06 Les Assises

L'Événement Européen de la Sécurité et des Systèmes d'Information

LIVRE BLEU

tome III

octobre 2006

avec le soutien

orange Business Services

produit par

NRG

SOMMAIRE

Vers une nouvelle sécurité : la sécurité globale

Le formidable développement des technologies de l'information, avec la convergence de l'informatique et des télécommunications, nous a fait entrer dans une nouvelle ère de prospérité : la société de l'information.

L'évolution constante et rapide, le déploiement de plus en plus large des technologies, placent les systèmes d'information au cœur des enjeux stratégiques. Et cette évolution affecte profondément la sécurité de l'information : ceci tant pour le milieu professionnel que privé ! Cela implique aussi une prise en compte de la sécurité qui doit être globale et non seulement à cause de la responsabilité des entreprises mais aussi parce que c'est un facteur de confiance pour le nouvel écosystème qui s'impose à nous.

Cette problématique nous concerne tous, à titre privé comme à titre professionnel. La sécurité trouve donc, tout naturellement, son espace légitime au sein de toutes les entreprises, au même titre que le marketing, les ressources humaines ou les achats. En revanche, son positionnement se situe en amont de ces activités car pour « être » en sécurité, il faut participer à la sécurité, en adopter une posture, s'en imprégner et diffuser la culture !

Englobant aujourd'hui tous les aspects liés à la dimension économique, la culture de la sécurité n'a donc plus cette connotation négative qui lui était accolée. C'est un concept intégrateur et créateur de richesse par opposition à un concept simplement défensif ; elle n'est pas un acquis mais une construction dynamique, un combat de tous les jours !

Aussi la sensibilisation, la formation des utilisateurs professionnels et la mise en œuvre de politiques de sécurité cohérentes, adaptées aux besoins réels doivent nécessairement accompagner la course technologique d'autant que chacun peut voir sa responsabilité juridique engagée, au civil comme au pénal, faute d'avoir mis en œuvre les règles de l'art en matière de sécurité.

C'est donc une évolution culturelle majeure que nous devons conduire, dont le principal enjeu est de vaincre les pesanteurs liées au passé.

Si chacun d'entre nous a sa part de responsabilité, il est préférable pour les entreprises et organisations d'en fixer le cadre en définissant une réelle politique de sécurité élaborée avec toutes les parties prenantes. Alors, il est du rôle des Directions Générales d'impulser la mise en œuvre des bonnes pratiques permettant aux salariés de développer cette culture de la sécurité.

Cet élément important de la bonne gouvernance de l'entreprise est un facteur du développement durable et favorisera une confiance mutuelle (entreprise-clients-fournisseurs).

La sécurité globale est bien une responsabilité citoyenne et une démarche d'entreprise dont nous sommes tous les acteurs et les garants.

© Philippe Duluc
Directeur de la Sécurité du Groupe France Télécom

« ÉVOLUTION DES METIERS DE LA SECURITE »

RESULTATS DE LA 4ème ENQUETE ANNUELLE

Introduction

Depuis 2003, le Cercle Européen de la Sécurité des Systèmes d'Information analyse le rôle et les activités des professionnels de la Sécurité en entreprise et au sein des administrations. Les résultats des enquêtes de 2004 et 2005 ont servi de base à la rédaction des Livres Blancs des Assises (téléchargeables sur www.assises-de-la-securite.com) produits ces deux dernières années :

- **En 2004 : *« Pour un management stratégique des cyber-risques ! »*** Nous avons mis en exergue la séparation essentielle entre le pilotage des risques (stratégique) et la mise en oeuvre des mesures de sécurité (opérationnelle). Les RSSI avaient encore du mal à trouver leur voie et leur place. Pour certains, clients et fournisseurs, les grands écarts voire les conflits d'intérêts sont fréquents. Mais d'autres ont pris de l'avance …

- **En 2005 : *« Vers un benchmarking de la sécurité ? »*** Nous avons analysé en quoi l'émergence des normes, des règlementations sectorielles et les questions économiques pouvaient influencer la mise en place de tableaux de bord, qui pourraient devenir à terme, de véritables outils de comparaison. Si la démarche semble bien engagée, la plus grande confusion semblait encore régner, sur le champ des indicateurs et sur les métriques pertinentes. Mais l'ISO avance …

Nous recommandons d'avoir à proximité ces deux documents pour bien appréhender certaines analyses présentées ci-après.

Cette année, nous avons à nouveau effectué la radioscopie des membres du panel qui se sont volontiers prêtés au jeu. Et, comme le lecteur pourra le constater, nous pouvons dépasser des convictions, parfois largement partagées, pour énoncer des certitudes. Désormais aussi, il est possible d'aller au-delà d'un constat brut et instantané pour mesurer des évolutions et tracer des perspectives éclairant l'avenir.

En 2006, nous nous attaquons aux « Grands défis de la Sécurité des SI ». Et ils concernent d'abord les RSSI eux-mêmes. A eux d'être les acteurs des évolutions inéluctables en cours et à venir. Conformité et Gouvernance des risques, Qualité et Sécurité informatique, Intelligence économique et protection de la vie privée, Sécurité économique et pôles de compétitivité, e-business et crime organisé, etc. ***Tout est lié et la sécurité des Systèmes d'Information historique est prise en étau de toutes parts !***

L'auteur de ces lignes avait osé dans un numéro de « NetCost & Security » un tonitruant : « le RSSI est mort … ». Sous entendu : « Vive le RSSI ! ». Aujourd'hui, plus que jamais, les RSSI sont vraiment dans tous leurs états. S'ils se ressemblent parfois, au sein d'un même secteur d'activité, peu d'entre eux assurent rigoureusement les mêmes missions et pilotent des activités comparables.

Ne sommes-nous pas à l'aube d'un « big-bang »
pour les métiers historiques de la Sécurité des SI ?

Car les évolutions structurelles ont toujours des impacts majeurs sur le management et les organisations. Mais ces dernières, et c'est humain, ne les intègrent que (très) lentement : La ***sécurité informatique*** des années 1970-80 s'est d'abord transformée en ***sécurité des systèmes d'information*** (par les mises en réseaux), puis s'est muée en ***sécurité de l'information*** (depuis la chute du mur de Berlin), s'est ensuite élargie à la ***cyber-sécurité*** (depuis l'avènement de l'Internet et sous la poussée de la dématérialisation), pour s'intégrer enfin à la ***gouvernance des risques*** (plaçant le Systèmes d'Information au cœur de la stratégie et des activités des entreprises).

Or, combien de « bonnes pratiques » de sécurité informatique ou des systèmes d'information ne sont toujours pas comprises, mises en œuvre et intégrées au sein des organisations ? Combien de RSSI demeurent des chefs de projets ou des chargés de mission / experts de la sécurité informatique ? Alors qu'à l'opposé, ***beaucoup sont rattrapés, absorbés, englués dans des démarches de conformité drastiques qui ont la bonne idée d'imposer des règles … de bon sens ou de bonne gouvernance !***

Le monde est ainsi fait ! Ceux qui n'ont pas (encore) fait, feront peut-être, un jour, si la loi l'impose ou si Dieu le veut. Mais plus vraisemblablement quand auront cessé le marketing de la peur et la pression médiatique poussant à la surconsommation de technologies au détriment de l'organisation et des comportements.

Car c'est d'une véritable éducation dont a besoin le marché. Eduquer pour expliquer à tous, les véritables enjeux, les risques réels et les bonnes pratiques, les aspects économiques et comportementaux avant d'imposer de nouveaux textes de loi et l'installation d'outils qui ont au mieux des limites, au pire des effets pervers.

Les résultats de l'enquête présentés aux pages suivantes démontrent que les professionnels du panel ont pour la plupart compris qu'ils étaient au cœur d'évolutions fondamentales de la vie de leur entreprise. La plus importante qui ne transparaît pas nécessairement est essentielle :

La sécurité est d'abord une valeur ajoutée,
un service, s'adressant aux clients, citoyens, salariés, usagers.
Et non, comme on l'entend encore trop souvent, un mal nécessaire !

Je tiens à les remercier ici chaleureusement de leurs réponses aux 27 questions de l'enquête. Ces 15 minutes prises sur leur temps précieux sont le signe de leur compréhension d'enjeux qui les concernent directement :

- Vous devez ***prendre la parole et le pouvoir*** face à vos responsables et aux offreurs. Cette enquête est faite pour vous !
- Vous devez ***sortir de la pression quotidienne*** pour imaginer un avenir à votre fonction. Cette enquête vous ouvre la voie !
- Vous devez ***être ou devenir des exemples*** au sein de vos organisations et sur le marché. Votre comportement et vos capacités d'écoute et de communication sont les clés de votre succès.

Cette enquête vous appartient. Utilisez-la !

© Pierre-Luc REFALO
Chargé de mission du Cercle Européen de la Sécurité

Chapitre 1
Des solitaires au pouvoir qui s'affirme

Les RSSI sont souvent des êtres solitaires qui doivent d'abord se vendre et bien communiquer sur leur rôle et leurs missions. Mais ce temps, s'il perdure pour certains encore trop nombreux, est révolu pour beaucoup aussi.

Il convient d'arrêter de se regarder le nombril en espérant un monde meilleur qui ne dépend souvent que de soi. Le panel 2006 montre d'une part que les RSSI sortent de plus en plus de la DSI (40% en 2006 contre 57% en 2005) pour intégrer des Directions de la Sécurité (25% contre 8%) ou des Risques (11% contre 9%). C'est très encourageant mais pas une fin en soi.

C'est la voie dans laquelle les « managers » pourront s'engager. ***Quels que soient leur rôle et leur champ d'actions qui peuvent être très nombreux, ils doivent surtout gagner en indépendance.*** Mais les DSI ne doivent pas et ne peuvent pas se décharger de responsabilités majeures en sécurité des SI. Le véritable RSSI doit d'ailleurs rester au sein de la DSI. Et il doit être appuyé par une fonction transverse dont la mission n'est pas de protéger le système d'information mais de piloter les risques liés aux SI et aux informations. Ce propos peut sembler adapté aux grandes entreprises. Certainement, mais désormais des PME, plus ou moins importantes, se doivent aussi de gérer les risques dans cette logique, notamment vis-à-vis de leurs prestataires informatiques et télécoms.

La position hiérarchique est par contre plus significative et on constate comme en 2005 qu'en sortant de la DSI, on ne gagne pas nécessairement de niveau dans l'organisation ! Cette année les RSSI dépendant d'un membre d'un comité de direction / exécutif sont 32% contre 45% en 2005. Les N-2 passe de 32% en 2005 à 37% en 2006, les N-3 de 23% à 32%.

Attention, il ne faut pas accorder plus d'importance à ces chiffres qu'ils n'en ont. Ils montrent surtout ***la grande diversité, régulièrement constatée, dans le rattachement organisationnel et hiérarchique des RSSI. Il n'a toujours pas de « modèle ».***

Nous ne saurons d'ailleurs que trop insister sur le manque de définition des métiers de ces professionnels en charge de la gestion des risques informatiques et informationnels en entreprise. Mais l'empirisme a des limites !

Il ne faudrait pas que le RSSI se cantonne dans un rôle de caméléon s'adaptant aux menaces, technologies et cadres juridiques qu'on lui impose en permanence.

Pourtant des évolutions structurelles majeures sont en cours et nous tenterons de les déchiffrer aux pages suivantes en s'appuyant sur les résultats de l'enquête.

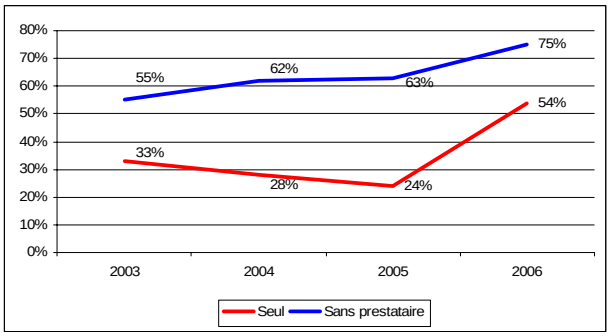

Figure 1 - Proportion du panel seul ou sans prestataire

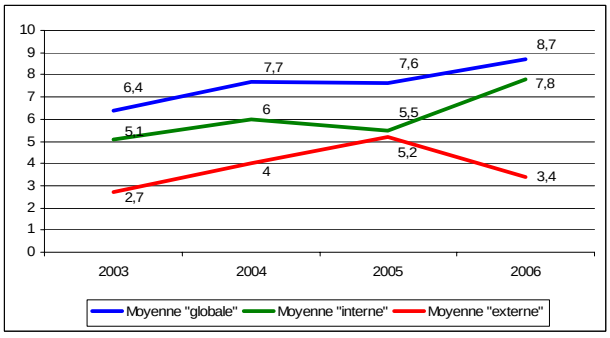

Figure 2 – Nombre moyen de collaborateurs dédiés à la SSI (par répondant)

Solitaires ou bien entourés ?

De nombreux RSSI sont seuls et parfois, ils ne sont pas dédiés aux questions de sécurité. Comment alors être responsable face aux nombreuses menaces visant un patrimoine informatique ou informationnel si complexe à protéger ?

La première surprise de l'enquête réside dans l'évolution du nombre de professionnels sans équipe. Nous sommes passés de 28% en 2004, à 24% en 2005. ***Mais en 2006, 54% du panel affirme travailler seul, sans équipe directe***. L'écart est considérable et doit être souligné.

En parallèle, le recours aux prestataires, évolue aussi significativement. Ils étaient 62% en 2004 et 63% en 2005 à ne pas s'appuyer sur des experts externes en régie. ***Or, en 2006, 75% du panel affirme ne pas avoir recours à des prestataires en régie.*** La progression est significative.

En revanche, l'évolution de la taille des équipes est aussi remarquable. A la hausse cette fois !

En effet, ***les équipes internes se sont étoffées.*** On atteint cette année la moyenne de 7,8 collaborateurs par équipe en moyenne, malgré les 54% de « solitaires ». C'est une évolution remarquable qui semble poursuivre l'évolution constatée depuis 2003, malgré la pause de 2005. Il y aurait une sorte de rattrapage qui s'explique dans un sens par un recours moindre à des prestataires en régie et sous un autre angle par la « mutation » d'informaticiens vers les métiers de la sécurité au sein d'équipes de pilotage, d'ingénierie ou d'assistance à maîtrise d'ouvrage. Ce point méritera d'être creusé en 2007.

Le recours aux prestataires en régie marque donc pour sa part une baisse significative après 3 années de hausse. L'internalisation s'accompagne aussi sans doute de missions au forfait, en mode projet. Les missions longues du ressort des équipes opérationnelles et informatiques ne dépendent souvent pas directement des professionnels du panel.

Les professionnels de la SSI qui réussissent dans leur mission augmentent donc considérablement leurs moyens humains sans faire appel à une forte expertise externe permanente. Inversement, les « solitaires » se développent, sans doute plus dans des rôles d'expertise ou de pilotage de correspondants au sein des métiers. Cette triple tendance doit être parfaitement intégrée dans les perspectives d'évolution des carrières. Trois profils se dégagent alors :

- un manager-directeur avec une équipe et un budget adaptés,
- un chargé de mission, d'abord expert du sujet,
- un pilote-coordinateur, bon communicateur avant tout.

Chacun, en fonction de son profil et de ses aspirations peut trouver le poste qui répondra à ses attentes. Mais les RSSI sans équipe sont aussi de faux solitaires tant ils doivent s'intégrer au sein de leur organisation, des projets et des processus critiques.

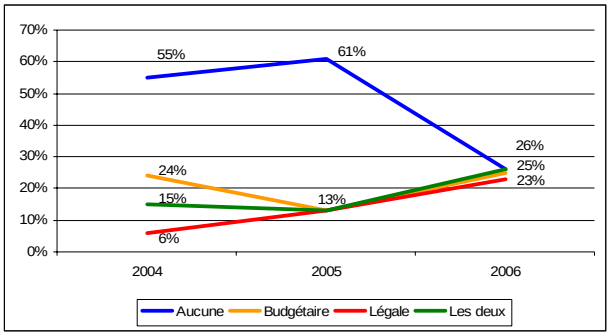

Figure 3 – Nature des délégations de responsabilités

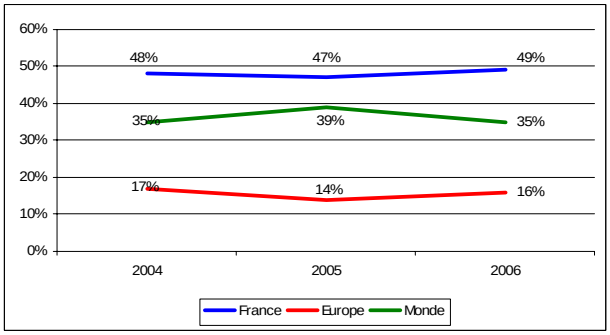

Figure 4 – Couverture géographique des RSSI

Part du panel qui intervient au moins une fois par an en Comité de direction / exécutif.

2006 : 53 % / 2005 : 55%

Un pouvoir qui s'affirme parfois à l'international

Avant d'obtenir du pouvoir et de l'assumer, les RSSI doivent souvent faire leurs preuves. C'est parfois un long cheminement, une bataille quotidienne, pour se faire connaître, reconnaître, comprendre, accepter, …

Et cela se complique encore plus lorsqu'on appartient à des groupes internationaux. Que l'on pilote des correspondants au sein de filiales à l'étranger ou qu'on soit, soi-même, membre d'un réseau, sous la responsabilité d'un patron de la sécurité basé à l'étranger, il convient toujours de faire comprendre et d'expliquer ses spécificités (souvent culturelles) à des interlocuteurs lointains ou d'imposer avec tact des mesures « Groupe » à des populations qui ont une vision très régionale du risque.

Certains témoignages de RSSI laissent néanmoins parfois penser que les « étrangers » (à la SSI) sont parfois très proches de notre beau pays !

Il s'avère donc logiquement plus simple d'intégrer une fonction de RSSI avec une bonne connaissance préalable de son entreprise, de son organisation, de ses hommes clés, de son histoire et de sa culture.

Il ressort de nos enquêtes menées depuis 2003, qu'une majorité de RSSI a pris ses fonctions dans le cadre d'une mobilité interne (voir Figure 5). Les écarts constatés depuis 3 ans ne sont pas significatifs et rentrent dans l'incertitude statistique. Environ 1/3 des RSSI n'a pas de connaissance de son entreprise à son arrivée. Ce n'est que plus difficile, plus long, pour eux, de lancer la démarche.

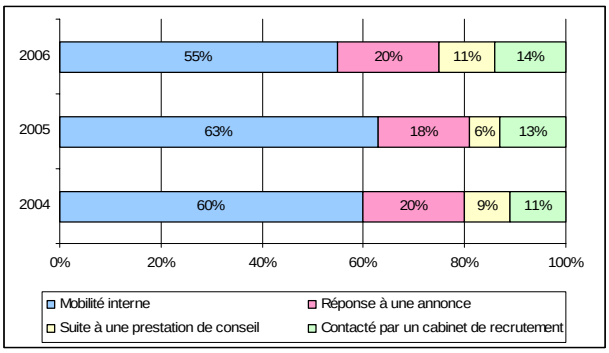

Figure 5 : Mode de recrutement dans le poste

La sécurité est d'abord une question de pouvoir. Pour le RSSI, elle ne peut s'exercer qu'au regard des responsabilités qui lui sont confiées que ce soit au plan du cadre légal ou des engagements budgétaires.

2006 est marquée par une très nette amélioration de la formalisation des responsabilités des RSSI. Cela peut sembler logique au regard de l'évolution des moyens humains. Cela peut néanmoins poser des problèmes lorsque les « solitaires » possèdent des pouvoirs de principe, sans réels moyens hiérarchiques et humains pour les assumer.

Si les professionnels de la SSI possèdent des responsabilités accrues, ils doivent néanmoins faire preuve de vigilance dans leur exercice quotidien.

- A lire : Maître Eric CAPRIOLI propose son approche détaillée du formalisme de la responsabilité légale du RSSI. A méditer et appliquer sans délai !

Le pouvoir du RSSI s'entend également au plan de son influence géographique. On observe une quasi-stagnation de leur champ d'action depuis que les enquêtes du Cercle sont réalisées. Il est néanmoins remarquable que la moitié du panel constitué de RSSI francophones œuvre dans des entreprises internationales. L'analyse des chiffres doit s'effectuer en tenant compte de ce paramètre essentiel.

Si les professionnels de la SSI exercent leur métier dans des entreprises nationales, ils doivent néanmoins faire preuve d'une observation quotidienne de la situation internationale.

- A lire : Mauro ISRAEL présente les convergences et divergences de vues entre les pays européens. La gestion du risque et de la sécurité repose toujours sur des approches culturelles propres à chaque pays. Mais des points communs existent néanmoins.

La mondialisation touche donc une part importante des RSSI, au quotidien. Des réseaux planétaires, une ouverture sur le monde ouvert via Internet, des clients ou fournisseurs internationaux, des menaces étrangères mais aussi domestiques. Tout concourt à leur donner une ouverture sur le monde tout en étant ancrés dans leur pays d'origine. Leur champ de responsabilité s'entend évidemment au regard du pays où ils exercent mais ils ne doivent pas ignorer les pratiques de leurs filiales, partenaires ou concurrents étrangers.

Une valeur qui se concrétise et se formalise

La reconnaissance d'un métier ou d'une fonction au sein d'une organisation est une préoccupation naturelle de tout individu. C'est notamment le cas pour ceux et celles qui interviennent en « support » dans des démarches souvent transverses. Ne pas appartenir au « business », aux équipes qui produisent, être un centre de coûts et non de profits, ne pas être en relation avec les clients et les usagers, etc. est parfois difficile à vivre, à l'heure des réductions d'effectif et de la quête permanente de productivité.

Par ailleurs, et c'est bien connu, la sécurité des SI est encore souvent perçue comme une contrainte lorsqu'on la présente comme un ensemble de règles et de processus qui perturbent l'efficacité d'activités qui n'ont parfois jamais vu l'ombre d'un virus, d'un pirate, d'un espion ou d'un escroc. Le RSSI est un « empêcheur de tourner en rond » comme on le lit parfois. Difficile d'exister dans un tel contexte !

Et pourtant, les professionnels de la sécurité ont désormais leur place dans les organigrammes. Ils possèdent aussi des cursus de formation et de certification individuelle. Et certains parviennent à posséder des salaires dignes de dirigeants.

Le salaire moyen calculé depuis 3 ans n'a de sens qu'au regard d'un panel restreint (60 à 80 RSSI plutôt avancés dans leur démarche) et d'une méthode de calcul particulière. Quelles que soient les bases de départ, l'enquête tend à fournir une valeur cohérente depuis 3 ans. C'est l'essentiel. Le salaire moyen n'augmente que de 1,3% entre 2005 et 2006. Mais la Figure 7, page suivante, apporte un autre éclairage intéressant.

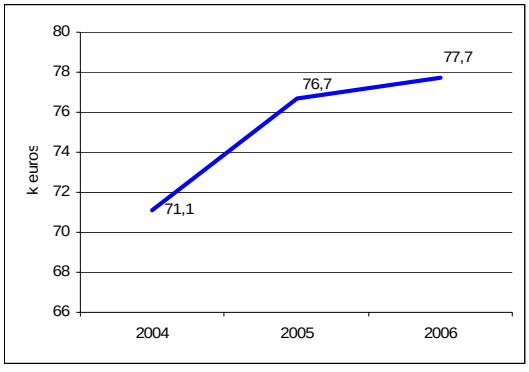

Figure 6 : Le salaire moyen des RSSI

Nous avions noté en 2005 une « prime à l'international » de l'ordre de 15% et des salaires « France » et « Europe » équivalents.

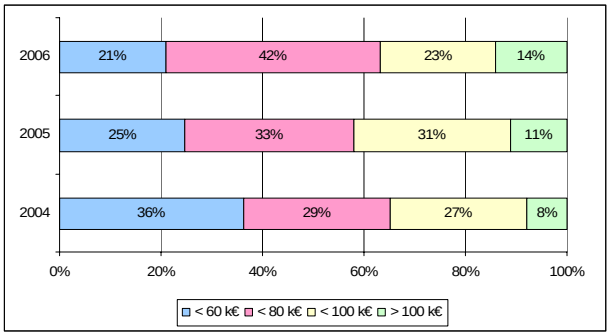

Figure 7 – Répartition des salaires des RSSI

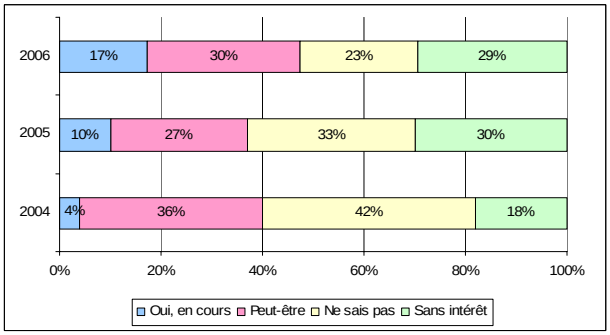

Figure 8 – Position sur les certifications individuelles

Avant de rentrer dans le détail de leur champ d'action et de leur rôle quotidien, analysons l'évolution des instruments de la reconnaissance formelle des RSSI.

Au plan salarial, l'analyse montre une progression des salaires « hauts » (supérieurs à 100 k€) et une diminution régulière des salaires « bas » (inférieurs à 60 k€). L'évolution est naturelle et logique. Le panel de RSSI est essentiellement composé de professionnels expérimentés.

Néanmoins, les postes de RSSI récemment ouverts sur le marché ne montraient pas des niveaux de salaire très élevés. L'influence du secteur d'activité comme la nature précise du poste influent considérablement sur les salaires proposés. La banque/finance/assurance et les télécoms proposent régulièrement les meilleurs revenus. Le profil de ces RSSI dépasse le cadre du SI et s'ouvrent depuis plusieurs années aux questions de « vie privée » et d'intelligence économique défensive avec un volet juridique et réglementaire très important.

La reconnaissance d'un métier tient aussi au diplôme et force est de constater que les progrès entraperçus les années précédentes se poursuivent, certes lentement.

	2004	2005	2006
RSSI avec diplôme / certification	21%	27%	31%

Une part toujours croissante du panel considère donc que diplômes et certificats sont un plus pour leur métier et leur carrière. On compte 17 diplômés / certifiés en SSI au sein du panel en 2006. Certains en possèdent d'ailleurs plusieurs.

Le CISM (Certified Information Security Manager délivré par l'AFAI-ISACA) est le plus représenté (5 citations) et c'est logique car il correspond le mieux au métier du RSSI « manager des risques ». Mais il est suivi avec 3 citations de 3 processus très variés : les formations SSI du Centre de Formation de la DCSSI, le ProCSSI (Professionnel Certifié en SSI – délivré par l'INSECA), et les Mastères SSI (délivrés par Sup Telecom ou l'UT de Troyes). On trouve enfin 2 CISSP (Certified Information System Security Professional – délivré par l'ISC2), 2 CISA (Certified Information System Auditor – délivré par l'AFAI-ISACA) et 1 auditeur certifié ISO 27001 (délivré par LSTI).

Comme pour les salaires, l'évolution est naturelle et quasi-mécanique mais elle peut encore paraître trop limitée. D'une part beaucoup de professionnels se sont formés « sur le tas » depuis de nombreuses années. A quoi bon retourner sur les bancs de l'école ou passer un examen ? D'autre part, la méconnaissance des processus de certification individuelle, désormais bien implantés dans les pays anglo-saxons et en Asie, explique aussi cette faiblesse. Ce n'est sans doute qu'une question de temps !
CFSSI : www.ssi.gouv.fr
CISM – CISA : www.afai.asso.fr ou www.isaca.org
ProCSSI : www.inseca.fr
CISSP : www.isc2.org
ISO27001 Lead auditor : www.lsti.fr

Chapitre 2
Patrimoine et vie privée au cœur des enjeux

Les bases de la sécurité des SI sont d'abord méthodologiques et techniques dans un cadre juridique donné. Depuis 20 ans, les entreprises ont d'abord cherché à protéger le système pour garantir la continuité des activités, se prémunir des attaques virales et des intrusions, respecter les obligations de protection des données personnelles.

Or, la lutte contre les pirates et la prévention des attaques logiques semblent être une histoire sans fin. Les menaces se renouvellent sans cesse et les collusions ou « convergences d'intérêts » sont de plus en plus flagrantes. Le marketing joue à plein et on n'y peut visiblement pas grand-chose, sous la pression des technologies et l'ingéniosité des pirates et criminels organisés. La lutte contre cette forme de cyber-criminalité n'est-elle pas perdue d'avance ? Mais il est vital qu'elle soit combattue !

Et les plans de secours informatiques. Seront-ils vraiment efficaces pour répondre à une crise majeure impactant une organisation, qui n'y sera pas nécessairement préparée ? Les analyses de risques, si utiles lors de l'étude des plans de prévention, demeurent indispensables. Malgré tout, lors de la crise, rien ou presque risque de se passer … « comme prévu ».

- A lire : Hervé SCHMIDT du Cercle Gaspar nous propose sous la forme de questionnements des alternatives pertinentes pour déterminer un meilleur équilibre entre prévention des risques et gestion de crise. Percutant !

Et que penser des bilans dressés par la CNIL sur le niveau de protection des données personnelles en France ? La situation ne semble pas très glorieuse tant au plan des déclarations, partielles ou incomplètes, qu'en termes de contrôles et de sanctions. Encore une loi trop peu appliquée ?

En clair, il fallait agir, cela a été fait, plus ou moins bien, avec plus ou moins de pertinence et d'efficacité, mais désormais d'autres horizons s'offrent aux RSSI. ***Les questions socio-économiques deviennent les clés de la démarche de sécurité des SI et de l'information.***

Ce chapitre apporte un éclairage détaillé du rôle et des activités des RSSI depuis 2004. Il confirme les constats des années précédentes.

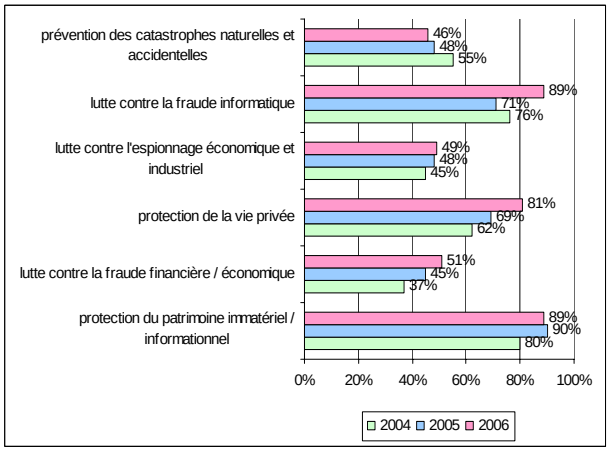

Figure 9 – Les enjeux couverts par les RSSI

Dès 2004, nous avons cherché à positionner le débat en termes d'enjeux et non plus d'objectifs de sécurité (confidentialité, disponibilité, intégrité, traçabilité). Car il nous a semblé évident que l'approche classique « technico-juridique » accompagnant la démarche de la Sécurité informatique (notamment les textes sur « informatique et libertés », et la « fraude informatique ») devait s'accompagner, sans la remplacer, d'une vision plus orientée vers les questions sociales et économiques.

L'évolution des centres d'intérêts stratégiques des RSSI est riche d'enseignement et préfigure sans doute des évolutions structurelles majeures.

Car on ne protège que ce qui a de la valeur : et qu'est-ce que le patrimoine d'une entreprise désormais ? En quoi les actifs incorporels se positionnent au cœur des démarches de gestion des risques ? ***Attention à l'amalgame, trop rapide, entre « système d'information » et « patrimoine immatériel » !***

Pour certains, la démarche est déjà bien engagée, mais peine à se concrétiser réellement. Pour les autres, il n'est jamais trop tard pour intégrer l'information, le savoir, la connaissance, les données financières et stratégiques, l'innovation au cœur même des questions de sécurité des systèmes d'information.

Ces résultats mettent encore une fois en évidence l'ambiguïté qu'il peut y avoir à être garant des libertés individuelles et responsable de la sécurité du système d'information.

L'éclatement de la SSI en 2 voire 3 domaines disjoints doit être clairement étudié. C'est une question clé sur laquelle nous reviendrons en conclusion.

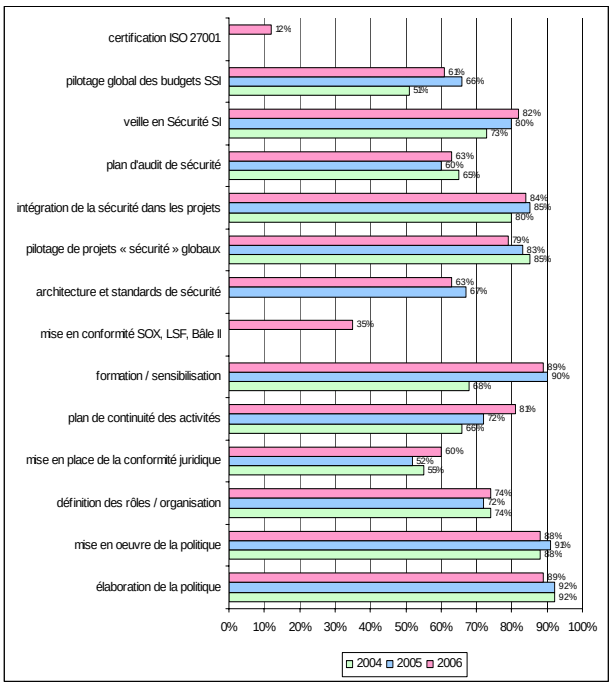

Figure 10 – Les actions transverses pilotées par les RSSI

Il est remarquable que d'une année sur l'autre, les variations sont extrêmement faibles pour de nombreuses actions transverses à l'exception de la continuité des activités.

Les incertitudes statistiques nous indiquent que pour la quasi-totalité des RSSI il y a 3 familles d'actions majeures et incontournables pour la fonction :

- Elaboration et mise en œuvre de la Politique
- Veille et Formation / Sensibilisation
- Démarches « projet »

Ce constat est globalement confirmé par les « fonctions clés » assumées par les répondants (voir Figure 12)

Néanmoins, pour 30 à 40% du panel, des questions majeures ne font plus ou pas partie du champ d'action :

- Les audits
- Les questions d'organisation
- Le pilotage budgétaire
- Les architectures et standards

Les raisons sont certainement plus structurelles que conjoncturelles. Par exemple, en ce qui concerne l'existence d'un budget « sécurité » centralisé, seulement 37% du panel affirment en disposer. Mais 60% néanmoins pilotent les dépenses, au moins à leur niveau.

37% des entreprises du panel ne possèdent pas de budget sécurité global.

De la même façon, les questions d'audit doivent être indépendantes des processus de sécurité eux-mêmes et les architectures de sécurité restent souvent du ressort des équipes informatiques. Il est compréhensible que certains, a priori, dans les petites structures, s'y impliquent, et que d'autres, non.

La plus belle progression concerne les démarches de continuité d'activité. S'il arrive parfois qu'elles sortent du champ d'action des RSSI dans le sens où une fonction spécifique peut exister dans certaines entreprises, les RSSI sont visiblement de plus en plus impliqués dans ces questions vitales à ne pas confondre avec les plans de secours informatiques.

Il est d'ailleurs désormais fréquent de voir des fonctions intitulées « Responsable Sécurité et Continuité ».

Enfin, les questions de conformité devenant de plus en plus pressantes, nous avons recueilli des réponses pour 3 thèmes.

La ***conformité juridique*** au sens large, touchant notamment à la vie privée, à la propriété intellectuelle, à la cryptographie, concerne 6 professionnels sur 10. La question est : pour les 40% autres, qui s'en occupe ?

Les ***règlementations sectorielles***, notamment dans les domaines de la Banque (Bâle II) et des activités financières (Loi Sarbanes Oxley, Loi sur la Sécurité Financière) ne doivent pas faire oublier que les domaines de la santé et des télécoms sont aussi fortement concernés. Elles représentent déjà une part significative du panel et les RSSI ont trouvé ici, un magnifique bras de levier, pour établir des états des lieux et améliorer les processus de base (gestion de la continuité, des identités ou des incidents).

Pour finir, nous ne pouvions pas ignorer la ***norme ISO27001***, véritable référentiel international des bonnes pratiques de management de la sécurité de l'information. En 2006, 12% du panel affirme s'être engagé dans une démarche de certification. Est-ce surprenant ou pas ? Beaucoup ou pas assez ? Le lecteur jugera …

La Sécurité des SI est véritablement (re) passée dans ***l'ère de la Protection des informations***, ce qu'elle est d'ailleurs depuis l'origine notamment dans les banques et le secteur gouvernemental (la cryptologie ou la science du secret !).

L'authentification / contrôle d'accès logique vise en 1er lieu aussi, à garantir un accès à ceux qui ont à « en connaître dans le cadre de leurs activités ». Nous vivons donc bien une sorte de retour aux sources.

Les questions de confidentialité passent en tête des processus.

Mais la Sécurité des SI doit aussi, plus que jamais, intégrer les infrastructures qui traitent et échanges les données. Et il n'est pas surprenant que la quasi-totalité du panel se préoccupe de gestion des attaques logiques, de correctifs, ou des plans de secours (qui progressent significativement aussi) etc. C'est le cœur du métier historique pour de nombreux RSSI.

Par contre, les questions plus « physiques » demeurent séparées pour plus de la moitié du panel. En clair, soit le RSSI s'en occupe parce que personne d'autre ne le fait, soit il ne le fait pas car un autre acteur s'en charge au sein d'une Direction de la Sécurité par exemple.

Mais insistons sur deux processus clés dont l'importance croissante se confirme. C'est une évolution fondamentale pour près de 70 % des professionnels :

- La cyber-surveillance et la supervision de la SSI
- La gestion des incidents et les investigations

Le RSSI s'implique clairement au-delà des missions classiques de prévention et protection pour incorporer des fonctions de contrôle voire d'enquête. Ce n'est pas nouveau et cela se confirme.

Néanmoins, attention danger ! Impossible à assumer au sein d'une DSI et sans une mission parfaitement formalisée. Si les apports méthodologiques et techniques de la SSI s'effacent, ils ne disparaissent pas. Ils restent du ressort d'une part des métiers (expression des exigences) et des équipes informatiques (ingénierie et architecture, production).

- A lire : Cyril AUTANT (Thalès) présente en quoi les services de supervision de la sécurité deviennent une des clés du management des risques.

Le rôle de « courroie de transmission » du RSSI doit tendre à s'estomper s'il souhaite devenir un véritable « manager – éducateur – contrôleur ».

Mais une chose est sûre : le cyber-surveillant est en marche.

Pour finir, on notera que la mise en place de la signature électronique et de mécanismes de sécurité pour les transactions dématérialisées stagne à 50% depuis 2004.

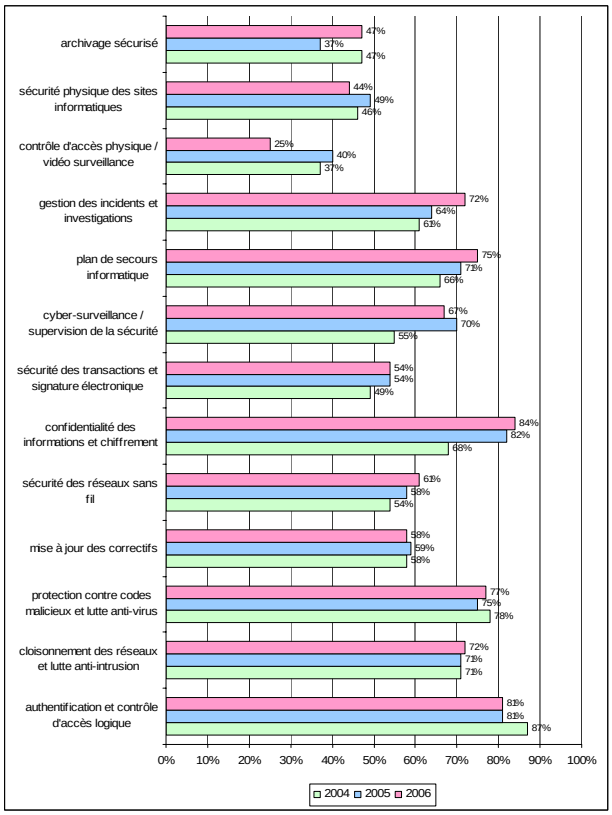

Figure 11 – Les processus opérationnels impliquant les RSSI

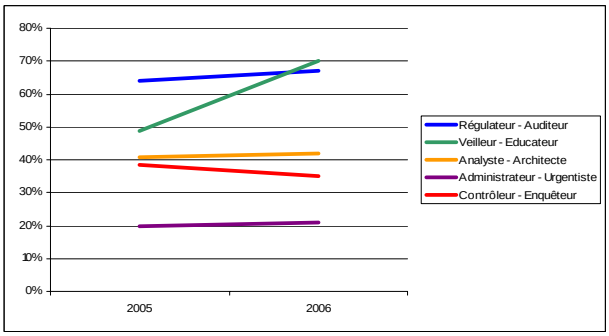

Figure 12 – Le poids des 5 fonctions clés de la SSI

RSSI aujourd'hui : un manager-éducateur avant tout

S'il n'y a sans doute pas deux RSSI qui se ressemblent, par leur parcours, leur personnalité et par le métier de leur entreprise, il convient néanmoins de dresser quelques points de repère essentiels. Un RSSI-manager est d'abord et avant tout en charge de piloter la démarche de protection des SI et des informations. En ce sens, il s'occupe avant tout des questions de « politique » et des « audits » de sécurité. A ce niveau, il sera assisté utilement par des collaborateurs et éventuellement par des prestataires. Il n'a pas à être un expert de tous les sujets pour réussir dans sa mission de pilotage. Ses relations avec des juristes notamment sont essentielles.

Néanmoins, sa démarche ne peut prendre de sens s'il reste dans sa tour d'ivoire : il doit être très ouvert sur le monde et sur son entreprise. C'est ici que ses activités de Veille et de Communication / Sensibilisation sont vitales. C'est à ces 2 niveaux qu'il exerce sa véritable expertise. Il possède alors un rôle essentiel d'aide à la décision.

RSSI demain : aussi un surveillant dans sa tour de contrôle ?

Mais demain, comment peut évoluer son rôle ? Les aspects techniques et opérationnels sont ou seront assumés par d'autres acteurs. Mais en ce qui concerne le contrôle et l'investigation, il est déjà acquis pour de nombreux RSSI que c'est une des voies d'avenir. Son indépendance, vis-à-vis des métiers et de la DSI, lorsqu'elle sera acquise, lui permettra d'intervenir au quotidien ou sur demande pour expliquer, analyser, comprendre des évènements anormaux, non conformes, … et la déontologie jouera un rôle essentiel. Cette évolution est à mettre en parallèle avec l'émergence du Correspondant Informatique et Libertés qui requiert le même type de positionnement (voir plus loin).

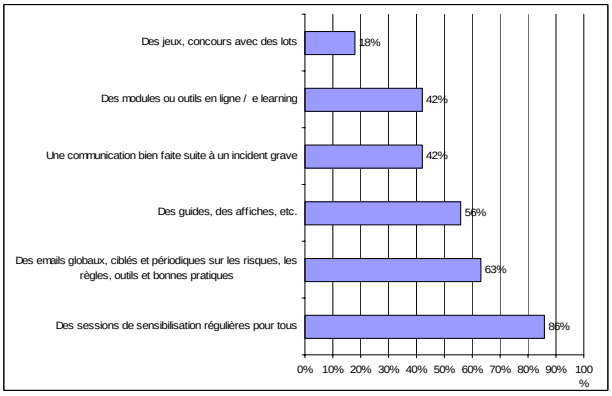

Figure 13 – Les meilleures démarche d'éducation en SSI

Nous avons vu que le veilleur-éducateur est la fonction clé au cœur de la démarche SSI. Elle progresse depuis 3 ans et démontre l'importance accordée au développement d'une culture du risque indispensable à la cohérence d'ensemble. Le RSSI doit réussir le bon cocktail : règlementation + technologie + organisation + comportement.

Le panel a donc été questionné sur ce qui lui semblait être les 3 meilleurs méthodes et outils de sensibilisation pour agir efficacement sur les comportements.

Le constat est clair : rien ne vaut le contact direct et le dialogue !

Néanmoins, il convient d'expliciter ce qu'est une session de sensibilisation en sécurité des SI. A qui s'adressent-elles ? Quels sont les messages que l'on souhaite faire passer ? A quel moment ? Pour quels motifs ? C'est un vrai projet, parfois complexe, quelque fois dangereux. Car le RSSI n'a pas droit à l'erreur, qu'il soit soutenu ou non, par sa direction et par le département formation, s'il existe.

On peut en effet, cibler les dirigeants, voire les managers. Ici, c'est d'abord au RSSI de se vendre : lui, sa démarche pour répondre aux véritables enjeux de son entreprise. Ensuite, on peut adopter une approche « grand public », visant tous les salariés. Mais comme souvent, à vouloir satisfaire les attentes de tous, on ne satisfait plus personne ! Sur la forme, il convient d'intéresser, de capter l'attention sur des sujets, quelques fois, contraignants ou rébarbatifs. Les jeux, les anecdotes (horror stories), les quiz sont très efficaces et donnent des résultats intéressants.

On peut parfois cibler les sessions par type de population (assistantes, commerciaux, équipes de R&D, informaticiens, etc.), et c'est certainement la

meilleure approche. Avec 56% de réponses, les supports matériels sont en 3ème position, bien placés. Ils sont souvent associés aux sessions de sensibilisation : le petit cadeau souvenir !

Mais le monde change et les sessions de sensibilisation, pour efficaces qu'elles soient, ne sont pas applicables pour tous. D'autres méthodes sont donc utiles, même si elles ne sont pas jugées « les meilleures » !

L'e-mail et l'Intranet sont des médias de communication idéaux pour communiquer sur la SSI. Tout RSSI se doit de s'appuyer sur eux à n'importe quel moment mais surtout pour de bonnes raisons (y compris lors d'incidents) ! Le seul et unique danger, résiduel, est qu'ils ne garantissent pas que les collaborateurs consultent, lisent, comprennent les messages et les documents que l'on met à leur disposition. C'est dommage, mais rien n'interdit de motiver toute l'entreprise à la démarche SSI, en associant à cette communication électronique, des « tests » ou des « quiz », pourquoi pas obligatoires, qui permettent de vérifier que les règles, pratiques, organisations, sont bien connues. Appliquées ? Seule l'expérience quotidienne peut le prouver ! C'est le sens qu'il faut sans doute donner aux 18% des jeux / concours avec lots que certains mettent en place. Ces pratiques ne sont pas dans la culture de nombreuses entreprises, mais parfois, dans l'industrie ou la finance, des RSSI ont mené des opérations avec succès.

Enfin, notons l'importance significative (42%) des solutions de sensibilisation, voire de formation en ligne. Les offres du marché sont très variées et la concurrence est en train d'apparaître. Elles vont d'un véritable cours avec test de connaissance à des animations / mises en situation expliquant le comportement adéquat. Des jeux ou des quiz proposent des solutions encore plus participatives et interactives. Bref, les solutions ne manquent pas et elles ne sont pas réservées à des grands comptes, loin de là. Il est possible d'atteindre des coûts inférieurs à 5 euros / personne. Est-ce beaucoup ? Est-ce trop ? Face aux enjeux, aux discours politiques et à l'importance accordée aux questions d'éducation ?

De toute façon, ***la clé de ces démarches consiste à cibler les messages et les contenus aux préoccupations précises de chaque entreprise.*** Toutes n'en sont pas au même degré d'avancement, n'ont pas défini les mêmes règles et pratiques, … Les produits du marché se doivent d'être suffisamment souples pour adapter leur contenu sans compromettre l'équilibre économique !

Chapitre 3
Le socio-économique doit prendre le relais

Comme nous l'avons dit plus haut, les RSSI ont depuis 20 ans et encore aujourd'hui une implication d'ordres technique et méthodologique. Les questions juridiques et réglementaires sont de plus en plus pressantes mais ne concernent pas toujours nécessairement une large proportion des professionnels.

La nature des enjeux couverts et l'importance accordée aux questions de confidentialité, de vie privée, de fraude et de protection du patrimoine, sont les signes évidents que les aspects sociaux et économiques sont au cœur de leur métier. Mais cela n'est pas encore suffisamment mis en évidence, ni très bien formalisé.

Nous souhaitons conclure et orienter l'analyse de l'enquête sur cet aspect majeur. En effet, il est devenu évident pour certains, car ils le vivent au quotidien, que la Sécurité des SI doit s'intéresser à la prévention des risques propres au SI (infrastructures et services en ligne), mais que la gestion des risques opérationnels doit aller au-delà : ***la protection de la vie privée et la protection des informations stratégiques de l'entreprise (sous entendu, les questions défensives des activités d'Intelligence Economiques) dépassent largement le cadre des fonctions des RSSI.***

- A lire : Paul-Olivier GIBERT (AG2R) explique que les questions de déontologie concernent au plus haut point les métiers de la sécurité. Plus que jamais, ayons à l'esprit le précepte du philosophe ALAIN : « Tout pouvoir sans contrôle rend fou. »
- A lire : Patrick LANGRAND (Natexis) présente sa vision et son expérience de RSSI ouvert aux questions d'Intelligence Economique. Un précurseur qui doit servir d'exemple.

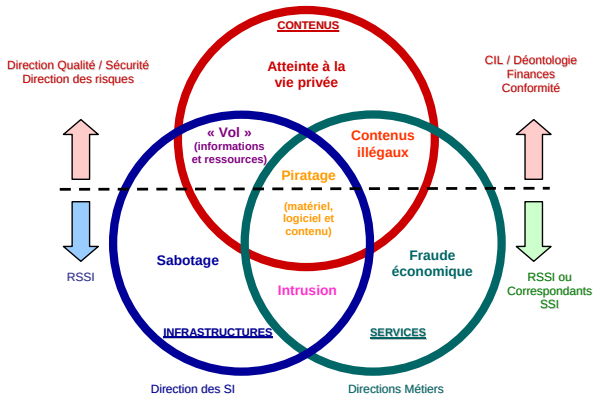

Figure 14 – Positionnement possible des sphères d'influence en relation avec la modélisation des risques

Depuis 2003, nous avons insisté sur l'apport d'une modélisation des risques en 7 familles s'adressant aux infrastructures, aux services et aux contenus. Force est de constater que ses apports vont au-delà d'une vision simplifiée et compréhensible des menaces qui intéressent directement la DSI, les métiers ou des fonctions spécifiques, plus transverses (risques, sécurité, finance, déontologie, etc).

Le schéma ci-dessus, s'il s'applique difficilement aux petites structures, est néanmoins éclairant sur les sphères d'influence qui existent dans les domaines de la gestion des risques et de la qualité/sécurité/conformité.

Le RSSI « opérationnel », au sein d'une DSI se préoccupe d'abord de qualité/sécurité informatique tandis que lorsqu'il collabore étroitement avec les métiers, éventuellement via des correspondants, c'est avant tout dans une démarche de lutte contre la fraude et la cybercriminalité qui peuvent impacter les activités à destination des clients ou des usagers.

Mais lorsque la préoccupation se concentre sur les informations en tant que patrimoine, force est de constater que l'on manque de repère. Les notions de propriétaire et de classification restent encore nébuleuses au sein de la majorité des entreprises.

C'est une prise de conscience collective au sein de l'entreprise qu'il faut créer. Et nous disposons maintenant de 2 bras de leviers essentiels :

- Les questions d'intelligence économique mettent en avant les menaces de nature « vol » (interception, appropriation, divulgation, etc.) et « contenus illégaux » (rumeurs, désinformation, etc.) et pourquoi pas de contrefaçon (ie. « Piratage » dans le modèle).

- Le développement du commerce en ligne démultiplie les menaces portant sur les individus et touchant à leur vie privée : profils comportementaux et de consommation, usurpation et vol d'identités, cyber-surveillance, …

Dans les deux cas, et pour des raisons différentes, ce sont les questions d'éthique qu'il faut mettre en exergue. Si l'on maintenait au XXIème siècle l'ancien précepte grec du Temple de Delphes, « Ne fais pas aux autres tout le mal que tu n'aimerais pas qu'il te fût fait ! », le développement de la société de l'information serait bien plus harmonieux.

Mais la guerre économique est parmi nous et le crime organisé ne cesse de gagner du terrain …

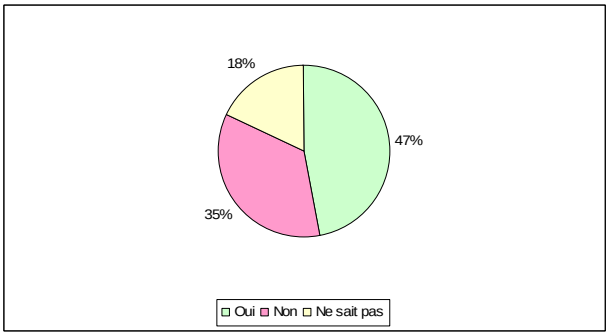

Figure 15 – Collaboration entre le RSSI et un Responsable de l'Intelligence Economique

La coupe est à moitié pleine, mais c'est déjà ça ! Tous les secteurs d'activité et toutes les entreprises n'ont pas la même sensibilité sur les questions liées à l'Intelligence et au Renseignement économiques et industriels. Néanmoins, toute entreprise qui n'innove pas, toute organisation (y compris certaines administrations) qui n'analyse pas, en permanence, son environnement en vue de ses décisions importantes, compromet ses capacités à répondre aux attentes de ses clients, usagers, actionnaires. De ce point de vue, ***il sera certainement intéressant d'analyser plus en détail les évolutions des métiers de la Sécurité des SI en relation avec les activités stratégiques de la veille, du marketing, de la R&D et de la finance.***

De la même façon, l'émergence des CIL (Correspondants Informatique et Libertés) au sein des entreprises apporte son lot d'incertitudes et d'adaptations. Créé par décret en octobre 2005, la fonction de Correspondant à la Protection des Données Personnelles (ou CIL) se développe lentement. En juillet 2006, moins de 200 ont été déclarés à la CNIL. Mais pour la moitié du panel, c'est déjà une réalité ou une perspective possible.

Question : le CIL est-il l'avenir du RSSI devenu Responsable de la Sécurité de l'Information ?

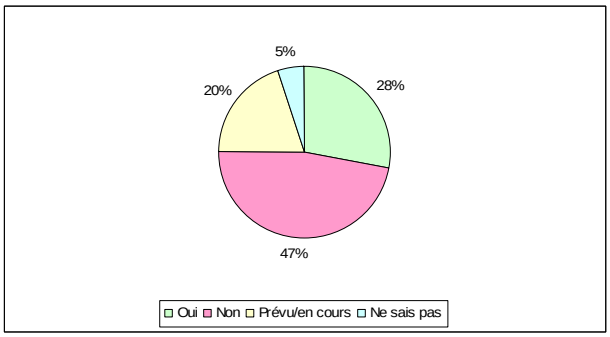

Figure 16 – Existence d'un Correspondant Informatique et Libertés

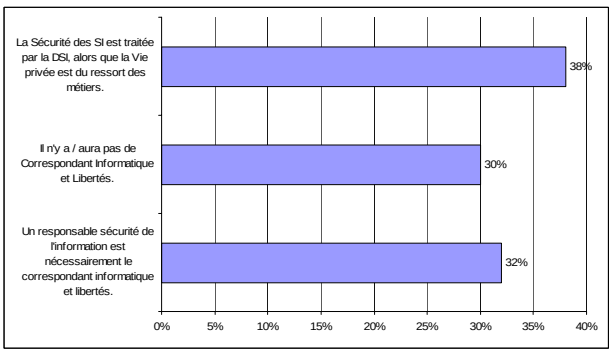

Figure 17 – Relations entre RSSI et CIL

Pour 30% du panel, il n'y aura pas de CIL dans leur entreprise. Certes ! Les procédures « CNIL » continueront donc d'exister et le RSSI collaborera avec des équipes juridiques, les DSI et les responsables des traitements. Comme depuis 1978.

Mais pour d'autres, ce n'est pas si simple. Pour 32% du panel, s'il existe un responsable sécurité de l'information, il est ou sera le CIL. Le mot « responsable » posera néanmoins problème vis-à-vis du « correspondant ».

Pour 38% du panel, le bon sens prime : Les métiers et les activités de l'entreprise sont les « responsables des traitements » donc les questions de « vie privée » et de « protection des données personnelles » sont de leur ressort. Néanmoins pas de manière exclusive ! Les équipes juridiques et informatiques doivent travailler étroitement avec les métiers et la DSI est considérée comme garante de la « protection des données personnelles ». Mais le CIL ne peut y être rattaché, pour garantir son indépendance.

Un bilan régulier de la mise en place des CIL en entreprise sera le bienvenu en provenance de la CNIL, notamment pour évaluer l'origine et les profils de ces nouveaux acteurs de la « sécurité de l'information ».

Conclusion : Un peu de prospective …

Gouvernance des risques et protection des informations (personnelles et stratégiques) sont les voies d'avenir « royales » pour de nombreux RSSI. Cela ne veut pas dire que la Sécurité des SI et les RSSI vont disparaître, bien au contraire. Mais ils doivent évoluer.

Certains iront donc vers les aspects les plus stratégiques liées à la guerre économique et aux menaces informationnelles, d'autres deviendront Correspondants Informatique et Libertés, d'autres encore seront plus que jamais concernés par la conformité réglementaire et normative. Il leur faudra sans doute se former aussi pour prendre à bras le corps leurs missions : aspects juridiques et économiques, déontologie, pilotage par indicateurs, … superbes perspectives ! Pour une sécurité des SI véritablement intégrée à la gestion des risques opérationnels de l'entreprise. Et non plus un « mal nécessaire ».

Nous avons justement posé 3 questions au panel pour apprécier leur vision sur ces évolutions possibles.

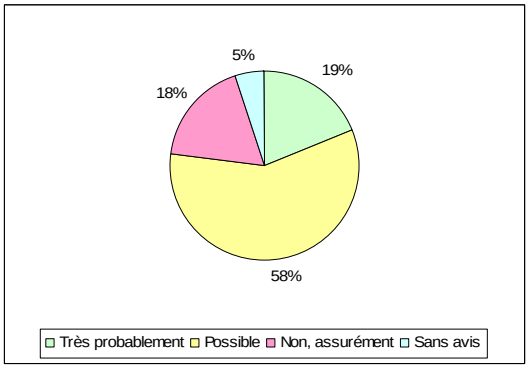

Figure 18 – La SSI historique sera-t-elle amenée à disparaître et se fondre au sein de la gestion des risques opérationnels ?

Pour une grande majorité du panel, la Sécurité du SI est une fonction à l'avenir incertain si se développent concrètement tous les métiers de la « gestion de risques ».

Dans ce cas, une sortie « par le haut » est envisageable mais reste à savoir qui garantira la mise en œuvre de systèmes d'information de qualité et sécurisés ? Les prestataires de service, hébergeurs et opérateurs uniquement ? Pourquoi pas !

Les questions de certification (ISO 27001 en particulier) seront alors vitales pour toutes les entreprises. Et les anglo-saxons comme les asiatiques l'ont bien compris. Rappelons que les années précédentes une majorité de RSSI considérait déjà qu'elles devraient être obligatoires au niveau de la société de service voire même, individuellement, au niveau de ses collaborateurs impliqués dans la sécurité.

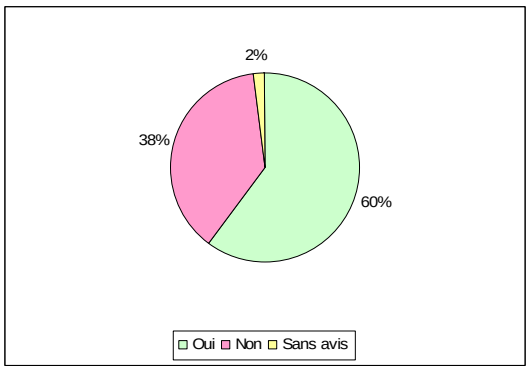

Figure 19 – Les innovations technologiques (sans fil, haut débit, VoIP, RFID, biométrie, etc.) révolutionnent-elles les approches historiques de la sécurité des SI ?

L'impact de la technologie peut aussi être significatif sur les métiers de la SSI et sur leur organisation. Le constat est partagé mais pour 60% du panel, le développement de nouveaux modes de communication aura des conséquences « révolutionnaires ». Nous n'avons pas étudié lesquelles ! Mais la vigilance s'impose. Il existe des invariants que la technologie ne modifie en rien et c'est sans doute plus dans les usages de la technologie, plus que dans la technologie elle-même, qu'il faut chercher les pistes de « révolution ».

Enfin, nous ne pouvions ignorer que, dans un contexte de « guerre économique » et sur un marché sensible comme celui de la sécurité, la faiblesse de l'offre européenne pose un problème de fond. ***Le sentiment européen est apparemment très fort ! 77% du panel souhaite voire émerger un « marché de l'offre » avec des produits et des services d'origine européenne.***

Espérons que l'innovation et le soutien à la formation seront importants et que surtout nos capacités à « vendre de la sécurité » s'amélioreront pour répondre à des enjeux d'évidence stratégiques.

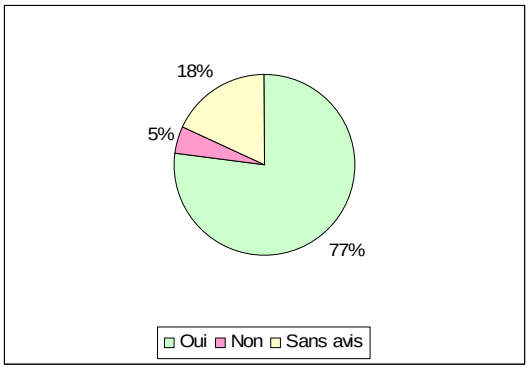

Figure 20 – L'émergence d'acteurs européens de la SSI contrebalançant l'offre américaine est selon vous un enjeu majeur.

Nous avons débuté cette synthèse par un rappel important : Une approche de la sécurité résolument orientée « client », une valeur ajoutée, et non une contrainte, un mal nécessaire.

Dans ce cadre, le RSSI - mais peut-on continuer à l'appeler ainsi ? – doit plus que jamais vêtir ses habits de « vendeur », de « promoteur » d'une culture de la sécurité qui intègre aspects juridiques, techniques, organisationnels et humains.

Face aux évolutions en cours, il convient désormais à la fois d'éclairer le présent mais aussi d'orienter l'avenir : où allons-nous ?

C'est ce que cette 4ème enquête propose dans la lignée des synthèses précédentes. ***Nous sommes face à une possible « explosion » de la fonction SSI selon deux scénarios.***

Du point de vue du marché, une triple segmentation s'opèrera en fonction des problématiques et des menaces concernées :

- La qualité / sécurité des SI : sabotage et intrusion
- La protection des données / informations : atteinte au patrimoine et à la vie privée
- La confiance du e-business / e-commerce : fraude et piratage

C'est plus un rappel qu'une nouveauté !

Du point de vue de l'organisation, la gestion des risques informatiques et informationnels intègrera :

- Des ***fonctions transverses*** : Gestion de risques, Déontologie, Conformité, Intelligence Economique, etc.
- Des ***fonctions opérationnelles*** : Qualité / Sécurité des SI au sein des DSI et chez les prestataires (SSII, opérateurs, hébergeurs, plates-formes de services, etc.)

Cette conclusion confirme les orientations des précédentes enquêtes. Les évolutions sont lentes mais réelles. Tout n'est question que de temps et parfois d'opportunisme.

Car le « temps réel » n'est pas celui de l'entreprise, ni celui du Web !

« LES GRANDS DEFIS DE LA SECURITE DES SI »

RECUEIL DES ARTICLES REDIGES PAR LES MEMBRES DU

PREFACE

par Isabelle TISSERAND
Coordinatrice du Cercle Européen de la Sécurité et des Systèmes d'Information

Ouverture des esprits et prise de conscience de l'ensemble des risques

En préambule, il nous paraît indispensable de souligner qu'en 2006, les experts en Sécurité des Systèmes d'Information se sont -enfin?- ouverts à tous les questionnements connexes que nécessite ce domaine. Plus question de se cantonner aux questions techniques. Nous avons tous compris que la SSI sert bien entendu la protection du patrimoine informationnel mais que sans un bon niveau de sécurité des patrimoines immobiliers et mobiliers, celle ci perd en puissance. De la même façon, nous sommes plus que jamais conscients qu'un travail reste à développer en sécurité comportementale. Les personnels doivent être de mieux en mieux informés, de plus en plus fiables, de plus en plus responsables, de plus en plus solides, de plus en plus citoyens.
Pourquoi? Tout simplement parce que nos systèmes de données véhiculent des informations professionnelles et nominatives de plus en plus stratégiques. La plus petite PME peut avoir un lien avec des entreprises et des projets plus importants et même s'ils paraissent éloignés, car les cloisonnements éclatent. N'importe quel réseau peut être utilisé, de manière séquencée, à des fins politique voire terroriste. N'importe quel maillon de la chaîne peut être détruit par un risque social, sanitaire, etc.
En synthèse, et même si nous répétons depuis maintenant plusieurs années qu'Internet n'a plus de frontières, la réalité est que tout se lie, que tous les niveaux de sécurité comptent et que nous devons apprendre à gérer des liaisons de crises. Le *leit motiv* des responsables de la Sécurité des Systèmes d'Information est resté durant des années concentré sur des objectifs technico-économiques. Voilà qu'on leur rappelle, grâce au droit, qu'ils ont des responsabilités civiles, pénales, sociales. Un utilisateur déviant peut mettre en péril l'image de marque d'une entreprise dans un monde devenu redoutablement concurrent, surveillé, fragilisé par la guerre de l'information. Un RSSI peut avoir à conduire ce même type d'individu devant la justice. Il lui aura fallut dans ce cas, être un as de la technique, avoir recours à ses connaissances sociales ainsi qu'à son potentiel humain pour gérer la situation.

Convictions et forces associées

Malgré la difficulté à prendre conscience des limites toujours plus vastes de notre domaine d'action, les forces se sont concentrées et se sont mélangées. Le Cercle Européen de la Sécurité des Systèmes d'Information a ouvert, autant qu'il l'était permis, tous les débats brûlants dont on parlait à mots couverts. Tous les membres du Cercle ont concouru à l'avancée de nos réflexions et de nos développements par leurs présences, leurs participations, leurs conférences, leurs interviews. Et c'est bien cela qui nous permettra de continuer à faire face à la complexité de nos missions et de nos métiers dans le futur. Ainsi, il est clair que l'effort porte plus que jamais sur la qualité des partenaires et des prestations techniques. Sans ce socle rassurant et toujours en évolution, les professionnels de la sécurité de l'information ne peuvent pas se consacrer aux autres questionnements que pose la protection des patrimoines. La consolidation de cet alliage est au centre des préoccupations

du Cercle durant les Assises de la Sécurité et des Systèmes d'Information. Les échanges, sans restriction, doivent converger vers la création future de politiques de sécurité pluridisciplinaires et qui ne négligeront aucun aspect à traiter. Les partenaires sont présents pour nous faire bénéficier de leurs avancées technologiques. Ces convictions et ces *task forces* reflètent les grands défis de la sécurité de demain. Par conséquent tous les articles sélectionnés pour notre LIVRE BLEU DE LA SECURITE doivent contribuer à une amélioration notable de nos pratiques.

Il ne s'agit pas d'apporter des réponses immédiates à toutes les questions posées. Il s'agissait, dans un premier temps, d'élargir nos consciences et il s'agit, demain, de mieux comprendre comment fonctionnent les autres systèmes européens de manière à fluidifier nos coopérations interculturelles qui seront de plus en plus nombreuses. La question des normes est importante car elle induit de nouvelles réflexions aussi bien pour ce qui concerne la formation des personnels que pour l'installation de nouvelles technologies. Le débat sur les formations homologuées reste d'actualité, le profil juridique des professionnels indispensable à connaître, le paysage interculturel bien utile à cerner tandis que la réflexion sur l'Intelligence Economique englobe quasiment tout le questionnement sans lequel nos méthodes ne pourront évoluer.

© Isabelle TISSERAND

« Etat, entreprises, individus : synergie des savoirs et culture du cyber-risque »

par Pierre-Luc REFALO
Directeur associé Icys-Formation

« *Si vous pensez que l'éducation coûte cher, essayez l'ignorance.* » A-t-on un jour mieux exprimé qu'Abraham LINCOLN (1809-1865), il y a près de 150 ans, à quel point l'ignorance était l'un des plus grands fléaux de l'humanité ? Internet n'existait pas et les conflits planétaires étaient d'abord idéologiques et religieux. Si ces derniers n'ont pas disparu, la 4ème guerre mondiale a débuté, initiée par la chute du mur de Berlin. Elle est économique mais toujours idéologique, planétaire mais désormais sans frontière. La menace n'est plus clairement identifiée, les « amis », les « enfants » sont aussi devenus des « ennemis ». Le crime organisé et les mafias sont dans la partie, et œuvrent au coin de la rue comme aux antipodes. Les impacts ne sont plus des destructions et des morts sur les champs de bataille, mais des chômeurs, des exclus et des affamés. Et si l'argent reste le nerf de tous les conflits, c'est désormais la maîtrise de l'information (stratégique, économique, personnelle) qui permet de gagner dans la compétition - guerre planétaire. Or cette information est de plus en plus numérique et s'échange à la vitesse de la lumière, parfois avec des tiers que l'on ne connaît pas.

Ce premier constat est bien connu des spécialistes, de certains dirigeants et de responsables politiques. Mais qu'en est-il pour les citoyens et les salariés ? Sécurité informatique, des Systèmes d'Information, de l'information, cyber-risques et espionnage économique, atteintes à la vie privée, rumeurs, manipulations, fraudes et chantages, escroqueries en col blanc, détournements, pédophilie sur le Net, etc. De quoi parle-t-on au fait ? Plus que jamais, face à cette complexité, un véritable enseignement sur les enjeux et les risques réels, selon une approche systémique et grand public devient une exigence majeure pour ne pas dire urgente. Le Député Pierre LASBORDES le rappelle avec insistance dans son rapport de novembre 2005 à l'attention du premier Ministre (« La sécurité des SI : un enjeu pour l'Etat »). ***Il n'est jamais trop tard, en effet, pour améliorer et renforcer nos organisations et nos actions de communication ou de sensibilisation !*** Nous avons ici beaucoup à apprendre des américains et des anglo-saxons. Mais …

Si l'Etat ne doit pas, ne peut pas être absent du débat, il ne peut pas tout faire. Car au-delà de la prise de conscience et la mise en place, pourquoi pas, de filières de formation structurées et adaptées aux besoins du marché, les contenus ne doivent pas ignorer le monde réel, celui de l'entreprise, des associations, du commerce en ligne, des échanges interpersonnels (le P2P, les blogs et les SMS en sont les meilleurs exemples). ***Un étroit partenariat public / privé sera la clé du succès de l'émergence de la culture « cyber-risques »***. Ici encore, nous pouvons nous inspirer de pratiques bien connues outre-Atlantique et outre-Manche. Mais …

Attention, en effet, aux abus et aux excès des comparatifs simplistes ! La vérité d'aujourd'hui n'étant pas celle de demain, prudence et souplesse doivent guider l'action. Car la communication sur les risques et sur les mesures de sécurité est depuis 20 ans le fait des offreurs (à 80% américains) qui ont d'abord créé des réflexes d'achat d'outils (« business is business ! »). On ne sait plus de quoi et pourquoi on doit se protéger, mais on sait comment !

Et qu'on le veuille ou non, ***les dispositions techniques et juridiques ont au mieux des limites, au pire des effets pervers.***

Le marketing de la peur, d'essence américaine, fonctionne mais au grand profit de l'économie US. Que penser d'un journal de 20h où l'on annonce que pour se protéger du phishing, il faut avoir un anti-virus à jour ?! Que penser aussi, bien qu'il faille s'en féliciter, d'un partenariat entre l'Education Nationale et Microsoft au sein du projet Confiance pour éduquer les enfants dans les écoles ? Les américains agissent et mobilisent des moyens pendant qu'on réfléchit. C'est ainsi !

De leur côté, les mesures législatives (souvent d'origines française et européenne) donnent bonne conscience mais les compromis sont très délicats à trouver. Les discussions et les conclusions de la loi DADVSI (Droits d'Auteur et Droits Voisins dans la Société de l'Information) le démontrent clairement. Existe-t-il seulement une solution acceptable pour tous ? Et quels seront ses effets dans le temps, si elle est appliquée un jour ? Les mesures techniques de protection seront « cassées » en quelques semaines par de simples chercheurs ou par les partisans de la liberté totale et du mythe de la gratuité. Les mesures de surveillance et de répression, soutenues par les producteurs et distributeurs, peuvent avoir un sens si elles ont un véritable effet dissuasif, sans enfreindre les libertés fondamentales. Délicat équilibre !

Sur le fond, des questions essentielles doivent être rappelées et précisées en permanence. Et les réponses ne sont pas aisées : Qui est **propriétaire** d'un contenant ou d'un contenu ? Qui possède les **droits d'usage** et non plus des droits d'accès, et selon quelles modalités ? Quelles sont les **espaces de liberté** ? Au profit de qui ? Qu'est-ce que la **confidentialité** aujourd'hui ? Et le **secret** a-t-il encore un sens ? ***Car, principes essentiels, on ne protège que ce qui a de la valeur -l'information, le savoir- en se focalisant toujours sur le maillon faible : l'individu.***

Et on le constate chaque jour, l'Etat, les entreprises et les individus sont tous impliqués dans cette révolution numérique. Dossier médical personnel, droits d'auteur et commerce en ligne, vie privée et terrorisme, modernisation de l'Etat, pôles de compétitivité, voire affaire Clearstream, tout est lié et les risques informatiques et informationnels sont omniprésents ! ***Donc, tous doivent partager des principes, des valeurs, un vocabulaire, une vision. Et surtout un discours qui évite de prendre les dirigeants, les parents et tous les citoyens pour des imbéciles ou des enfants. Et là est sans doute le véritable enjeu de société.***

Si tout individu doit être informé et conscient des risques, il doit aussi être acteur. Or, il ne peut le devenir que si on est capable de démontrer les causes et les conséquences des incidents réels. On ne peut plus rester dans la « potentialité » pour ne pas dire le virtuel. Il est bien dommage de n'avoir que des statistiques américaines ou celles de cabinets d'audit pour mesurer la nature et les impacts, notamment économiques des cyber-risques. Il est encore plus dommage qu'une association professionnelle fasse l'effort, louable, de dresser des bilans de la cybercriminalité mais qui sont surtout des revues de presse de faits divers un peu trop sensationnels. Quelle est la vraie réalité, qu'elle concerne la multinationale, la PME, l'Etat, le cyber-consommateur ou l'adolescent chez ses parents ?

Pour en avoir, ne serait-ce, qu'une petite idée, ***il faut rompre avec le mythe de la sécurité totale et du risque zéro***, pourtant toujours bien présent. Si tout ne peut pas être public, les expériences positives et négatives doivent être exploitées pour justifier, améliorer les pratiques de sécurité en entreprise, dans les administrations, au domicile, en déplacement. Seule la transparence sur la réalité des cyber-risques facilitera la prise de conscience du plus grand nombre. Un grand opérateur britannique publiait sur son Intranet, la liste de tous les incidents, piratages, fraudes, sabotages, vols, … détectés et investigués. Or, ce qui transparaît dans les médias n'est que la partie immergée de l'iceberg ! Et nombreux sont ceux qui parlent de cyber-risques sans en avoir la moindre expérience …

Enfin, si chacun doit être acteur de sa propre sécurité, des professionnels de la sécurité des SI sont chargés d'assister les organisations avant, pendant ou après un incident ou un sinistre quelconque. Néanmoins, très peu ont reçu une véritable formation initiale ou continue. Des séminaires et conférences d'offreurs, des groupes de travail associatifs apportent le minimum de connaissances utiles au quotidien. Pourtant, depuis quelques années, une offre de formation s'est structurée et des certifications individuelles sont désormais disponibles. Le danger est grand, notamment pour les PME, les plus vulnérables, qui font appel, sans véritable contrôle, à des prestataires pour le gardiennage et l'entretien et désormais pour des services informatiques et télécoms. ***Le marché doit enfin se structurer et se professionnaliser*** pour éviter, notamment, que des « audits » ou de la « sensibilisation » ne soient réalisés par des vendeurs de solutions. Il sera notamment nécessaire de décrire les fonctions clés de la gestion des cyber-risques et de proposer des cursus de formation adaptés. Des bases de travail solides existent déjà au sein de la DCSSI (Direction Centrale à la Sécurité des Systèmes d'Information) et d'écoles à l'enseignement de qualité impliquant des professionnels issus de l'entreprise. ***Mais un processus qualitatif doit se mettre en place et le rôle des associations professionnelles doit être rappelé ici.***

« A pratiquer plusieurs métiers, on ne réussit dans aucun. » L'enseignement de Platon (427 av JC – 348 av JC) n'est pas inutile pour rappeler que n'est pas manager, architecte, policier ou éducateur qui veut. L'heure des choix a sonné pour que chacun comprenne enfin qu'il est acteur de sa propre sécurité mais aussi que le recours à des professionnels ne peut plus s'opérer sans une réelle qualification / certification. ***La synergie des savoirs concerne donc essentiellement un réseau de formateurs, éducateurs indépendants et des donneurs d'ordre qui s'accordent d'une part sur une pédagogie claire, d'autre part sur la diffusion de contenus de grande qualité, éprouvés au quotidien, auprès du plus grand nombre comme des professionnels de la sécurité dévoués à des enjeux stratégiques et avant tout d'ordre socio-économique.***

Sinon, le marketing de la peur vaincra, l'ignorance des foules perdurera, les « juges et parties » continueront d'abuser de leur pouvoir et les catastrophes ne trouveront d'explication que dans la trop facile erreur humaine ou la défaillance du « système » !

© Pierre-Luc REFALO
www.icys-formation.com

Régime juridique du Responsable Sécurité des Systèmes d'Information

par Eric A. CAPRIOLI
Docteur en droit, Avocat à la Cour de Paris, Caprioli & Associés Société d'avocats

Le RSSI (ou le Responsable Sécurité de l'Information) « *incarne* » la sécurité de l'information au sein de l'entreprise (ou dans un groupe d'entreprises) ou de l'autorité administrative. Le périmètre de son intervention est essentiel, mais la position hiérarchique et nécessairement transversale du Responsable de la sécurité des systèmes d'information (RSSI) est également très importante dans la mesure où elle influe directement sur les pouvoirs et responsabilités de celui-ci. L'efficacité de la sécurité des systèmes d'information est ainsi conditionnée par son positionnement interne**.** La sécurité des systèmes d'information s'entend de la sécurité physique des matériels et systèmes (ordinateurs, réseaux etc.) mais aussi d'une approche proactive et réactive en termes stratégiques et organisationnels.

Sa fonction est d'assurer la protection et la valorisation du patrimoine informationnel de l'entreprise. Et pour ce faire, plusieurs missions peuvent lui être confiées :

- **le conseil** pour ce qui concerne *les risques dans le domaine de la sécurité des systèmes d'information à l'intérieur de l'entreprise ou du groupe* ;
- **la conception de la sécurité des systèmes d'information** en termes organisationnels, procéduraux, stratégiques, technologiques, juridiques et de produits. Il lui incombe aussi d'établir tous les documents lui paraissant nécessaires pour garantir la sécurité au sein de l'entreprise (politique de sécurité, guides, chartes, …). Il doit également disposer d'une équipe tant dans la société mère que dans ses filiales pour la maîtrise d'ouvrage de la sécurité et travailler en collaboration avec les personnes adéquates au sein de la direction des systèmes d'information et notamment de « *correspondants* » : sécurité logique, SSI dans les entités d'un groupe, plans de secours métiers et PCA/PRA[1], …, données à caractère personnel ;
- **le rôle de contrôle et de surveillance des systèmes d'information**. Le RSSI veille à la détection des risques et à l'efficacité des plans d'action menés afin de les réduire et d'en pallier les impacts. Le RSSI doit mettre en œuvre des outils de contrôle des modalités d'utilisation des systèmes d'information et assurer ce contrôle au regard des problématiques de sécurité, *dans les limites autorisées au niveau légal et jurisprudentiel du contrôle de l'activité des salariés*[2]. Ce rôle s'inscrit également pour les cas d'incidents (procédure de détection des risques, alertes pénales, indisponibilité, substitution, mise en route des plans de continuité et de secours des SI, …). Il doit le cas échéant, alerter les responsables techniques, superviser la mise en œuvre des procédures et rendre compte. Une véritable approche de « *risk management* » doit en découler ;

[1] V. Eric A. Caprioli, *Plan de continuité d'activité des systèmes d'information : aspects juridiques*, octobre 2005, disponible sur www.caprioli-avocats.com.
[2] V. infra.

- **la veille stratégique et l'intelligence économique**. La veille permet au RSSI d'anticiper les nouveaux risques pour l'entreprise (ou l'autorité administrative), de mieux les prévenir, voire de les éviter mais aussi de mettre à jour de nouvelles opportunités économiques, stratégiques et technologiques. C'est pourquoi cette veille doit aussi porter sur les projets de textes (directive européenne, lois, décrets, …), règles, jurisprudences ou normes ayant une incidence sur le périmètre de la sécurité des systèmes d'information de l'entreprise. Il est vrai que le patrimoine informationnel des entreprises constitue un enjeu économique majeur[3]. Dans ce cadre, la dimension juridique ne doit pas être négligée, bien au contraire et une démarche d'intelligence stratégique et juridique doit être mise en place[4]. L'installation d'un tableau de bord de l'intelligence juridique et stratégique de la SI permet un pilotage adapté aux besoins de l'entité.
- **la conformité (« compliance »)**. Les axes et procédures en matière de sécurité des systèmes d'information doivent être en adéquation avec toutes les obligations légales, réglementaires et normatives applicables en la matière (et ce y compris les bonnes pratiques). Par exemple, les secteurs de la banque, de la finance et de l'assurance y sont soumis dans le cadre du contrôle interne. Le RSSI doit agir dans le respect de la législation applicable (directement ou indirectement) à la sécurité informatique. L'évolution des règles juridiques relatives aux secteurs d'activité de l'entreprise devra donc être connue et surtout anticipée par le RSSI. En effet, une évolution du cadre juridique peut imposer des modifications organisationnelles, la mise en place de nouvelles procédures ou des changements techniques. L'anticiper permet donc d'éviter toute désorganisation liée à l'urgence, de prendre les bonnes décisions et de les mettre en œuvre progressivement.

Pour appréhender l'incidence du droit sur le RSSI, il est capital de partir de l'organisation de l'entité en cause (organigramme et périmètre des fonctions attribuées). Cette démarche est nécessaire puisqu'elle permet d'analyser les contraintes propres à l'entité et de prévoir les règles de sécurité qui lui seront applicables. A ce titre, il conviendra de mettre en place une politique de sécurité de l'information mais aussi une formalisation des obligations et responsabilités du RSSI **: le Guide juridique du RSSI. Cela permet de mieux évaluer les risques juridiques qui relèvent de la fonction.** Nous prendrons le parti de ne traiter que de certaines obligations auxquelles le RSSI peut être assujettis, mais d'autres obligations existent, elles doivent être définies aussi précisément que possible en raison des responsabilités qui en découlent dans le cadre du guide juridique du RSSI.

La prise en compte de l'ensemble des missions du RSSI, permet de déterminer au mieux ses obligations juridiques (I) et le régime des responsabilités applicables (II).

[3] V. Rapport d'information sur *la* stratégie de sécurité économique nationale, N°1664, déposé le 9 juin 2004, présenté par M. B. Carayon, disponible à l'adresse : http://www.assemblee-nat.fr/12/rap-info/i1664.asp.
[4] V. Eric A. Caprioli, *L'intelligence économique dans l'économie numérique*, Netcost & Security, en octobre 2005 et disponible sur le site : www.caprioli-avocats.com. .

I. Les obligations du RSSI

Le RSSI est en charge de la responsabilité de la sécurité des systèmes d'information. A ce titre, de nombreuses obligations peuvent trouver à s'appliquer en fonction du périmètre de ses fonctions et des délégations de pouvoirs qui en découlent.

A. Les obligations découlant du contrôle interne

La loi de sécurité financière du 1er août 2003 (dite LSF) impose aux présidents de sociétés anonymes ou de sociétés **faisant appel public à l'épargne** de rendre compte, à travers un rapport de gestion relatif aux comptes, « *des procédures de contrôle interne mises en place par la société* »[5]. Cette obligation vise à renforcer la transparence au sein des sociétés et implique pour les dirigeants que leurs responsabilités puissent être engagées, notamment en cas de dysfonctionnement du système d'information, **dans la mesure où celui-ci impacte directement le contrôle interne[6].**

Le système d'information est à la fois objet et support du contrôle interne. Le RSSI doit donc être en mesure de s'assurer de la conformité dans les domaines suivants :

- organisation, stratégie et fonctionnement du système d'information ;
- présence de contrôles importants au sein des applications et des interfaces, ainsi que l'utilisation transversale des systèmes ;
- mise en place des plans de continuité et de reprise d'activité (PCA/PRA) et donc y compris les plans de secours.

Le RSSI est tenu de définir les moyens, les procédures et les règles liées à la sécurité informatique nécessaires pour répondre aux exigences et caractéristiques du contrôle interne.

B. Les obligations relatives aux données à caractère personnel

Les données circulant sur les systèmes d'information d'une entreprise permettent souvent d'identifier une personne déterminée (clients, prospects, fournisseurs, salariés). Il s'agit donc de données à caractère personnel. A ce titre, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée notamment par la loi du 6 août 2004[7] trouve à s'appliquer. Elle définit les principes à respecter lors de la collecte, du traitement et de la conservation de ces données (information de la personne, consentement préalable pour l'utilisation des données, respect de la finalité du traitement, conservation des données et anonymisation, sécurité et confidentialité des données, droit d'accès, de rectification et d'opposition quant au traitement des données qui concernent le titulaire, respect des formalités préalables à la mise en œuvre des traitements).

[5] Article 117 de la loi n°2003-706 du 1er août 2003, dite Loi de sécurité financière, J.O. du 2 août 2003, p. 13220.
[6] V. pour le domaine bancaire, Eric A. Caprioli, *Commentaire de l'arrêté du 31 mars 2005 modifiant le règlement du comité de la réglementation bancaire et financière n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement*, Com. Comm. Electr., octobre 2005, p. 49 et s.
[7] J.O. du 7 août 2004, p. 12483 et s.

La loi précise les sanctions pénales applicables pour toute entreprise qui ne respecterait pas ces obligations[8]. Aux termes de la loi, c'est en principe le responsable du traitement qui engagera sa responsabilité pénale.

Le RSSI devra mettre en place la sécurité informatique conformément à l'article 34 de la loi de 1978. Cet article dispose que le responsable du traitement doit prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Selon les missions qui lui sont confiées, **le RSSI peut amener à élaborer une politique « *Vie privée et données personnelles* » pour son entreprise** (mais d'autres services ou directions peuvent en être chargés).

C. Les obligations relatives à la cryptologie

Dans le cadre de la mission de sécurité dont il a la charge le RSSI va devoir mettre en place des procédés garantissant la confidentialité de certaines données et/ou documents. En outre, la mise en place de signature électronique ou de certificats électroniques notamment à des fins « *d'authentification* » pourra être réalisée[9].

Le RSSI doit s'assurer que les règles juridiques applicables sont respectées[10].

D. Les obligations relatives à la traçabilité

Sans être visés par un texte particulier, les **entreprises** – et les RSSI plus particulièrement - doivent prendre les mesures techniques nécessaires à la conservation des données de connexion des salariés[11]. Il s'agit, de se prémunir contre toute utilisation illicite des moyens informatiques mis à disposition de leurs employés et ainsi, d'éviter de voir leur responsabilité pénale mise en cause devant les tribunaux. Ces mesures techniques doivent être complétées par un document juridique permettant la surveillance des salariés : la charte d'utilisation des moyens informatiques[12]. Il est admis, que sur le lieu et pendant le temps de travail, soient mis en place des règles et des moyens de surveillance et de contrôle des salariés.

[8] V. en ce sens, Isabelle Cantéro, *Présentation de la nouvelle réglementation applicable à la protection des données à caractère personnel*, Journal des sociétés, mai 2005, p. 28 et 29.
[9] V. Eric A. Caprioli, *Ecrit et preuve électroniques dans la loi n°2000-230 du 13 mars 2000*, JCP, éd. E, Cah. Dr. Entrep., n°2, année 2000, p. 1 et s ; *La loi française sur la preuve et la signature électroniques dans la perspective européenne*, JCP éd. G, I, 224, mai 2000, p. 787 et s ; *Le juge et la preuve électronique*, 10 janvier 2000, disponible sur www.juriscom.net.
[10] V. Eric A. Caprioli, Pascal Agosti, *La confiance dans l'économie numérique*, Petites Affiches du 3 juin 2005, p. 4 et s
[11] Eric A. Caprioli, *Responsabilité des prestataires du commerce électronique et conservation des données aux fins de traçabilité*, in *Traçabilité et responsabilité*, sous la direction de Ph. Pédrot, éd. Economica, 2003, p. 114 et s. et www.caprioli-avocats.com.
[12] V. Eric A. Caprioli, *Cybersurveillance des salariés : du droit à la pratique des chartes informatiques*, Petites Affiches du 29 sept. 2004. V. également la Table ronde intitulée *Cybersurveillance – Plaidoyer pour un humanisme numérique*, avec Agathe Lepage, Eric A. Caprioli, Norbert Fort, Cah. Dr. Entrep., n°4, juillet-août 2005, p. 11 et s.

La sécurité des systèmes d'information passe par cette « *cyber surveillance* ». Toutefois, les obligations dont le RSSI a la charge doivent être exécutées dans le respect des libertés individuelles et collectives des salariés.

Le RSSI devra s'assurer que cette traçabilité respecte les principes du droit du travail et de la vie privée et que la traçabilité des données de connexion[13] est bien effective.

II. La responsabilité du RSSI

La responsabilité du RSSI doit être appréhendée sous trois angles : sa responsabilité civile, sa responsabilité pénale et sa responsabilité professionnelle.

A. La responsabilité civile du RSSI

Les articles 1382 et 1383 du Code civil énoncent un principe de responsabilité à raison des dommages causés de son propre fait mais encore par sa négligence ou par son imprudence. Pour écarter cette responsabilité de droit commun, il est possible d'apporter la preuve que la cause du dommage relève d'un cas de force majeure. L'appréciation de ces cas d'exonération de responsabilité ne pourra se faire qu'au cas par cas.

Dans le cadre des relations de travail, l'article 1384, al.5 du Code civil pose le principe de responsabilité de l'employeur du fait des dommages causés par ses salariés (les « *préposés* ») dans les fonctions pour lesquelles ils sont employés. Ainsi, le préjudice causé à un tiers du fait du manquement ou d'une faute incombant au RSSI engage la responsabilité du dirigeant. Les cas d'exonération de l'employeur sont interprétés très strictement pas les tribunaux, spécialement lorsque le salarié utilise des moyens de communications électroniques mis à sa disposition par l'employeur, dans le cadre de son travail[14].

B. La responsabilité pénale du RSSI

A la différence de la responsabilité civile, en matière pénale, il existe un principe général selon lequel « *nul n'est responsable que de son propre fait* » en application de l'article 121-1 du Code pénal. Chaque personne sera donc considérée comme responsable pénalement dès lors que l'agissement ou le manquement qui lui est reproché est constitutif d'une infraction visée en tant que telle par le code pénal. Néanmoins, à cette responsabilité pénale personnelle **s'ajoute à celle des personnes morales,** quand les infractions sont commises

[13] V. Eric A. Caprioli, Les technologies de l'information et la lutte anti-terroriste, Comm. comm. électr. à paraître ; *Conservation des données relatives au trafic et à la localisation dans les communications électroniques*, Comm. com. électr., Novembre 2005, n°178, p. 40 et s.
[14] TGI Marseille, Première chambre civile, 11 juin 2003, Escota contre Lucent Technologies, http://www.juriscom.net; confirmé par CA Aix en Provence, 13 mars 2006, n° pourvoi : n°2006/170, disponible sur le site www.legalis.net.

« *pour leur compte, par leurs organes ou représentants* » (article 121-2, al. 1er du Code pénal)[15].

Du fait de son rôle et de ses attributions, le RSSI est plus particulièrement concerné par des catégories d'infractions liées aux systèmes d'information dans une acception large. La liste des infractions ne saurait en ce sens être exhaustive. A titre principal, le RSSI devra être particulièrement vigilant en ce qui concerne les infractions visées en matière de cryptologie, de systèmes de traitement automatisé de données (STAD), de données à caractère personnel, de secret professionnel (médical, bancaire, ...), et de secret des correspondances privées.

Si le RSSI agit dans le cadre d'une délégation de pouvoir valable, il pourra voir sa responsabilité pénale engagée du fait des préjudices causés par les salariés placés sous son autorité.

Le régime des délégations et subdélégations a une incidence directe sur le régime des responsabilités. Ainsi, lorsqu'il y a délégation de pouvoir, le représentant légal de la personne morale confie, au nom et pour le compte de l'entreprise, à une personne qu'il investit d'un pouvoir déterminé (direction administrative, direction juridique, direction commerciale...), le mandat de représenter l'entreprise dans les limites de ses attributions. L'intérêt pour le dirigeant de recourir à une délégation de pouvoir réside dans le transfert de la responsabilité pénale qu'elle implique. Le bénéficiaire d'une délégation de pouvoir est en effet considéré comme responsable pénalement des agissements ou manquements commis dans le cadre des fonctions qui lui ont été déléguées, déchargeant par là même la personne morale de la responsabilité y afférent. **La délégation de pouvoir s'accompagne donc par principe d'un transfert de responsabilité pénale (mais la personne morale peut aussi être responsable !).**

De plus, une bonne gestion des délégations de pouvoirs au sein d'une structure est nécessaire. En effet, la Cour de cassation a considéré qu'une « *société reste engagée par la délégation de pouvoirs faite par un président du conseil d'administration agissant au nom et pour le compte de la société, et non en son nom personnel, à un préposé de celle-ci, malgré le changement de président du conseil d'administration, tant que cette délégation n'a pas été révoquée* »[16]. En conséquence, pour que les délégations faites en son nom et pour son compte par un de ses dirigeants n'engagent plus la société en cas de départ de celui-ci (démission, révocation, décès), celle-ci doit les révoquer. A défaut, la société reste engagée par la délégation ; ce qui au regard de la règle énoncée ci-dessus peut être problématique puisque le nouveau dirigeant nommé pourrait déléguer des pouvoirs à une personne alors même que ceux-ci seraient encore délégués à une autre personne du fait de l'ancien dirigeant.

Enfin, la délégation doit respecter certaines conditions :

- Le délégataire doit être un préposé (un salarié) de la société, à l'exclusion de toute autre personne
- Le délégataire doit être une personne compétente, pourvue de **l'autorité et des moyens nécessaires pour faire assurer le respect des mesures réglementaires**
- La délégation doit être certaine et dépourvue d'ambiguïté

[15] Eric A. Caprioli, *Le risque pénal dans l'entreprise et les technologies de l'information*, JCP E, 2006, Cah. Dr. Entrep., janvier-février 2006, n°10.
[16] Cass. Com., 15 mars 2005, n° 03-13032, disponible à partir du site www.legifrance.fr (rubrique jurisprudence Cour de Cassation).

- La délégation doit être opportune, c'est-à-dire être justifiée au regard de la taille de la société et de son organisation interne

C. La responsabilité professionnelle du RSSI

L'entreprise dispose d'un pouvoir disciplinaire à l'encontre du RSSI en sa qualité de salarié de l'entreprise. Les sanctions prononcées dans le cadre de l'exercice de ce pouvoir disciplinaire seront celles définies le cas échéant par le règlement intérieur et/ou le contrat de travail. La condition de validité de ces sanctions disciplinaires réside dans leur justification et leur caractère proportionné au regard des obligations dont le RSSI a la charge en vertu de son contrat de travail.

La rédaction d'un guide juridique spécifique et adapté à l'organisation permet de préciser et de clarifier les contours des missions du RSSI, et en fin de compte de mieux évaluer les risques juridiques et les responsabilités qu'il encourt (ainsi que son entité) dans le cadre de son activité professionnelle.

Les systèmes d'information constituent la colonne vertébrale de toute organisation et le patrimoine informationnel son système nerveux. Au vu de son caractère transversal, la sécurité des systèmes d'information doit être décidée au niveau de la direction générale de l'entreprise tant en termes techniques, organisationnels que juridiques.

© Eric A. CAPRIOLI
www.caprioli-avocats.com

Sécurité des systèmes d'information et déontologie

par Paul-Olivier GIBERT
Directeur de la sécurité et de la déontologie - AG2R

L'utilisation des systèmes d'information dans le fonctionnement des entreprises - et d'une façon plus générale dans la société - amène la Sécurité des Systèmes d'Information à faire face à de nouveaux défis.

L'étude réalisée par le CIGREF et le Cercle d'Ethique des Affaires (CEA) en 2006 en a identifié les principes fondamentaux.

En premier lieu, le recours croissant à l'usage des Technologies de l'Information et de la Communication (TIC) pose la question du sens et des valeurs qui devraient en guider l'utilisation. Ces technologies ont, en effet, atteint désormais un degré de maturité qui ouvre des possibilités de traitement et de transmission de l'information encore inédites. Au même titre que les biotechnologies, elles nécessitent une réflexion morale et éthique.

En second lieu, et en corollaire de ce premier constat, l'encadrement juridique de cet usage s'est fortement renforcé depuis le début des années 2000[17]. Les contraintes légales et réglementaires sont à la fois plus lourdes pour les entreprises et organisations et de nature à porter plus gravement atteinte à leur image.

Enfin, la rencontre entre ces technologies, qui commencent à cesser d'être nouvelles, et les évolutions sociétales, a d'une certaine façon « libéré la parole ». Il est désormais possible non seulement de publier un message mais aussi de lui donner une audience sans passer par les filtres traditionnels des médias.

Face à ces nouveaux risques plus liés à l'usage qui est fait des systèmes d'information qu'à leur fonctionnement propre, la sécurité des systèmes d'information prend de nouvelles dimensions.

Non que les problèmes de conformité juridique ou de risque d'atteinte à l'image à la suite de dysfonctionnement n'existaient pas il y a 10 ans, mais parce que leur ampleur et leur nature ont changé.

La messagerie électronique et ses avatars nomades sont devenus les principaux modes de communication au sein des organisations. Leur protection et leur contrôle relèvent donc d'une mesure de sécurité globale de l'entreprise et non plus d'une mesure simplement technique.

L'espace de diffusion de l'information aujourd'hui presque sans frein que représente Internet constitue une caisse de résonance d'une rare puissance, exposant les entreprises à de nouvelles formes de malveillance. Phishing, dénigrement, appel au boycott peuvent y être réalisés avec une efficacité décuplée et une relative impunité

[17] Loi du 21/06/2004 pour la confiance dans l'économie numérique, loi du 6/08/2004 modifiant la loi informatique et libertés principalement

tant il est facile - sans se déplacer - de mettre une ou plusieurs frontières entre l'auteur d'un acte et sa victime.

Face à ces enjeux, une démarche de type déontologique appliquée à l'usage des systèmes d'information s'impose. Elle comprend deux dimensions complémentaires :

- la mise en place de processus de contrôle et de maîtrise de la conformité juridique des traitements mis en œuvre au sein de l'organisation ;
- une démarche éthique visant à identifier les limites que doivent s'imposer les organismes, au-delà du respect de leurs obligations légales, pour que les traitements de données qu'ils mettent en œuvre soient socialement acceptables et ne présentent pas un risque d'altération de leur image.

En d'autres termes, les entreprises et les organisations doivent prendre la mesure de leurs responsabilités et en particulier prendre conscience que les risques liés à l'usage des systèmes d'information sont désormais des risques centraux pour elles et non plus des risques techniques.

Ces nouvelles préoccupations se traduisent par l'apparition de nouveaux acteurs de la sécurité des systèmes d'information.

A ce titre, la Loi Informatique et Libertés modifiée en août 2004 permet aux organismes de se doter d'un Correspondant à la Protection des Données à caractère Personnel. Cette fonction, transposition aux systèmes d'information des déontologues de la sphère financière, permet d'identifier un collaborateur chargé de veiller au respect des dispositions de cette loi. Son indépendance est reconnue par loi.

Pour une fonction récente - le décret d'application n'a été publié qu'en octobre 2005, son développement est très rapide. D'ici 5 ans, le Correspondant devrait s'imposer comme le mode dominant de protection des données à caractère personnel en France pour les grandes organisations.

De nouveaux thèmes de travail apparaissent : au-delà de la prévention des dysfonctionnements, la prévention et le traitement des mésusages des systèmes d'information vont dans les années à venir avoir une place croissante dans les préoccupations des entreprises.

A titre d'exemple, les organisations utilisent des informations fournies par leurs clients ou leurs partenaires dans le cadre d'une relation contractuelle ou réglementaire. Elles n'en sont pas propriétaires mais dépositaires et à ce titre ont le devoir de les protéger et de ne pas les exploiter au-delà des termes du contrat. Elles doivent donc repenser leur obligation de secret professionnel.

Ce n'est qu'un exemple. Les TIC *« sont récentes et leur généralisation non encore achevée [….]. Les problèmes éthiques et déontologiques liés à l'usage des Technologies de l'Information et de la Communication sont donc encore largement*

émergeants.[18] ». Le chantier de la déontologie de l'usage des systèmes d'information vient juste de s'ouvrir. Nous en reparlerons dans les prochaines années.

© Paul-Olivier GIBERT

[18] Entreprise Ethique avril 2006 Comment faire face aux risques éthiques liés à l'usage des technologies de l'information et de la communication ? Paul Olivier GIBERT

Apport et évolution du rôle des MSSP dans la gestion du risque

par Cyril AUTANT et Luis DELABARRE
THALES SECURITY SYSTEMS

I- Préambule

Face aux menaces croissantes liées au système d'information, les entreprises et les administrations s'assurent de la sécurité de leur système, mais toutes n'ont pas aujourd'hui les moyens de maîtriser l'ensemble des paramètres qui contribuent à leur sécurité.
La diversité des équipements, la multiplicité des configurations, l'évolution permanente des technologies complexifient la gestion de la sécurité des systèmes d'information. D'autre part, les moyens dédiés à ces tâches sont souvent insuffisants. Ils ne permettent pas toujours de garantir un suivi rigoureux de la déclinaison de la politique de sécurité de l'organisation dans l'ensemble de ses composantes techniques et organisationnelles.

Dès lors, le risque apparaît de ne plus disposer des moyens d'anticiper, de détecter, ou de réagir face à un risque. D'autre part, la spécialisation nécessaire à une gestion appropriée de ces risques contraint à des investissements humains qui ne contribuent pas directement à la croissance de l'organisation. Le rôle du MSSP (Managed Security Services Provider) consiste alors à décharger l'entreprise de cette contrainte en assumant la complexité inhérente à la gestion du risque sécurité du système d'information, tout en apportant des garanties de conformité à la politique de sécurité préalablement définie.

II- Le rôle du MSSP

Face à la difficulté et aux coûts liés à la mise en œuvre et au maintien de la sécurité de leur système d'information, les entreprises et administrations confient depuis plusieurs années tout ou partie de la mise en place ou de l'administration de leur équipements de sécurité à des tiers.
Sur la base des études IDC19, nous reprenons les trois segments de services de sécurité confiés aux MSSP :

- les services « basiques »
  - gestion de pare-feux
  - protection contre les intrusions
  - sécurisation des accès distants
  - protection contre les virus
- les services « avancés »
  - mise à jour des logiciels de sécurité
  - audit externe de vulnérabilité
  - mise à jour des OS et des applications (hors sécurité)
  - gestion des identités
- Les services « sur-mesure »
  - service de veille sécuritaire
  - contrôle et gestion de la conformité réglementaire
  - contrôle et gestion de la conformité métier

[19] « Le marché français des services d'externalisation de la gestion de la sécurité informatique », Eric Domage, Karim Bahloul, IDC, juin 2006

Le premier segment est historique, et correspond aux services les plus aisés à confier à un tiers. Une part de ces services est souvent couplée à une offre plus large de connexion via un opérateur.

Les services avancés demandent une intimité plus forte avec le système d'information de l'organisation. Ils sont en cela plus significatifs de la capacité du MSSP à endosser une part de la complexité de la gestion d'équipements de sécurité. Si l'audit de vulnérabilité a un sens immédiat à être réalisé à partir de l'extérieur, les opérations de mise à jour de logiciels de sécurité, d'OS ou d'applications entraînent des contraintes (tests de non-régression, capacités de retour arrière), sur lesquelles un MSSP devra s'engager, permettant à l'organisation de s'affranchir de tâches complexes, sans valeur ajoutée.

Enfin, les services sur-mesure présentent une réelle nouveauté dans la capacité à déléguer des rôles qui relevaient jusqu'à récemment du pré-carré de l'organisation. Au-delà de la délégation de tâches de sécurité, nous y trouvons un véritable accompagnement dans la réalisation du métier, et un transfert de responsabilités.
Le service de veille sécuritaire, dans lequel nous incluons la supervision des équipements de sécurité, implique un engagement fort du prestataire dans la compréhension du métier et des enjeux de l'organisation. La délégation de tâches purement techniques est dépassée pour transférer la gestion d'informations de sécurité critiques.
Le prestataire doit alors offrir non seulement des garanties techniques, qui étaient jusque-là indispensables dans la délégation des services « basiques » et « avancés », mais également assumer des responsabilités dans sa capacité à répondre en temps réel à des menaces qui pèseraient sur l'organisation. Le contrôle et la gestion de conformité participent à cette démarche en dépassant le cadre technique pour relever de compétences métier et réglementaires, sur des volets impactant fortement l'organisation car liés à sa crédibilité sur son marché, à travers sa capacité à se conformer aux règles du métier.

III- L'évolution de l'offre MSSP

Même si comme nous venons de le voir, le troisième segment des offres MSSP reste émergent, il constitue néanmoins une avancée incontestable dans la capacité des organisations à déléguer tout ou partie de la gestion de leur sécurité, y compris sur des segments critiques de leur métier.

Cette délégation a plusieurs causes. La première, mentionnée en préambule, est la conséquence directe du manque de moyens disponibles. Le coût des spécialistes en sécurité, associé aux difficultés de recrutement de ces profils, conduit à externaliser ces tâches.
La deuxième est la rationalisation des investissements de l'organisation, qui se concentre sur métier. C'est probablement cette seconde composante qui conduira à l'évolution de l'offre, en externalisant la sécurité plus largement qu'elle ne l'est aujourd'hui, même au niveau des services « avancés ».
L'ensemble participe à considérer une part de plus en plus large de la sécurité comme une tâche complexe, nécessitant des spécialistes, critique mais sans valeur ajoutée immédiate pour l'organisation.

Au même titre que de nombreuses prestations autour du système d'information, la sécurité peut se mesurer, faire l'objet de contrôles externes, et d'engagements de résultat. Elle peut donc être confiée plus largement à des tiers qu'elle ne l'est aujourd'hui.
Ainsi, au-delà de la gestion et de la supervision des équipements de sécurité d'infrastructure, il est probable que des services de fourniture de flux « propres » sont à même de séduire des structures n'ayant pas les moyens ou le souhait de procéder à la mise en place et à la gestion des équipements permettant de filtrer les flux de type trafic Web, messagerie, transfert de données etc.… De même, des services de gestion de preuves, garants de la traçabilité de transactions au sein d'applications, permettent d'offrir une valeur légale à ces transactions, tout en confiant à un tiers la responsabilité du bon fonctionnement et de l'adéquation des moyens de construction et de restitution de la preuve avec les engagements de l'organisation.

Le champ des possibilités est large pour des services de sécurité à valeur ajoutée pouvant être confiés à des tiers. En permettant à l'organisation de se concentrer sur son métier, les MSSP contribuent à améliorer la gestion du risque. La définition des responsabilités qui leur sont confiés, associée à une délégation qui va au-delà de tâches purement techniques, oblige l'organisation à mieux identifier, mesurer et suivre ses risques, en exigeant des résultats sur les moyens mis en œuvre pour leur prévention et leur gestion. En transférant la complexité de la gestion de tâches de sécurité récurrentes, l'organisation peut se concentrer sur les indicateurs qui lui permettent de gagner en efficacité et en compétitivité avec l'assurance d'une sécurité opérationnelle garantie.

© Cyril AUTANT et Luis DELABARRE

Risques et gestion de crise

par Hervé SCHMIDT
Président du Directoire - GASPAR S.A.

Que le lecteur averti ne soit pas déçu. J'ai voulu faire simple et j'ai fait simple. Mais n'est ce pas ce qu'attend réellement un chef d'entreprise, surtout en matière d'imprévisible ?
De quels risques parle-t-on ? De quelle crise parle-t-on ? N'est-ce pas quelque part antinomique de parler de risques, si nombreux, et de gestion de crise, si rare et si peu probable ? Beaucoup d'acteurs gèrent les risques et veulent gérer la crise. Comment des Hommes, au sens large du terme, en parfaite possession de leurs moyens, qui ont a priori pensé à tout pour que la crise ne se produise pas, peuvent imaginer un seul instant que l'accident soit possible ? Ne serait-ce pas leur dire « vous n'avez pas tout prévu » alors que c'est dans leur fonction même que de prévenir un maximum. Voici réellement une attitude contre nature. Et puis, peut-on imaginer un évènement de nature imprévisible ? Imprévisible dans sa date d'apparition, imprévisible dans sa durée, imprévisible dans ses conséquences, imprévisible dans sa nature… Alors ? Peu de Responsables imaginent qu'il est utile de se préparer en priorité à faire face à une crise, surtout quand les ressources humaines, techniques et financières de l'entreprise ne permettent pas de prévenir tous les risques. Certains diront que l'assurance est suffisante. Et beaucoup considèrent qu'il faut se préparer un maximum pour prévenir les risques les plus « probables » pour l'entreprise et construire ainsi de façon préventive les procédures qui permettront de faire face si le risque, ainsi prévenu, devenait réalité. Ils ont sûrement raison sauf si la loi de Murphy (*) les prend en défaut. Le lecteur averti comprendra néanmoins que je ne partage pas cette approche. Comment gérer la crise sans forcément gérer les risques ?

(*) L'accident arrive là, où et quand on ne l'attendait pas !

De quels risques parle-t-on ?

Le chef d'entreprise est confronté à un ensemble de risques auxquels il ne pense pas forcément. En effet, quel chef d'entreprise se présenterait tous les matins à son bureau en imaginant tous les accidents auxquels il peut être confronté ? Quel chef d'entreprise ne pense qu'à prévenir tous les risques auxquels il devrait et pourrait faire face ? Un chef d'entreprise est quelqu'un qui parie qu'il va gagner mais jamais qu'il pourrait perdre. A-t-il les ressources nécessaires pour faire face à tous les risques ? Doit-il choisir tel ou tel autre risque ? Peut-il se protéger contre la jungle d'experts prêts à lui proposer du conseil pour prévenir ses risques ? Or, sa seule préoccupation quand il arrive à son bureau, c'est de pouvoir atteindre ses objectifs, quoiqu'il arrive. Dans cette perspective, il prend des risques en permanence, car c'est une nécessité. Dans ces conditions, de quels risques parlons-nous ? Et il en existe pléthore ! Citons-en néanmoins quelques uns, ne serait-ce que pour « alerter » le lecteur :
Une agression médiatique, un détournement de biens, une interdiction préfectorale, un braquage, un salarié mécontent, un client qui dépose le bilan, la dévaluation d'une monnaie étrangère, un virus informatique corrompu, un produit défectueux,

une intoxication alimentaire, le vol d'un secret de fabrication, la perte de parts de marché, l'arrêt prolongé d'un outil stratégique, une catastrophe naturelle, etc. Et puis, pourquoi pas ? L'incendie ou l'inondation. La liste pourrait très facilement s'agrandir. Comment un chef d'entreprise pourrait-il faire face à tous ces risques simultanément ? Alors il devrait choisir ? Et si, d'aventures, la crise se produisait. Et si les procédures n'étaient pas prêtes pour y faire face ? C'est pourtant le plus probable et la loi de Murphy nous le rappelle en permanence. Dans ces conditions, comment réagir face à tous ces risques ? Considérons que le chef d'entreprise ne pourra jamais se préparer face à la « bonne » crise. N'oublions pas également qu'il est intelligent ! Pourquoi devrait-il réduire tel ou tel risque et pas les autres ? Enfin, rappelons-nous que le chef d'entreprise gère des risques au quotidien, qu'il a probablement déjà géré des crises et, qu'en tout état de cause, il ne nous a certainement pas attendus !

De quelle crise parle-t-on ?

Peut-on imaginer, ne serait-ce que quelques instants, l'inimaginable ? Mais est-ce concevable ? Par principe, le chef d'entreprise prend des risques au quotidien. Quelque part, il parie que l'imprévisible ne sera jamais réalité. Il suppose, du moins le pense-t-il, qu'il pourra faire face.
Et pourtant, voilà ! Il est confronté subitement à cet évènement qui va le déstabiliser, qui va probablement lui faire perdre le contrôle, qu'il va devoir gérer probablement seul, etc. Cet évènement appelé communément « crise ». Le chef d'entreprise va devoir faire face à un certain nombre d'acteurs externes qui vont sans doute le perturber et qui ne sont sûrement pas là pour l'aider, en tous les cas, ce n'est pas leur priorité absolue. Nous parlons des autorités, des pompiers, de la police ou de la gendarmerie, du public, des médias, de la presse, de la préfecture – organe suprême en charge de la gestion de crise, en France -, et de bien d'autres encore ! Il va devoir également gérer tous les autres acteurs, ceux qui sont probablement de son côté, quoique pas toujours. Nous les appellerons les acteurs « internes ». Citons, par exemple, et de façon non exhaustive, le personnel, les clients, les fournisseurs, le banquier, le courtier, les huissiers, les syndicats, le CHSCT, etc.
Coordonner tous ces acteurs est un problème supplémentaire pour un chef d'entreprise non préparé un minimum. Et puis ce n'est pas tout. Ce chef d'entreprise va avoir un certain nombre de problèmes à résoudre, un certain nombre de questions auxquelles il devra répondre.
Mais de quelle crise parlons-nous ? Celle, la seule, qui vient frapper de plein fouet l'entreprise et que le chef d'entreprise va devoir affronter, a priori souvent seul, pendant plusieurs heures. Pouvons-nous parler de crise en particulier ? Au risque de perturber les assureurs qui ont besoin de définir des situations de risques pour lesquelles il propose des couvertures adaptées, en fonction des mesures de prévention mises en place, pourquoi ne pas tout simplement dire au chef d'entreprise : « déterminez vous-même quand vous considérez que vous êtes en crise » ? Ce jour-là, et si nous avons les outils pour permettre au chef d'entreprise de gagner en toutes circonstances, alors, nous aurons probablement apporté la vraie solution au chef d'entreprise. Ce qui ne veut sûrement pas dire qu'il ne faut pas faire de prévention…

Doit-on s'intéresser aux causes ou aux conséquences ?

La plupart des acteurs de la sécurité n'ont pas de réponse à cette question. En effet, ne pas s'intéresser aux causes, c'est quelque part nier qu'une prévention est nécessaire, voire indispensable. Mais c'est également refuser d'admettre que quoi que l'on ait pu prévenir, la loi de Murphy nous prendra toujours en défaut.

S'intéresser aux conséquences, c'est quelque part penser à protéger les objectifs de l'entreprise. C'est quelque part vouloir anticiper une situation dont l'impact empêcherait l'atteinte des objectifs en toutes circonstances. Personnellement, je préfère cette option.

Conclusion / Un peu d'espoir

Gérer la crise, pour un chef d'entreprise, c'est être en mesure d'anticiper un minimum l'absence de ressources fondamentales à l'atteinte de ses objectifs. C'est pouvoir mieux gérer pendant une crise et, sommes toutes, gagner après afin de ne pas se trouver devant une situation de non retour.

Anticiper avant, le minimum nécessaire, ce n'est certainement pas prévenir tous les risques. Il n'est pas non plus dit qu'il ne fallait pas ignorer les risques ni les prévenir. Si l'entreprise a les moyens de prévenir des risques et de se préparer encore mieux pour faire face à l'imprévisible, pourquoi pas ? Pour ma part, ce n'est pas mon opinion et je ne pense pas qu'un chef d'entreprise de PME-PMI soit dans cet état d'esprit. Mes 20 années d'expérience m'ont déjà montré qu'il fallait être pragmatique avec un chef d'entreprise. Entre deux maux, il faut choisir le moindre. Mieux vaut se préparer à faire face à l'imprévisible, quitte à faire l'impasse sur certaines mesures préventives, que de se focaliser essentiellement sur la prévention et ne pas se préparer à affronter le pire.

Il n'est pas dit dans ces quelques lignes qu'il ne fallait pas faire de la prévention. Le chef d'entreprise gère au quotidien des ressources dynamiques qui lui permettent d'atteindre ses objectifs. Charge à lui de trouver un juste équilibre entre la défense des causes et la protection des conséquences. Autrement dit, si le raisonnement était poussé à l'absurde, voilà deux options qui sont laissées à l'appréciation du lecteur :

- Un chef d'entreprise qui a beaucoup de moyens devrait chronologiquement faire de la prévention (analyse de risque), s'intéresser aux aspects liés à l'imprévisible (comment se préparer à gérer la crise) et faire ce qu'il faut pour assurer la reprise des activités plan de continuité des activités).
- Un chef d'entreprise qui n'a pas les moyens devrait se concentrer en priorité sur la protection de ses objectifs.

Comment gérer une bonne crise en prévenant les bons risques ? Le lecteur méditera.

© Hervé SCHMIDT

La sécurité des Systèmes d'Information en Europe

par Mauro ISRAEL
RSSI de CYBER NETWORKS - groupe NET2S

Il est intéressant de comparer les sujets qui sont traités par les RSSI de différents pays d'Europe, voire de les comparer aux pratiques américaines. Cet article reprend les principaux thèmes de la sécurité des systèmes d'information, en les comparant entre les Français d'une part, les Britanniques, les Allemands, les Belges, les Espagnols en Europe, et les Américains d'autre part.

Ces thèmes sont issus d'interviews avec les RSSI et DSI des entités du groupe NET2S, et de la compilation de groupes de travail qui se tiennent sur le thème de la sécurité des SI en Europe. En complément, vous trouverez les principales instances et initiatives européennes sur le sujet.

I- Les points de convergence

Tous les Européens et les Américains sont sensibles de manière commune au problème de *l'identity Management* et à l'authentification forte. Il semble que le *« login-passoire »* n'en a plus pour très longtemps. Les banques Italiennes dotent leurs clients de dispositifs physiques de calculette *« one time password »,* et en font un argument commercial de lutte contre la fraude et le phishing. Les solutions d'authentification biométrique et de carte à puce se répandent dans l'ensemble des pays Européens, notamment pour les dirigeants et les populations « sensibles », qui ont à protéger leur ordinateur portable et les données sensibles. De la même manière, la gestion sécurisée des « nomades » et les technologies connexes, WIFI, voix et téléphone sur IP, chat, peer to peer et autres clefs USB, sont une préoccupation commune.

Naturellement, tout le monde se pose des questions sur la conformité règlementaire et législative, avec une mention particulière pour la France et le fameux « correspondant CNIL ». Dans le même registre, l'insertion de clauses de sécurité dans les contrats d'*outsourcing* interpellent les RSSI. A noter l'initiative de la DCSSI, qui cherche à standardiser ces clauses pour les appels d'offres de l'Etat. Ces bonnes pratiques pourraient être reprises par les grandes entreprises françaises, voire européennes.

La norme ISO27001 est un sujet à la mode, y compris aux Etats-Unis. Faut-il y aller ou pas ? Quelles interactions avec les autres normes et règlements ? Est-ce utile ? La réponse proviendra des retours d'expérience des premières sociétés à se faire certifier. Le Royaume-Uni est assez en avance sur le sujet (mais ce sont les inventeurs de la norme à travers la BS7799) et la France assez à la traîne quantitativement.

La sensibilisation des utilisateurs interpelle les RSSI de tous les pays, notamment à travers les nouvelles menaces de « social engineering » et de manipulation psychologique dans le but de récupérer les mots de passe ou l'accès à des données confidentielles.

II- Les points de divergence

Alors que les anglo-saxons (Royaume-Uni, Allemagne, Etats-Unis) s'intéressent au budget et à la justification des coûts, les latins (France, Espagne), eux, s'intéressent plutôt à la manière de faire passer le message à leur Direction Générale.

Visiblement les plans de continuité d'activité et les plans de secours font partie de problèmes résolus en France, alors que les Anglais et les Allemands cherchent encore à trouver la bonne formule pour créer une cellule de crise efficace, et un plan de secours. Il est d'ailleurs notable que les anglo-saxons se concentrent plus sur la mise en œuvre, alors que les Français prennent plus de temps pour la planification et la documentation.
Tout le monde se demande quelles sont les bonnes pratiques vis-à-vis des outils pour les nomades, mais les décisions concernant l'utilisation de ces nouvelles technologies est diamétralement opposée : Les Français veulent bannir l'usage de la téléphonie sur Skype, du *peer to peer*, du *chat,* du *Blackberry* et d'autres outils typiques de l'informatique « pervasive », alors que les Anglais l'adoptent pour des raisons d'efficacité. La vraie question est : qui peut écouter ces communications, et dans quel but ?

III- Les initiatives européennes

Alors que chaque pays s'est organisé autour d'associations nationales, voire internationales, il existe désormais une entité européenne qui s'occupe explicitement de la sécurité des systèmes d'information, et de répandre les bonnes pratiques. Il s'agit de l'ENISA : www.enisa.eu.int. Située à Héraklion en Crète, cette agence est en charge notamment de mettre en œuvre un système d'alerte de sécurité coordonné au niveau européen, commun à plusieurs pays, au même titre que les « CERT » nationaux (Computer Emergency Response Team). Cette initiative s'inscrit dans le plan « Europe 2005 », voté en mai 2002, précisant que *« La sécurité des systèmes d'information est un élément clé pour la croissance d'Internet, en particulier avec le développement du haut débit ».*
Par ailleurs, l'Europe, afin notamment de lutter contre l'immigration illégale, prépare un immense système biométrique, le ***VIS*** (Visa Information System). Ce dispositif va recenser à terme 70 millions de personnes, et sera déployé à partir de fin 2006 pour tous les ressortissants d'Afrique du Nord qui solliciteront un visa d'entrée en Europe. Le cœur du système -couplé au passeport- dénommé ***BMS*** (Biometric Matching System), sera installé sur les quelque 3500 ordinateurs consulaires et alimentera une base de données globale Européenne. Un « centre d'excellence » basé à Bruxelles tente de réunir toutes les parties prenantes du projet, et peut constituer une source de bonnes pratiques pour l'ensemble de la profession.
Enfin, rappelons que la convention Européenne sur la cybercriminalité est signée ou ratifiée depuis Juillet 2004 par 37 états (en particulier les 25 pays d'Europe, plus l'Albanie, la Croatie, l'Afrique du Sud, le Canada, les USA et le Japon, entre autres), et permet notamment les poursuites légales sur un territoire autre que celui de la « victime ».
Cette convention s'applique notamment pour les actions pénales liées aux crimes de pornographie enfantine, la fraude informatique et les intrusions dans les réseaux

et systèmes. Notons à propos de la lutte contre la pédopornographie l'initiative ***« SAFER INTERNET »*** qui regroupe deux sites web et un réseau d'alerte :
INHOPE www.inhope.org qui permet au public de donner l'alerte sur un contenu illégal vu sur Internet, et INSAFE www.saferinternet.org qui regroupe tous les conseils et informations aux parents, enfants et éducateurs, sur l'utilisation sans risque d'Internet.

IV- Coupe du Monde de la Sécurité

Enfin, en cette année de coupe du monde de football, on ne pouvait pas passer sous silence l'enquête de McAfee, menée par MORI Research en mai 2006 auprès de 600 professionnels de l'informatique, à propos de leur sentiment sur la sécurité de leur système d'information.
Ce n'est pas une surprise de constater que l'Allemagne présente la « défense la plus solide » contre les cyber-menaces, alors que l'Italie arrive en 4ème… Comme quoi le football et la logique ne sont pas sœurs jumelles ! Les « Bleus » sont en tête du rapport « efficacité/prix en sécurité» ce qui ressemble pas mal à notre équipe de foot, -surtout de la tête…- Alors que le Royaume-Uni lutte pour les places d'honneur, les Espagnols et les Hollandais sont dans une phase de réforme et ont du mal à contrer des menaces de plus en plus sophistiquées. Il est clair pour tout le monde qu'une défense « en béton » est la clef du succès. L'évaluation a porté sur la satisfaction en matière de sécurité du réseau, le retour sur investissement, et les parades aux attaques constatées dans les derniers six mois.

© Mauro ISRAEL

Développer l'intelligence économique dans un environnement à risque

par Patrick LANGRAND
RSSI- Natexis Banque Populaire

Il nous apparaît nécessaire, quatre ans après le lancement de l'Espace Européen en Intelligence Economique et Numérique, de traiter ce thème au sein du Livre Bleu.

Avant toute chose, il convient de rappeler le contexte dans lequel les entreprises évoluent aujourd'hui. L'émergence des Technologies de l'Information et de la Communication (TIC) a permis de repousser les frontières des entreprises et provoqué l'ouverture et la facilité d'accès au patrimoine informationnel (PI) de celles-ci.

Ces deux phénomènes induisent des nouveaux risques auxquels les sociétés ne sont pas préparées. Certes nous avons vu la Sécurité des Systèmes d'Information (SSI) se développer et conduire des programmes qui tendent à sécuriser les entreprises mais le dernier rapport conduit sous l'autorité de Monsieur le Député Pierre LASBORDES démontre des carences et des faiblesses sur les dispositifs de sécurité mis en œuvre. Pourquoi ?

La France est-elle organisée pour répondre à ces besoins ?
N'ayons pas peur des mots et ayons le courage de faire tomber des tabous ! NON ! Notre société est basée depuis plus de dix ans sur la culture de l'individualisme, premier facteur de risque dans une chaîne de sécurité ! Nos entreprises sont soumises à la même loi de cette économie à risque que nous n'avons pas redéfinie dans ce nouveau siècle. L'actualité est là, les entreprises se font clairement agressées. D'abord par les hommes -et nous avons vu précédemment que c'était le risque majeur- puis, par l'information, ce qui m'amène à parler d'Intelligence Economique (IE).

Je laisse à chacun d'entre nous le soin de s'approprier les centaines de définitions qui existent sur le thème de l'I.E. Abordons la réalité quotidienne au travers de saines pratiques que je vous livre.

Tout d'abord il convient de retenir, comme dans toute démarche, des hypothèses. Si celles-ci se vérifient au sein de vos entreprises alors vous êtes sur un gisement très prometteur.

Hypothèse 1 : êtes-vous citoyen de votre entreprise ?

En effet, l'I.E. n'est pas seulement la dimension stratégique du management de l'information mais elle doit devenir une « culture ». Toute absence de référentiel de valeurs d'entreprise, de non-existence d'instrument comportemental, d'évaluation des pratiques managériales et du maintien en compétence sont des signes inquiétants pour le développement de la « culture I.E. ».

Hypothèse 2 : connaissez-vous votre patrimoine informationnel ?

Cette hypothèse sert à vérifier si votre patrimoine informationnel est clairement défini. Afin de vous aider, je vous propose une définition, qui pour notre démarche, n'est pas dépourvue d'intérêts.
« Le Patrimoine Informationnel (PI) est l'ensemble des informations utilisées par les entreprises dans le cadre de leurs activités, ainsi que les processus de transformation et d'exploitation de ces informations. Il est organisé en actifs d'entreprises (AE) et s'appuie sur une typologie des sources d'informations. L'information en est son atome. Elle doit faire l'objet d'une protection adaptée et contrôlée que nous baptiserons pour la compréhension Sécurité de l'Information. »

Hypothèse 3 : comment protégez-vous votre patrimoine informationnel ?

La protection du patrimoine informationnel passe par une politique cohérente de gestion de l'information où l'objectif poursuivi est de maîtriser la diffusion de l'information et son usage. Elle est complétée par des mesures drastiques sur la propriété intellectuelle. Elle ne saurait être efficace sans des dispositions adaptées aux comportements humains tout en préservant la vie privée de chacun. Son efficience se mesure au travers d'un dispositif de maîtrise de gestion des risques. Enfin, elle est toujours complétée par une politique de sécurité de l'information où seront proportionnés les moyens de protection par rapport à la valeur de l'information.

Hypothèse 4 : parlez-vous couramment sécurité de l'information ?

Cette hypothèse permet d'évaluer votre culture en sécurité de l'information. Afin de vous aider, je vous propose, là encore, une définition.

« La sécurité de l'information est l'état de protection, face aux risques identifiés, qui résulte de l'ensemble des mesures générales et particulières prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée, où :

- *la confidentialité est le caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins de l'entreprise,*
- *l'intégrité de l'information traitée garantit que celle-ci n'est modifiée que par un acte volontaire et légitime,*
- *la disponibilité est l'aptitude d'un système d'accéder à l'information dans des conditions définies de temps, de performances et d'environnements. »*

Hypothèse 5 : avez-vous un RSSI ?

Idée saugrenue mais diantre que faire de ce Responsable de la Sécurité des Systèmes d'Information. Désolé, plus court je n'ai pas trouvé !

Le RSSI peut jouer un rôle déterminant au sein des entreprises en matière d'Intelligence Economique. Beaucoup ignorent que les mesures prises en matière de sécurité sont souvent les premières fondations de l'Intelligence Economique dite défensive qui servent à consolider et protéger le patrimoine de l'entreprise. Ce rôle vient enrichir notre démarche dès lors où le RSSI devient créateur de valeur et

contribue au développement de son entreprise. Ce phénomène est baptisé Intelligence Economique offensive mais n'est pas le seul élément à considérer dans cette approche.

Nous avons émis nos hypothèses. Venons-en aux saines pratiques. Là encore, nous garderons l'humilité d'une recette qui se voudrait miraculeuse mais qui en certaines circonstances deviendrait très vite une recette de « tarte à la crème » (hommage au Sherpa, les initiés comprendront).

Tout d'abord, il faut s'organiser! Pas si simple car les chantiers de gouvernance sont souvent très avancés et ils ont « séché » cette problématique. L'I.E. n'est pas structurelle et il convient d'adopter un modèle hybride où seront privilégiés les mises en réseau des acteurs et les processus de pilotage stratégique et opérationnel. En clair, un monsieur I.E. dans une entreprise ne peut être qu'un très bon communicant et un facilitateur de relations. En aucun cas, il incarne à lui seul cette culture. Un groupe de réflexion inter disciplinaire et inter culturel devra être constitué pour définir les objectifs à atteindre en cohérence avec la stratégie de l'entreprise. Cette équipe constituera une cartographie de la gestion de l'information et des acteurs/consommateurs. Elle élaborera un programme de sensibilisation pour tous les acteurs de l'entreprise afin de développer la culture I.E.

L'intelligence économique sert uniquement si les risques ont bien été identifiés !

Je conclurais par cette phrase de J. F. KENNEDY *« La seule chose au monde qui coûte plus cher que l'information, c'est l'ignorance des hommes.* »

© Patrick LANGRAND

Parce qu'le cyberterrorisme et cyber-terrorisme sont devenus des menaces actuelles pesant sur l'activité des entreprises et des services de l'Etat autant que sur la vie des citoyens, la Sécurité des Systèmes d'Information est, aujourd'hui, un enjeu vital. Il est plus important que jamais de s'informer, de se protéger, de se connaître et de partager expériences, solutions et enjeux.

Constitué de Responsables, de Directeurs de la Sécurité des Systèmes d'Information et d'Experts en sécurité ainsi que de personnalités reconnues, le Cercle compte déjà plus de 200 adhérents actifs appartenant à des entreprises privées et à des organisations gouvernementales européennes. Ses objectifs visent à fédérer une communauté de professionnels, à participer à l'élargissement des compétences, à échanger sur tous les enjeux liés aux risques, solutions et moyens de protection des patrimoines numériques stratégiques des entreprises et institutions.

Accompagner les initiatives privées et gouvernementales, favoriser l'acquisition de connaissances et la détection de projets, développer l'esprit établi par une « communauté de compétences » pragmatique et disposant des mêmes valeurs de référence et de citoyenneté, sont le programme du Cercle Européen de la Sécurité et des Systèmes d'Information.

Le cercle
Européen de la Sécurité et des Systèmes d'Information

06 Les Assises

Pour plus d'informations contactez-nous au **01 41 93 09 14**
par courriel **contact@lecercle.biz** ou sur notre site web **www.lecercle.biz**

2

Monaco
11-14 octobre 2006
6e édition

L'Événement Européen de la Sécurité et des Systèmes d'Information

Les enjeux vitaux de la Sécurité des Systèmes d'Information

Phishing, Robots, chevaux de Troie, virus, rootkits, espionnage économique : 2005 a subi une explosion sans précédent de la cybercriminalité. La sécurité informatique est, plus que jamais, un enjeu vital et les menaces et vulnérabilités qui pèsent sur les systèmes d'information sont aujourd'hui au cœur des préoccupations des DSI, DSSI, RSI et même de leurs Directions Générales. En thermométrant aussi bien un enjeu stratégique pour toutes les entreprises qu'une préoccupation sécuritaire de plus haut niveau, pour le fonctionnement et la continuité des services publics.

La réflexion sur la gestion des risques à différents atteint sa maturité et devient un enjeu de Défense, de Citoyenneté, d'Intelligence Économique.

Comment alors anticiper les grands mouvements de la SSI en apportant des réponses pragmatiques et stratégiques, échanger les expériences, s'informer sur les paradoxes ?

C'est le but des **Assises de la Sécurité et des Systèmes d'Information**, dont la 6e édition est organisée à Monaco du 11 au 14 Octobre 2006, et qui constituent l'événement incontournable et le point d'ancrage de toutes les réflexions sur la Sécurité et les Systèmes d'Information.

Cette édition 2006 permettra à ses participants et aux partenaires réunis à Monaco, de comparer réalisations, innovations et expériences, de définir des synergies et d'enrichir leurs connaissances en n'ayant de nombreux liens grâce à la connexité, à la disponibilité et au networking d'une communauté de compétences reconnue et sans équivalent.

Echanges, innovations, études exclusives, un retour sur investissement assuré.

06 Les Assises
L'Événement Européen de la Sécurité et des Systèmes d'Information

Nos partenaires

Avec la participation de

Pour plus d'informations téléphonez au **01 41 93 07 07**
www.les-assises-de-la-securite.com

Le cercle