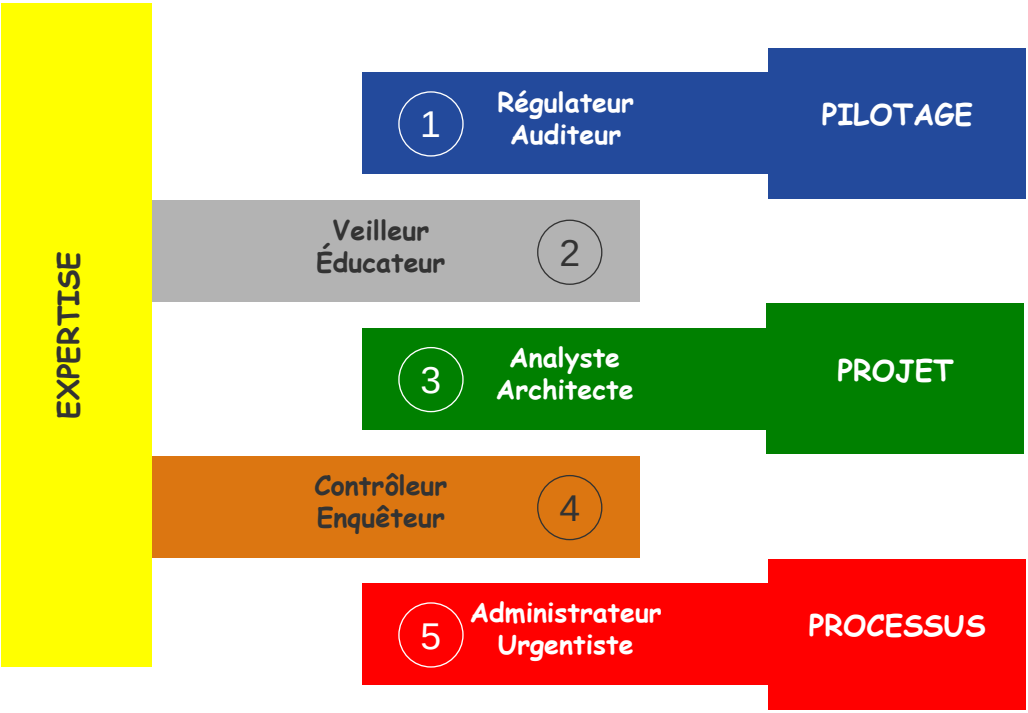
"Un fichier log seul n'est pas une preuve mais un éléments probatoire."

Didier Gras
Responsable sécurité Noos

Volet 3

L'integration dans l'entreprise

Des synergies se nouent…
… mais dans la difficulté



Dans son dossier "spécial emploi" du 12 mars 2004, 01 Informatique a proposé deux définitions de poste : le RSSI et l'Ingénieur sécurité. Nous les reprenons ci-dessous à titre de rappel. On notera la similitude des 2 fonctions.

"RSSI : Il effectue une **veille** technologique et réglementaire et **propose les évolutions** garantissant la sécurité logique et physique du SI. Susceptible d'intervenir directement sur tout ou partie des systèmes informatiques et télécoms de son entreprise, il joue un rôle de **conseil**, d'assistance, d'information, de **formation** et d'**alerte**. Il est généralement rattaché à la fonction informatique."

"Ingénieur Sécurité : Il effectue une **veille** technologique et a pour mission d'**évaluer** le niveau de vulnérabilité des systèmes d'information et de **proposer des solutions** pour les sécuriser. Il assure une fonction de **conseil**, d'assistance, d'information, de **formation** et d'**alerte** dans son domaine d'expertise. Il travaille dans les SSII ou dans les grandes entreprises utilisatrices, où il joue le rôle d'**interface** avec les spécialistes externes de la sécurité."

Mais de toute évidence, ces deux postes ne répondent pas à l'ensemble de la problématique.

Les 5 fonctions clés de la SSI

L'intégration de la fonction SSI s'exerce de multiples façons et au travers de nombreux acteurs. Il n'y a pas que le RSSI qui importe. L'analyse des rôles assurés par les professionnels de la SSI permet de dresser une typologie en 5 "fonctions clés". Comme les 10 rôles, elles aident les professionnels à se situer, au quotidien comme dans leur parcours professionnel et dans leur positionnement dans l'entreprise.

LE PILOTAGE (régulateur / auditeur) : C'est une fonction de **"direction"** dont la principale mission est d'être le "chef de bord" du management des cyber-risques. Elle se concrétise d'une part par une Politique de Sécurité (un référentiel), d'autre part, par un plan d'audit des risques liés au SI. Elle est dévolue à des professionnels aguerris, aux bonnes bases techniques et financières, et ayant la fibre du management. Il doit être un meneur d'hommes et un bon communicateur.

L'EXPERTISE "AMONT" (veilleur / éducateur) : C'est une fonction d' **"aide à la décision"** dont la principale mission est d'observer et de faire passer des messages en développant la culture de la SSI. Elle est dévolue à des professionnels aguerris qui doivent être crédibles et très bon communicateurs. Elle peut être sous-traitée mais sous la maîtrise de la fonction de "Pilotage".

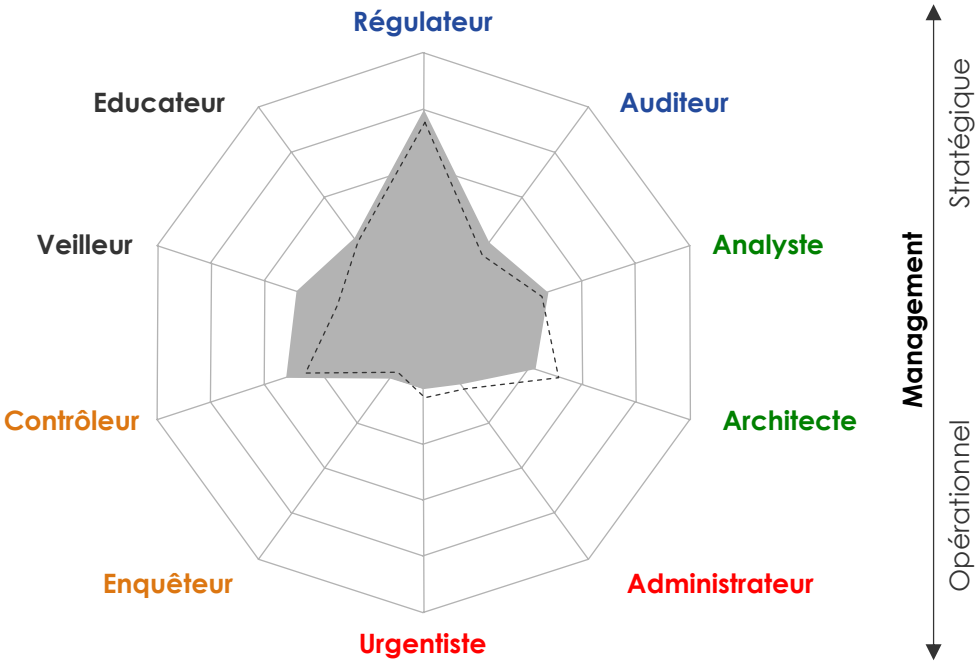
LES PROJETS (analyste / architecte) : C'est une fonction d' **"ingénierie"** dont la principale mission est d'être concepteur de moyens adaptés aux risques dans le respect de la politique. Elle est assumée par des professionnels aux bases techniques et méthodologiques très solides. Ils sont à l'écoute des clients, férus de technologies, et créatifs. Leur externalisation totale auprès de SSII ou de cabinets spécialisés est un dilemme car l'entreprise perd alors son indépendance.

L'EXPERTISE "AVAL" (contrôleur / enquêteur) : C'est une fonction émergente qui, bien qu'opérationnelle, est proche du "pilotage". Elle doit produire des indicateurs et des **"tableaux de bord"** sur l'état de la sécurité (au quotidien et dans le cadre des incidents). Elle travaille étroitement avec l' "analyste-architecte" et l' "administrateur-urgentiste" pour garantir une remontée d'informations fiables, au bon moment.

LES PROCESSUS (administrateur / urgentiste) : C'est une fonction purement **"opérationnelle"** dont le rôle est d'opérer au quotidien les moyens mis en œuvre dans le respect des règles et des procédures tirées de la Politique. Elle est assumée par des professionnels de devoir et très fiables (disponibilité, éthique). La sensibilité des opérations qu'ils mènent et les pouvoirs conférés à leur mission obligent l'entreprise à les contrôler étroitement. Le recours à des SSII ou des intégrateurs spécialisés est possible en veillant à leur formation et en requérant éventuellement une certification individuelle.

Tous les métiers de la sécurité possèdent de telles fonctions. L'avenir des professionnels peut-il s'envisager sans cet effort de clarification ?

Fig.26



Ensemble du panel

RSSI et équivalents

Positionnement "moyen" des 5 fonctions clés

Les 5 fonctions clés de la SSI

Le schéma de la fig.26 propose une grille d'analyse des rôles assumés par les professionnels. Les répondants à l'enquête 2004, tout comme les autres, peuvent se positionner par rapport à ces moyennes que nous rappelons ci-dessous.

LE PILOTAGE : la direction de la gestion des cyber-risques

Ensemble du panel	Professionnels dédiés
Régulateur = 76 %	Régulateur = 80 %
Auditeur = 35 %	Auditeur = 40 %

L'EXPERTISE "AMONT" : l'aide à la décision sans laxisme ni paranoïa

Ensemble du panel	Professionnels dédiés
Veilleur : 33 %	Veilleur : 48 %
Educateur : 41 %	Educateur : 42 %

LES PROJETS : l'ingénierie des solutions adaptées aux risques évalués

Ensemble du panel	Professionnels dédiés
Analyste : 44%	Analyste : 47%
Architecte : 50 %	Architecte : 42 %

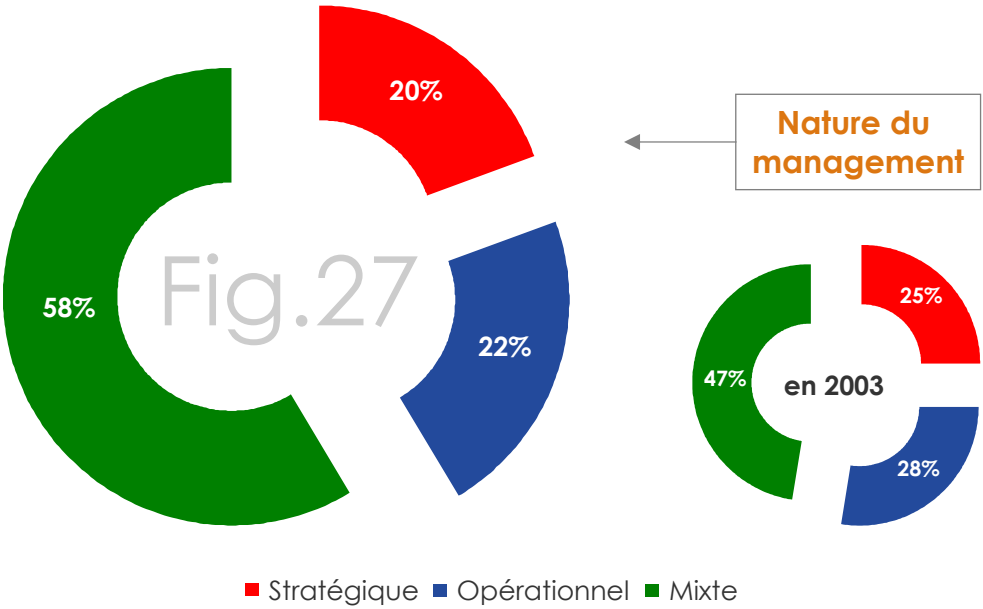
L'EXPERTISE "AVAL" : la cyber-surveillance et l'investigation

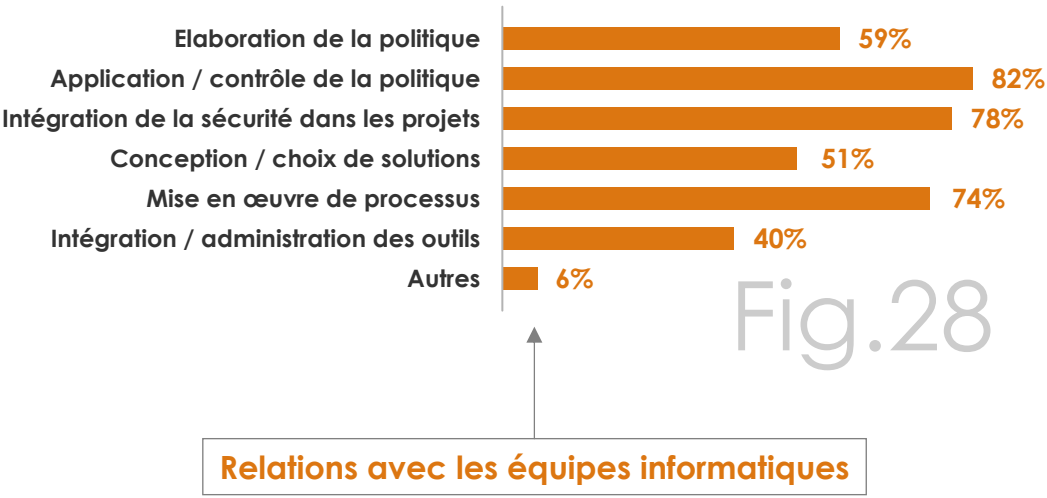
Ensemble du panel	Professionnels dédiés
Enquêteur = 17 %	Enquêteur = 20 %
Contrôleur = 45 %	Contrôleur = 52 %

LES PROCESSUS : l'application quotidienne des règles et des procédures

Ensemble du panel	Professionnels dédiés
Administrateur = 24 %	Administrateur = 23 %
Urgentiste = 23 %	Urgentiste = 20 %

47


20%
58%
22%
Fig.27
Nature du management
25%
47%
en 2003
28%
Stratégique
Opérationnel
Mixte


Elaboration de la politique 59%
Application / contrôle de la politique 82%
Intégration de la sécurité dans les projets 78%
Conception / choix de solutions 51%
Mise en œuvre de processus 74%
Intégration / administration des outils 40%
Autres 6%
Fig.28
Relations avec les équipes informatiques

Un positionnement toujours ambiguë

Un des critères permettant de mesurer si la fonction "SSI" est bien intégrée au sein d'une entreprise est tout simplement de mesurer si celui ou celle qui "détient les rennes" a un droit d'accès aux comités de direction. On constate qu'en 2004 :

54 % des professionnels interviennent effectivement en Comité de direction.

Au-delà de ces interventions plus ou moins ponctuelles et sur des sujets très variés (budgets, retour sur incident, lancement de projet important, etc.), il convient aussi de regarder la nature du management mené par les professionnels. On constate cette année une évolution intéressante par rapport à 2003.

En effet, la part du management "stratégique" diminue au profit du management "mixte". C'est-à-dire que les professionnels sont de manière encore plus flagrante des intermédiaires entre les décideurs et les responsables d'activité et en particulier les équipes informatiques.

C'est la vision optimiste par laquelle, la SSI justifie son existence en comblant un manque. "Que se passerait-il si nous n'étions pas là ?"

Mais ce management "mixte" est porteur d'ambiguïté et de malaise pour certains. N'est-on pas un peu trop "juge et partie" ? Ou pire des "faire valoir" ? On n'est ni vraiment décideur, ni vraiment acteur de la sécurité ! Si on définit une politique, jusqu'où s'impliquer dans sa mise en œuvre ? Comment est-on audité ? Et par qui ? Si on ne gère ni les budgets, ni les équipes opérationnelles, en quoi est-on responsable de la sécurité ?

La coopération avec les équipes informatiques est ici d'une première importance. On constate effectivement que les synergies sont fortes (plus de 70% de réponses) aux 3 degrés du management : politique / projet / processus. Les équipes informatiques sont, à juste titre, assez impliquées dans l'élaboration de la politique, vue ici dans un sens sans doute large dépassant la directive ou la règle (configurations des systèmes et des réseaux).

Les questions d'architecture (conception/intégration/administration) ne viennent qu'en second plan (entre 40 et 50%). Ce constat est cohérent avec les rôles assumés par les professionnels. Il est très rare, enfin, que les professionnels soient des fournisseurs d'outils pour la DSI.

Notons aussi des positions intéressantes sur cette collaboration : certains RSSI affirment aider les informaticiens à "vendre" leurs attentes et leurs projets auprès du management, chose qu'ils ont parfois du mal à faire. D'autres interviennent conjointement et étroitement dans la gestion de crise et dans des audits.

Fig.29

Collaboration avec un correspondant "données personnelles"

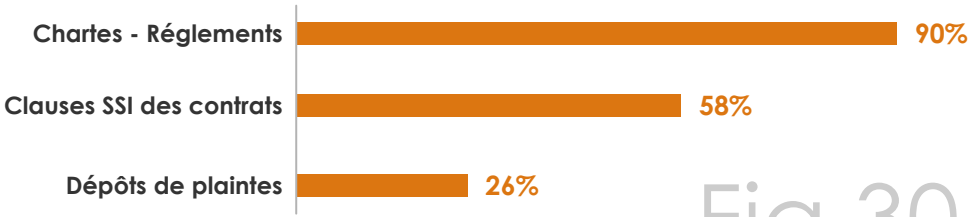


Fig.30

Collaboration avec les équipes juridiques

Zoom "juridique"

La protection des données personnelles est une des premières justifications (juridiques) de la sécurité des SI. Veiller aux déclarations, à des collectes et des traitement licites ne concerne pas directement la fonction SSI. Mais assurer la protection des données et garantir un droit d'accès rentrent dans son périmètre. Cette dimension prend un visage nouveau lorsque dans la lignée des rapports de la CNIL sur la cyber-surveillance, il est stipulé dans la loi votée le 6 août 2004 que les entreprises devraient créer la fonction de "délégué à la protection des données personnelles". Alors que rien n'est encore défini sur son détenteur, on constate que :

42% des professionnels collaborent avec un correspondant "données personnelles".

Cette collaboration ne s'exerce pas exclusivement au plan de la déclaration (près de 20% des répondants ne le font d'ailleurs pas). Elle s'étend surtout à tous les moyens de protection utiles. La fonction SSI intervient ici encore comme une "fonction intermédiaire" entre une exigence et un moyen. Moins d'un répondant sur deux participe à la définition des moyens de protection. Enfin, il est remarquable qu'une minorité (un peu plus d'un tiers) s'implique jusqu'aux audits des moyens de protection.

La collaboration de la fonction SSI et des services juridiques paraît aussi évidente tant les exigences de sécurité trouvent leurs justifications dans des textes législatifs et réglementaires. Or, dans la pratique, ils se sont longtemps observés, ignorés parfois et coopèrent plutôt sous la contrainte. En 2004, signe encourageant,

76% des professionnels collaborent avec les services juridiques.

Cette collaboration concerne très largement l'élaboration des chartes et des règlements intérieurs sur l'utilisation et la sécurité du système d'information. Le début des années 2000 a vu se multiplier ces démarches et il n'est pas surprenant que 9 répondants sur 10 travaillent en synergie avec les services juridiques sur ce thème.

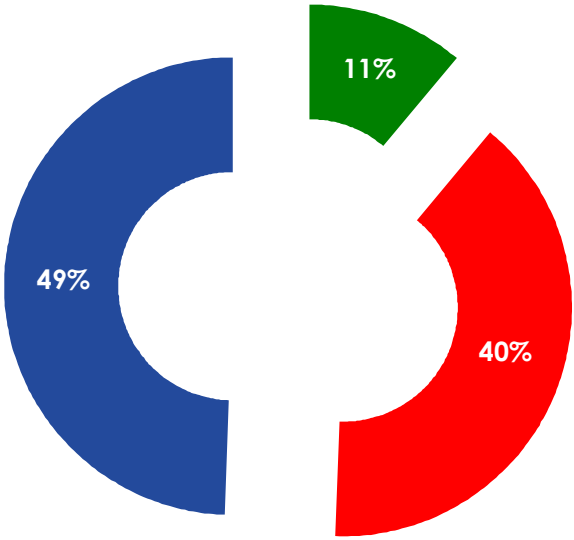
La dimension contractuelle prend elle aussi une importance accrue. L'externalisation du SI, la dématérialisation sont deux facteurs qui poussent les entreprises à "blinder" leurs contrats en termes de sécurité. Les questions de continuité et de confidentialité sont essentielles à cet égard.

Enfin, notons que les dépôts de plainte intéressent environ un quart des répondants. Cela ne signifie pas qu'ils déposent plainte systématiquement, après analyse et réflexion. Ce chiffre est à rapprocher de l'enquête du CSI/FBI qui nous apprend que 48% des 320 répondants de 2004 ne font aucun reporting des incidents (essentiellement pour des raisons d'image de marque et de publicité négative) et que seulement 20% déposent plainte.

51

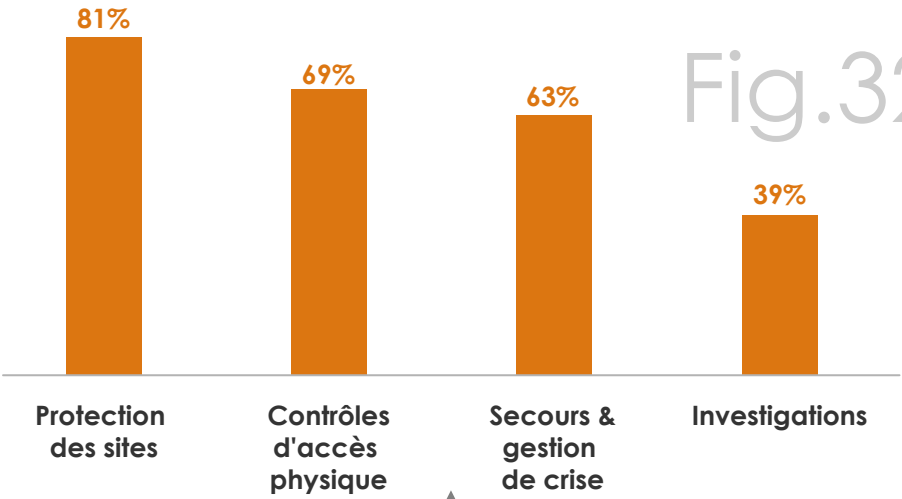
Fig.31

Collaboration avec la "sécurité physique"



Très étroite ■ Ponctuelle ■ Jamais

Fig.32



Nature de la collaboration avec la "sécurité physique"

Zoom "sécurité physique"

Séparer le management de la sécurité "logique" des aspects "physiques" est fréquemment dénoncé, à la fois par le bon sens et par l'expérience quotidienne. La synergie est fondamentale en amont de la démarche lors de l'élaboration de la cartographie des risques, et souvent en aval, lors d'investigations.

Et pourtant, bon nombre d'entreprises continuent de laisser les services généraux s'occuper de la téléphonie (donc des abonnements télécoms), de faire gérer les systèmes d'accès physiques (qui sont aussi un système d'information sensible) par des sociétés tierces.

Le regroupement du management de la sécurité physique et logique est également important lors des investigations : localisation d'un individu sur un site (via son badge ou une vidéosurveillance). Si ce management n'est pas intégré au sein d'une Direction centrale, il est au minimum utile que des liens étroits soient établis. En 2004, le constat est très mitigé car :

4 professionnels sur 10 collaborent étroitement avec la sécurité physique.

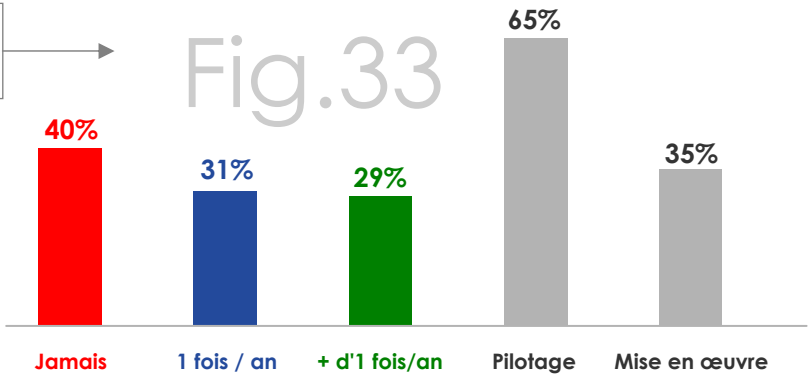
Le schéma de la fig.22 (les 12 processus opérationnels) démontre d'une autre façon cette séparation encore majoritaire.

Les professionnels qui travaillent avec les équipes des services généraux se focalisent (81%) d'abord sur la protection physique des sites (informatiques) pour tenir compte des menaces environnementales. Il est surprenant que la coopération sur les plans de secours et la gestion de crise (plus réactive) ne soient pas au même niveau. La prévention apparaît plus importante que la capacité à réagir à des sinistres.

Enfin, les questions d'investigation intéressent 39% du panel. C'est un chiffre significatif qui démontre que dans l'urgence, il est fort utile de savoir dialoguer et échanger de l'information. La réalité des incidents qu'ils soient matériels ou immatériels, démontre que leur gestion nécessite des professionnels aguerris et maîtrisant l'organisation interne des entreprises, en plus d'un profond sens du devoir.

Encore une fois, si un management intégré du physique et du logique présente des avantages évidents, faute de mieux, c'est par la capacité des professionnels à se connaître et à coopérer que les entreprises parviendront à améliorer leurs actions de prévention et de réaction.

Coopération avec l'audit



Des évènement récents (affaires Enron, WorldCom, etc.) ont démontré à quel point la confiance que l'on pouvait accorder à certains acteurs supposés indépendants devait être limitée.

De nombreux audits de sécurité des SI sont encore réalisés par des sociétés qui ne brillent pas non plus par leur autonomie vis-à-vis des fournisseurs de solutions. C'est ainsi, mais il faut le rappeler de temps à autre. **La vraie question est "qui est légitime pour auditer la sécurité d'un SI ?"**

Le RSSI est dans la grande majorité des cas, bien mal placé. Et les équipes d'audit interne ne disposent pas, généralement, des compétences techniques nécessaires. Elles apportent néanmoins une maîtrise méthodologique et une rigueur indépendantes de la nature du risque.

Nous avons vu qu'environ 1/3 des professionnels se reconnaissait un rôle d'auditeur de la SSI. C'est le fait des acteurs indépendants de la DSI qui s'intégrent dans un management de nature "stratégique" et non "opérationnel". Ils sont encore peu nombreux. Il est ici remarquable que :

40% des professionnels ne collaborent jamais avec l'audit interne.

Les professionnels sont néanmoins majoritairement impliqués dans le pilotage des recommandations d'audit. L'évolution de la fonction SSI en entreprise se doit d'améliorer les processus d'audit, notamment en les distinguant du contrôle permanent. Le recours à des prestataires réellement indépendants, expérimentés et demain individuellement certifiés sera sans doute requis.

NOTA : en 2004, l'étude du CSI/FBI indiquait qu'aux USA, encore 20% du panel d'entreprises américaines ne pratiquent pas d'audit en SSI.

Volet 4

Les ressources humaines, cles de la reussite

La mobilisation des troupes

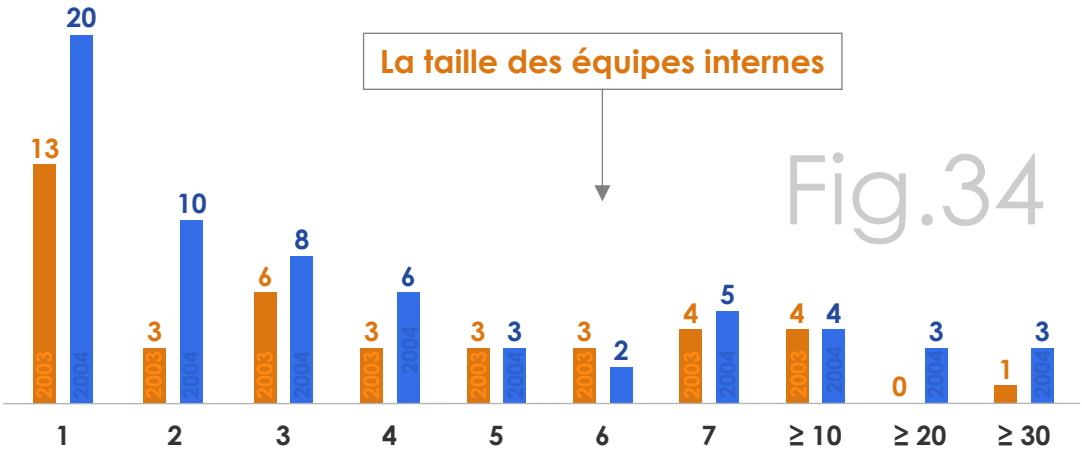

La taille des équipes internes
2003
2004
13
20
3
10
6
8
3
6
3
3
3
2
4
5
4
4
0
3
1
3
1
2
3
4
5
6
7
≥ 10
≥ 20
≥ 30

Fig.34

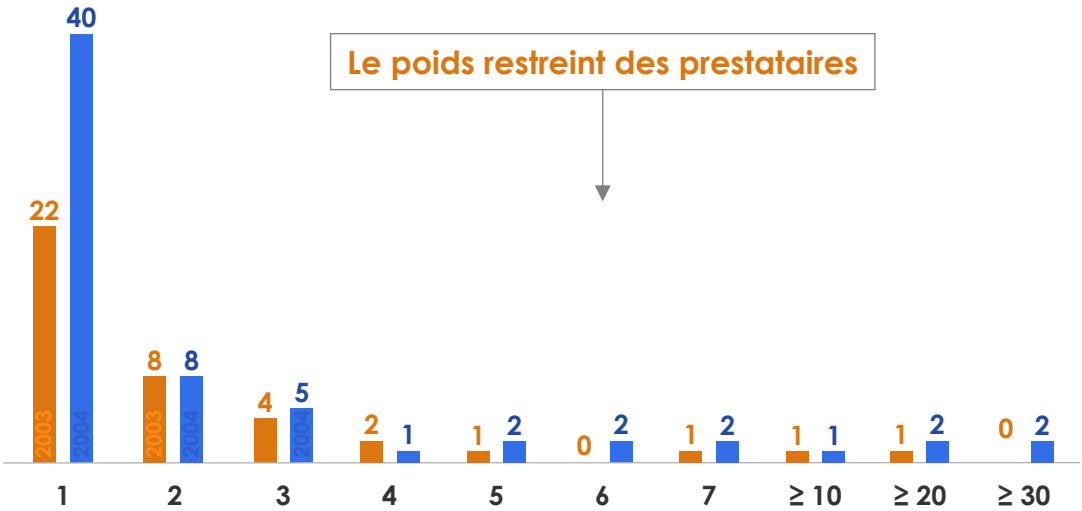

Le poids restreint des prestataires
2003
2004
22
40
8
8
4
5
2
1
1
2
0
2
1
2
1
1
1
2
0
2
1
2
3
4
5
6
7
≥ 10
≥ 20
≥ 30

Fig.35

Une forte internalisation

Le panel de 2004 représente 496 professionnels soit une moyenne de 7,7 personnes par entreprise. En 2003, la moyenne s'établissait à 6,4 personnes.

La taille moyenne des équipes "SSI" en entreprise est en progression de 20%.

Les équipes internes représentent 6,1 collaborateurs en moyenne (393 professionnels) contre 5,1 en 2003. Les prestataires représentent 1,6 collaborateurs (103 professionnels) contre 1,3 en 2003. On constate que la part des prestataires augmente de manière similaire (23% contre 20%) aux recrutements internes.

La part des prestataires SSI ne subit apparemment pas de réduction sous le double effet :

- de l'internalisation de fonctions sensibles
- de la pression économique et des arrêts de mission au sein des DSI

La fonction SSI ne souffre pas des mêmes pressions que les fonctions informatiques, mais les disparités sont très fortes (fig.34 & fig.35) et quelques singularités doivent être mentionnées.

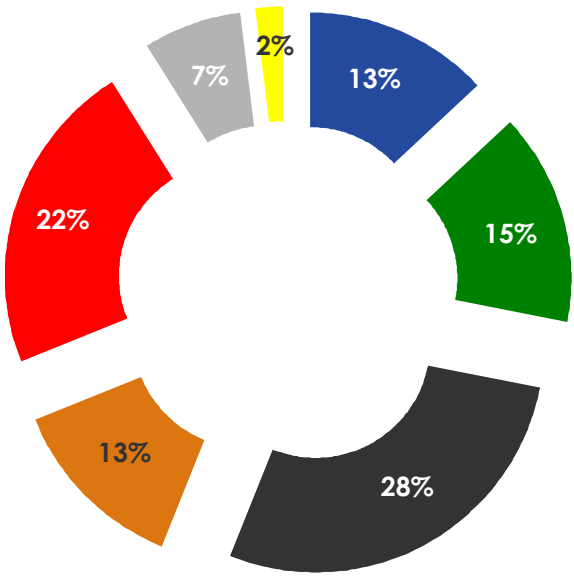
Le nombre d'entreprises ne faisant appel à aucun prestataire est en légère augmentation : 62% en 2004 contre 55% en 2003. Un signe de l'internalisation accrue de fonctions sensibles ou d'une défiance plus prononcée vis-à-vis de fournisseurs dont la qualité peut sans doute s'améliorer ?

On constate également que si en 2003, 33% des répondants étaient seuls, ils ne sont plus que 28% en 2004. La part des équipes constituées de 2 personnes progresse considérablement (de 7% à 15 %) : les singletons de 2003 sont devenus binômes ! Les RSSI "gourous" ou "experts" renforceraient-ils leurs moyens d'action et surtout de pilotage ?

L'importance de quelques "poids lourds" ne doit pas être ignorée. En 2004, les 5 grands comptes aux équipes les plus importantes représentent 37 % du total des professionnels recensés (contre 42% en 2003). Des multinationales françaises se sont dotées de ressources humaines à la hauteur des enjeux propres à leurs métiers et à leur environnement concurrentiel.

57

Des réseaux de tailles très variables
(base : 45 réponses)



- 2 à 5
- 6 à 9
- 10 à 15
- 20 à 25
- 30 à 50
- 300 à 400
- ≥ 1 000

Fig.36

Une quête de perfectionnement
(base : 35 réponses)

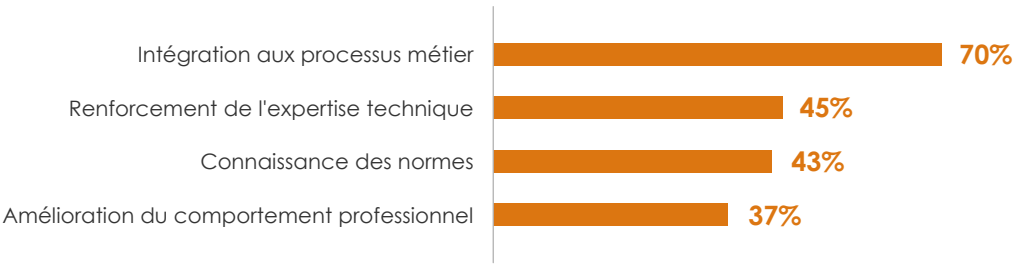


Fig.37

L'importance des correspondants

L'intégration de la fonction SSI, comme celle de la qualité, s'exerce souvent par la mise en place d'un réseau de correspondants. Nombre de RSSI étant seuls, il va de soi que leur action n'aurait eu aucun sens sans des relais au sein des fonctions informatiques, mais aussi et surtout auprès des métiers, des utilisateurs du SI.

70% des managers de la SSI possèdent un réseau de correspondants.

Leur action de communication descendante et ascendante est primordiale dans les grosses structures. Leur rôle premier est bien de faire connaître la fonction auprès de leurs collègues.

- acteurs
- règles
- procédures

La taille des réseaux est très variable d'une entreprise à l'autre. Une multinationale industrielle en aura des centaines, une compagnie d'assurance nationale quelques uns. Un des problèmes de fond réside dans leur affectation partielle aux questions de sécurité. C'est mieux qu'ils existent que le contraire, mais entre la sécurité et son activité première, on imagine celle qui primera sur l'autre, à une époque où le temps de travail se réduit, à tort ou à raison.

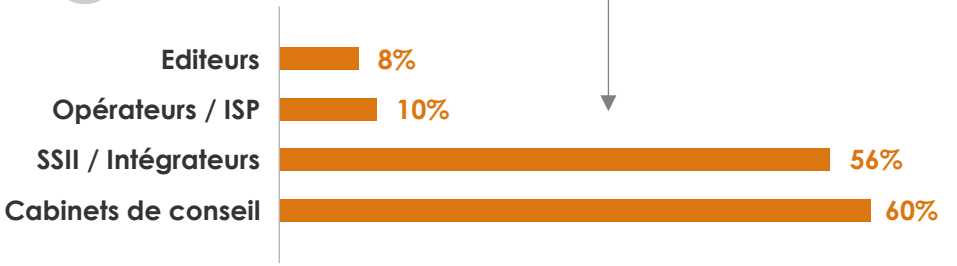
Près des 3/4 de ces relais, éducateurs et informateurs, consacrent moins de la moitié de leur temps à leur fonction SSI (73%). Néanmoins, 17% y sont détachés à plus d'un mi-temps et près de 10% s'y consacrent totalement.

L'axe d'amélioration privilégié des managers de la SSI concerne une meilleure intégration des équipes et des correspondants dans les processus métiers. Cela signifierait que ce n'est encore pas suffisamment le cas. Il va de soi que ces correspondants ne peuvent réussir dans leur mission que si le dialogue et la coopération s'installent au sein de leur entité et avec leurs collaborateurs.

Les améliorations plus techniques (expertise, normes, etc.) sont souhaitées par moins d'un professionnel sur deux. Et l'amélioration du comportement professionnel (la dimension humaine, communicante, éducative) ne concerne ici qu'1/3 des réponses. Ce n'est pas ce qui est requis en premier lieu mais c'est ce qui peut faire tout échouer, si "on passe mal" ou si on manque de crédibilité dans son discours.

Fig.38

Les prestataires privilégiés des entreprises
(base : 50 réponses)



La qualité des prestations
(base : 50 réponses)

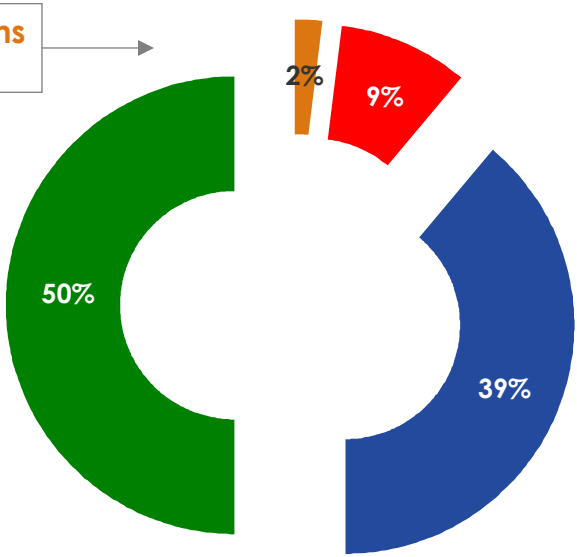


Fig.39

■ Excellente ■ Correcte ■ Médiocre ■ Sans avis

Le poids très relatif des prestataires

Le marché de la SSI s'est considérablement développé depuis une dizaine d'années et on constate encore des croissances à 2 chiffres, dans les technologies plus que dans les services. Le nombre d'acteurs ne cesse d'augmenter et s'il y a eu des échecs retentissants, il reste des marges de croissance quantitatives et qualitatives.

Face à des menaces nouvelles, plus stratégiques souvent, et des technologies de plus en plus "douteuses" dans leur conception et leur développement, les entreprises ne peuvent plus se tromper, ni dans l'outil, ni dans le prescripteur, ni dans l'installateur. Elles requièrent désormais des consultants indépendants et très expérimentés.

Les cabinets de conseil : prestataires privilégiés des entreprises.

Même s'ils sont suivis de près par les SSII et les intégrateurs, les prestataires privilégiés des entreprises sont les cabinets de conseil spécialisés. Des acteurs sont aujourd'hui des références car ils ont su maintenir leur indépendance et la qualité de leurs méthodes de travail. Mais la concurrence est rude et les SSII / intégrateurs comme les opérateurs et les acteurs de l'Internet se placent de plus en plus en concurrents directs pour : l'élaboration des politiques, l'aide aux choix des architectures et des outils, les services à valeur ajoutée (veille, gestion d'incidents, etc.), l'intégration et l'exploitation des outils.

Le recours aux éditeurs pour des "services" pose un problème de fond qu'il conviendrait d'analyser en détail. S'ils se placent sur ce créneau en sortant du cadre de ce qui touche directement à leurs technologies, leurs clients prennent le risque d'avoir un fournisseur / prescripteur. Attention danger ! Notons simplement qu'une très petite part des entreprises s'appuie sur des éditeurs pour leurs prestations (support, veille, alertes, etc.)

On constate que les entreprises portent un jugement assez modéré sur leurs prestataires. 9% jugent leur qualité médiocre, et la majorité ne la juge que "correcte". Il y a des marges de manœuvre qui pourront sans doute être comblées par des processus de formation et de certification. Rappelons que le panel est constitué de professionnels souvent expérimentés. Il n'intègre pas de responsables d'entreprises sans équipe sécurité qui auraient sans doute plus à se plaindre de leurs prestataires.

Pourtant, le bon sens dicte une règle essentielle que les secteurs du bâtiment ou des transports appliquent depuis bien longtemps. L'implication de SSII est si tentaculaires qu'il faudra encore quelques années pour bien segmenter ce qui peut l'être et voir disparaître les auditeurs / installateurs !

Fig.40

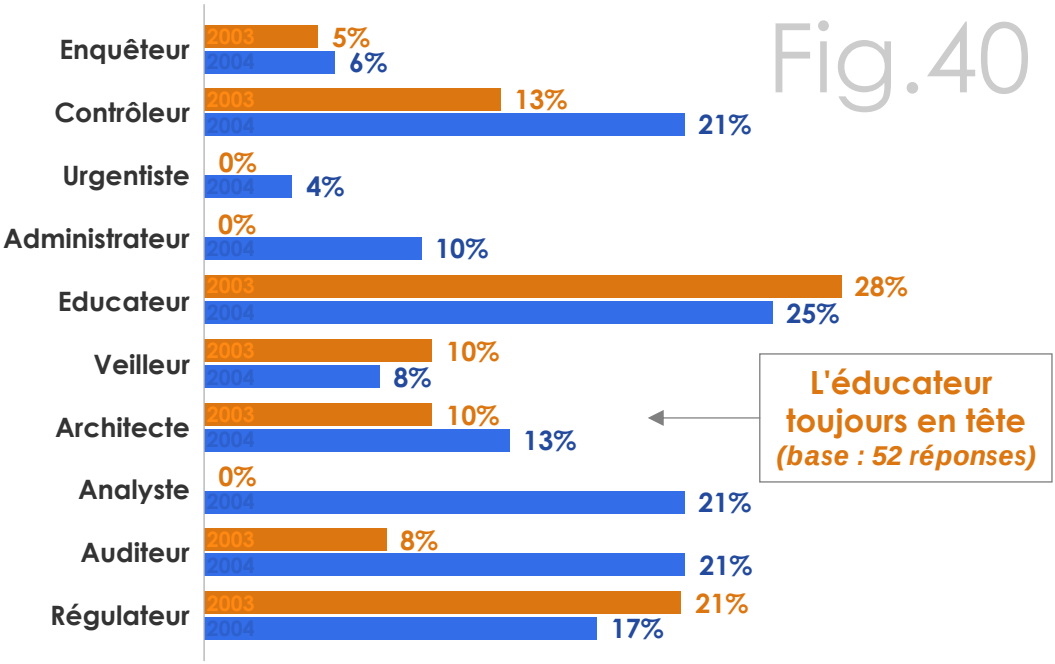
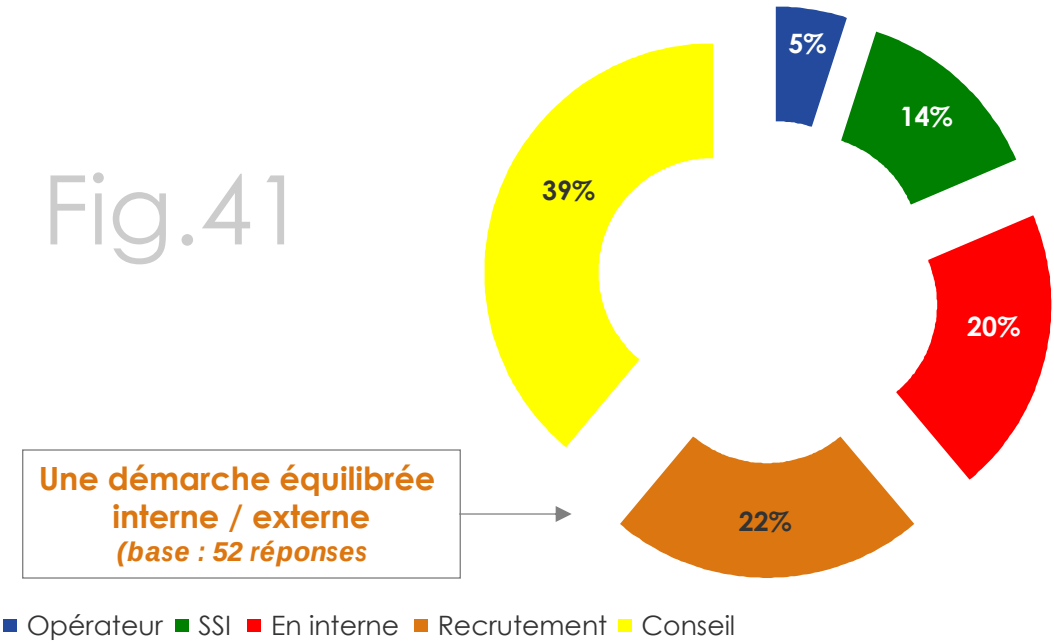

Enquêteur
2003 5%
2004 6%
Contrôleur
2003 13%
2004 21%
Urgentiste
2003 0%
2004 4%
Administrateur
2003 0%
2004 10%
Educateur
2003 28%
2004 25%
Veilleur
2003 10%
2004 8%
Architecte
2003 10%
2004 13%
Analyste
2003 0%
2004 21%
Auditeur
2003 8%
2004 21%
Régulateur
2003 21%
2004 17%
L'éducateur toujours en tête
(base : 52 réponses)

Fig.41


5%
14%
20%
22%
39%
Une démarche équilibrée interne / externe
(base : 52 réponses
Opérateur
SSI
En interne
Recrutement
Conseil

Des rôles à renforcer

Les professionnels assument des tâches nombreuses et complexes. Certains rôles sont aussi parfois délaissés par manque de temps. Leur renforcement à 12 mois est une préoccupation pour 80% du panel.

Cette année encore, l'éducateur arrive en tête. Un quart du panel souhaite développer la formation / sensibilisation. De nombreuses entreprises ont en effet intégré les dimensions "culturelle" et "comportementale" à leur management. Les limites des techniques et des règlements qu'elles ont désormais déployés les engagent vers une plus grande implication individuelle.

Environ un professionnel sur 5 souhaite ensuite améliorer les processus classiques dévolus à l'analyste et à l'auditeur, un peu oubliés en 2003. Il faut parfois revenir aux fondamentaux.

Mais le plus important concerne la très forte progression du rôle de "contrôleur" qui a contrario de l'auditeur, "surveille" en permanence, au quotidien, le respect des règles et l'application de la politique. Le développement de la "cyber-surveillance" est réel, qu'elle touche les aspects techniques (mise à jour des correctifs, vérification des configurations systèmes, etc.), les usages abusifs (internet, messagerie), l'état des outils de sécurité (mise à jour des anti-virus, remontée d'alerte, etc.), les investigations (analyse et corrélation de traces, etc.).

Les efforts de réglementation semblent se tasser en 2004. Le régulateur passe de 21 à 17 %.

Pour mener à bien ce renfort humain, les entreprises se tournent principalement vers le marché (environ 60%) mais n'omettent pas une démarche interne, ni les recrutements.

Les cabinets de conseil spécialisés sont encore une fois placés en tête. Une meilleure qualité tirée de l'expérience de consultants aguerris est sans doute recquise.

Mais les recrutements ne sont pas omis et près d'une entreprise sur 5 en envisage pour répondre à ses besoins.

Enfin, les SSII et les opérateurs sont requis pour les postes les plus opérationnels (architecte, administrateur) par un peu moins de 20% du panel.

"Je consacre une parte importante de mon budget à la sensibilisation des utilisateurs."

Michel Harouard
Directeur sécurité des données Bosch France

63

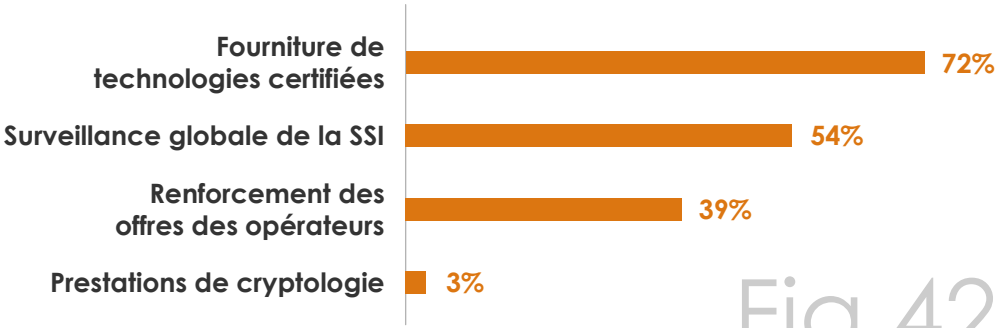


Fig.42

Attentes vis à vis des intégrateurs
(base : 65 réponses)

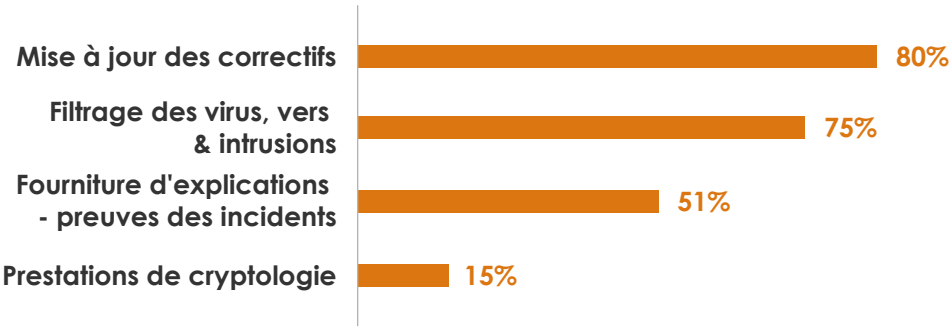


Fig.43

Attentes vis à vis des opérateurs
(base : 65 réponses)

L'externalisation des services

L'externalisation des aspects les plus opérationnels de la SSI est de plus en plus recquise. Les Managed Security Services Providers apparus début 2000 ne parviennent pas à percer en France alors qu'ils rencontrent un certain succès dans les pays anglo-saxons. Cela ne veut pas dire que ce n'est pas une perspective majeure du marché. L'enquête 2004 du Cercle met en évidence une donnée essentielle :

88% du panel ne confieraient pas l'ensemble de la SSI à un prestataire unique.

Mais entre les SSII/intégrateurs et les opérateurs/ISPs, la balance penche fortement pour les premiers à 73% contre 27%. La question reste de savoir ce que l'on ferait faire à ces prestataires techniques au-delà des missions de conseil (politique, formation, audit, …) ou des activités classiques d'exploitation de systèmes, de réseaux et des dispositifs de sécurité.

La première attente vis-à-vis des intégrateurs et des SSII concerne la fourniture de technologies certifiées. Cela les placerait en "donneurs d'ordres" vis-à-vis des éditeurs et industriels. Un bon intégrateur se devrait donc d'avoir au catalogue des technologies qui soient passées pas les fourches caudines de la certification, critères communs ou pas (voir chapitre suivant).

Les intégrateurs sont ensuite sollicités pour des activités classiques qui consistent à fournir des ressources humaines, spécialisées, aptes à exploiter et surveiller l'infrastructure de sécurité. Le taux de réponse assez moyen montre que d'autres acteurs (plus spécialisés) sont certainement requis (MSSPs par exemple).

Les prestations de cryptologie, que ce soit pour le chiffrement ou la signature électronique, ne sont pas requises pour les SSII (3%) mais plus significativement pour les opérateurs (15%). Les VPN expliquent sans doute ce besoin.

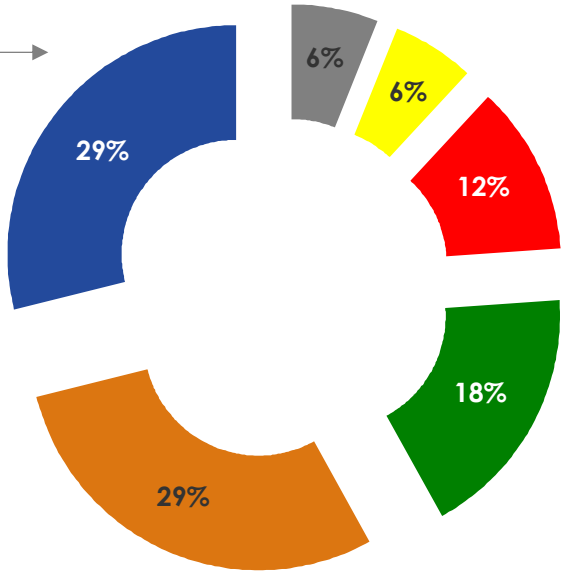
Les attentes vis-à-vis des opérateurs sont globalement plus fortes et s'adressent sans surprise aux infrastructures pour lutter contre les risques de sabotage et d'intrusion. La mise à jour des correctifs apparaît comme une exigence très forte (80%) notamment pour tout ce qui concerne les routeurs, pare-feu, sites web, serveurs de messagerie, etc.

Enfin, le recours aux opérateurs et ISP pour fournir des explications ou des preuves lors d'attaques n'est pas marginal (50%). La mise en place d'une organisation adéquate dans l'entreprise et avec ses opérateurs/ISP est cruciale pour y parvenir (rapidité de réaction, précision des requêtes, etc.). Notons enfin que :

La certification des prestataires devrait être obligatoire pour 55% du panel.

17 professionnels (21%) diplômés / certifiés

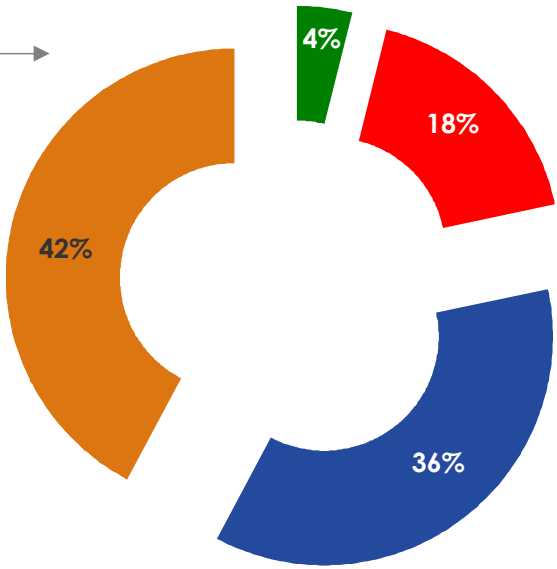
Fig.44



- DESS UTT
- MASTERE SUP TEL
- BADGE INT
- DCSSI
- CISSP
- CISM

Perspectives sur la certification individuelle

Fig.45



- En cours
- Sans doute
- Ne sait pas
- Sans intérêt

Perplexité sur la formation / certification

Les formations en SSI ont débuté au milieu des années 90 (Mastère Sup Télécom de Paris) et elles se sont multipliées depuis le début des années 2000. Mais tous ces diplômés qui peuvent être évalués à quelques centaines ne se retrouvent pas dans le panel. Ils sont certainement plus chez des prestataires qu'en entreprise.

En formation initiale ou continue, des cursus de qualité peuvent répondre aux attentes des entreprises comme à l'UT de Troyes, à Sup Telecom Rennes et Paris et à l'INT, sans oublier le Centre de Formation de la DCSSI.

Si la meilleure formation reste celle du terrain, des besoins sont aussi comblés par de nombreux séminaires ou conférences en SSI. Souvent gratuits, quelques fois payants, ils consistent généralement à écouter le discours d'offreurs et de prestataires.

La confusion est trop fréquente entre "veille" / "information" et "formation". Participer à des salons et des conférences participe à la formation mais ce n'est pas à proprement parler de la formation.

Tous les professionnels, notamment les plus aguerris ne retourneront pas sur les bancs de l'université. Les processus de certification, une sorte d' "anti-rouille" du diplôme répondent alors à des besoins essentiels : garantir dans le temps la qualité d'un professionnel.

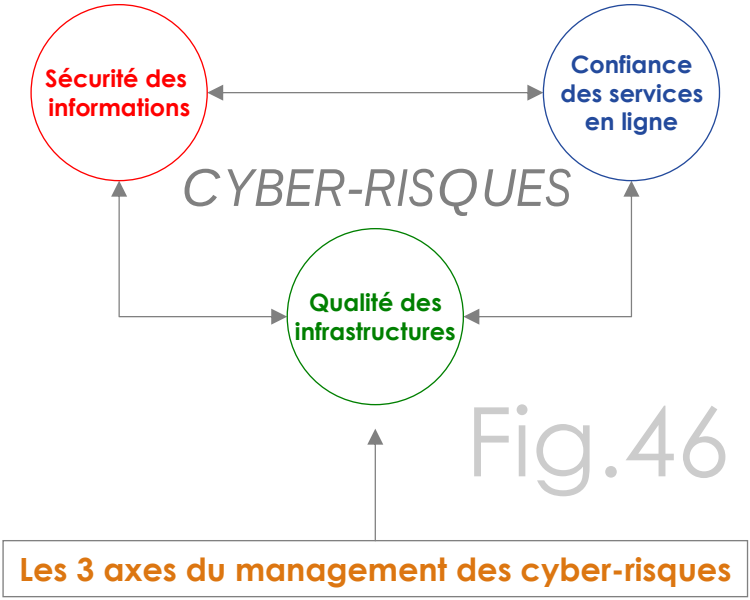
Ici aussi, bien peu de professionnels français se sont engagés dans cette voie. Il existe entre 80 et 100 CISSPs (Certified Information System Security Professional) en France. Mais les perspectives pour les entreprises sont mitigées. Environ 40% du panel envisagent de suivre une certification individuelle. Ce processus s'adresse sans doute en premier lieu à des prestataires (SSII, consultants, etc.).

18% du panel, en général des professionnels très expérimentés, ne trouvent aucun intérêt à un processus qui peut paraître un peu lourd et scolaire. Mais n'ont-ils pas aussi la crainte de ne pas réussir l'examen ?!!

Orientations

Des pistes de reflexion, et d'action...

Structurer, organiser, certifier, quantifier



En repartant du modèle des cyber-risques (fig.2), peuvent se dessiner 3 axes de management des cyber-risques. Ceux-ci s'articulent autour de 3 mots-clés : qualité, sécurité et confiance.

Il serait faux de penser que ces 3 axes sont indépendants. Et il serait dangereux de les séparer ! Il faut, autant que possible, les réunir, les relier en plaçant le centre du management là où c'est le plus pertinent dans chaque entreprise.

- Direction de la sécurité
- Direction des risques
- Secrétariat général
- Direction qualité / sécurité du SI

Ce centralisme, utile, ne doit pas faire oublier leurs devoirs aux métiers et aux DSI, qu'ils soient donneurs d'ordres ou maîtres d'œuvre des moyens adaptés aux risques.

Structurer : de l'infrastructure au contenu

Certains professionnels se nomment désormais "IT risk manager" ou "information risk manager". D'autres sont "responsable sécurité/qualité informatique". C'est dire les divergences d'approche dans l'art du management des cyber-risques. Un management efficace des cyber-risques doit finalement s'effectuer dans trois dimensions.

LA QUALITE : tout ce qui touche aux **"infrastructures"** et aux risques de sabotage et d'intrusion ne trouve sa source que dans une "insécurité", une sorte de "non qualité" des systèmes et des réseaux, voire des applications. C'est la sécurité informatique historique. L'enjeu est désormais de respecter des normes, des meilleures pratiques, de disposer de produits, de fournisseurs, de professionnels "qualifiés" voire "certifiés". La Qualité / Sécurité informatique prend tout son sens ici. Les professionnels disposent aujourd'hui des normes ISO qui les aident grandement dans leur tache. Mais de nombreux autres référentiels peuvent aussi être mis à profit dans les différents secteurs d'activité : finance, santé, télécoms, etc.

LA CONFIANCE : cette notion émergente a pris en 2004 un essor nouveau avec la loi sur la "confiance dans l' économie numérique" et avec les débats parlementaires sur l'évolution de la Loi Informatique et Libertés (tous traduisant des directives européennes). Les questions d'atteinte à la vie privée, de fraude en ligne, de contrat, de signature et de preuve électroniques génèrent de vastes champs d'investigation totalement orientés **"services"**. Les points d'ancrage de cet axe sont d'essence juridique et s'adressent en premier lieu aux métiers dans le cadre de la dématérialisation des processus. Les questions d'horodatage, de traçabilité et d'archivage prennent ici une importance accrue.

LA SECURITE : Dans l'inconscient collectif, la sécurité est souvent synonyme de "police" avec ses implications dans la surveillance, le contrôle, l'investigation. A tort ou à raison, elle ramène plus à des questions de dissuasion et de répression. Si nous appliquons ces principes aux cyber-risques, on constate qu'il y a bien des domaines d'intervention qui sont véritablement du domaine du "militaire" et qui nécessitent des liens forts avec la sécurité des biens et des personnes, avec les pouvoirs publics aussi. Les questions de secret, donc de cryptographie, sont d'évidence de son ressort. Malgré la libéralisation de l'utilisation du chiffrement, ces technologies restent extrêmement sensibles. Cet axe est donc principalement orienté **"contenus"** et se nommerait avec pertinence "Sécurité des informations".

POLITIQUE
Juridique
RH
Comm
Qualité
Audit
Métiers
PROJET
Métiers
IT
PROCESSUS
IT
Régulateur
Auditeur
Contrôleur
Enquêteur
Veilleur
Educateur
Analyste
Architecte
Administrateur
Urgentiste
Cellule
"Politique et pilotage"
Cellule
"Mise en oeuvre "
MEILLEURES
PRATIQUES
(RÈGLES)
Enjeux
Management
stratégique
Management
opérationnel
Processus
Une séparation claire des rôles

Fig.47

Organiser : de la stratégie aux opérations

On a coutume de dire que la SSI s'adapte à l'organisation de l'entreprise et que les processus de sécurité du SI s'intègrent au mieux au management d'ensemble. Certes ! Mais peut-on se satisfaire de ce "mieux que rien" ? Il existe aujourd'hui des exigences si fortes que les entreprises ne peuvent pas rester ni sourdes, ni aveugles au monde dans lequel elles évoluent. Et s'organiser avec efficacité est une exigence réelle.

Tout repart des enjeux. La désignation d'un correspondant aux "données personnelles", d'un "monsieur intelligence économique" et pourquoi pas l'attribution d'un titre de "cyber-risk manager" ou encore d'un "gestionnaire du patrimoine immatériel" structurent une fonction qui s'ouvre bien au-delà du SI.

Dans ce contexte, la cellule de "pilotage" regroupe finalement 3 des 5 fonctions clés, quand bien même 2 sont encore insuffisamment loties. Ce constat ne démontre rien d'autre que face au contexte actuel, il est plus que nécessaire de **renforcer le management "stratégique"** en termes de prérogatives et de champs d'action. Celà s'intègre très bien dans ce que l'on a coutume d'appeler la "gouvernance".

La fonction d' "analyste-architecte" est un dilemme. Est-elle du ressort de la stratégie ou de l'opérationnel ? On retrouve ici un des rôles historique du RSSI, ancienne courroie de transmission entre les décideurs et l'informatique. Les plus aguerris peuvent évoluer vers cette fonction de "pilotage", les plus attirés par la technique continueront à s'impliquer avec les DSI dans les projets, la conception et la mise en œuvre des moyens.

Mais ce temps est sans doute révolu. Place aux vrais décideurs de la SSI, correctement positionnés, dûment formés et entourés, y compris dans tout ce qui concerne les choix technologiques plus que jamais politiques. Le management stratégique n'est sans doute rien d'autre qu'une fonction de pilotage et de contrôle de fonctions souvent externalisées.

Car en définitive c'est d'efficacité, notamment économique qu'il faut parler. Certes, les anti-virus et les pare-feu se doivent d'être utiles et efficaces face aux nouvelles attaques, bien sûr la cryptographie et la signature électronique devraient se développer et favoriser un marché encore un peu atone. Mais en final, il faudra bien corréler l'ampleur des dépenses avec la réalité du terrain que ce soit en termes d'évaluation d'enjeux ou de préjudices subis. Les systèmes bogués, les portes dérobées, etc. ont et auront des effets importants sur la démarche sécurité des entreprises, en amont et en aval. Car l'application d'un correctif qui "plante" une application commerciale n'est pas un incident mineur.

"Le métier de RSSI ne peut se faire correctement sans une bonne dose d'engagement personnel, le soutien de sa hiérarchie, et un certain sens de... l'organisation ! "

Eric Larcher

RSSI Accor Services

Type	Niveau	Nombre	Exemple
Micro-circuits	CC EAL4+ CC EAL1+ ITSEC E3 moy	16 2 2	Micro circuit ST19 (STM)
Cartes à puce	CC EAL4+ CC EAL4 ITSEC E3 élevé ITSEC E3 moy CC EAL1+	11 2 10 8 12	 PM électronique (Modéus)
Produits réseaux	ITSEC E4 moyen ITSEC E3 moyen CC EAL 2+	2 3 1	 EADS Telecom M>tunnel
Lecteurs / terminaux	ITSEC E3 moyen	1	Lecteur PIN-Pad Bull CP8/Ingénico et GIE CB
Produits PC	CC EAL4+ ITSEC E2 élémentaire	1 1	Librairie Security Box 6.0 MSI
Systèmes	CC EAL1+	4	IP VPN V1.0 (Equant)

Fig.48

Les produits certifiés
(source www.ssi.gouv.fr)

Les certifications individuelles
(source www.icys-formation.com

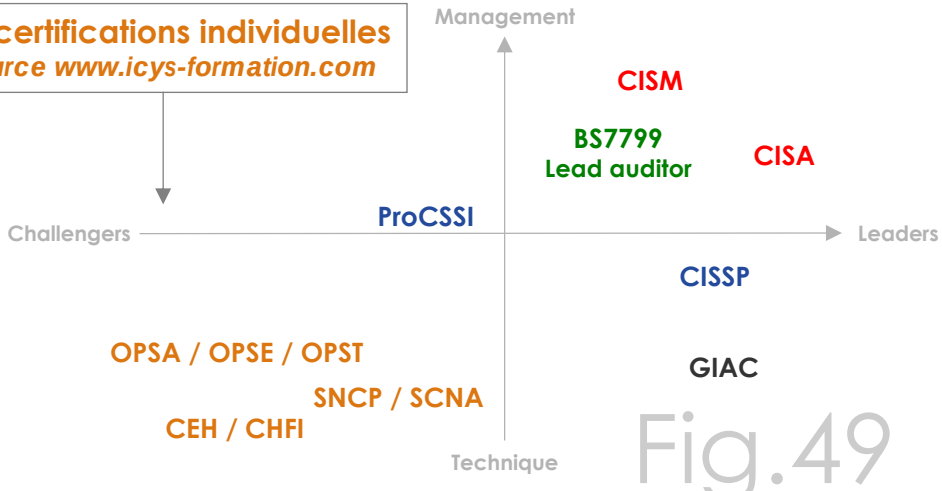


Fig.49

Certifier : des produits aux individus

Certains métiers se sont engagés dans des démarches d'évaluation et de certification depuis des décennies. En général, c'est à la suite d'une catastrophe et il a fallu, à chaque fois améliorer les critères de qualité et de sécurité pour que cela n'arrive plus. Après le naufrage du Titanic, réputé insubmersible, construit avec l'acier le plus pur du monde, il a suffit de modifier les routes des paquebots dans l'Atlantique nord.

Quoiqu'il en soit, lorsqu'on est confronté au "drame", l'homme a toujours 2 attitudes : trouver les responsables ou chercher des solutions. Mauvais matériaux, erreurs de conception, de fabrication, erreurs humaines dans l'utilisation et l'exploitation, défaut de contrôle. Toutes les pistes sont ouvertes.

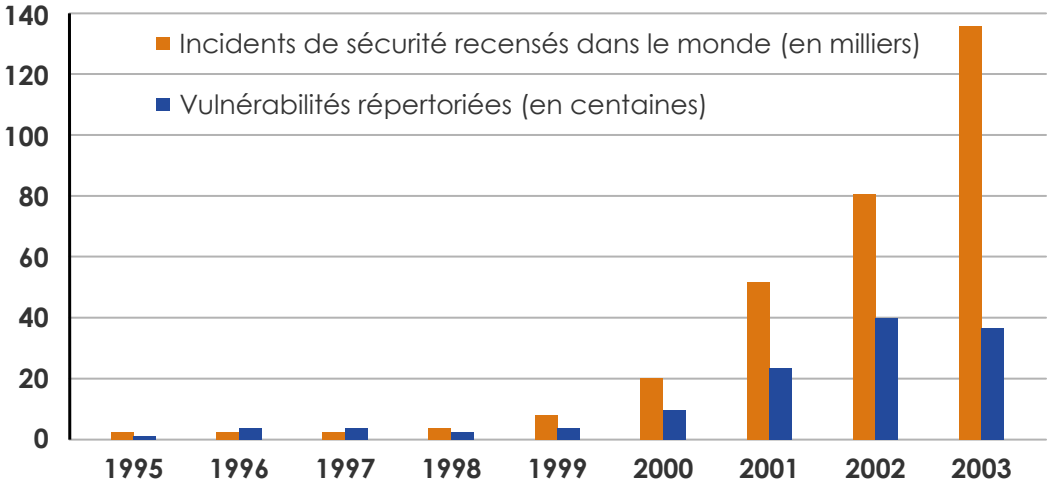
Le domaine de la Sécurité des SI, malgré sa jeunesse, n'échappe pas à la règle. Dès les années 80, l'Europe et les Etats-Unis ont dévéloppé leurs "critères d'évaluation de la sécurité informatique". Orange book outre Atlantique, ITSEC de ce côté ci. Ils se sont regroupés en 2000 sous la bannière ISO : **Les critères communs**. Les entreprises peuvent désormais, devront peut-être demain, s'équiper de technologies évaluées et certifiées selon des schémas et des critères rigoureux. Le tableau (fig.48) présente quelques exemples de produits certifiés (source : www.ssi.gouv.fr).

Ce qui intéresse aussi un "donneur d'ordres" c'est que ses fournisseurs soient "dignes de confiance". Des actionnaires peuvent aussi très bien requérir ce type de démarche auprès de leurs participations. De grandes entreprises britanniques ont publié un standard en 1999 (BS7799) qui sert de base à la certification du **"management de la sécurité de l'information"**. La norme ISO 17799 ne possède pas, quant à elle, de schéma de certification. Elle reste une "check list" tirée de la BS 7799. Les entreprises peuvent désormais s'appuyer sur des "auditeurs BS7799" qui évalueront sa conformité aux critères de management.

Enfin, il est bien connu que l'homme reste le maillon faible de tout processus. Les anglo-saxons ont ici aussi pris les devants en mettant en place dès les années 90, les CISSPs (www.isc2.org). 2004 a vu l'apparition de nombreuses autres certifications, certaines très pointues et techniques (notamment le GIAC du SANS Institute) et une d'origine française, le ProCSSI (inseca@devinci.fr). Seules les certifications de l'ISC² et de l'INSECA sont conformes à la norme ISO 17024 relative à la certification des individus. Le CISM et le CISA sont issus des métiers de l'audit et du conseil en informatique.

Ces processus visent à placer les professionnels dans un parcours "métier" alliant expériences pratiques, formations et audits d'évaluation. Ils mesurent le "savoir être", le **comportement professionnel**, non une expertise, et visent à améliorer l'employabilité et pourquoi pas les revenus d'experts recherchés et souvent sensibles.

75



Vulnérabilités et incidents identifiés
(source www.cert.org)

Fig.50

Fig.51

Impacts économiques des cyber-risques
(à partir des chiffres CSI/FBI : www.gocsi.com)

	2001		2002		2003	
	Pertes déclarées	%	Pertes déclarées	%	Pertes déclarées	%
Vol d'information	161 M$	43%	189 M$ (+17%)	42%	78 M$ (-59%)	39%
Fraude économique	102 M$	27%	116 M$ (+14%)	25%	11 M$ (-91%)	5%
Intrusion	60 M$	16%	68 M$ (+13%)	15%	15 M$ (-78%)	7%
Sabotage	55 M$	14%	83 M$ (+51%)	18%	98 M$ (+18%)	49%
Total	378 M$	100%	456 M$ (+21%)	100%	202 M$ (-56%)	100%

Quantifier : failles, incidents, budgets...

Comment prendre des décisions sans indicateurs fiables, pertinents, concrets ?

L'idée de tableaux de bord de la SSI circule depuis des années sans que l'on sache encore très bien en quoi ils consistent, à qui ils s'adressent et surtout à quoi ils servent vraiment. On entend parler d'indicateurs "techniques", de "management". Que se cache-t-il derrière les mots ? Schématiquement, il est possible de distinguer divers types de tableaux de bord selon qu'ils s'adressent aux décideurs (métiers, DG), aux managers et opérationnels de la SSI. En observant les statistiques qui existent aujourd'hui, on peut connaître :

- les failles et les correctifs publiés (fig.50) : sont-ils pris bien en compte ?
- Les meilleures pratiques de la SSI (ISO 17799) : sont-elles mises en œuvre ?
- Les impacts économiques des incidents (fig.51) : combien m'a coûté la dernière infection virale ?
- Les efforts budgétaires par type de dépense : où se concentrent les moyens ?

Des chiffres publiés par des organismes officiels (Cert-CC, CSI, ...), les résultats d'audit, d'enquêtes, d'études de marché permettent de positionner l'entreprise par rapport à une certaine réalité. Les banques possèdent aujourd'hui le Comité de Bâle qui définit une métrique et des indicateurs de gestion des risques opérationnels.

D'une manière ou d'une autre, tout professionnel qui souhaite agir avec rigueur se doit de définir quelques familles d'indicateurs pertinents. Au niveau de l'entreprise, on a du mal à imaginer qu'elle ne puisse posséder une vision aussi précise que possible sur :

- la cartographie des risques
- le niveau de vulnérabilité système / réseau : application des correctifs
- L'efficacité des moyens en place : anti-virus, détection d'intrusion, mots de passe, etc.
- Les moyens humains : internes et externes
- Le suivi de la mise en œuvre des recommandations d'audit
- La nature et le nombre des incidents vécus et leurs impacts
- L'ampleur des dépenses selon un référentiel qualifié et accepté
- la conformité aux normes et référentiels

Peu importe à qui ils s'adressent et quand. Ils sont de toute façon utiles !

Remerciements

Le premier Livre blanc des Assises est né de l'idée de Gérard RIO, sans qui le Cercle Européen et les Assises de la Sécurité ne seraient pas.

Merci à Gérard pour son soutien permanent.

Il n'aurait pu être réalisé, tout comme l'enquête 2004 du Cercle Européen, sans le concours de nos quatre parrains. Merci encore à Adeline Siracusa (DG Consultants), François Corbasson (France Telecom), Eric Darras (Demos) et Eric Krzyzosiak (NRG).

Il n'aurait pas non plus la légitimité qu'il requiert sans le soutien d'organismes qui ont compris qu'il pouvait être un outil essentiel de perfectionnement pour tous les professionnels. Merci donc à Jean-François Pépin (CIGREF), Jean-François Violette (INT), Philippe Cornu (UTT) et Francis Moaty (ESIEE/IMSIS).

Remercions également Jean-Philippe Bichard, rédacteur en chef de Netcost & Security, pour sa collaboration.

N'oublions pas évidemment les 82 professionnels du panel qui ont permis la production de nouvelles statistiques sur les métiers de la SSI.

Enfin, quatre experts ont effectué la relecture indispensable de ce travail. Merci à Isabelle Petit et Paul Grassart (Arséo), Pierre-Yves Bouf (Avixa) et Hervé Schauer (Hervé Schauer Consultants).

Pierre-Luc REFALO
Directeur Associé
Comprendre&Réussir

Couverture : la triple enceinte celtique.

Ce symbôle représentait les 3 mondes, les 3 degrés de la prêtrise et les 3 composantes de l'esprit humain. Le carré extérieur figurait la conscience reliée à la réalité physique par les sens, le carré intérieur l'inconscient recevant les messages des dieux, et le carré intermédiaire la partie de l'esprit percevant le monde matériel et le monde spirituel.

Le langage secret des symboles - Editions Solar 1995

79

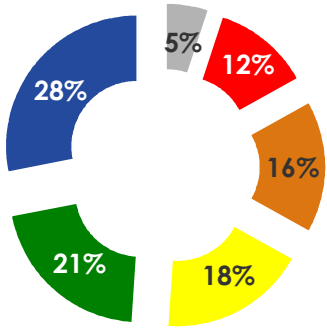
Annexes

Le panel de l'enquete

81

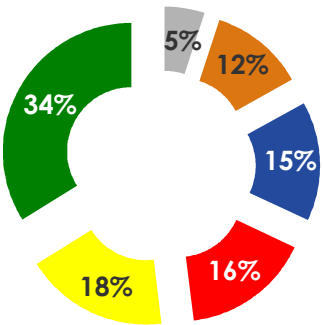
La participation des banques/assurances s'est améliorée passant de 23 à 28 % au détriment de l'industrie (16% contre 22 %). Les entreprises et services publics sont aussi trop peu représentés.

Les secteurs d'activité du panel



- Banque-Assurances
- High Tech-Médias
- Fonction publique
- Industries
- Services
- Distribution

Des entreprises de toutes tailles se sont impliquées. Aux grands groupes internationaux s'ajoutent de nombreuses grosses PME qui possèdent aussi des RSSI souvent dédiés. Près de la moitié du panel est composé d'entreprises de moins de 5000 salariés (contre 38% en 2003).



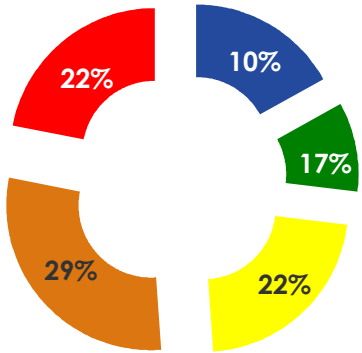
La taille des entreprises du panel

- ≤ 1 000
- ≤ 5 000
- ≤ 10 000
- ≤ 50 000
- ≤ 100 00
- > 100 000

82 professionnels / 65 entreprises

L'expérience moyenne en 2004 est de 6,8 ans contre 8 ans en 2003. Le panel, en s'élargissant s'est rajeuni. La part des néophytes (1 an d'expérience) est significative. La frontière entre les +/- 5 ans d'expérience se situe à 49% contre 41% en 2003.

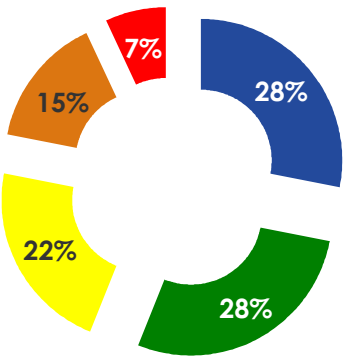
L'expérience du panel en SSI



■ ≤ 1 an ■ ≤ 3 ans ■ ≤ 5 ans ■ ≤ 10 ans ■ > 10 ans

L'expérience moyenne dans le poste en 2004 est de 4,0 ans contre 3,8 ans en 2003. Elle se stabilise et peut servir de « référence » pour tout projet de mobilité. La proportion des professionnels ayant entre 3 et 5 ans d'expérience (susceptibles d'évoluer dans les 2 ans) se situe à 22% contre 32% en 2003.

L'expérience du panel dans le poste actuel



■ ≤ 1 an ■ ≤ 3 ans ■ ≤ 5 ans ■ ≤ 10 ans ■ > 10 ans

Le Cercle Européen de la Sécurité

« … le Cercle Européen m'a permis de nouer des relations très enrichissantes avec des DSI et RSSI des grandes société et les responsables des grands acteurs de la sécurité informatique »

Gilles BERTHELOT
Directeur Informatique – SAPEURS POMPIERS de PARIS

« Le Cercle Européen de la Sécurité est un lieu d'échanges sur la sécurité des SI où convivialité rime avec professionnalisme et expertise. »

Didier TORTOLERO
RSSI dans le secteur Bancaire

« C'est aujourd'hui au sein du Cercle Européen de la Sécurité que se retrouvent les principaux acteurs et décideurs du monde de la SSI »

Eric LARCHER
RSSI – Axa Services

…et Vous ?*

***Vous êtes DI, DSI, RSSI, DSSI ou responsable d'un réseau d'entreprise alors rejoignez-nous !**

Le Cercle Européen de la Sécurité

- Vos confrères consolident leur réseau d'influences et de connaissances…
- Vos confrères confrontent et échangent leurs expériences…
- Vos confrères partagent des moments conviviaux et professionnels au cours des Dîners Thématiques…
- Vos confrères rencontrent les plus grands experts…
- Vos confrères accèdent à l'actualité nationale et internationale de leur marché…
- Vos confrères ont rejoint **une véritable communauté de professionnels**…

Les Assises de la Sécurité

A votre tour de vous connecter sur www.lecercle.biz

Pour plus d'informations et vous inscrire, contactez-nous au 01 41 93 09 14, par courriel contact@lecercle.biz ou sur le site web www.lecercle.biz.

QUATRIÈME ÉDITION

L'événement incontournable pour tous les acteurs de la Sécurité.

Comment s'effectue la cyber-surveillance de vos systèmes ?
Quelles actions à mener ? Quelles procédures utiliser ?
Quelles précautions allez-vous adopter ?
Vos coûts...? Comment arbitrez-vous ?
Quelles dimensions économiques la sécurité implique-t-elle ?
Vos données sont-elles sécurisées en intra muros ? Et en extra muros ? Comment les maîtriser ?
Quelles mesures préventives pour anticiper attaques et intrusions ?

Confrontez vos expériences et disposez des outils d'aide à la décision avec les conférences, les ateliers thématiques, le Forum permanent et l'espace rencontres

Les Assises de la Sécurité

21 AU 23 OCTOBRE 2004 - DEAUVILLE

Les Assises de la Sécurité

NOS PARTENAIRES

APC · Avocent · deny all · enterasys · protect · INTRANCOD · LEXMARK · Microsoft · McAfee · NETASQ · NOKIA · Novell · RICOH · RSA · SOPHOS · symantec · THALES · TREND · UNISYS

OLES ESPACES SOLUTIONS

Nexus · ARCHE · NORTEL NETWORKS · CITRIX · azlan · IBM · CROSSBEAM · NEOCLES · TELMOUS · tiscali · TOSHIBA

www.les-assises-de-la-securite.com

NOS PARTENAIRES PRESSE

Pour de plus amples informations, merci de nous contacter au 01 41 93 09 15 ou par mail stephane@dgconsultants.fr